# EXAM CRAM

CompTIA®

# Network+

N10-008


Cram Sheet


Flash Cards


Practice Tests

EMMETT DULANEY

EXAM CRAM

# CompTIA® Network+ N10-008 Exam Cram

**Emmett Dulaney**

**CompTIA® Network+ N10-008 Exam Cram**



ISBN-13: 978-0-13-737576-9

ISBN-10: 0-13-737576-X

ScoutAutomatedPrintCode



**Editor-in-Chief**
Mark Taub

**Director ITP Production Management**
Brett Bartow

**Executive Editor**
Nancy Davis

**Development Editor**
Ellie Bru

**Managing Editor**
Sandra Schroeder

**Senior Project Editor**
Tonya Simpson

**Copy Editor**
Chuck Hutchinson

**Indexer**
Timothy Wright

**Proofreader**
Abigail Manheim

**Technical Editor**
Chris Crayton

**Publishing Coordinator**
Cindy Teeters

**Cover Designer**
Chuti Prasertsith

**Compositor**
codeMantra

# Contents at a Glance


| | | |
|---|---|---|
| | Introduction | xxiii |
| CHAPTER 1 | Network Technologies, Topologies, and Types | 1 |
| CHAPTER 2 | Models, Ports, Protocols, and Network Services | 41 |
| CHAPTER 3 | Addressing, Routing, and Switching | 93 |
| CHAPTER 4 | Network Implementations | 151 |
| CHAPTER 5 | Cabling Solutions and Issues | 183 |
| CHAPTER 6 | Wireless Solutions and Issues | 235 |
| CHAPTER 7 | Cloud Computing Concepts and Options | 269 |
| CHAPTER 8 | Network Operations | 283 |
| CHAPTER 9 | Network Security | 343 |
| CHAPTER 10 | Network Troubleshooting | 403 |
| | Glossary | 461 |
| | Index | 511 |

# Table of Contents

**Introduction** . . . . . **xxiii**

**CHAPTER 1:**
**Network Technologies, Topologies, and Types** . . . . . **1**

Wired and Wireless Network Topologies . . . . . 2
Bus Topology . . . . . 2
Ring Topology . . . . . 3
Star Topology (Hub-and-Spoke) . . . . . 5
Mesh Topology . . . . . 6
Hybrid Topology . . . . . 7
Bringing Wireless to a Topology . . . . . 8
Infrastructure Wireless Topology . . . . . 8
Ad Hoc Wireless Topology . . . . . 9
Wireless Mesh Topology . . . . . 10
Network Types and Characteristics . . . . . 14
To Server or Not . . . . . 14
LANs . . . . . 15
WLANs . . . . . 15
WANs . . . . . 16
MANs . . . . . 16
CANs . . . . . 17
SANs . . . . . 17
PANs . . . . . 17
SDWANs . . . . . 18
MPLS . . . . . 18
mGRE . . . . . 19
Network Links and Concepts . . . . . 22
DSL Internet Access . . . . . 23
Cable Broadband . . . . . 25
The Public Switched Telephone Network . . . . . 26
Leased Lines . . . . . 27
T3 Lines . . . . . 28
Metro-Optical . . . . . 29
Satellite Internet Access . . . . . 31
Termination Points . . . . . 32
Demarc, Demarc Extension, and Smart Jacks . . . . . 32
CSUs/DSUs . . . . . 34

Verify Wiring Installation and Termination . . . . . 34
Virtual Networking . . . . . 34
What's Next? . . . . . 39

**CHAPTER 2:**
**Models, Ports, Protocols, and Network Services . . . . . 41**

The OSI Networking Model . . . . . 42
The OSI Seven-Layer Model . . . . . 42
Physical Layer (Layer 1) . . . . . 43
Data Link Layer (Layer 2) . . . . . 44
Network Layer (Layer 3) . . . . . 44
Transport Layer (Layer 4) . . . . . 45
Session Layer (Layer 5) . . . . . 46
Presentation Layer (Layer 6) . . . . . 46
Application Layer (Layer 7) . . . . . 47
OSI Model Summary . . . . . 47
Comparing OSI to the Four-Layer TCP/IP Model . . . . . 48
Identifying the OSI Layers at Which Various Network Components Operate . . . . . 49
Data Encapsulation/Decapsulation and OSI . . . . . 49
Ports and Protocols . . . . . 53
Connection-Oriented Protocols Versus Connectionless Protocols . . . . . 54
Internet Protocol . . . . . 54
Transmission Control Protocol . . . . . 55
How TCP Works . . . . . 56
User Datagram Protocol . . . . . 56
Internet Control Message Protocol . . . . . 57
IPSec . . . . . 57
Generic Routing Encapsulation . . . . . 58
File Transfer Protocol . . . . . 58
Secure Shell . . . . . 60
Secure File Transfer Protocol . . . . . 61
Telnet . . . . . 61
Simple Mail Transfer Protocol . . . . . 62
Domain Name System (DNS) . . . . . 62
Dynamic Host Configuration Protocol (DHCP) . . . . . 62
Trivial File Transfer Protocol . . . . . 63
Hypertext Transfer Protocol . . . . . 64

Network Time Protocol (NTP) . . . 64
Post Office Protocol Version 3/Internet Message Access Protocol Version 4 . . . 65
Simple Network Management Protocol . . . 66
Components of SNMP . . . 66
SNMP Management Systems . . . 67
SNMP Agents . . . 67
Management Information Bases . . . 68
SNMP Communities . . . 69
SNMPv3 . . . 69
Lightweight Directory Access Protocol . . . 69
Hypertext Transfer Protocol Secure . . . 70
Server Message Block . . . 70
Syslog . . . 70
SMTP TLS . . . 71
LDAPS . . . 71
IMAP over SSL . . . 71
POP3 over SSL . . . 71
SQL, SQLnet, and MySQL . . . 71
Remote Desktop Protocol . . . 72
Session Initiation Protocol . . . 72
Understanding Port Functions . . . 73
Network Services . . . 78
Domain Name Service (DNS) . . . 78
The DNS Namespace . . . 81
Types of DNS Entries . . . 83
DNS Records . . . 83
DNS in a Practical Implementation . . . 85
Dynamic Host Configuration Protocol . . . 86
The DHCP Process . . . 88
DHCP and DNS Suffixes . . . 89
DHCP Relays and IP Helpers . . . 89
Network Time Protocol . . . 89
What's Next? . . . 92

**CHAPTER 3:**
**Addressing, Routing, and Switching . . . 93**

IP Addressing . . . 94
IPv4 . . . 95
IP Address Classes . . . 95

Subnet Mask Assignment . . . . . 97
Subnetting . . . . . 97
Identifying the Differences Between IPv4 Public and Private Networks . . . . . 98
Private Address Ranges . . . . . 99
Classless Interdomain Routing . . . . . 100
Default Gateways . . . . . 100
Virtual IP . . . . . 102
IPv4 Address Types . . . . . 102
Unicast Address . . . . . 102
Broadcast Address . . . . . 102
Multicast . . . . . 102
IPv6 Addressing . . . . . 103
Where Have All the IPv4 Addresses Gone? . . . . . 103
Identifying IPv6 Addresses . . . . . 103
IPv6 Address Types . . . . . 105
Global Unicast Addresses . . . . . 105
Link-Local Addresses . . . . . 106
Site-Local Addresses . . . . . 106
Neighbor Discovery . . . . . 107
Comparing IPv4 and IPv6 Addressing . . . . . 107
Assigning IP Addresses . . . . . 108
Static Addressing . . . . . 108
Dynamic Addressing . . . . . 108
BOOT Protocol (BOOTP) . . . . . 111
Automatic Private IP Addressing . . . . . 111
Identifying MAC Addresses . . . . . 112
NAT and PAT . . . . . 114
NAT . . . . . 114
PAT . . . . . 115
SNAT . . . . . 116
DNAT . . . . . 116
Managing Routing and Switching . . . . . 120
The Default Gateway . . . . . 120
Routing Tables . . . . . 121
Static Routing . . . . . 122
Default Route . . . . . 123
Switching Methods . . . . . 123

Packet Switching . . . 123
Circuit Switching . . . 124
Comparing Switching Methods . . . 125
Dynamic Routing . . . 126
Distance-Vector Routing . . . 126
Link-State Routing . . . 129
Hybrid Routing Protocols . . . 130
Network Traffic . . . 130
Routing Metrics . . . 133
Virtual Local-Area Networks . . . 133
VLAN Membership . . . 135
VLAN Segmentation . . . 137
The Spanning Tree Protocol . . . 138
Interface Configuration and Switch Management . . . 140
MDI-X . . . 142
Trunking . . . 142
Port Mirroring . . . 142
Port Authentication . . . 143
Power over Ethernet (PoE and PoE+) . . . 143
MAC Address Table . . . 144
Switch Management . . . 144
Managed and Unmanaged . . . 144
Quality of Service . . . 145
Traffic Shaping . . . 146
Access Control Lists . . . 146
ARP and RARP . . . 147
What's Next? . . . 150

**CHAPTER 4:**
**Network Implementations . . . 151**

Common Networking Devices . . . 152
Firewall . . . 153
IDS/IPS . . . 154
Router . . . 155
Switch . . . 157
Hub and Switch Cabling . . . 158
Multilayer Switch . . . 159
Hub . . . 160

Bridge . . . 161
DSL and Cable Modems . . . 161
Access Point . . . 162
Media Converter . . . 163
Voice Gateway . . . 164
Repeater . . . 165
Wireless LAN Controller . . . 165
Load Balancer . . . 165
Proxy Server . . . 166
VPN Concentrators and Headends . . . 168
Networked Devices . . . 168
Networking Architecture . . . 172
Three-Tiered Architecture . . . 172
Core Layer . . . 173
Distribution/Aggregation Layer . . . 173
Access/Edge Layer . . . 174
Software-Defined Networking . . . 174
Application Layer . . . 174
Control Layer . . . 175
Infrastructure Layer . . . 175
Management Plane . . . 175
Spine and Leaf . . . 175
Traffic Flows . . . 176
Datacenter Location Types . . . 176
Storage-Area Networks . . . 177
iSCSI . . . 178
Fibre Channel and FCoE . . . 178
Network-Attached Storage . . . 179
What's Next? . . . 181

**CHAPTER 5:**
**Cabling Solutions and Issues . . . 183**

General Media Considerations . . . 184
Broadband Versus Baseband Transmissions . . . 185
Simplex, Half-Duplex, and Full-Duplex Modes . . . 185
Data Transmission Rates . . . 186
Types of Network Media . . . 186
Twisted-Pair Cabling (Copper) . . . 187
Coaxial Cables . . . 190

Twinaxial Cables . . . 191
Fiber-Optic Cables . . . 192
Plenum Versus PVC Cables . . . 194
Types of Media Connectors . . . 194
BNC Connectors . . . 194
RJ-11 Connectors . . . 195
RJ-45 Connectors . . . 196
F-Type Connectors and RG-59 and RG-6 Cables . . . 197
Fiber Connectors . . . 197
Transceivers . . . 199
Media Couplers/Converters . . . 200
TIA/EIA 568A and 568B Wiring Standards . . . 200
Straight-Through Versus Crossover Cables . . . 201
Rollover and Loopback Cables . . . 203
Components of Wiring Distribution . . . 204
Network Cross-Connects . . . 204
Horizontal Cabling . . . 205
Vertical Cables . . . 206
Patch Panels . . . 207
Fiber Distribution Panels . . . 208
66 and 110 Blocks (T568A, T568B) . . . 208
MDF and IDF Wiring Closets . . . 209
Ethernet Copper and Fiber Standards . . . 210
10BASE-T . . . 210
100BASE-TX . . . 211
1000BASE-T . . . 212
10GBASE-T . . . 212
40GBASE-T . . . 213
1000BASE-LX and 1000BASE-SX . . . 213
10GBASE-LR and 10GBASE-SR . . . 214
Multiplexing Options . . . 214
Troubleshooting Common Cable Connectivity Issues . . . 217
Limitations, Considerations, and Issues . . . 218
Throughput, Speed, and Distance . . . 218
Cabling Specifications/Limitations . . . 220
Cabling Considerations . . . 220
Cabling Applications . . . 221
Attenuation and dB Loss . . . 221
Interference . . . 222

Incorrect Pinout . . . . . 222
Bad Ports . . . . . 223
Open/Short . . . . . 223
LED Status Indicators . . . . . 224
Incorrect Transceivers . . . . . 224
Duplexing Issues . . . . . 224
TX/RX Reversed . . . . . 225
Dirty Optical Cables . . . . . 225
Common Tools . . . . . 226
Cable Crimpers, Strippers, and Snips/Cutters . . . . . 226
Punchdown Tools . . . . . 227
Tone Generator . . . . . 228
Loopback Adapter . . . . . 228
OTDR . . . . . 229
Multimeter . . . . . 230
Cable Tester . . . . . 230
Wire Map . . . . . 231
Tap . . . . . 231
Fusion Splicer . . . . . 231
Spectrum Analyzer . . . . . 231
Fiber Light Meter . . . . . 232
What's Next? . . . . . 234

**CHAPTER 6:**
**Wireless Solutions and Issues . . . . . 235**

Understanding Wireless Basics . . . . . 236
Wireless Channels and Frequencies . . . . . 236
Cellular Technology Access . . . . . 241
Speed, Distance, and Bandwidth . . . . . 241
Channel Bonding . . . . . 242
MIMO/MU-MIMO/Directional/Omnidirectional . . . . . 243
Antenna Ratings . . . . . 244
Antenna Coverage . . . . . 244
Establishing Communications Between Wireless Devices . . . . . 246
Configuring the Wireless Connection . . . . . 248
Troubleshooting Wireless Issues . . . . . 257
Site Surveys . . . . . 262
Factors Affecting Wireless Signals . . . . . 262

Interference . . . 262
Reflection, Refraction, and Absorption . . . 263
Troubleshooting AP Coverage . . . 264
What's Next? . . . 267

**CHAPTER 7:**
**Cloud Computing Concepts and Options . . . 269**

Cloud Concepts . . . 270
Service Models . . . 271
Software as a Service . . . 271
Platform as a Service . . . 272
Infrastructure as a Service . . . 273
Desktop as a Service . . . 274
Deployment Models . . . 275
Private Cloud . . . 275
Public Cloud . . . 275
Hybrid and Community Clouds . . . 276
Infrastructure as Code . . . 276
Connectivity Options . . . 277
Multitenancy . . . 278
Elasticity . . . 278
Scalability . . . 278
Security Implications . . . 278
The Relationship Between Resources . . . 279
What's Next? . . . 281

**CHAPTER 8:**
**Network Operations . . . 283**

Organizational Documents and Policies . . . 284
Wiring and Port Locations . . . 287
Troubleshooting Using Wiring Schematics . . . 289
Physical and Logical Network Diagrams . . . 290
Baseline Configurations . . . 293
Policies, Procedures, Configurations, and Regulations . . . 295
Policies . . . 295
Password-Related Policies . . . 298
Procedures . . . 301
Change Management Documentation . . . 302
Configuration Documentation . . . 303
Regulations . . . 303

Labeling . . . 304
High Availability and Disaster Recovery . . . 308
Backups . . . 309
Full Backups . . . 309
Differential Backups . . . 310
Incremental Backups . . . 310
Snapshots . . . 312
Backup Best Practices . . . 312
Using Uninterruptible Power Supplies . . . 313
Why Use a UPS? . . . 313
Power Threats . . . 313
Beyond the UPS . . . 314
Cold, Warm, Hot, and Cloud Sites . . . 315
High Availability and Recovery Concepts . . . 316
Active-Active Versus Active-Passive . . . 318
Monitoring Network Performance . . . 323
Common Performance Metrics . . . 324
SNMP Monitors . . . 328
Management Information Base (MIB) . . . 329
Network Performance, Load, and Stress Testing . . . 329
Performance Tests . . . 330
Load Tests and Send/Receive Traffic . . . 330
Stress Tests . . . 331
Performance Metrics . . . 331
Network Device Logs . . . 332
Security Logs . . . 332
Application Log . . . 334
System Logs . . . 334
History Logs . . . 335
Log Management . . . 335
Patch Management . . . 336
Environmental Factors . . . 339
What's Next? . . . 342

CHAPTER 9:
**Network Security** . . . **343**

Common Security Concepts . . . 344
Access Control . . . 346
Mandatory Access Control . . . 346

Discretionary Access Control . . . 346
Rule-Based Access Control . . . 347
Role-Based Access Control . . . 348
Defense in Depth . . . 349
Network Segmentation . . . 349
Screened Subnet . . . 349
Separation of Duties . . . 351
Honeypots . . . 351
RADIUS and TACACS+ . . . 352
Kerberos Authentication . . . 353
Local Authentication . . . 355
Lightweight Directory Access Protocol . . . 356
Using Certificates . . . 356
Auditing and Logging . . . 357
Multifactor Authentication Factors . . . 357
Additional Access Control Methods . . . 358
802.1X . . . 358
Extensible Authentication Protocol (EAP) . . . 358
Network Access Control (NAC) . . . 359
MAC Filtering . . . 360
Risk Management . . . 361
Penetration Testing . . . 361
Security Information and Event Management . . . 362
Common Networking Attacks . . . 365
Denial-of-Service and Distributed Denial-of-Service Attacks . . . 365
Types of DoS Attacks . . . 366
Other Common Attacks . . . 368
Social Engineering . . . 368
Logic Bomb . . . 368
Rogue DHCP . . . 369
Rogue Access Points and Evil Twins . . . 369
Advertising Wireless Weaknesses . . . 369
Phishing . . . 369
Ransomware . . . 370
DNS Poisoning . . . 370
ARP Cache Poisoning . . . 370
Spoofing . . . 370

Deauthentication . . . 370
Brute Force . . . 371
On-Path Attack . . . 371
VLAN Hopping . . . 371
ARP Spoofing . . . 372
Vulnerabilities and Prevention . . . 372
Network Hardening and Physical Security . . . 377
Disposing of Assets . . . 379
Implementing Physical Security . . . 379
Lock and Key . . . 380
Swipe Card and PIN Access . . . 381
Biometrics . . . 381
Two-Factor and Multifactor Authentication . . . 382
Secured Versus Unsecured Protocols . . . 382
Hardening Best Practices . . . 384
Wireless Security . . . 387
MAC Filtering . . . 388
Antenna Placement and Power Levels . . . 388
Isolation . . . 388
Preshared Keys . . . 388
Geofencing . . . 389
Captive Portal . . . 390
IoT Access Considerations . . . 390
Remote-Access Methods . . . 392
Remote File Access . . . 394
VPNs . . . 394
Components of the VPN Connection . . . 395
VPN Connection Types . . . 396
VPN Pros and Cons . . . 396
IPSec . . . 397
SSL/TLS/DTLS . . . 398
Site-to-Site and Client-to-Site . . . 399
Virtual Desktops . . . 399
HTTPS/Management URL . . . 400
Authentication and Authorization Considerations . . . 400
Out-of-Band Management . . . 400
What's Next? . . . 402

**CHAPTER 10:**
**Network Troubleshooting . . . . . 403**

Troubleshooting Steps and Procedures . . . . . 404
Identify the Problem . . . . . 405
Identify Symptoms . . . . . 406
Determine Whether Anything Has Changed . . . . . 406
Duplicate the Problem if Possible . . . . . 407
Approach Multiple Problems Individually . . . . . 407
Establish a Theory of Probable Cause . . . . . 407
Test the Theory to Determine the Cause . . . . . 408
Establish a Plan of Action . . . . . 408
Implement the Solution or Escalate . . . . . 409
Determine Whether Escalation Is Necessary . . . . . 409
Verify Full System Functionality . . . . . 410
Document Findings, Actions, Outcomes, and Lessons . . . . . 411
Software Troubleshooting Tools . . . . . 414
Wi-Fi Analyzer . . . . . 415
Protocol Analyzer . . . . . 415
Bandwidth Speed Tester . . . . . 416
Port Scanner . . . . . 416
iperf . . . . . 418
NetFlow Analyzer . . . . . 419
TFTP Server . . . . . 419
Terminal Emulator . . . . . 419
IP Scanner . . . . . 419
Command-Line Tools . . . . . 420
The Trace Route Utility (tracert/traceroute) . . . . . 421
ping . . . . . 425
The Destination Host Unreachable Message . . . . . 426
The Request Timed Out Message . . . . . 426
The Unknown Host Message . . . . . 427
The Expired TTL Message . . . . . 428
Troubleshooting with ping . . . . . 428
hostname . . . . . 430
ARP . . . . . 430
arp ping . . . . . 431
The netstat Command . . . . . 432
netstat -e . . . . . 434
netstat -a . . . . . 434

netstat -r . . . 435
netstat -s . . . 436
telnet . . . 437
ipconfig . . . 437
ifconfig . . . 440
nslookup . . . 441
dig . . . 442
The tcpdump Command . . . 443
The route Utility . . . 443
nmap . . . 445
Basic Network Platform Commands . . . 445
Troubleshooting General Networking Issues . . . 448
Common Considerations . . . 449
Common Problems to Be Aware Of . . . 449
Collisions . . . 450
Broadcast Storm . . . 450
Multicast Flooding . . . 450
Asymmetrical Routing . . . 450
Switching Loops . . . 450
Routing Loops . . . 451
Missing Route . . . 451
Low Optical Link Budget . . . 451
Incorrect VLAN . . . 451
DNS Issues . . . 451
Incorrect Gateway . . . 452
Incorrect Subnet Mask . . . 452
Duplicate or Incorrect IP Address . . . 452
Duplicate MAC Addresses . . . 453
Expired IP Address . . . 453
Rogue DHCP Server . . . 454
Certificate Issues . . . 454
NTP Issues/Incorrect Time . . . 454
DHCP Scope Exhaustion . . . 454
Blocked Ports, Services, or Addresses . . . 454
Incorrect Firewall Settings . . . 455
Incorrect ACL Settings . . . 455
Unresponsive Service . . . 455
BYOD Challenges . . . 455
Licensed Feature Issues . . . 456

Hardware Failure . . . . . 456
Network Performance Issues . . . . . 457
What's Next? . . . . . 459

**Glossary** . . . . . **461**

**Index** . . . . . **511**

# About the Author

**Emmett Dulaney** (CompTIA Network+, Cloud+, Security+, A+, and others) has been the author of several books on certifications and operating systems over the past 20 years. He is a columnist for *Certification Magazine* and a professor at a small university in Indiana. He is currently the editor of a journal devoted to business education (and the business of education).

# Dedication

*For Elijah, Wolfgang, Teresa, and Harrison: the second round*
*—Emmett Dulaney*

# Acknowledgments

Thanks are due to Eleanor (Ellie) Bru for working on this title once more and making it as strong as it can be. An enormous amount of credit for this book goes to Chris Crayton, without whom this edition would be only a shadow of what it is. It was an honor to work with him again, and I owe him enormous gratitude. Thanks continue to be due to Mike Harwood, who wrote the first few editions, and to the team of talented individuals at Pearson who work behind the scenes and make each title the best it can be.

# About the Technical Reviewer

**Chris Crayton** is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge.

# We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

*Please note that we cannot help you with technical problems related to the topic of this book.*

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

# Reader Services

Register your copy of *CompTIA Network+ N10-008 Exam Cram* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780137375769 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

# Introduction

Welcome to *CompTIA Network+ N10-008 Exam Cram*. This book is designed to prepare you to take—and pass—the CompTIA Network+ exam. The Network+ exam has become the leading introductory-level network certification available today. It is recognized by both employers and industry giants as providing candidates with a solid foundation of networking concepts, terminology, and skills. The Network+ exam covers a broad range of networking concepts to prepare candidates for the technologies they are likely to work with in today's network environments.

# About Network+ Exam Cram

Exam Crams are designed to give you the information you need to know to prepare for a certification exam. They cut through the extra information, focusing on the areas you need to get through the exam. With this in mind, the elements within the Exam Cram titles are aimed at providing the exam information you need in the most succinct and accessible manner.

In this light, this book is organized to closely follow the actual CompTIA objectives for exam N10-008. As such, it is easy to find the information required for each of the specified CompTIA Network+ objectives. The objective focus design used by this Exam Cram is an important feature because the information you need to know is easily identifiable and accessible. To see what we mean, compare the CompTIA objectives to the book's layout, and you can see that the facts are right where you would expect them to be.

Within the chapters, potential exam hotspots are clearly highlighted with Exam Alerts. They have been carefully placed to let you know that the surrounding discussion is an important area for the exam. To further help you prepare for the exam, a Cram Sheet is included that you can use in the final stages of test preparation. Be sure to pay close attention to the bulleted points on the Cram Sheet because they pinpoint the technologies and facts you probably will encounter on the test.

Finally, great effort has gone into the questions that appear throughout the chapter and the practice tests to ensure that they accurately represent the look and feel of the ones you will see on the real Network+ exam. Be sure, before taking the exam, that you are comfortable with both the format and content of the questions provided in this book.

# About the Network+ Exam

The Network+ (N10-008 Edition) exam is the newest iteration of several versions of the exam. The new Network+ objectives are aimed toward those who have at least nine months of experience in network support or administration. CompTIA believes that new Network+ candidates should have A+ certification (or its equivalent), but it is not required, and this should not discourage those who do not.

You will have a maximum of 90 minutes to answer the 90 questions on the exam. The allotted time is quite generous, so when you finish, you probably will have time to double-check a few of the answers you were unsure of.

By the time the dust settles, you need a minimum score of 720 to pass the Network+ exam. This is on a scale of 100 to 900. For more information on the specifics of the Network+ exam, refer to CompTIA's main website at http://certification.comptia.org/.

# CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (that is, objectives) and specific topics under each general topic (that is, subobjectives) for the CompTIA Network+ N10-008 exam. This table also lists the chapter in which each exam topic is covered.

TABLE I-1 **CompTIA Network+ Exam Topics**

| Chapter | N10-008 Exam Objective | N10-008 Exam Subobjective |
|---|---|---|
| 1 (Network Technologies, Topologies, and Types) | 1.0 Networking Fundamentals | 1.2 Explain the characteristics of network topologies and network types. |
| 2 (Models, Ports, Protocols, and Network Services) | 1.0 Networking Fundamentals | 1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.<br>1.5 Explain common ports and protocols, their application, and encrypted alternatives.<br>1.6 Explain the use and purpose of network services. |
| 3 (Addressing, Routing, and Switching) | 1.0 Networking Fundamentals<br>2.0 Network Implementations | 1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.<br>2.2 Compare and contrast routing technologies and bandwidth management concepts.<br>2.3 Given a scenario, configure and deploy common Ethernet switching features. |

| Chapter | N10-008 Exam Objective | N10-008 Exam Subobjective |
|---|---|---|
| 4 (Network Implementations) | 1.0 Networking Fundamentals<br>2.0 Network Implementations | 1.7 Explain basic corporate and datacenter network architecture.<br>2.1 Compare and contrast various devices, their features, and their appropriate placement on the network. |
| 5 (Cabling Solutions and Issues) | 1.0 Networking Fundamentals<br>5.0 Network Troubleshooting | 1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.<br>5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tool. |
| 6 (Wireless Solutions and Issues) | 2.0 Network Implementations<br>5.0 Network Troubleshooting | 2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.<br>5.4 Given a scenario, troubleshoot common wireless connectivity issues. |
| 7 (Cloud Computing Concepts and Options) | 1.0 Networking Fundamentals | 1.8 Summarize cloud concepts and connectivity options. |
| 8 (Network Operations) | 3.0 Network Operations | 3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.<br>3.2 Explain the purpose of organizational documents and policies.<br>3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution. |
| 9 (Network Security) | 4.0 Network Security | 4.1 Explain common security concepts.<br>4.2 Compare and contrast common types of attacks.<br>4.3 Given a scenario, apply network hardening techniques.<br>4.4 Compare and contrast remote access methods and security implications.<br>4.5 Explain the importance of physical security. |
| 10 (Network Troubleshooting) | 5.0 Network Troubleshooting | 5.1 Explain the network troubleshooting methodology.<br>5.3 Given a scenario, use the appropriate network software tools and commands.<br>5.5 Given a scenario, troubleshoot general networking issues. |

# Booking and Taking the Network+ Certification Exam

Unfortunately, testing is not free. You're charged for each test you take, whether you pass or fail. In the United States and Canada, tests are administered by Pearson VUE testing services. To access the VUE contact information and book an exam, refer to the website at http://www.pearsonvue.com or call 1-877-551-7587. When booking an exam, you need to provide the following information:

- Your name as you would like it to appear on your certificate.
- Your Social Security or Social Insurance number.
- Contact phone numbers (to be called in case of a problem).
- Mailing address, which identifies the address to which you want your certificate mailed.
- Exam number and title.
- Email address for contact purposes. This often is the fastest and most effective means to contact you. Test vendors require it for registration.
- Credit card information so that you can pay online. You can redeem vouchers by calling the respective testing center.

# What to Expect from the Exam

If you haven't taken a certification test, the process can be a little unnerving. Even if you've taken numerous tests, it is not much better. Mastering the inner mental game often can be as much of a battle as knowing the material. Knowing what to expect before heading in can make the process a little more comfortable.

Certification tests are administered on a computer system at a VUE authorized testing center. The format of the exams is straightforward: each question has several possible answers to choose from. The questions in this book provide a good example of the types of questions you can expect on the exam. If you are comfortable with them, the test should hold few surprises. Many of the questions vary in length. Some of them are longer scenario questions, whereas others are short and to the point. Carefully read the questions; the longer questions often have a key point that will lead you to the correct answer.

Most of the questions on the Network+ exam require you to choose a single correct answer, but a few require multiple answers. When there are multiple correct answers, a message at the bottom of the screen prompts you to "Choose all that apply." Be sure to read these messages.

## A Few Exam-Day Details

It is recommended that you arrive at the examination room at least 15 minutes early, although a few minutes earlier certainly would not hurt. This will give you time to prepare and will give the test administrator time to answer any questions you might have before the test begins. Many people suggest that you review the most critical information about the test you're taking just before the test. (Exam Cram books provide a reference—the Cram Sheet, located inside the front of this book—that lists the essential information from the book in distilled form.) Arriving a few minutes early will give you some time to compose yourself and mentally review this critical information.

You will be asked to provide two forms of ID, one of which must be a photo ID. Both of the identifications you choose should have a signature. You also might need to sign in when you arrive and sign out when you leave.

Be warned: The rules are clear about what you can and cannot take into the examination room. Books, laptops, note sheets, and so on are not allowed in the examination room. The test administrator will hold these items, to be returned after you complete the exam. You might receive either a wipe board or a pen and a single piece of paper for making notes during the exam. The test administrator will ensure that no paper is removed from the examination room.

## After the Test

Whether you want it or not, as soon as you finish your test, your score displays on the computer screen. In addition to the results appearing on the computer screen, a hard copy of the report prints for you. Like the onscreen report, the hard copy displays the results of your exam and provides a summary of how you did on each section and on each technology. If you were unsuccessful, this summary can help you determine the areas you need to brush up on.

When you pass the Network+ exam, you will have earned the Network+ certification, and your certificate will be mailed to you within a few weeks. Should you not receive your certificate and information packet within five weeks of passing your exam, contact CompTIA at fulfillment@comptia.org, or call 1-630-678-8300 and ask for the fulfillment department.

# Last-Minute Exam Tips

Studying for a certification exam is no different than studying for any other exam, but a few hints and tips can give you the edge on exam day:

- **Read all the material:** CompTIA has been known to include material not expressly specified in the objectives. This book has included additional information not reflected in the objectives to give you the best possible preparation for the examination.
- **Watch for the Exam Tips and Notes:** The Network+ objectives include a wide range of technologies. Exam Tips and Notes found throughout each chapter are designed to pull out exam-related hotspots. These can be your best friends when preparing for the exam.
- **Use the questions to assess your knowledge:** Don't just read the chapter content; use the exam questions to find out what you know and what you don't. If you struggle, study some more, review, and then assess your knowledge again.
- **Review the exam objectives:** Develop your own questions and examples for each topic listed. If you can develop and answer several questions for each topic, you should not find it difficult to pass the exam.

Good luck!

# Companion Website

Register this book to get access to the Pearson Test Prep practice test software and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exams. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: 9780137375769.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following these steps, please visit www.pearsonITcertification.com/contact and select the Site Problems/Comments option. Our customer service representatives will assist you.

# Pearson Test Prep Practice Test Software

As noted previously, the print book comes with the Pearson Test Prep practice test software containing two full exams. (The ebook edition of the *CompTIA Network+ N10-008 Exam Cram* does not include access to the Pearson Test Prep practice exams that come with the print edition.) These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep practice test software.

> **Note**
>
> The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exams associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

# Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, follow these steps:

1. Go to www.PearsonTestPrep.com.
2. Select **Pearson IT Certification** as your product group.
3. Enter your email/password for your account. If you don't have an account on PearsonITCertification.com, you will need to establish one by going to PearsonITCertification.com/join.

4. In the My Products tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product.
6. The product will now be listed in your My Products page. Click the **Exams** button to launch the exam settings screen and start your exam.

# Accessing the Pearson Test Prep Software Offline

If you want to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website, or you can enter the following link in your browser:

www.pearsonitcertification.com/content/downloads/pcpt/engine.zip

To access the book's companion website and the software, follow these steps:

1. Register your book by going to PearsonITCertification.com/register and entering the ISBN: 9780137375769.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. After the software downloads, unzip all the files on your computer.
7. Double-click the application file to start the installation, and follow the onscreen instructions to complete the registration.
8. When the installation is complete, launch the application and select the **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book, and click the **Activate** button.
11. Click **Next** and then **Finish** to download the exam data to your application.
12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will sync together, so saved exams and grade results recorded on one version will be available to you on the other as well.

## Customizing Your Exams

After you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study Mode
- Practice Exam Mode
- Flash Card Mode

Study Mode enables you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps. Practice Exam Mode locks certain customization options because it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card Mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode will not provide the detailed score reports that the other two modes will, so it should not be used if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all the chapters, or you can narrow your selection to a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, first deselect all the chapters; then select only those on which you want to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

You can make several other customizations to your exam from the exam settings screen, such as the time of the exam, the number of questions, whether to randomize questions and answers, whether to show the number of correct answers for multiple answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

# Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes that were made since the last time you used the software. This requires that you are connected to the Internet at the time you launch the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams.

To update a particular exam you have already activated and downloaded, select the **Tools** tab and then click the **Update Products** button. Again, this is an issue only with the desktop Windows application.

If you want to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, select the **Tools** tab and click the **Update Application** button. This will ensure that you are running the latest version of the software engine.

# Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30 percent of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the CramSaver quizzes at the beginning of each chapter and review the exam objectives and Exam Alerts presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

# Premium Edition eBook and Practice Tests

The print book also includes an exclusive offer for 80 percent off the Premium Edition eBook and Practice Tests edition of this title. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

CHAPTER 1

# Network Technologies, Topologies, and Types

**This chapter covers the following official Network+ objective:**

- Explain the characteristics of network topologies and network types.

This chapter covers CompTIA Network+ objective 1.2. For more information on the official Network+ exam topics, see the "About the Network+ Exam" section in the Introduction.

A variety of physical and logical network layouts are in use today. As a network administrator, you might find yourself working on these different network layouts or topologies. Therefore, you must understand how they are designed to function.

This chapter reviews general network considerations, such as the various topologies used on today's networks, *local-area networks* (LANs), *wide-area networks* (WANs), and some of the *Institute of Electrical and Electronics Engineers* (IEEE) standards.

# Wired and Wireless Network Topologies

- **Explain the characteristics of network topologies and network types.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. Which topology (star, bus, or ring) would utilize a switch?
2. With which topology does every node have a direct connection to every other node?

### Answers

1. Of the choices given, only a star topology would utilize a switch.
2. With a mesh topology, every node has a direct connection to every other node.

A *topology* refers to a network's physical and logical layout. A network's *physical* topology refers to the actual layout of the computer cables and other network devices. A network's *logical* topology refers to the way in which the network appears to the devices that use it.

Several topologies are in use on networks today. Some of the more common topologies are the bus, ring, star, mesh, and wireless. The following sections provide an overview of each.

## Bus Topology

A *bus topology* uses a trunk or backbone to connect all the computers on the network, as shown in Figure 1.1. Systems connect to this backbone using *T connectors* or taps (known as a vampire tap, if you must pierce the wire). To avoid signal reflection, a physical bus topology requires that each end of the physical bus be terminated, with one end also being grounded. Note that a hub or switch is not needed in this installation.

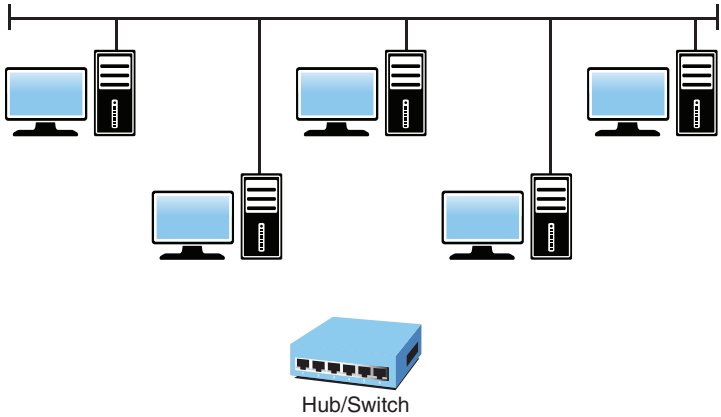



FIGURE 1.1 **Physical bus topology**

**ExamAlert**

Loose or missing terminators from a bus network disrupt data transmissions.

The most common implementation of a linear bus is the IEEE 802.3 Ethernet standard. Table 1.1 summarizes the advantages and disadvantages of the bus topology.

TABLE 1.1 **Advantages and Disadvantages of the Bus Topology**

| Advantages | Disadvantages |
|---|---|
| Compared to other topologies, a bus is cheap and easy to implement. | Network disruption might occur when computers are added or removed. |
| A bus requires less cable than other topologies. | Because all systems on the network connect to a single backbone, a break in the cable prevents all systems from accessing the network. |
| A bus does not use any specialized network equipment. | It is difficult to troubleshoot. |

# Ring Topology

The *ring topology* is a logical ring, meaning that the data travels in a circular fashion from one computer to another on the network. It is not a physical ring topology. Figure 1.2 shows the logical layout of a ring topology. Note that a hub or switch is not needed in this installation either.

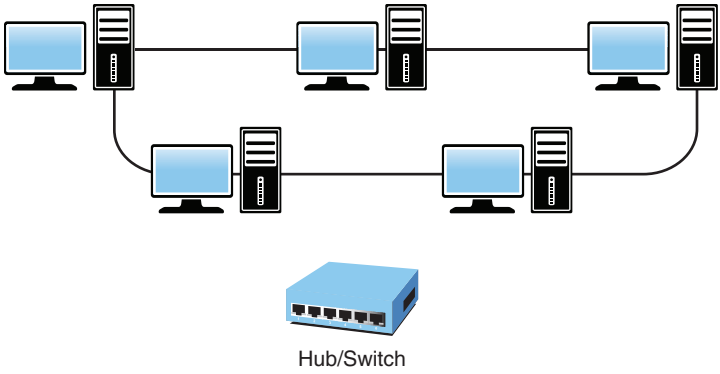



FIGURE 1.2 **Logical design of a ring topology**

In a true ring topology, if a single computer or section of cable fails, the signal is interrupted. The entire network becomes inaccessible. Network disruption can also occur when computers are added to or removed from the network, making it an impractical network design in environments where the network changes often.

As just mentioned, if a single system on the ring fails, the whole network fails. This is why ring networks can be set up in a fault-tolerant design, meaning that they have primary and secondary rings. If one ring fails, data can use the second ring to reach its destination. Naturally, the addition of the second ring adds to the cost of the network as well as the complexity.

Ring networks are most commonly wired in a star configuration. In a token ring network, a *multistation access unit (MSAU)* is equivalent to a hub or switch on an Ethernet network. The MSAU performs the token circulation internally. To create the complete ring, the *ring-in (RI)* port on each MSAU is connected to the *ring-out (RO)* port on another MSAU. The last MSAU in the ring is then connected to the first to complete the ring. Table 1.2 summarizes the advantages and disadvantages of the ring topology.

TABLE 1.2 **Advantages and Disadvantages of the Ring Topology**

| Advantages | Disadvantages |
|---|---|
| Cable faults are easily located, making troubleshooting easier. | Expansion to the network can cause network disruption. |
| Ring networks are moderately easy to install. | A single break in the cable can disrupt the entire network. |

# Star Topology (Hub-and-Spoke)

In the *star topology*, all computers and other network devices connect to a central device called a *hub* or *switch* and, for that reason, is sometimes called a *hub-and-spoke network*. Each connected device requires a single cable to be connected to the hub or switch, creating a point-to-point connection between the device and the hub or switch.

Using a separate cable to connect to the hub or switch allows the network to be expanded without disruption. A break in any single cable does not cause the entire network to fail. Figure 1.3 shows a star topology.

**ExamAlert**

Among the network topologies discussed in this chapter, the star topology is the easiest to expand in terms of the number of devices connected to the network.

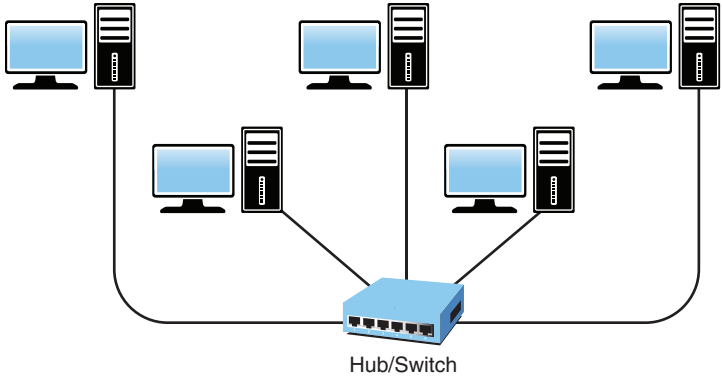



FIGURE 1.3 **Star topology**

The star topology is the most widely implemented network design in use today, but it is not without shortcomings. Because all devices connect to a centralized hub or switch, this creates a single point of failure for the network. If the hub or switch fails, any device connected to it cannot access the network. Because of the number of cables required and the need for network devices, the cost of a star network is often higher than other topologies. Table 1.3 summarizes the advantages and disadvantages of the star topology.

TABLE 1.3 **Advantages and Disadvantages of the Star Topology**

| Advantages | Disadvantages |
|---|---|
| Star networks are easily expanded without disruption to the network. | This topology requires more cable than most of the other topologies. |
| Cable failure affects only a single user. | A central connecting device allows for a single point of failure. |
| It is easy to troubleshoot and implement. | It requires additional networking equipment to create the network layout. |

# Mesh Topology

The *wired mesh topology* incorporates a unique network design in which each computer on the network connects to every other, creating a point-to-point connection between every device on the network. Since this is often done physically, the term *wired mesh* or *wired mesh topology* is sometimes used. The purpose of the mesh design is to provide a high level of *redundancy*. If one network cable fails, the data always has an alternative path to get to its destination; each node can act as a relay.

The wiring for a mesh network can be complicated, as illustrated by Figure 1.4. Furthermore, the cabling costs associated with the mesh topology can be high, and troubleshooting a failed cable can be tricky. As a result, the mesh topology is not the first choice for many wired networks but is more popular with servers/routers.

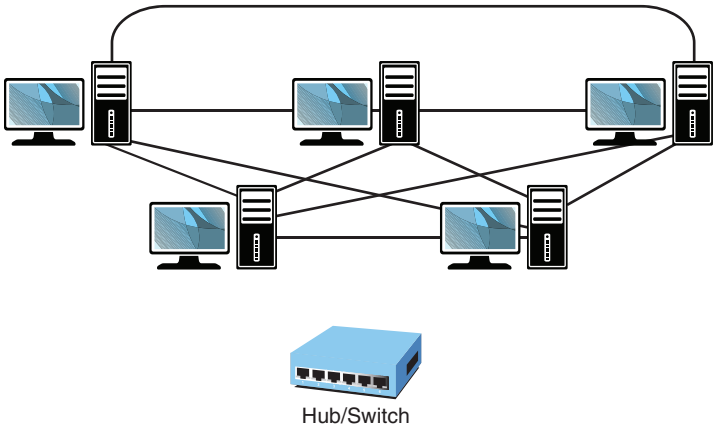



FIGURE 1.4 **Mesh topology**

Table 1.4 summarizes the advantages and disadvantages of the mesh topology.

**ExamAlert**

Because of the redundant connections, the mesh topology offers better fault tolerance than other topologies.

TABLE 1.4 **Advantages and Disadvantages of the Mesh Topology**

| Advantages | Disadvantages |
|---|---|
| Mesh provides redundant paths between LAN topologies. | It requires more cable than the other topologies. |
| The network can be expanded without disruption to current users. | The implementation is complicated. |

# Hybrid Topology

A variation on a true mesh topology is the *hybrid* or *hybrid mesh*. It creates a redundant point-to-point network connection between only specific network devices (such as the servers). The hybrid mesh is most often seen in WAN implementations but can be used in any network.

Another way of describing the degree of mesh implementation is by labeling it as either *partial* or *full*. If it is a true mesh network with connections between each device, it can be labeled full mesh, and if it is less than that—a hybrid of any sort—it is called a *partial mesh network*.

Many of the topologies found in large networking environments are a hybrid of physical topologies. An example of a hybrid topology is the star bus—a combination of the star topology and the bus topology. Figure 1.5 shows how this might look in a network implementation.

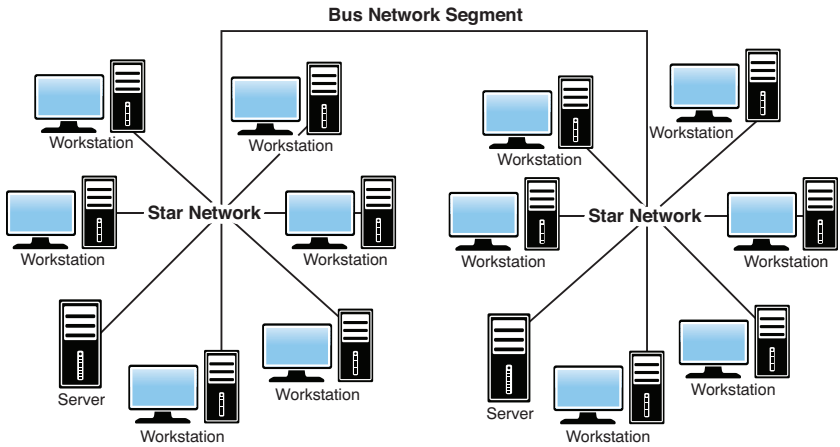



FIGURE 1.5 **A star bus topology**

**ExamAlert**

Another meaning: The term *hybrid topology* also can refer to the combination of wireless and wired networks. For the Network+ exam, however, the term *hybrid* most likely refers to the combination of physical networks.

# Bringing Wireless to a Topology

When cabling is run from one office to another, you can easily look at the layout and see whether the topology is a star, mesh, bus, ring, or hybrid. When the wires are absent, however, then it may not be as readily apparent what is being deployed. Wireless networks typically are implemented using one of three wireless topologies:

- The *infrastructure*, or managed, wireless topology
- The *ad hoc*, or unmanaged, wireless topology
- The *mesh* wireless topology

The following sections describe these three wireless topologies in greater detail.

## Infrastructure Wireless Topology

The infrastructure wireless topology is commonly used to extend a wired LAN to include wireless devices. Wireless devices communicate with the wired LAN through a base station known as an *access point (AP)* or *wireless access point*. The AP forms a bridge between a wireless and wired LAN, and all transmissions between wireless stations, or between a system and a wired network client, go through the AP. APs are not mobile and have to stay connected to the wired network; therefore, they become part of the wired network infrastructure (thus the name). In infrastructure wireless networks, there might be several access points providing wireless coverage for a large area or only a single access point for a small area, such as a single home or small building.

**Note**

**WAP or AP?** Notice that although we call it a wireless access point, it is commonly referred to as an AP. As you study for the exam, know that it can be called either an AP or a WAP, and—just to make matters confusing—WAP is also the acronym for the Wireless Application Protocol.

## Ad Hoc Wireless Topology

In a wireless ad hoc topology, devices communicate directly among themselves without using an access point. This peer-to-peer network design is commonly used to connect a small number of computers or wireless devices. For example, an ad hoc wireless network may be set up temporarily between laptops in a boardroom or to connect systems in a home instead of using a wired solution. The ad hoc wireless design provides a quick method to share files and resources among a small number of systems. Connecting mobile devices together or to a printer using Bluetooth is an example of an ad hoc network.

Figure 1.6 shows an ad hoc wireless network, and Figure 1.7 shows an infrastructure network using the AP.

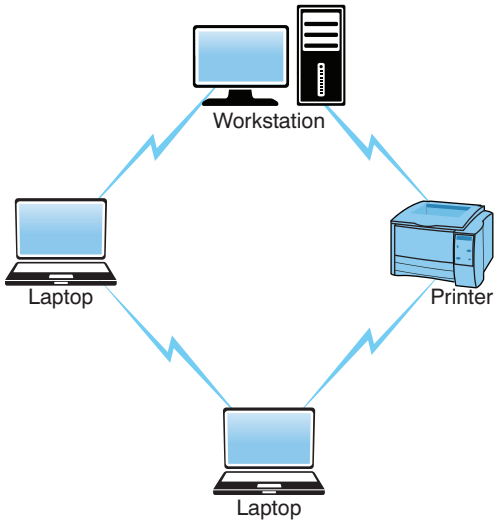



FIGURE 1.6 **Ad hoc wireless topology**

**Tip**

The ad hoc, or unmanaged, network design does not use an AP. All wireless devices connect directly to each other.

**Note**

In an infrastructure wireless network, devices use a wireless AP to connect to the network.

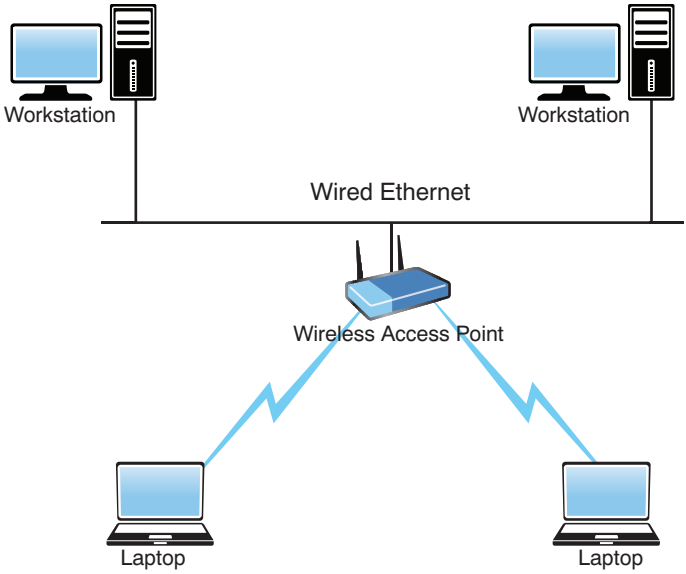



FIGURE 1.7 **Infrastructure wireless topology**

## Wireless Mesh Topology

As discussed earlier, wired mesh networks are costly because of the cabling required to interconnect all computer systems. Wireless mesh networks obviously do not need cables running between systems, making wireless mesh networks fairly common in the networking world. In the wireless mesh network, as with the wired mesh, each network node is interconnected to other nodes on the network. With a wired mesh, the wireless signal starts at a wireless base station (access point) attached to a wired network. A wireless mesh network extends the transmission distance by relaying the signal from one computer to another. Unlike the wired mesh, in which a complex and expensive collection of physical cables is required to create the mesh, the wireless mesh is inexpensive to implement. Figure 1.8 shows a wireless mesh topology.

**Note**

A wireless mesh network is created through the connection of wireless access points installed at each network user's locale. Data signals in a wireless mesh rely on all nodes to propagate signals. Wireless mesh networks can be identified by the interconnecting signals between each node.

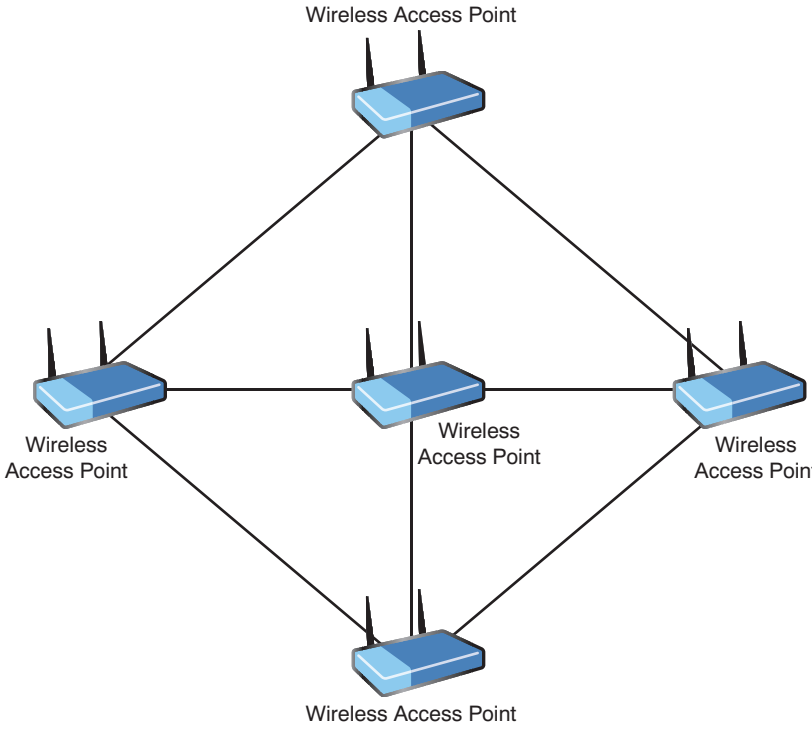



FIGURE 1.8 **A wireless mesh topology**

The wireless mesh network has several key advantages. Because a wireless mesh network is interconnected with one or more nodes on the network, the data can travel multiple paths to reach its destination. When a new node is added, it provides new paths for other nodes, which in turn improves network performance and decreases congestion. Advantages of the wireless mesh include the following:

- **Self-healing:** Wireless mesh networks are known as self-healing, which refers to the network's ability to adapt to network failure and even function should a node be moved from one location to another. Self-healing in a wireless mesh environment is possible because of the interconnected connections and because of the wireless media.
- **Scalable:** Wireless mesh networks are highly scalable. Using wireless, you are able to add new systems to the network without the need for expensive cables.

- **Reliability:** Of all network topologies, the mesh network provides the greatest reliability. The redundant number of paths for the data to travel ensures that data can reach its destination.
- **Cost:** One disadvantage of the wired mesh is the cost associated with running the cabling and the support costs of such a complex network. Wireless mesh networks are essentially self-configuring and do not have cabling requirements. Therefore, systems can be added, removed, and relocated with little cost or disruption to the network.

## Cram Quiz

1. You have been asked to install a network that will give the network users the greatest amount of fault tolerance. Which of the following network topologies would you choose?
   - ❍ **A.** Star/hub-and-spoke
   - ❍ **B.** Ring
   - ❍ **C.** Mesh
   - ❍ **D.** Bus

2. Which of the following topologies allows for network expansion with the least amount of disruption for the current network users?
   - ❍ **A.** Bus
   - ❍ **B.** Ring
   - ❍ **C.** LAN
   - ❍ **D.** Star/hub-and-spoke

3. Which network topology offers the greatest level of redundancy but has the highest implementation cost?
   - ❍ **A.** Wireless mesh
   - ❍ **B.** Wired mesh
   - ❍ **C.** Hybrid star
   - ❍ **D.** Bus network

4. Which of the following statements are associated with a bus LAN network? (Choose all correct answers.)
   - ❍ **A.** A single cable break can cause complete network disruption.
   - ❍ **B.** All devices connect to a central device.
   - ❍ **C.** It uses a single backbone to connect all network devices.
   - ❍ **D.** It uses a dual-ring configuration.

5. As a network administrator, you are called in to troubleshoot a problem on a token ring network. The network uses two MSAUs connected using the ring-in ports on both devices. All network cards are set at the same speed. What is the likely cause of the problem?
   - ❍ **A.** Bad network card
   - ❍ **B.** Faulty cabling
   - ❍ **C.** MSAU configuration
   - ❍ **D.** Network card configuration

# Cram Quiz Answers

1. **C.** A mesh network uses a point-to-point connection to every device on the network. This creates multiple points for the data to be transmitted around the network and therefore creates a high degree of redundancy. The star/hub-and-spoke, ring, and bus topologies do not offer the greatest amount of fault tolerance.
2. **D.** On a star/hub-and-spoke network, each network device uses a separate cable to make a point-to-point connection to a centralized device, such as a hub or a switch. With such a configuration, a new device can be added to the network by attaching the new device to the hub or switch with its own cable. This process does not disrupt the users who are currently on the network. Answers A and B are incorrect because the addition of new network devices on a ring or bus network can cause a disruption in the network and cause network services to be unavailable during the installation of a new device.
3. **B.** The wired mesh topology requires each computer on the network to be individually connected to every other device. This configuration provides maximum reliability and redundancy for the network. However, it is very costly to implement because of the multiple wiring requirements.
4. **A and C.** In a bus network, a single break in the network cable can disrupt all the devices on that segment of the network, a significant shortcoming. A bus network also uses a single cable as a backbone to which all networking devices attach. A star network requires networked devices to connect to a centralized device such as a hub, switch, or MSAU. Therefore, answer B is incorrect. Answer D is also incorrect because it does not use a dual-ring configuration.
5. **C.** To create the complete ring, the ring-in (RI) port on each MSAU is connected to the ring-out (RO) port on another MSAU. The last MSAU in the ring is then connected to the first to complete the ring.

# Network Types and Characteristics

▶ **Explain the characteristics of network topologies and network types.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. True or false: The biggest difference between a LAN and a WAN is usually the size of the network.
2. What network type is essentially a LAN created to share data among devices associated with you?
3. In what networking type is consolidated, block-level data storage made available to networked devices?

### Answers

1. True. A WAN is a network that spans more than one geographic location, often connecting separated LANs.
2. A personal-area network (PAN) is essentially a LAN created to share data among devices associated with you.
3. A storage-area network (SAN) makes block-level data storage available to devices on the network.

Networks are classified according to their geographic coverage and size. The two most common network classifications are local-area networks (LANs) and wide-area networks (WANs). Choosing between the two is often a matter of understanding the requirements.

### ExamAlert

For the exam, you should be able to differentiate between the various types of networks discussed here.

## To Server or Not

Sometimes there is a tendency to take concepts that are simple and complicate them when there is no real need for it. The truth of the matter is that every network is either a *peer-to-peer network* or a *client/server network* and the difference between the two is whether or not there is a dedicated server.

Any networking environment that does not have dedicated servers, and where communication occurs between similarly capable network nodes that act as both clients and servers, is a peer-to-peer network. Any network that has a dedicated server is a client/server network. Period.

# LANs

A *local-area network (LAN)* is a data network that is restricted to a single geographic location and typically encompasses a relatively small area, such as an office building or school. The function of the LAN is to interconnect workstation computers for the purpose of sharing files and resources. Because of its localized nature, the LAN typically is high speed and cheaper to set up than a WAN. Figure 1.9 shows an example of a LAN.

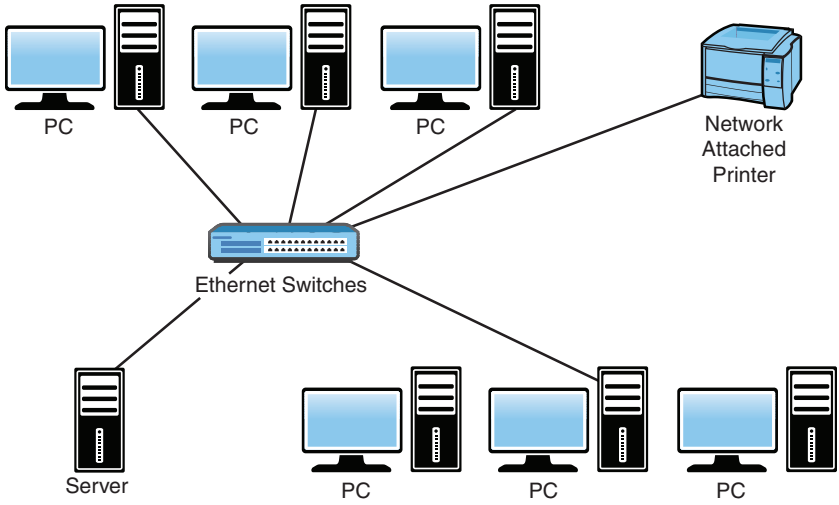



FIGURE 1.9 **A local-area network**

# WLANs

Instead of being wholly dependent on wiring for your local network, the *wireless LAN (WLAN)* provides a flexible and secure data communications system that augments an Ethernet LAN or, in some cases, replaces it altogether. Wireless transmissions send and receive data using *radio frequency (RF)* signals, freeing you from wired solutions, and are dependent on a hotspot. That hotspot can be in a coffee shop, a train station, a restaurant, or almost any public place. Security should be a prime concern of public hotspot users, and encryption should be used everywhere possible.

In a common wireless implementation, a wireless transceiver (transmitter/receiver), known as an access point, connects to the wired network from a fixed location using standard cabling. The wireless access point receives and then transmits data between the wireless LAN and the wired network infrastructure.

Client systems communicate with a wireless access point using wireless LAN adapters. Such adapters are built in to or can be added to laptops and other mobile devices or desktop computers. Wireless LAN adapters provide the communication point between the client system and the airwaves via an antenna.

# WANs

A *wide-area network (WAN)* is a network that spans more than one geographic location, often connecting separated LANs. WANs are slower than LANs and often require additional and costly hardware, such as routers, dedicated leased lines, and complicated implementation procedures. Figure 1.10 shows an example of a WAN.

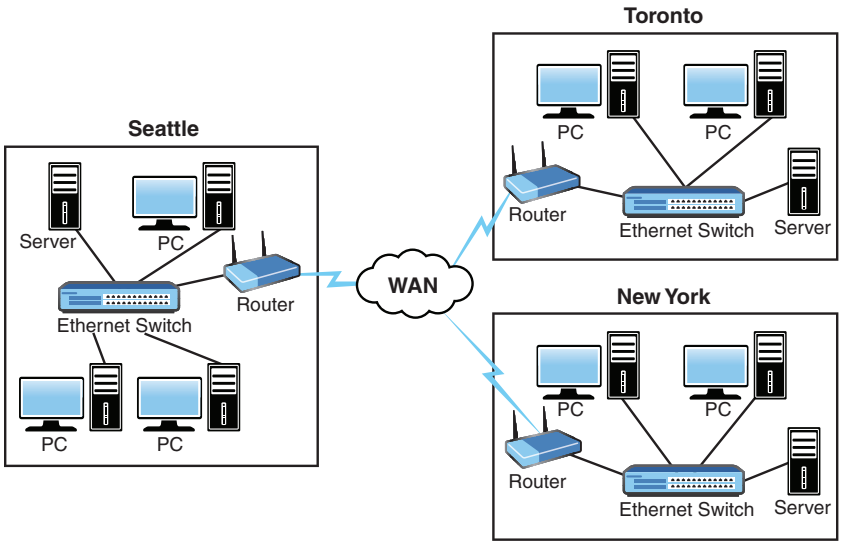



FIGURE 1.10 **A wide-area network**

# MANs

Occasionally, a WAN will be called a *metropolitan-area network (MAN)* when it is confined to a certain geographic area, such as a university campus or city. No formal guidelines dictate the differences between a MAN and a WAN;

technically, a MAN *is* a WAN. Perhaps for this reason, the term *MAN* is used less often than *WAN*. If any distinction exists, it is that a MAN is smaller than a WAN. A MAN is almost always bigger than a LAN and usually is smaller than or equal to a WAN. MANs utilize an Internet service provider (ISP) or telecommunications (telco) provider.

## CANs

When it comes to terminology and definitions, a computer network in a defined area that links buildings and consists of multiple LANs within that limited geographical area is usually called a *campus-area network (CAN)*. The CAN may encompass the whole college campus, or a portion of it. It may also have nothing to do with a college but consists of office buildings in an enterprise "campus," industrial complex, military base, or anywhere else. In reality, a CAN is a WAN, but what makes it distinct is the confined geographic area it includes.

## SANs

A *storage-area network (SAN)* consists of just what the name implies: networked/shared storage devices. With clustered storage, you can use multiple devices to increase performance. SANs are subsets of LANs and offer block-level data storage that appears within the operating systems of the connected devices as locally attached devices.

File systems built on top of SANs can provide file-level access, but the SAN itself does not provide file abstraction, only block-level operations.

## PANs

A *personal-area network (PAN)* is essentially a LAN created to share data among devices associated with you. Wireless technologies have taken PAN further and introduced a new term—*wireless personal-area network (WPAN)*. WPAN refers to the technologies involved in connecting devices in very close proximity to exchange data or resources, usually through the use of Bluetooth, infrared, or *near-field communication (NFC)*. An example is connecting a laptop with a smartphone to synchronize an address book. Because of their small size and the nature of the data exchange, WPAN devices lend themselves well to ad hoc wireless networking. Ad hoc wireless networks are those that have devices connect to each other directly, not through a wireless access point.

# SDWANs

A *software-defined wide area network (SDWAN)* is an extension of *software-defined networking (SDN)*—which is commonly used in telco and data centers—on a large scale. The concept behind it is to take many of the principles that make cloud computing so attractive and make them accessible at the WAN level. This is done by adopting a virtual WAN architecture leveraging a combination of transport services (MPLS, 5G, LTE, broadband, and so on) to connect users to applications.

Moving away from the router-centric WAN architecture that has always been used, SDWANs support applications hosted pretty much anywhere: public or private clouds, or on-premises data centers. As with an SDN, an SDWAN enables services on-demand, reduces operational costs, and is intended to improve network scalability and performance.

The SDWAN evolved from MPLS technology (which is explored next) and implements a centralized controller for setting and maintaining policies—managing the implementation.

**ExamAlert**

For the exam, think of SDWAN as a software abstraction of MPLS technology.

An SDN is a dynamic approach to computer networking intended to allow administrators to get around the static limitations of physical architecture associated with traditional networks. The goal of SDN is to not only add dynamic capabilities to the network but to also reduce IT costs through implementation of cloud architectures. SDN combines network and application services into centralized platforms that can automate provisioning and configuration of the entire infrastructure.

# MPLS

*Multiprotocol Label Switching (MPLS)* is a WAN technology used in high-performance-based telco networks. MPLS is a technology that uses short path labels instead of longer network addresses to direct data from one node to another. These "labels" are used to identify shorter virtual links between nodes instead of endpoints. MPLS supports technologies such as ATM, Frame Relay, DSL, T1, and E1.

MPLS has been used for more than 20 years to provide secure, private connectivity, but it has limits to what it can do and is costly.

**ExamAlert**

While SDWANs can utilizes MPLS technology, the goal is often to eliminate or minimize its usage due to cost. Administrators are often seeking lower-cost, higher-speed connectivity options (such as broadband and DSL).

## mGRE

*Multipoint Generic Routing Encapsulation (mGRE)* is an extension of *GRE (Generic Routing Encapsulation)* that expands its capabilities. GRE can be configured as a point-to-point tunnel between two sites, and mGRE extends this capability from a limited number of sites by dynamically establishing tunnels without the need to explicitly configure mapping entries between each and every potential next-hop destination.

**Note**

The exam objectives mix in a few protocols and technologies, such as mGRE and MPLS, with the network types and characteristics, and that is why their discussion appears so early in this book.

## Cram Quiz

1. When a WAN is confined to a certain geographic area, such as a city, it is known as a
   - ❍ **A.** LAN
   - ❍ **B.** MAN
   - ❍ **C.** VAN
   - ❍ **D.** VPN

2. Which of the following is a computer network in a defined area that links buildings and consists of multiple LANs within that limited geographical area?
   - ❍ **A.** SAN
   - ❍ **B.** PAN
   - ❍ **C.** DAN
   - ❍ **D.** CAN

3. Which of the following provides a flexible and secure data communications system that augments an Ethernet LAN or, in some cases, replaces it altogether?
   - ❍ **A.** PHLAN
   - ❍ **B.** MAN
   - ❍ **C.** WLAN
   - ❍ **D.** CRAN

4. Which technology uses short path labels instead of longer network addresses to direct data from one node to another?
   - ❍ **A.** MPLS
   - ❍ **B.** Metropolitan Ethernet
   - ❍ **C.** DMVPN
   - ❍ **D.** PPP

5. Which WAN architecture allows an enterprise to leverage a combination of transport services such as MPLS, 5G, LTE, or broadband to securely connect users to applications?
   - ❍ **A.** WPAN
   - ❍ **B.** SDWAN
   - ❍ **C.** GRE
   - ❍ **D.** mGRE

# Cram Quiz Answers

1. **B.** A WAN can be referred to as a metropolitan-area network (MAN) when it is confined to a certain geographic area, such as a city.
2. **D.** A campus-area network (CAN) is a computer network in a defined area that links buildings and consists of multiple LANs within that limited geographical area.
3. **C.** A wireless LAN (WLAN) augments an Ethernet LAN or, in some cases, replaces it altogether.
4. **A.** Used in high-performance-based telco networks, MPLS is a technology that uses short path labels instead of longer network addresses to direct data from one node to another. Metropolitan Ethernet is nothing more than an Ethernet-based MAN (metropolitan-area network). DMVPN offers the capability to create a dynamic-mesh VPN network without having to preconfigure all the possible tunnel endpoints. PPP is a data link protocol that is used to establish a connection between two nodes. PPP works with *plain old telephone service (POTS)*, ISDN, fiber links such as SONET, and other faster connections, such as T1.

5. **B.** The concept behind an SDWAN is to take many of the principles that make cloud computing so attractive and make them accessible at the WAN level. This is done by adopting a virtual WAN architecture leveraging a combination of transport services (MPLS, 5G, LTE, broadband, and so on) to securely connect users to applications. WPAN refers to the technologies involved in connecting devices in very close proximity to exchange data or resources, usually through the use of Bluetooth, infrared, or NFC. GRE provides a secure private path for packets through a public network using a point-to-point tunnel between two sites. mGRE extends this capability from a limited number of sites by dynamically establishing tunnels without the need to explicitly configure mapping entries.

# Network Links and Concepts

▶ **Explain the characteristics of network topologies and network types.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What is VHDSL commonly used for?
2. True or false: DSL using regular phone lines transfers data over the same copper wire.
3. What is the difference between a one-way and a two-way satellite system?
4. What hardware is located at the demarcation point?

### Answers

1. VHDSL supports high-bandwidth applications such as VoIP and HDTV.
2. True. DSL using regular phone lines transfers data over the same copper wire.
3. A *one-way satellite system* requires a satellite card and a satellite dish installed at the end user's site. This system works by sending outgoing requests on one link using a phone line, with inbound traffic returning on the satellite link. A *two-way satellite system*, in contrast, provides data paths for both upstream and downstream data.
4. The hardware at the demarcation point is the smart jack, also known as the network interface device (NID).

Internet access has become an integral part of modern business. You can obtain Internet access in several ways. Which type you choose often depends on the cost and what technologies are available in your area. This section explores some of the more common methods of obtaining Internet access.

### Note

The term *broadband* often refers to high-speed Internet access. Both DSL and cable modems are common broadband Internet technologies. Broadband routers and broadband modems are network devices that support both DSL and cable.

# DSL Internet Access

*Digital subscriber line (DSL)* is an Internet access method that uses a standard phone line to provide high-speed Internet access. DSL was most commonly associated with high-speed Internet access, but is fading in popularity and availability. Because it is a relatively inexpensive Internet access, it is often found in homes and small businesses, but even there it is quickly being replaced by fiber. With DSL, a different frequency can be used for digital and analog signals, which means that you can talk on the phone while you upload data.

For DSL services, two types of systems exist: *asymmetric digital subscriber line (ADSL)* and *high-rate digital subscriber line (HDSL)*. ADSL provides a high data rate in only one direction. It enables fast download speeds but significantly slower upload speeds. ADSL is designed to work with existing analog telephone service (POTS) service. With fast download speeds, ADSL is well suited for home-use Internet access where uploading large amounts of data isn't a frequent task.

In contrast to ADSL, HDSL provides a bidirectional high-data-rate service that can accommodate services such as videoconferencing that require high data rates in both directions. A variant of HDSL is *very high-rate digital subscriber line (VHDSL)*, which provides an HDSL service at very high data transfer rates.

DSL arrived on the scene in the late 1990s and brought with it a staggering number of flavors. Together, all these variations are known as *xDSL*:

- **Asymmetric DSL (ADSL):** Probably the most common of the DSL varieties is ADSL, which uses different channels on the line. One channel is used for POTS and is responsible for analog traffic. The second channel provides upload access, and the third channel is used for downloads. With ADSL, downloads are faster than uploads, which is why it is called *asymmetric* DSL.

> **Note**
>
> ADSL2 made some improvements in the data rate and increased the distance from the telephone exchange that the line can run. ADSL2+ doubled the downstream bandwidth and kept all the features of ADSL2. Both ADSL2 and ADSL2+ are compatible with legacy ADSL equipment.

- **Symmetric DSL (SDSL):** A version that offers the same speeds for uploads and downloads, making it most suitable for business applications such as web hosting, intranets, and e-commerce. It is not widely implemented in the home/small business environment and cannot share a phone line.

- **ISDN DSL (IDSL):** A symmetric type of DSL commonly used in environments in which SDSL and ADSL are unavailable. IDSL does not support analog phones.
- **Rate-adaptive DSL (RADSL):** A variation on ADSL that can modify its transmission speeds based on signal quality. RADSL supports line sharing.
- **Very high-bit-rate DSL (VHDSL or VDSL):** An asymmetric version of DSL and, as such, can share a telephone line. VHDSL supports high-bandwidth applications such as VoIP and HDTV. VHDSL can achieve data rates up to approximately 10 Mbps, making it the fastest available form of DSL. To achieve high speeds, VHDSL uses fiber-optic cabling.
- **High-bit-rate DSL (HDSL):** A symmetric technology that offers identical transmission rates in both directions. HDSL does not allow line sharing with analog phones.

Why are there are so many DSL variations? The answer is quite simply that each flavor of DSL is aimed at a different user, business, or application. Businesses with high bandwidth needs are more likely to choose a symmetric form of DSL, whereas budget-conscious environments such as home offices are likely to choose an option that enables phone line sharing at the expense of bandwidth. In addition, some of the DSL variants are older technologies. Although the name persists, they have been replaced with newer DSL implementations. When you work in a home/small office environment where DSL is present, you are usually working with an ADSL system.

Table 1.5 summarizes the maximum speeds of the various DSL options. Maximum speeds are rarely obtained.

TABLE 1.5 **DSL Speeds**

| DSL Variation | Upload Speed* | Download Speed* |
|---|---|---|
| ADSL | 1 Mbps | 3 Mbps |
| ADSL2 | 1.3 Mbps | 12 Mbps |
| ADSL2+ | 1.4 Mbps | 24 Mbps |
| SDSL | 1.5 Mbps | 1.5 Mbps |
| IDSL | 144 Kbps | 144 Kbps |
| RADSL | 1 Mbps | 7 Mbps |
| VHDSL | 1.6 Mbps | 13 Mbps |
| HDSL | 768 Kbps | 768 Kbps |

*Speeds may vary greatly, depending on the technologies used and the quality of the connection.

**ExamAlert**

For the exam, focus on ADSL as you study, but be able to put it in perspective with other varieties.

**Note**

DSL using regular phone lines transfers data over the same copper wire. The data and voice signals are sent over different frequencies, but sometimes the signals interfere with each other. This is why you use DSL filters. A DSL filter works by minimizing this interference, making for a faster and cleaner DSL connection.

At the risk of being repetitive, it is worth pointing out again that DSL is fading in popularity as other technologies, such as cable and fiber, grow in marketplace adoption.

# Cable Broadband

*Cable broadband* Internet access is an always-on Internet access method available in areas that have digital cable television. Cable Internet access is attractive to many small businesses and home office users because it is both inexpensive and reliable. Most cable providers do not restrict how much use is made of the access, but they do control the speed. Connectivity is achieved by using a device called a *cable modem*. It has a coaxial connection for connecting to the provider's outlet and an *unshielded twisted-pair (UTP)* connection for connecting directly to a system or to a hub, switch, or router.

Cable providers often supply the cable modem, with a monthly rental agreement. Many cable providers offer free or low-cost installation of cable Internet service, which includes installing a network card in a PC. Some providers also do not charge for the network card. Cable Internet costs are comparable to DSL subscription.

Most cable modems offer the capability to support a higher-speed Ethernet connection for the home LAN than is achieved. The actual speed of the connection can vary somewhat, depending on the utilization of the shared cable line in your area.

**ExamAlert**

A cable modem generally is equipped with a *medium-dependent interface crossed (MDI-X)* port, so you can use a straight-through UTP cable to connect the modem to a system.

One of the biggest disadvantages of cable access is that you share the available bandwidth with everyone else in your cable area. As a result, during peak times, performance of a cable link might be poorer than in low-use periods. In residential areas, busy times are evenings and weekends, and particularly right after school. In general, though, performance with cable systems is good, and in low-usage periods, it can be fast.

**Note**

A debate between cable and DSL went on for many years. Although cable modem technology delivers *shared bandwidth* within the local neighborhood, its speeds are theoretically higher but influenced by this shared bandwidth. DSL delivers *dedicated local bandwidth* but is sensitive to distance that impacts overall performance. In recent years, DSL has faded in popularity as cable and fiber have grown.

# The Public Switched Telephone Network

The public switched telephone network (PSTN), often considered a POTS, is the entire collection of interconnected telephone wires throughout the world. Discussions of the PSTN include all the equipment that goes into connecting two points, such as the cable, the networking equipment, and the telephone exchanges.

**ExamAlert**

Although PSTN is not specifically listed as an exam objective, you need to know how it compares with other technologies. Know that if money is a major concern, the PSTN is the method of choice for creating a WAN.

The modern PSTN is largely digital, with analog connections existing primarily between homes and local phone exchanges. Modems are used to convert the computer system's digital signals into analog so that they can be sent over the analog connection.

Using the PSTN to establish WAN connections is a popular choice, although the significant drawback is the limited transfer speeds. Transfer on the PSTN is limited to 56 Kbps with a modem and 128 Kbps with an ISDN connection, and it is difficult to share large files or videoconferencing at such speeds. However, companies that need to send only small amounts of data remotely can use the PSTN as an inexpensive alternative for remote access, particularly when other resources such as the Internet are unavailable.

# Leased Lines

*T-carrier lines* are high-speed dedicated digital lines that can be leased from telephone companies. They create an always-open, always-available line between you and whomever you choose to connect to when you establish the service.

T-carrier lines can support both voice and data transmissions and are often used to create point-to-point private networks. Because they are a dedicated link, they can be a costly WAN option. Four types of T-carrier lines are available:

- **T1:** Offers transmission speeds of 1.544 Mbps and can create point-to-point dedicated digital communication paths. T1 lines have commonly been used for connecting LANs. In North America, DS (digital signal) notation is used with T-lines to describe the circuit. For all practical purposes, DS1 is synonymous with T1.
- **T2:** Offers transmission speeds of 6.312 Mbps. It accomplishes this by using 96 64-Kbps B channels.
- **T3:** Offers transmission speeds of up to 44.736 Mbps, using 672 64-Kbps B channels. Digital signal 3 (DS3) is a more accurate name in North America, but T3 is how most people refer to the link.

**ExamAlert**

When you take the exam, think of DS3 and T3 as synonymous.

- **T4:** Offers impressive transmission speeds of up to 274.176 Mbps by using 4,032 64-Kbps B channels.

**ExamAlert**

Of these T-carrier lines, the ones commonly associated with networks and the ones most likely to appear on the exam are the T1 and T3 lines.

**Note**

Because of the cost of a T-carrier solution, you can lease portions of a T-carrier service. This is known as *fractional T*. You can subscribe and pay for service based on 64 Kbps channels.

T-carrier is the designation for the technology used in the United States and Canada. In Europe, they are called E-carriers, and in Japan, J-carriers. Table 1.6 describes the T/E/J carriers.

TABLE 1.6 **Comparing T/E/J Carriers**

| Name | Transmission Speed |
|---|---|
| T1 | 1.544 Mbps |
| T1C | 3.152 Mbps |
| T2 | 6.312 Mbps |
| T3 | 44.736 Mbps |
| T4 | 274.176 Mbps |
| J0 | 64 Kbps |
| J1 | 1.544 Mbps |
| J1C | 3.152 Mbps |
| J2 | 6.312 Mbps |
| J3 | 32.064 Mbps |
| J3C | 97.728 Mbps |
| J4 | 397.200 Mbps |
| E0 | 64 Kbps |
| E1 | 2.048 Mbps |
| E2 | 8.448 Mbps |
| E3 | 34.368 Mbps |
| E4 | 139.264 Mbps |
| E5 | 565.148 Mbps |

**ExamAlert**

Ensure that you review the speeds of the T1, T3, E1, and E3 carriers.

## T3 Lines

For a time, the speeds offered by T1 lines were sufficient for all but a few organizations. As networks and the data they support expanded, T1 lines did not provide enough speed for many organizations. T3 service answered the call by providing transmission speeds of 44.736 Mbps.

T3 lines are dedicated circuits that provide high capacity; generally, they are used by large companies, ISPs, and long-distance companies. T3 service offers all the strengths of a T1 service (just a whole lot more), but the cost associated with T3 limits its use to the few organizations that have the money to pay for it.

# Metro-Optical

Metro-optical networks (also known as MONs) are optical networks that can span up to several hundred kilometers and are used to serve metropolitan areas in which there is a large, concentrated population. A metropolitan-area Ethernet (Ethernet MAN, or metro Ethernet network) is one form of a metro-optical network, with the typical service provider's network including a collection of switches and routers connected through optical fiber.

**Note**

Think of metro-optical as the "fiber to the home" connection. Many large metropolitan areas have undertaken initiatives to make this an affordable option for residents.

As a bit of background, in 1984, the U.S. Department of Justice and AT&T reached an agreement stating that AT&T was a monopoly that needed to be divided into smaller, directly competitive companies. This created a challenge for local telephone companies, which were faced with the task of connecting to an ever-growing number of independent long-distance carriers, each of which had a different interfacing mechanism. Bell Communications Research answered the challenge by developing *Synchronous Optical Network (SONET)*, a fiber-optic WAN technology that delivers voice, data, and video at speeds starting at 51.84 Mbps. Bell's main goals in creating SONET were to create a standardized access method for all carriers within the newly competitive U.S. market and to unify different standards around the world. SONET is capable of transmission speeds from 51.84 Mbps to 2.488 Gbps and beyond.

One of Bell's biggest accomplishments with SONET was that it created a new system that defined data rates in terms of *Optical Carrier (OCx)* levels. Table 1.7 lists the OCx levels you should be familiar with.

**ExamAlert**

Before taking the exam, review the information provided in Table 1.7. Be sure that you are familiar with OC-3 and OC-192 specific transmission rates.

TABLE 1.7 **OCx Levels and Transmission Rates**

| OCx Level | Transmission Rate |
|---|---|
| OC-1 | 51.84 Mbps |
| OC-3 | 155.52 Mbps |
| OC-12 | 622.08 Mbps |
| OC-24 | 1.244 Gbps |
| OC-48 | 2.488 Gbps |
| OC-96 | 4.976 Gbps |
| OC-192 | 9.953 Gbps |
| OC-768 | 39.813 Gbps |

**Note**

*Optical carrier (OCx)* levels represent the range of digital signals that can be carried on SONET fiber-optic networks. Each OCx level defines the speed at which it operates.

*Synchronous Digital Hierarchy (SDH)* is the European counterpart to SONET.

**ExamAlert**

When you take the exam, equate SDH with SONET.

A *passive optical network (PON)* is one in which unpowered optical splitters are used to split the fiber so it can service a number of locations, and it brings the fiber either to the curb, the building, or the home. It is known as a passive system because there is no power to the components and it consists of an *optical line termination (OLT)* at the split and a number of *optical network units (ONUs)* at the end of each run (typically near the end user). It can be combined with wavelength division multiplexing and is then known as WDM-PON.

A form of multiplexing optical signals is *dense wavelength-division multiplexing (DWDM)*. This method replaces SONET/SDH regenerators with *erbium-doped fiber amplifiers (EDFAs)* and can also amplify the signal and enable it to travel a greater distance. The main components of a DWDM system include the following:

- Terminal multiplexer
- Line repeaters
- Terminal demultiplexer

**Note**

Chapter 5, "Cabling Solutions and Issues," discusses several other methods of multiplexing.

**ExamAlert**

Make sure that you understand that DWDM works with SONET/SDH.

An alternative to DWDM is *coarse wavelength-division multiplexing (CWDM)*. This method is commonly used with television cable networks. The main thing to know about it is that it has relaxed stabilization requirements; thus, you can have vastly different speeds for download than upload.

**ExamAlert**

Make sure that you associate CWDM with television cabling.

# Satellite Internet Access

Many people take DSL and cable Internet access for granted, but these technologies are not offered everywhere. Many rural areas do not have cable Internet access. For areas where cheaper broadband options are unavailable, a limited number of Internet options are available. One of the primary options is Internet via satellite. Recently, SpaceX has launched Starlink Internet satellites with the intent of increasing the number of low-cost global broadband capabilities.

*Satellite* access provides a viable Internet access solution for those who cannot get other methods of broadband. Satellite Internet offers an always-on connection with download speeds considerably faster than an old dial-up connection. Satellite Internet access does have a few drawbacks, though, such as cost and high latency. *Latency* is the time it takes for the signal to travel back and forth from the satellite.

Although satellite Internet is slower and costlier than DSL or cable, it offers some attractive features, the first of which is its portability. Quite literally, wherever you go, you have Internet access with no phone lines or other cables. For businesses with remote users and clients, the benefit is clear. But the technology has a far-reaching impact; it is not uncommon to see *recreational vehicles (RVs)* with a satellite dish on the roof. They have 24/7 unlimited access to the Internet as they travel.

Many companies offer satellite Internet services; a quick Internet search reveals quite a few. These Internet providers offer different Internet packages that vary greatly in terms of price, access speeds, and service. Some target businesses, whereas others aim for the private market.

Two different types of broadband Internet satellite services are deployed: one-way and two-way systems. A *one-way satellite system* requires a satellite card and a satellite dish installed at the end user's site. This system works by sending outgoing requests on one link using a phone line, with inbound traffic returning on the satellite link. A *two-way satellite system*, in contrast, provides data paths for both upstream and downstream data. Like a one-way system, a two-way system uses a satellite card and a satellite dish installed at the end user's site; bidirectional communication occurs directly between the end user's node and the satellite.

Home satellite systems are asymmetric; that is, download speeds are faster than upload speeds. A home satellite system is likely to use a modem for the uplink traffic, with downloads coming over the satellite link. The exact speeds you can expect with satellite Internet depend on many factors. As with other wireless technologies, atmospheric conditions can significantly affect the performance of satellite Internet access. One additional consideration for satellite Internet is increased *propagation time*—how long it takes the signal to travel back and forth from the satellite. In networking terms, this time is long and therefore is an important consideration for business applications.

# Termination Points

To work properly, a network must have termination points. These endpoints stop the signal and prevent it from living beyond its needed existence. For the exam, CompTIA wants you to be familiar with a number of termination-related topics, all of which are discussed in the sections that follow.

## Demarc, Demarc Extension, and Smart Jacks

A network's *demarcation point* is the connection point between the operator's part of the network and the customer's portion of the network. This point is important for network administrators because it distinguishes the portion of the network that the customer is responsible for from the section the owner is responsible for. For example, for those who have high-speed Internet, the boundary between the customer's premises and the ISP typically is mounted on the wall on the side of the home. However, high-speed service providers support everything from the cable modem back to their main distribution center. This is why, if a modem fails, it is replaced by the ISP and not by the customer. This is true for the wiring to that point as well.

Knowing the location of the demarcation point is essential because it marks the point between where the customer (or administrator) is responsible and where the owner is. It also identifies the point at which the customer is responsible should a problem occur, and who should pay for that problem. The ISP is responsible for ensuring that the network is functional up to the demarcation point. The customer/administrator is responsible for ensuring that everything from that point is operational.

The demarcation point is the point at which the ISP places its services in your network. There is not always a choice of where this demarcation is placed. This means that a company might have six floors of offices, and the demarcation point is in the basement—impractical for the network. In this case you need a demarcation extension, which extends the demarcation point to a more functional location. This solution might sound simple, but it involves knowledge of cabling distances and other infrastructure needs. The demarcation extension might be the responsibility of the administrator, or for a fee, owners might provide extension services.

As you might imagine, you need some form of hardware at the demarcation point. This is the *smart jack*, also known as the *network interface device (NID)*. The smart jack performs several primary functions:

- **Loopback feature:** The loopback feature is built in to the smart jack. Like the Ethernet loopback cable, it is used for testing purposes. In this case, the loopback feature enables remote testing so that technicians do not always need to be called to visit the local network to isolate problems.
- **Signal amplification:** The smart jack can amplify signals. This feature is similar to that of the function of repeaters in an Ethernet network.
- **Surge protection:** Lightning and other environmental conditions can cause electrical surges that can quickly damage equipment. Many smart jacks include protection from environmental situations.
- **Remote alarms:** Smart jacks typically include an alarm that enables the owner to identify if something goes wrong with the smart jack and therefore the connections at the demarcation point.

ExamAlert

*Demarcation point* is the telephone company or ISP term for where their facilities or wires end and where yours begin.

## CSUs/DSUs

A *channel service unit/data service unit (CSU/DSU)* acts as a translator between the LAN data format and the WAN data format. Such a conversion is necessary because the technologies used on WAN links are different from those used on LANs. Some consider a CSU/DSU a type of digital modem. But unlike a normal modem, which changes the signal from digital to analog, a CSU/DSU changes the signal from one digital format to another.

A CSU/DSU has physical connections for the LAN equipment, normally via a serial interface, and another connection for a WAN.

**ExamAlert**

Traditionally, the CSU/DSU has been in a box separate from other networking equipment. However, the increasing use of WAN links means that some router manufacturers are now including CSU/DSU functionality in routers or are providing the expansion capability to do so.

## Verify Wiring Installation and Termination

After a segment of network cable has been placed where it needs to go, whether run through the plenum or connecting a patch cable, the final task is wiring termination. Termination is the process to connect the network cable to the wall jack, plug, or patch panel. Termination generally is a straightforward process. You can quickly see if the wiring and termination worked if the LED on the connected network card is lit. Also, if you connect a client system, you can ping other devices on the network if all works.

**Note**

Cabling topics, such as patch cables and plenums, are discussed in Chapter 5, "Cabling Solutions and Issues."

# Virtual Networking

Cloud computing is built on virtualization; it is the foundation on which cloud computing stands. At the core of virtualization is the *hypervisor* (the software/hardware combination that makes it possible to manage multiple virtual machines existing on one host). There are two methods of implementation: Type I (known as *bare metal*) and Type II (known as *hosted*). Type I is independent of the operating system and boots before the OS, whereas Type II is dependent on the operating system and cannot boot until the OS is up; it needs

the OS to stay up so that it can operate. From a performance and scalability standpoint, Type I is considered superior to Type II.

**ExamAlert**

Know that the hypervisor is used to manage multiple virtual machines (VMs) existing on one host.

**Tip**

The machine on which virtualization software is running is known as a *host*, and the virtual machines are known as *guests*.

*Network function virtualization (NFV)* is a method of virtualizing network services instead of running them on proprietary hardware: think routers, firewalls, and load balancers. These virtual services allow service providers to run their network on standard servers instead of proprietary ones—improving scalability, agility, and on-demand services without needing additional hardware resources.

**Note**

Whereas once it was the case that hypervisors were the only way to have virtualization, now most people think of containers as their successor. You should know that the use of containers (a piece of software bundled with everything that it needs to run—code, runtime, system tools, system libraries, and so on) are becoming more common.

Cloud computing holds great promise when it comes to scalability, cost saving, rapid deployment, and empowerment. As with any technology where so much is removed from your control, however, risks are involved. Each risk should be considered and thought through to identify ways to help mitigate them. Data segregation, for example, can help reduce some of the risks associated with multitenancy. Common virtual network components include *virtual network interface cards (vNICs)*, virtual routers and switches, shared memory, virtual CPUs, and storage (shared or clustered).

A NIC card within a machine can be either virtual or physical and will be configured the same. Existing on the virtual network, it must have an IP address, a MAC address, a default gateway, a subnet mask value, and can have a connection that is bridged or not. A vNIC is software only but allows interaction with other devices on the network. (The VLAN makes it possible for vNICs to communicate with other network devices.)

**ExamAlert**

For the exam, you should be able to differentiate between the various virtualization concepts: hypervisor, network function virtualization (NFV), vNIC, and vSwitch.

In a discussion of virtual networking, it is important to note that so much of what is discussed is software based. Never forget that the goal of virtualization is to emulate physical environments and devices without actually having those physical elements.

Just as physical routers establish communication by maintaining tables about destinations and local connections, a *virtual router* works similarly but is software only. Remember that a router contains information about the systems connected to it and where to send requests if the destination is not known. These routing tables grow as connections are made through the router. Routing can occur within the network (interior) or outside it (exterior). The routes themselves can be configured as static or dynamic.

A *virtual switch (vSwitch)*, similarly, is a software program that allows one virtual machine (VM) to communicate with another. The virtual switch allows the VM to use the hardware of the host OS (the NIC) to connect to the Internet and can be configured through an interface similar to the one shown in Figure 1.11.

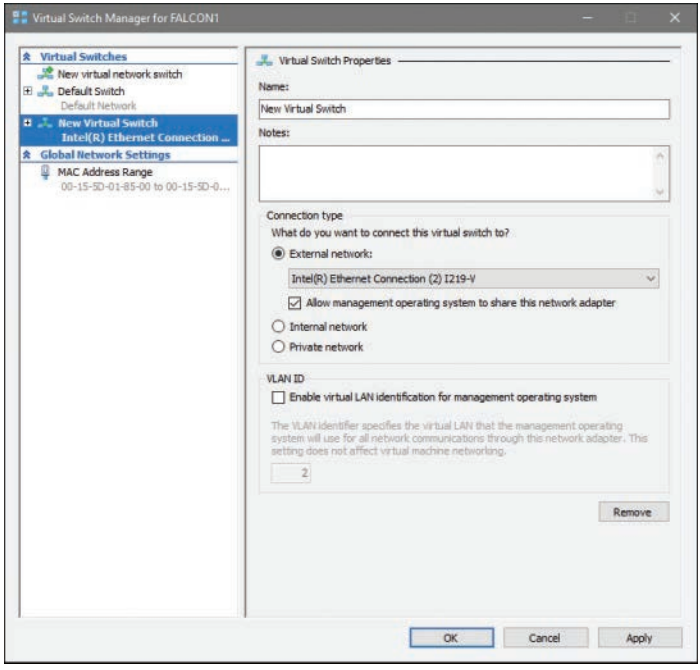



FIGURE 1.11 **Virtual switch configuration**

Switches are multiport devices that improve network efficiency. A switch typically contains a small amount of information about systems in a network—a table of MAC addresses as opposed to IP addresses. Switches improve network efficiency over routers because of the virtual circuit capability. Switches also improve network security because the virtual circuits are more difficult to examine with network monitors. The switch maintains limited routing information about nodes in the internal network, and it enables connections to systems such as a hub or a router.

## Cram Quiz

1. Which of the following technologies require dial-up access? (Choose the best answer.)
   - ❍ **A.** Fiber
   - ❍ **B.** ISDN
   - ❍ **C.** Packet switching
   - ❍ **D.** DMVPN

2. Which of the following is an advantage of ISDN over a public switched telephone network?
   - ❍ **A.** ISDN is more reliable.
   - ❍ **B.** ISDN is cheaper.
   - ❍ **C.** ISDN is faster.
   - ❍ **D.** ISDN uses 53 Kbps fixed-length packets.

3. Which of the following is the time lapse between sending or requesting information and the time it takes to return?
   - ❍ **A.** Echo
   - ❍ **B.** Attenuation
   - ❍ **C.** Bandwidth
   - ❍ **D.** Latency

4. What is the speed usually offered with dial-up service?
   - ❍ **A.** 1 Gbps
   - ❍ **B.** 256 Kbps
   - ❍ **C.** 144 Kbps
   - ❍ **D.** 56 Kbps

5. What device acts as a translator between the LAN data format and the WAN data format?
   - ❍ **A.** SIP Trunk
   - ❍ **B.** PRI
   - ❍ **C.** MPLS
   - ❍ **D.** CSU/DSU

6. Which virtual technology enables service providers to run their network on standard servers instead of proprietary ones?
   - ❍ **A.** vNIC
   - ❍ **B.** vSwitch
   - ❍ **C.** NFV
   - ❍ **D.** Hypervisor

7. Which implementation of DSL is the most common?
   - ❍ **A.** VDSL
   - ❍ **B.** ADSL
   - ❍ **C.** IDSL
   - ❍ **D.** SDSL

8. Which of the following are optical networks used to serve metropolitan areas in which there is a large, concentrated population?
   - ❍ **A.** MONs
   - ❍ **B.** PSTNs
   - ❍ **C.** ISDNs
   - ❍ **D.** NFVs

# Cram Quiz Answers

1. **B.** ISDN requires a dial-up connection to establish communication sessions.
2. **C.** One clear advantage that ISDN has over the PSTN is its speed. ISDN can combine 64 Kbps channels for faster transmission speeds than the PSTN can provide. ISDN is no more or less reliable than the PSTN. ISDN is more expensive than the PSTN.
3. **D.** Latency refers to the time lapse between sending or requesting information and the time it takes to return.
4. **D.** Almost without exception, ISPs offer 56 Kbps access, the maximum possible under current dial-up standards.

5. **D.** A channel service unit/data service unit (CSU/DSU) acts as a translator between the LAN data format and the WAN data format. Such a conversion is necessary because the technologies used on WAN links are different from those used on LANs.
6. **C.** Network function virtualization (NFV) allows providers to run their network on standard servers instead of proprietary ones—improving scalability, agility, and on-demand services without needing additional hardware resources. A virtual network interface card (vNIC) is the software emulation of a physical NIC card. It allows interaction with other devices on network. A virtual switch (vSwitch), similarly, is a software program that allows one virtual machine (VM) to communicate with another. A hypervisor is used to manage multiple virtual machines existing on one host.
7. **B.** The most common implementation of DSL is ADSL (asymmetric), which provides a high data rate in only one direction. While the other variants of DSL are available, they are not as popular as ADSL. All variants of DSL are decreasing in popularity in recent years as more are turning to cable and fiber solutions for high-speed Internet and network access.
8. **A.** Metro-optical networks (also known as MONs) are optical networks that can span up to several hundred kilometers and are used to serve metropolitan areas in which there is a large, concentrated population.

# What's Next?

This chapter created a foundation upon which Chapter 2, "Models, Ports, Protocols, and Network Services," builds. It examines the Open Systems Interconnection (OSI) reference model—a conceptual model describing how network architecture allows data to be passed between computer systems. It also examines how common network devices relate to the model.

*This page intentionally left blank*

CHAPTER 2

# Models, Ports, Protocols, and Network Services

**This chapter covers the following official Network+ objectives:**

- Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
- Explain common ports and protocols, their application, and encrypted alternatives.
- Explain the use and purpose of network services.

This chapter covers CompTIA Network+ objectives 1.1, 1.5, and 1.6. For more information on the official Network+ exam topics, see the "About the Network+ Exam" section in the Introduction.

One of the most important networking concepts to understand is the *Open Systems Interconnection (OSI)* reference model. This conceptual model, created by the *International Organization for Standardization (ISO)* in 1978 and revised in 1984, describes a network architecture that enables data to be passed between computer systems.

This chapter looks at the OSI and describes how it relates to real-world networking. It also examines how common network devices relate to the OSI model. Even though the OSI model is conceptual, an appreciation of its purpose and function can help you better understand how protocol suites and network architectures work in practical applications.

**Note**

The TCP/IP model, which performs the same functions as the OSI model, except in four layers instead of seven, is no longer a Network+ objective. Because this is the protocol suite predominantly in use today, it is still important to know it to understand the underlying principles of networking, and we refer to it where it is appropriate to do so.

# The OSI Networking Model

▶ **Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. Which layer of the OSI model converts data from the application layer into a format that can be sent over the network?
2. True or false: Transport protocols, such as UDP, map to the transport layer of the OSI model and are responsible for transporting data across the network.
3. At what layer of the OSI model do HTTP and SSH map?

### Answers

1. The presentation layer converts data from the application layer into a format that can be sent over the network. It also converts data from the session layer into a format the application layer can understand.
2. True. Transport protocols map to the transport layer of the OSI model and are responsible for transporting data across the network. UDP is a transport protocol.
3. HTTP and SSH (along with many other protocols) map to the application layer of the OSI model.

For networking, two models commonly are referenced: the OSI model and the TCP/IP model. Both offer a framework, theoretical and actual, for how networking is implemented. Objective 1.1 of the Network+ exam focuses only on the OSI model. A thorough discussion of it follows with a brief discussion of the TCP/IP model tossed in for further understanding.

# The OSI Seven-Layer Model

As shown in Figure 2.1, the OSI reference model is built, bottom to top, in the following order: physical, data link, network, transport, session, presentation, and application. The physical layer is classified as Layer 1, and the top layer of the model, the application layer, is Layer 7.

**ExamAlert**

The OSI model can be used as a bottom-to-top troubleshooting tool. For example, troubleshooting a network interface card (NIC) or network wiring would begin at layer 1, the physical layer where electrical functions support physical connections. If the problem is not found there, then the next step would be run a loopback test on the NIC (moving up to layer 2), and so on.


FIGURE 2.1 **The OSI seven-layer model**

**ExamAlert**

On the Network+ exam, you might see an OSI layer referenced either by its name, such as network layer, or by its layer number. For instance, you might find that a router is referred to as a Layer 3 device. An easy mnemonic that you can use to remember the layers from top to bottom is: All People Seem To Need Data Processing.

Each layer of the OSI model has a specific function. The following sections describe the function of each layer, starting with the physical layer and working up the model.

## Physical Layer (Layer 1)

The physical layer of the OSI model identifies the network's physical characteristics, including the following specifications:

- **Hardware:** The type of media used on the network, such as type of cable, type of connector, and pinout format for cables.

- **Topology:** The physical layer identifies the topology to be used in the network. Common topologies include ring, mesh, star, bus, and hybrid.

Protocols and technologies such as USB, Ethernet, DSL, ISDN, T-carrier links (T1 and T3), GSM, and SONET operate at the physical layer.

In addition to these characteristics, the physical layer defines the voltage used on a given medium and the frequency at which the signals that carry the data operate. These characteristics dictate the speed and bandwidth of a given medium, as well as the maximum distance over which a certain media type can be used.

## Data Link Layer (Layer 2)

The data link layer is responsible for getting data to the physical layer so that it can transmit over the network. The data link layer is also responsible for error detection, error correction, and hardware addressing. The term *frame* describes the logical grouping of data at the data link layer.

The data link layer has two distinct sublayers:

- **Media Access Control (MAC) layer:** The MAC address is defined at this layer. The MAC address is the physical or hardware address burned into each NIC. The MAC sublayer also controls access to network media. The MAC layer specification is included in the IEEE 802.1 standard.
- **Logical Link Control (LLC) layer:** The LLC layer is responsible for the error and flow-control mechanisms of the data link layer. The LLC layer is specified in the IEEE 802.2 standard.

Protocols and technologies such as *High-Level Data Link Control (HDLC)*, *Layer 2 Tunneling Protocol (L2TP)*, *Point-to-Point Protocol (PPP)*, *Point-to-Point Tunneling Protocol (PPTP)*, *Spanning Tree Protocol (STP)*, and *virtual LANs (VLANs)* operate at the data link layer.

## Network Layer (Layer 3)

The primary responsibility of the network layer is *routing*—providing mechanisms by which data can be passed from one network system to another. The network layer does not specify how the data is passed but rather provides the mechanisms to do so. Functionality at the network layer is provided through routing protocols, which are software components.

Protocols at the network layer are also responsible for *route selection*, which refers to determining the best path for the data to take throughout the network. In contrast to the data link layer, which uses MAC addresses to communicate on the LAN, network layer protocols use software-configured addresses and special routing protocols to communicate on the network. The term *packet* describes the logical grouping of data at the network layer.

When you're working with networks, routes can be configured in two ways: *statically* or *dynamically*. In a static routing environment, routes are manually added to the routing tables. In a dynamic routing environment, routing protocols such as *Routing Information Protocol (RIP)* and *Open Shortest Path First (OSPF)* are used. These protocols communicate routing information between networked devices on the network. Other important network layer protocols include *Internet Protocol (IP)*, *Address Resolution Protocol (ARP)*, *Reverse Address Resolution Protocol (RARP)*, *Asynchronous Transfer Mode (ATM)*, *Intermediate System-to-Intermediate System (IS-IS)*, *IP Security (IPSec)*, *Internet Control Message Protocol (ICMP)*, and *Multiprotocol Label Switching (MPLS)*.

## Transport Layer (Layer 4)

The basic function of the transport layer is to provide mechanisms to transport data between network devices. Primarily, it does this in three ways:

- **Error checking:** Protocols at the transport layer ensure that data is correctly sent or received.
- **Service addressing:** A number of protocols support many network services. The transport layer ensures that data is passed to the right service at the upper layers of the OSI model.
- **Segmentation:** To traverse the network, blocks of data need to be broken into packets of a manageable size for the lower layers to handle. This process, called *segmentation*, is the responsibility of the transport layer.

Protocols that operate at the transport layer can either be connectionless, such as *User Datagram Protocol (UDP)*, or connection oriented, such as *Transmission Control Protocol (TCP)*.

The transport layer is also responsible for *data flow control*, which refers to how the receiving device can accept data transmissions. Two common methods of flow control are used:

- **Buffering:** When buffering flow control is used, data is temporarily stored and waits for the destination device to become available.

Buffering can cause a problem if the sending device transmits data much faster than the receiving device can manage.

- **Windowing:** In a windowing environment, data is sent in groups of segments that require only one acknowledgment. The size of the window (that is, how many segments fit into one acknowledgment) is defined when the session between the two devices is established. As you can imagine, the need to have only one acknowledgment for every five segments, for instance, can greatly reduce overhead.

## Session Layer (Layer 5)

The session layer is responsible for managing and controlling the synchronization of data between applications on two devices. It does this by establishing, maintaining, and breaking sessions. Whereas the transport layer is responsible for setting up and maintaining the connection between the two nodes, the session layer performs the same function on behalf of the application. Protocols that operate at the session layer include NetBIOS, *Network File System (NFS)*, and *Server Message Block (SMB)*.

## Presentation Layer (Layer 6)

The presentation layer's basic function is to convert the data intended for or received from the application layer into another format. Such conversion is necessary because of how data is formatted so that it can be transported across the network. Applications cannot necessarily read this conversion. Some common data formats handled by the presentation layer include the following:

- **Graphics files:** JPEG, TIFF, GIF, and so on are graphics file formats that require the data to be formatted in a certain way.
- **Text and data:** The presentation layer can translate data into different formats, such as *American Standard Code for Information Interchange (ASCII)* and *Extended Binary Coded Decimal Interchange Code (EBCDIC)*.
- **Sound/video:** MPEG, MP3, and MIDI files all have their own data formats to and from which data must be converted.

Another important function of the presentation layer is *encryption*, which is the scrambling of data so that it can't be read by anyone other than the intended recipient. Given the basic role of the presentation layer—that of data-format translator—it is the obvious place for encryption and decryption to take place. For example, the cryptographic protocol *Transport Layer Security (TLS)* operates at the presentation layer.

## Application Layer (Layer 7)

In simple terms, the function of the application layer is to take requests and data from the users and pass them to the lower layers of the OSI model. Incoming information is passed to the application layer, which then displays the information to the users. Some of the most basic application layer services include file and print capabilities.

The most common misconception about the application layer is that it represents applications used on a system, such as a web browser, word processor, or spreadsheet. Instead, the application layer defines the processes that enable applications to use network services. For example, if an application needs to open a file from a network drive, the functionality is provided by components that reside at the application layer. Protocols defined at the application layer include *Secure Shell (SSH)*, *Border Gateway Protocol (BGP)*, *Dynamic Host Configuration Protocol (DHCP)*, *Domain Name System (DNS)*, *Network Time Protocol (NTP)*, *Real-time Transport Protocol (RTP)*, *Session Initiation Protocol (SIP)*, *Simple Mail Transfer Protocol (SMTP)*, *Server Message Block (SMB)*, *File Transfer Protocol (FTP)*, *Hypertext Transfer Protocol (HTTP)*, *Hypertext Transfer Protocol Secure (HTTPS)*, *Internet Message Access Protocol (IMAP)*, and *Post Office Protocol version 3 (POP3)*.

**ExamAlert**

Be sure you understand the OSI model and its purpose. You will almost certainly be asked questions on it during the exam.

## OSI Model Summary

Table 2.1 summarizes the seven layers of the OSI model and describes some of the most significant points of each layer.

TABLE 2.1 **OSI Model Summary**

| OSI Layer | Major Function |
|---|---|
| Physical (Layer 1) | Defines the physical structure of the network and the topology. |
| Data link (Layer 2) | Provides error detection and correction. Uses two distinct sublayers: the Media Access Control (MAC) and Logical Link Control (LLC) layers. Identifies the method by which media are accessed. Defines hardware addressing through the MAC sublayer. |
| Network (Layer 3) | Handles the discovery of destination systems and addressing. Provides the mechanism by which data can be passed and routed from one network system to another. |

| OSI Layer | Major Function |
|---|---|
| Transport (Layer 4) | Provides connection services between the sending and receiving devices and ensures reliable data delivery. Manages flow control through buffering or windowing. Provides segmentation, error checking, and service identification. |
| Session (Layer 5) | Synchronizes the data exchange between applications on separate devices. |
| Presentation (Layer 6) | Translates data from the format used by applications into one that can be transmitted across the network. Handles encryption and decryption of data. Provides compression and decompression functionality. Formats data from the application layer into a format that can be sent over the network. |
| Application (Layer 7) | Provides access to the network for applications. |

# Comparing OSI to the Four-Layer TCP/IP Model

The OSI model does a fantastic job outlining how networking should occur and the responsibility of each layer. However, TCP/IP also has a reference model and has to perform the same functionality with only four layers. Figure 2.2 shows how these four layers line up with the seven layers of the OSI model.

| TCP/IP Model | OSI Model |
|---|---|
| Application Layer | Application Layer<br>Presentation Layer<br>Session Layer |
| Transport Layer | Transport Layer |
| Internet Layer | Network Layer |
| Network Interface Layer | Data Link Layer<br>Physical Layer |

FIGURE 2.2 **The TCP/IP model compared to the OSI model**

The network interface layer in the TCP/IP model is sometimes referred to as the network access or link layer, and this is where Ethernet, FDDI, or any other physical technology can run. The Internet layer is where IP runs (along with ICMP and others). The transport layer is where TCP and its counterpart UDP operate. The application layer enables any number of protocols to be plugged in, such as HTTP, SMTP, *Simple Network Management Protocol (SNMP)*, DNS, and many others.

# Identifying the OSI Layers at Which Various Network Components Operate

When you understand the OSI model, you can relate network connectivity devices to the appropriate layer of the OSI model. Knowing at which OSI layer a device operates enables you to better understand how it functions on the network. Table 2.2 identifies various network devices and maps them to the OSI model.

**ExamAlert**

For the Network+ exam, you are expected to identify at which layer of the OSI model certain network devices operate.

TABLE 2.2 **Mapping Network Devices to the OSI Model**

| Device | OSI Layer |
|---|---|
| Hub | Physical (Layer 1) |
| Wireless bridge | Data link (Layer 2) |
| Switch | Data link (Layer 2) or network (Layer 3) |
| Router | Network (Layer 3) |
| NIC | Data link (Layer 2) |
| Access point (AP) | Data link (Layer 2) |

# Data Encapsulation/Decapsulation and OSI

As data moves down the model (and through the devices on that host), it is encapsulated with a header added to the beginning and a trailer to the end. Once the data arrives at the receiving host, it moves up the model (and through the devices) and is decapsulated in that the header and trailer are stripped off as it moves up.

**Note**

There are a great many topics beneath exam objective 1.1. In the interest of our discussion building in a logical way, the focus here is still on the networking model in order to complete the discussion of it. Later in this chapter, we visit headers again and some of the other topics the objectives include but that do not fit well with the dialogue yet.

**ExamAlert**

Adding protocol information to data as it passes through layers is known as encapsulation. Removing protocol information to data as it passes through layers is known as decapsulation.

In the encapsulation/decapsulation process, each layer on the receiving host does the opposite of what was done at that layer on the sending host: the receiving host's network layer, for example, strips off what was added by the network layer on the sending host. Table 2.3 shows what encapsulation/decapsulation occurs at each of the layers of the OSI model.

TABLE 2.3 **OSI Model Encapsulation/Decapsulation**

| OSI Layer | Encapsulation/ Decapsulation Function | Representation |
|---|---|---|
| Application (Layer 7)<br>Presentation (Layer 6)<br>Session (Layer 5) | The data is created in the application(s) and passed to/from the Transport layer. | DATA |
| Transport (Layer 4) | A segment header is added to, or removed from, the data. | SEGMENT HEADER \| DATA |
| Network (Layer 3) | A packet header is added to, or removed from, the data. | PACKET HEADER \| SEGMENT HEADER \| DATA |
| Data link (Layer 2) | A frame header is added to, or removed from, the data.<br>A frame trailer is added to, or removed from, the data. | FRAME HEADER \| PACKET HEADER \| SEGMENT HEADER \| DATA \| FRAME TRAILER |

It should be noted that the Physical layer (Layer 1) does not appear in Table 2.3 because it does not add or remove anything, but sends what it has (on the sending host) and receives what comes to it (on the receiving host).

It should also be noted that the unit of data worked with at each layer of the model (such as a frame at layer 2 or a packet at layer 3) is called a *protocol data unit (PDU)*.

# Cram Quiz

**1.** At which OSI layer does an AP operate?

- ❍ **A.** Network
- ❍ **B.** Physical
- ❍ **C.** Data link
- ❍ **D.** Session

**2.** Which of the following are sublayers of the data link layer? (Choose two.)

- ❍ **A.** MAC
- ❍ **B.** LCL
- ❍ **C.** Session
- ❍ **D.** LLC

**3.** At which OSI layers can a switch operate? (Choose two.)

- ❍ **A.** Layer 1
- ❍ **B.** Layer 2
- ❍ **C.** Layer 3
- ❍ **D.** Layer 4

**4.** Which of the following OSI layers is responsible for establishing connections between two devices?

- ❍ **A.** Network
- ❍ **B.** Transport
- ❍ **C.** Session
- ❍ **D.** Data link

**5.** What happens to data as it moves from the upper to the lower layers of the OSI model on a host system?

- ❍ **A.** The header and trailer are stripped off through decapsulation.
- ❍ **B.** The data is sent in groups of segments that require two acknowledgments.
- ❍ **C.** The data moves from the physical layer to application layer.
- ❍ **D.** It is encapsulated with a header at the beginning and a trailer at the end.

# Cram Quiz Answers

1. **C.** A wireless access point (AP) operates at the data link layer of the OSI model. An example of a network layer device is a router. An example of a physical layer device is a hub. Session layer components normally are software, not hardware.
2. **A and D.** The data link layer is broken into two distinct sublayers: Media Access Control (MAC) and Logical Link Control (LLC). LCL is not a valid term. Session is another of the OSI model layers.
3. **B and C.** A switch uses the MAC addresses of connected devices to make its forwarding decisions. Therefore, it is called a data link, or Layer 2, network device. It can also operate at Layer 3 or be a multilayer switch. Devices or components that operate at Layer 1 typically are media based, such as cables or connectors. Layer 4 components typically are software based, not hardware based.
4. **B.** The transport layer is responsible for establishing a connection between networked devices. The network layer is most commonly associated with route discovery and datagram delivery. Protocols at the session layer synchronize the data exchange between applications on separate devices. Protocols at the data link layer perform error detection and handling for the transmitted signals and define the method by which the medium is accessed.
5. **D.** As data moves down the model (and through the devices on that host), it is encapsulated with a header added to the beginning and a trailer to the end. Once the data arrives at the receiving host, it moves up the model (and through the devices) and is decapsulated in that the header and trailer are stripped off as it moves up. In a windowing environment, data is sent in groups of segments that require only one acknowledgment. On the sending host system, data moves from the application layer down to the physical layer. On the receiving system, data moves from the physical layer upwards to the application layer.

# Ports and Protocols

- **Explain common ports and protocols, their application, and encrypted alternatives.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. With TCP, a data session is established through a three-step process. This is known as a three-way _____.
2. What FTP command uploads multiple files to the remote host?
3. The SSH protocol is a more secure alternative to what protocol?
4. What ports do the HTTPS, RDP, and DHCP protocols use?

### Answers

1. This is known as a three-way handshake.
2. The **mput** command uploads multiple files to the remote host in FTP.
3. SSH is a more secure alternative to Telnet.
4. HTTPS uses port 443, RDP uses port 3389, and DHCP uses ports 67 and 68.

When computers were restricted to standalone systems, there was little need for mechanisms to communicate between them. However, it wasn't long before the need to connect computers for the purpose of sharing files and printers became a necessity. Establishing communication between network devices required more than a length of cabling; a method or a set of rules was needed to establish how systems would communicate. Protocols provide that method.

It would be nice if a single protocol facilitated communication between all devices, but this is not the case. You can use a number of protocols on a network, each of which has its own features, advantages, and disadvantages. What protocol you choose can have a significant impact on the network's functioning and performance. This section explores some of the more common protocols you can expect to work with as a network administrator.

# Connection-Oriented Protocols Versus Connectionless Protocols

Before getting into the characteristics of the various network protocols and protocol suites, you must first identify the difference between connection-oriented and connectionless protocols.

In a *connection-oriented* communication, data delivery is guaranteed. The sending device resends any packet that the destination system does not receive. Communication between the sending and receiving devices continues until the transmission has been verified. Because of this, connection-oriented protocols have a higher overhead and place greater demands on bandwidth.

**ExamAlert**

Connection-oriented protocols such as TCP can accommodate lost or dropped packets by asking the sending device to retransmit them. They can do this because they wait for all the packets in a message to be received before considering the transmission complete. On the sending end, connection-oriented protocols also assume that a lack of acknowledgment is sufficient reason to retransmit.

In contrast to connection-oriented communication, *connectionless* protocols such as User Datagram Protocol (UDP) offer only a best-effort delivery mechanism. Basically, the information is just sent; there is no confirmation that the data has been received. If an error occurs in the transmission, there is no mechanism to resend the data, so transmissions made with connectionless protocols are not guaranteed. Connectionless communication requires far less overhead than connection-oriented communication, so it is popular in applications such as streaming audio and video, where a small number of dropped packets might not represent a significant problem.

**ExamAlert**

As you work through the various protocols, keep an eye out for those that are connectionless and those that are connection oriented. Also, look for protocols such as TCP that guarantee delivery of data and those such as UDP that are a fire-and-forget or best-delivery method.

# Internet Protocol

Internet Protocol (IP), which is defined in RFC 791, is the protocol used to transport data from one node on a network to another. IP is connectionless,

which means that it doesn't guarantee the delivery of data; it simply makes its best effort to do so. To ensure that transmissions sent via IP are completed, a higher-level protocol such as TCP is required.

**Note**

In this chapter and throughout the book, the term *Request For Comments (RFC)* is used. RFCs are standards published by the *Internet Engineering Task Force (IETF)* and describe methods, behaviors, research, or innovations applicable to the operation of the Internet and Internet-connected systems. Each new RFC has an associated reference number. Looking up this number gives you information on the specific technology. For more information on RFCs, look for the Internet Engineering Task Force online.

**ExamAlert**

IP operates at the network layer of the OSI model.

In addition to providing best-effort delivery, IP also performs fragmentation and reassembly tasks for network transmissions. Fragmentation is necessary because the *maximum transmission unit (MTU)* size is limited in IP. In other words, network transmissions that are too big to traverse the network in a single packet must be broken into smaller chunks and reassembled at the other end. Another function of IP is addressing. IP addressing is a complex subject. Refer to Chapter 3, "Addressing, Routing, and Switching," for a complete discussion of IP addressing.

# Transmission Control Protocol

*Transmission Control Protocol (TCP)*, which is defined in RFC 793, is a connection-oriented transport layer protocol. Being connection-oriented means that TCP establishes a mutually acknowledged session between two hosts before communication takes place. TCP provides reliability to IP communications. Specifically, TCP adds features such as flow control, sequencing, and error detection and correction. For this reason, higher-level applications that need guaranteed delivery use TCP rather than its lightweight and connectionless brother, UDP.

## How TCP Works

When TCP wants to open a connection with another host, it follows this procedure:

1. It sends a message called a SYN to the target host.
2. The target host opens a connection for the request and sends back an acknowledgment message called an ACK (or SYN ACK).
3. The host that originated the request sends back another acknowledgment, saying that it has received the ACK message and that the session is ready to be used to transfer data.

When the data session is completed, a similar process is used to close the session. This three-step session establishment and acknowledgment process is called the *TCP three-way handshake*.

**ExamAlert**

TCP operates at the transport layer of the OSI model.

TCP is a reliable protocol because it has mechanisms that can accommodate and handle errors. These mechanisms include timeouts, which cause the sending host to automatically retransmit data if its receipt is not acknowledged within a given time period.

# User Datagram Protocol

*User Datagram Protocol (UDP)*, which is defined in RFC 768, is the brother of TCP. Like TCP, UDP is a transport protocol, but the big difference is that UDP does not guarantee delivery like TCP does. In a sense, UDP is a "fire-and-forget" protocol; it assumes that the data sent will reach its destination intact. The checking of whether data is delivered is left to upper-layer protocols. UDP operates at the transport layer of the OSI model.

Unlike TCP, with UDP no session is established between the sending and receiving hosts, which is why UDP is called a connectionless protocol. The upshot of this is that UDP has much lower overhead than TCP. A TCP packet header has 14 fields, whereas a UDP packet header has only 4 fields. Therefore, UDP is much more efficient than TCP. In applications that don't need the added features of TCP, UDP is much more economical in terms of bandwidth and processing effort.

ExamAlert

Remember that TCP is a connection-oriented protocol and UDP is a connectionless protocol.

# Internet Control Message Protocol

*Internet Control Message Protocol (ICMP)*, which is defined in RFC 792, is a protocol that works with the IP layer to provide error checking and reporting functionality. In effect, ICMP is a tool that IP uses in its quest to provide best-effort delivery.

ICMP can be used for a number of functions. Its most common function is probably the widely used and incredibly useful ping utility, which can send a stream of ICMP echo requests to a remote host. If the host can respond, it does so by sending echo reply messages back to the sending host. In that one simple process, ICMP enables the verification of the protocol suite configuration of both the sending and receiving nodes and any intermediate networking devices.

However, ICMP's functionality is not limited to the use of the ping utility. ICMP also can return error messages such as "Destination unreachable" and "Time exceeded." (The former message is reported when a destination cannot be contacted and the latter when the *time to live [TTL]* of a datagram has been exceeded.)

In addition to these and other functions, ICMP performs source quench. In a source quench scenario, the receiving host cannot handle the influx of data at the same rate as the data is sent. To slow down the sending host, the receiving host sends ICMP source quench messages, telling the sender to slow down. This action prevents packets from dropping and having to be re-sent.

ICMP is a useful protocol. Although ICMP operates largely in the background, the ping utility makes it one of the most valuable of the protocols discussed in this chapter.

# IPSec

The *IP Security (IPSec)* protocol is designed to provide secure communications between systems. This includes system-to-system communication in the same network, as well as communication to systems on external networks. IPSec is an IP layer security protocol that can both encrypt and authenticate network transmissions. In a nutshell, IPSec is composed of two separate protocols: *Authentication Header (AH)* and *Encapsulating Security Payload (ESP)*. AH provides the authentication and integrity checking for data packets, and ESP provides encryption services.

**ExamAlert**

IPSec relies on two underlying protocols: AH and ESP. AH provides authentication services, and ESP provides encryption services.

Using both AH and ESP, data traveling between systems can be secured, ensuring that transmissions cannot be viewed, accessed, or modified by those who should not have access to them. It might seem that protection on an internal network is less necessary than on an external network; however, much of the data you send across networks has little or no protection, allowing unwanted eyes to see it.

**Note**

The Internet Engineering Task Force (IETF) created IPSec, which you can use on both IPv4 and IPv6 networks.

IPSec provides three key security services:

- **Data verification:** Verifies that the data received is from the intended source
- **Protection from data tampering:** Ensures that the data has not been tampered with or changed between the sending and receiving devices
- **Private transactions:** Ensures that the data sent between the sending and receiving devices is unreadable by any other devices

IPSec operates at the network layer of the Open Systems Interconnection (OSI) reference model and provides security for protocols that operate at the higher layers. Thus, by using IPSec, you can secure practically all TCP/IP-related communications.

# Generic Routing Encapsulation

*Generic Routing Encapsulation (GRE)* is a Cisco-created tunneling protocol. It is an encapsulating protocol used to wrap data and securely send it across VPNs and Point-to-Point (or point-to-multipoint) links.

# File Transfer Protocol

As its name suggests, *File Transfer Protocol (FTP)* provides for the uploading and downloading of files from a remote host running FTP server software.

As well as uploading and downloading files, FTP enables you to view the contents of folders on an FTP server and rename and delete files and directories if you have the necessary permissions. FTP, which is defined in RFC 959, uses TCP as a transport protocol to guarantee delivery of packets.

FTP has weak security mechanisms used to authenticate users. However, rather than create a user account for every user, you can configure FTP server software to accept anonymous logons. When you do this, the username is anonymous, and the password normally is the user's email address. Most FTP servers that offer files to the general public operate in this way. Even when logins are used, FTP is still considered insecure in today's environment. SFTP/SSH should be used in its place in almost every scenario.

In addition to being popular as a mechanism for distributing files to the general public over networks such as the Internet, FTP can also be used by organizations that need to frequently exchange large files with other people or organizations. Such a system can be used when the files being exchanged are larger than can be easily accommodated using email. A number of apps/programs are available that simplify the process. For example, FileZilla is a cross-platform graphical FTP, SFTP, and FTPS file management tool for Windows, Linux, macOS, and more (more information on FileZilla can be found at https://sourceforge.net/projects/filezilla/).

**ExamAlert**

Remember that FTP is an application layer protocol. FTP uses ports 20 and 21 and sends information unencrypted, making it unsecure.

All the common network operating systems offer FTP server capabilities; however, whether you use them depends on whether you need FTP services. All popular workstation operating systems offer FTP client functionality, although it is common to use third-party utilities such as FileZilla (mentioned earlier), CuteFTP, or SmartFTP instead. By default, FTP operates on ports 20 and 21.

FTP assumes that files uploaded or downloaded are straight text (that is, ASCII) files. If the files are not text, which is likely, the transfer mode must be changed to binary. With sophisticated FTP clients, such as CuteFTP, the transition between transfer modes is automatic. With more basic utilities, you must manually perform the mode switch.

Unlike some of the other protocols discussed in this chapter that perform tasks transparent to the user, FTP is an application layer service frequently called upon.

Therefore, it can be useful to know some of the commands supported by FTP. If you use a client such as CuteFTP, you might never need to use these commands, but they are useful to know in case you use a command-line FTP client. Table 2.4 lists some of the most commonly used FTP commands.

**ExamAlert**

You might be asked to identify the appropriate FTP command to use in a given situation.

TABLE 2.4 **Commonly Used FTP Commands**

| Command | Description |
|---|---|
| **ls** | Lists the files in the current directory on the remote system |
| **cd** | Changes the working directory on the remote host |
| **lcd** | Changes the working directory on the local host |
| **put** | Uploads a single file to the remote host |
| **get** | Downloads a single file from the remote host |
| **mput** | Uploads multiple files to the remote host |
| **mget** | Downloads multiple files from the remote host |
| **binary** | Switches transfers into binary mode |
| **ascii** | Switches transfers into ASCII mode (the default) |

# Secure Shell

Created by students at the Helsinki University of Technology, *Secure Shell (SSH)* is a secure alternative to Telnet. SSH provides security by encrypting data as it travels between systems. This makes it difficult for hackers using packet sniffers and other traffic-detection systems. It also provides more robust authentication systems than Telnet.

Two versions of SSH are available: SSH1 and SSH2. Of the two, SSH2 is considered more secure. The two versions are incompatible. If you use an SSH client program, the server implementation of SSH that you connect to must be the same version. By default, SSH operates on port 22.

Although SSH, like Telnet, is associated primarily with UNIX and Linux systems, implementations of SSH are available for all commonly used computing platforms, including Windows and macOS.

ExamAlert

Remember that SSH uses port 22 and is a more secure alternative to Telnet.

## Secure File Transfer Protocol

One of the big problems associated with FTP is that it is considered unsecure. Even though simple authentication methods are associated with FTP, it is still susceptible to relatively simple hacking approaches. In addition, FTP transmits data between sender and receiver in an unencrypted format. By using a packet sniffer, a hacker could easily copy packets from the network and read the contents. In today's high-security computing environments, you need a more robust solution.

That solution is the *Secure File Transfer Protocol (SFTP)*, which, based on Secure Shell (SSH) technology, provides robust authentication between sender and receiver. It also provides encryption capabilities, which means that even if packets are copied from the network, their contents remain hidden from prying eyes.

SFTP is implemented through client and server software available for all commonly used computing platforms. SFTP uses port 22 (the same port SSH uses) for secure file transfers.

## Telnet

Telnet, which is defined in RFC 854, is a virtual terminal protocol. It enables sessions to be opened on a remote host, and then commands can be executed on that remote host. For many years, Telnet was the method by which clients accessed multiuser systems such as mainframes and minicomputers. It also was the connection method of choice for UNIX systems. Today, Telnet is still used to access routers and other managed network devices. By default, Telnet operates on port 23.

One of the problems with Telnet is that it is not secure. As a result, remote session functionality is now almost always achieved by using alternatives such as SSH.

**ExamAlert**

Telnet is used to access UNIX and Linux systems. Telnet uses port 23 and is insecure. SSH is considered the secure replacement for Telnet.

# Simple Mail Transfer Protocol

*Simple Mail Transfer Protocol (SMTP)*, which is defined in RFC 821, is a protocol that defines how mail messages are sent between hosts. SMTP uses TCP connections to guarantee error-free delivery of messages. SMTP is not overly sophisticated and requires that the destination host always be available. For this reason, mail systems spool incoming mail so that users can read it later. How the user then reads the mail depends on how the client accesses the SMTP server. The default port used by SMTP is 25.

**Note**

SMTP can be used to both send and receive mail. Post Office Protocol version 3 (POP3) and Internet Message Access Protocol version 4 (IMAP4) can be used only to receive mail.

# Domain Name System (DNS)

*Domain Name System (DNS)*—also known as *Domain Name Service*—resolves hostnames, such as www.pearsonitcertification.com, to IP addresses, such as 168.146.67.180. By default, DNS operates on port 53 and it constitutes one of the few network services that CompTIA wants you to know quite a bit about. As such, it is discussed in more detail in the third section of this chapter.

# Dynamic Host Configuration Protocol (DHCP)

*Dynamic Host Configuration Protocol (DHCP)* is defined in RFC 2131. It enables ranges of IP addresses, known as *scopes*, or predefined groups of addresses within *address pools* to be defined on a system running a DHCP server application. When another system configured as a DHCP client is initialized, it asks the server for an address and is leased one. By default, DHCP uses ports 67 and 68. Figure 2.3 shows an example of a configuration interface for DHCP on a SOHO router.

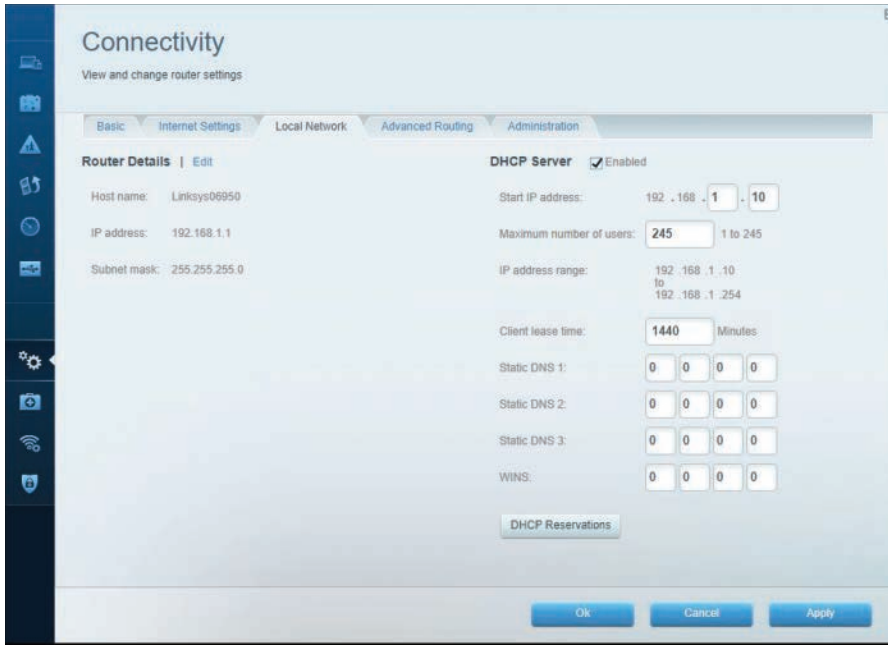



FIGURE 2.3 **Configuring DHCP on a SOHO router**

> **Note**
>
> DNS, DHCP, and NTP appear in the exam objectives for this section, but also appear in much more depth in the next set of objectives. To avoid overlap with the discussion of the objectives, all three are discussed in more depth later in this chapter.

# Trivial File Transfer Protocol

A variation on FTP is *Trivial File Transfer Protocol (TFTP)*, which is also a file transfer mechanism. However, TFTP does not have the security capability or the level of functionality that FTP has. TFTP, which is defined in RFC 1350, is most often associated with simple downloads, such as those associated with transferring firmware to a device such as a router and booting diskless workstations.

Another feature that TFTP does not offer is directory navigation. Whereas in FTP, commands can be executed to navigate and manage the file system, TFTP offers no such capability. TFTP requires that you request not only exactly what you want but also the particular location. Unlike FTP, which uses TCP as its transport protocol to guarantee delivery, TFTP uses UDP. By default, TFTP operates on port 69.

**ExamAlert**

TFTP is an application layer protocol that uses UDP, which is a connectionless transport layer protocol. For this reason, TFTP is called a *connectionless file transfer method*.

# Hypertext Transfer Protocol

*Hypertext Transfer Protocol (HTTP)*, which is defined in RFC 2068, is the protocol that enables text, graphics, multimedia, and other material to be downloaded from an HTTP server. HTTP defines what actions can be requested by clients and how servers should answer those requests.

In a practical implementation, HTTP clients (that is, web browsers) make requests on port 80 in an HTTP format to servers running HTTP server applications (that is, web servers). Files created in a special language such as *Hypertext Markup Language (HTML)* are returned to the client, and the connection is closed.

**ExamAlert**

Make sure that you understand that HTTP is a connection-oriented protocol that uses TCP as a transport protocol. By default, it operates at port 80.

Today, HTTP over port 80 is considered insecure and often replaced by HTTPS (over port 443). Both HTTP and HTTPS use a *uniform resource locator (URL)* to determine what page should be downloaded from the remote server. The URL contains the type of request (for example, http:// or https://), the name of the server contacted (for example, www.microsoft.com or just microsoft.com since the web portion is the default), and optionally the page requested (for example, /support). The result is the syntax that Internet-savvy people are familiar with: https://support.microsoft.com/.

# Network Time Protocol (NTP)

*Network Time Protocol (NTP)*, which is defined in RFC 958, is the part of the TCP/IP protocol suite that facilitates the communication of time between systems. NTP operates over UDP port 123.

# Post Office Protocol Version 3/Internet Message Access Protocol Version 4

Both *Post Office Protocol Version 3 (POP3)*, which is defined in RFC 1939, and *Internet Message Access Protocol Version 4 (IMAP4)*, the latest version of which is defined in RFC 1731, are mechanisms for downloading, or pulling, email from a server. They are necessary because although the mail is transported around the network via SMTP, users cannot always immediately read it, so it must be stored in a central location. From this location, it needs to be downloaded or retrieved, which is what POP3 and IMAP4 enable you to do.

POP3 and IMAP4 are popular, and many people access email through applications that are POP3 and IMAP4 clients. The default port for POP3 is 110, and for IMAP4, the default port is 143.

One of the problems with POP3 is that the password used to access a mailbox is transmitted across the network in clear text. This means that if people want to, they could determine your POP3 password with relative ease. This is an area in which IMAP4 offers an advantage over POP3. It uses a more sophisticated authentication system, which makes it more difficult for people to determine a password.

**ExamAlert**

POP3 and IMAP4 can be used to download, or pull, email from a server, but they cannot be used to send mail. That function is left to SMTP, which can both send and receive. Also remember, POP3 uses port 110 and IMAP4 uses port 143.

**Note**

Although accessing email by using POP3 and IMAP4 has many advantages, such systems rely on servers to hold the mail until it is downloaded to the client system. In today's world, a more sophisticated solution to anytime/anywhere email access is needed. For many people, that solution is web-based mail. Having an Internet-based email account enables you to access your mail from anywhere and from any device that supports a web browser. Recognizing the obvious advantages of such a system, all the major email systems have, for some time, included web access gateway products.

# Simple Network Management Protocol

The *Simple Network Management Protocol (SNMP)* uses port 161 to send data and port 162 to receive it. It enables network devices to communicate information about their state to a central system. It also enables the central system to pass configuration parameters to the devices.

**ExamAlert**

SNMP uses ports 161 and 162. It is a protocol that facilitates network management functionality. It is not, in itself, a *network management system (NMS)*, simply the protocol that makes NMS possible.

## Components of SNMP

In an SNMP configuration, a central system known as a *manager* acts as the central communication point for all the SNMP-enabled devices on the network. On each device to be managed and monitored via SNMP, software called an SNMP agent is set up and configured with the manager's IP address. Depending on the configuration, the SNMP manager then communicates with and retrieves information from the devices running the SNMP agent software. In addition, the agent can communicate the occurrence of certain events to the SNMP manager as they happen. These messages are known as *traps*. Figure 2.4 shows how an SNMP system works.

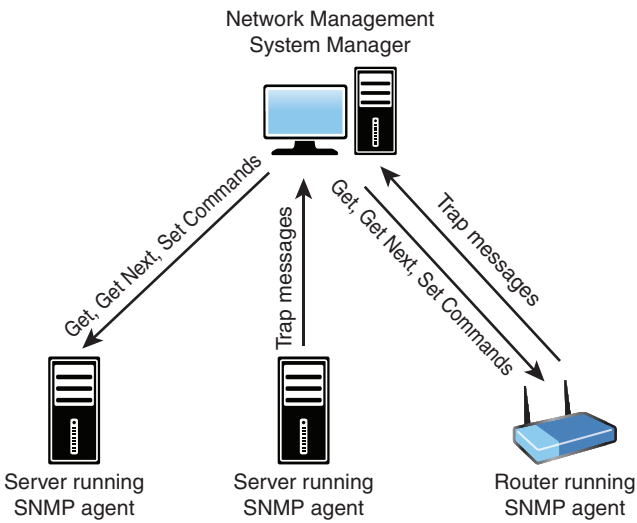



FIGURE 2.4 **How SNMP works**

As Figure 2.4 illustrates, there are a number of components to SNMP. The following discussion looks at the management system, the agents, the management information base, and communities.

## SNMP Management Systems

An SNMP management system is a computer running a special piece of software called a *network management system (NMS)*. These software applications can be free, or they can cost thousands of dollars. The difference between the free applications and those that cost a great deal of money normally boils down to functionality and support. All NMS applications, regardless of cost, offer the same basic functionality. Today, most NMS applications use graphical maps of the network to locate a device and then query it. The queries are built in to the application and are triggered by pointing and clicking. You can issue SNMP requests from a command-line utility, but with so many tools available, this is unnecessary.

> **Note**
>
> Some people call SNMP managers or NMSs *trap managers*. This reference is misleading, however, because an NMS can do more than just accept trap messages from agents.

Using SNMP and an NMS, you can monitor all the devices on a network, including switches, hubs, routers, servers, and printers, as well as any device that supports SNMP, from a single location. Using SNMP, you can see the amount of free disk space on a server in Jakarta or reset the interface on a router in Helsinki—all from the comfort of your desk in San Jose. Such power, though, brings with it some considerations. For example, because an NMS enables you to reconfigure network devices, or at least get information from them, it is common practice to implement an NMS on a secure workstation platform such as a Linux or Windows server and to place the NMS PC in a secure location.

## SNMP Agents

Although the SNMP manager resides on a PC or server, each device that is part of the SNMP structure also needs to have SNMP functionality enabled. This is performed through a software component called an *agent*.

An SNMP agent can be any device that can run a small software component that facilitates communication with an SNMP manager. SNMP agent functionality is supported by almost any device designed to be connected to a network.

In addition to providing a mechanism for managers to communicate with them, agents can tell SNMP managers when a threshold is surpassed. When this happens, on a device running an SNMP agent, a trap is sent to the NMS, and the NMS then performs an action, depending on the configuration. Basic NMS systems might sound an alarm or flash a message on the screen. Other more advanced products might dial a cell phone or send an email message.

## Management Information Bases

Although the SNMP trap system might be the most commonly used aspect of SNMP, manager-to-agent communication is not a one-way street. In addition to reading information from a device using the SNMP commands **Get** and **Get Next**, SNMP managers can issue the **Set** command. If you have a large sequence of **Get Next** commands to perform, you can use the **Walk** command to automatically move through them. The purpose of this command is to save a manager's time: you issue one command on the root node of a subtree, and the command "walks" through, getting the value of every node in the subtree.

To demonstrate how SNMP commands work, imagine that you and a friend each have a list on which the following four words are written: *four*, *book*, *sky*, and *table*. If you, as the manager, ask your friend for the first value, she, acting as the agent, can reply "four." This is analogous to an SNMP **Get** command. Now, if you ask for the next value, she would reply "book." This is analogous to an SNMP **Get Next** command. If you then say "set green," and your friend changes the word *book* to *green*, you have performed the equivalent of an SNMP **Set** command. Sound simplistic? If you can imagine expanding the list to include 100 values, you can see how you could navigate and set any parameter in the list, using just those commands. The key, though, is to make sure that you and your friend have exactly the same list—which is where *Management Information Bases (MIBs)* come in.

SNMP uses databases of information called MIBs to define what parameters are accessible, which of the parameters are read-only, and which can be set. MIBs are available for thousands of devices and services, covering every imaginable need.

To ensure that SNMP systems offer cross-platform compatibility, MIB creation is controlled by the *International Organization for Standardization (ISO)*. An organization that wants to create a MIB can apply to the ISO. The ISO then assigns the organization an ID under which it can create MIBs as it sees fit. The assignment of numbers is structured within a conceptual model called the *hierarchical name tree*.

## SNMP Communities

Another feature of SNMP that enables manageability is communities. *SNMP communities* are logical groupings of systems. When a system is configured as part of a community, it communicates only with other devices that have the same community name. In addition, it accepts **Get**, **Get Next**, or **Set** commands only from an SNMP manager with a community name it recognizes. Typically, two communities are defined by default: a public community, intended for read-only use, and a private community, intended for read-and-write operations.

> **ExamAlert**
>
> For the exam, you should understand the SNMP concepts of **Get**, Trap, **Walk**, and MIBS.

Whether you use SNMP depends on how many devices you have and how distributed your network infrastructure is. Even in environments that have just a few devices, SNMP can be useful because it can act as your eyes and ears, notifying you if a problem on the network occurs.

## SNMPv3

SNMP, which runs by default on port 161, is now on its third version, and this version has some significant differences. One of the most noticeable changes is that, unlike SNMPv1 and SNMPv2, SNMPv3 supports authentication and encryption:

- **Authentication:** Authentication protocols ensure that the message is from a valid source.
- **Encryption:** Encryption protocols ensure that data cannot be read by unintended sources.

> **ExamAlert**
>
> You might be asked to know the differences between SNMPv2 and SNMPv3. Remember, SNMPv3 supports authentication and encryption.

# Lightweight Directory Access Protocol

*Lightweight Directory Access Protocol (LDAP)* is a protocol that provides a mechanism to access and query directory services systems. LDAP uses port 389.

In the context of the Network+ exam, these directory services systems are most likely to be UNIX/Linux based or Microsoft Active Directory based. Although LDAP supports command-line queries executed directly against the directory database, most LDAP interactions are via utilities such as an authentication program (network logon) or locating a resource in the directory through a search utility.

## Hypertext Transfer Protocol Secure

One of the downsides of using HTTP is that HTTP requests are sent in clear text. For some applications, such as e-commerce, this method to exchange information is unsuitable—a more secure method is needed. The solution is *Hypertext Transfer Protocol Secure (HTTPS)*, which encrypts the information sent between the client and host (changing the port from 80 to 443). The data is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

For HTTPS to be used, both the client and server must support it. All popular browsers now support HTTPS, as do web server products, such as Microsoft *Internet Information Services (IIS)*, Apache, and almost all other web server applications that provide sensitive applications. When you access an application that uses HTTPS, the URL starts with https rather than http—for example, https://www.mybankonline.com.

## Server Message Block

Server Message Block (SMB) is used on a network for providing access to resources such as files, printers, ports, and so on that are running on Windows. If you were wanting to connect Linux-based hosts to Windows-shared printers, for example, you would need to implement support for SMB; it runs, by default, on port 445.

One of the most common ways of implementing SMB support is by running Samba.

## Syslog

Most UNIX/Linux-based systems include the capability to write messages (either directly or through applications) to log files via *syslog*. This can be done for security or management reasons and provides a central means by which devices that otherwise could not write to a central repository can easily do so (often by using the logger utility). The default port is 514.

# SMTP TLS

SMTP TLS, more commonly known as *SMTPS (Simple Mail Transfer Protocol Secure)* uses transport layer security (TLS) to provide authentication of the communication partners along with data integrity and confidentiality by wrapping SMTP data in TLS. This is similar to how HTTPS wraps HTTP data inside TLS. The default port is 587.

**Note**

Some implementations of SMTP with security use port 465. This port was proposed for SMTP with SSL and was never officially approved. It is good practice to avoid using this port and to use 587 instead.

# LDAPS

*Lightweight Directory Access Protocol over SSL (LDAPS)*, also known as Secure LDAP, adds an additional layer of security to LDAP. It operates at port 636 and differs from LDAP in two ways: (1) upon connection, the client and server establish a TLS session before any LDAP messages are transferred (without a start operation) and (2) the LDAPS connection must be closed if TLS closes.

**ExamAlert**

Remember that LDAP uses port 389, and LDAPS (secure LDAP) uses port 636.

# IMAP over SSL

When security is added to IMAP, through the use of SSL/TLS, the default port changes from 143 to 993.

# POP3 over SSL

When security is added to POP3, through the use of SSL/TLS, the default port changes from 110 to 995.

# SQL, SQLnet, and MySQL

The SQL database server uses port 1433 by default, while Oracle's SQLnet uses port 1521 and the default port for MySQL is 3306. The most common language used to speak to databases is *Structured Query Language (SQL)*.

SQL allows queries to be configured in real time and passed to database servers. This flexibility causes a major vulnerability when it isn't implemented securely.

> **Note**
>
> Most commercial relational database management systems (Oracle, Microsoft SQL Server, MySQL, PostgreSQL, and so forth) use SQL. A NoSQL database is a relatively new phenomenon—it is a relational database that does not use SQL. These databases are less common than relational databases but often used where scaling is important.

# Remote Desktop Protocol

*Remote Desktop Protocol (RDP)* is used in a Windows environment for remote connections. It operates, by default, on port 3389. *Remote Desktop Services (RDS*, formerly known as Terminal Services) provides a way for a client system to connect to a server, such as Windows Server, and, by using RDP, operate on the server as if it were a local client application. Such a configuration is known as *thin client computing*, whereby client systems use the resources of the server instead of their local processing power.

Windows Server products and recent Windows client systems have built-in support for remote connections using the Windows program Remote Desktop Connection. The underlying protocol used to manage the connection is RDP. RDP is a low-bandwidth protocol used to send mouse movements, keystrokes, and bitmap images of the screen on the server to the client computer. RDP does not actually send data over the connection—only screenshots and client keystrokes.

# Session Initiation Protocol

Long-distance calls are expensive, in part because it is costly to maintain phone lines and employ technicians to keep those phones ringing. *Voice over IP (VoIP)* provides a cheaper alternative for phone service. VoIP technology enables regular voice conversations to occur by traveling through IP packets and via the Internet. VoIP avoids the high cost of regular phone calls by using the existing infrastructure of the Internet. No monthly bills or expensive long-distance charges are required. But how does it work?

Like every other type of network communication, VoIP requires protocols to make the magic happen. For VoIP, one such protocol is *Session Initiation Protocol (SIP)*, which is an application layer protocol designed to establish and maintain multimedia sessions, such as Internet telephony calls. This means that SIP can create communication sessions for such features as audio/videoconferencing, online gaming, and person-to-person conversations over the Internet. SIP does not operate alone; it uses TCP or UDP as a transport protocol. Remember, TCP enables guaranteed delivery of data packets, whereas UDP is a fire-and-forget transfer protocol. The default ports for SIP are 5060 and 5061.

**ExamAlert**

SIP operates at the application layer of the OSI model and is used to maintain a multimedia session. SIP uses ports 5060 and 5061.

**Tip**

SIP also includes a suite of security services, which include denial-of-service (DoS) prevention, authentication (both user-to-user and proxy-to-user), integrity protection, and encryption and privacy services.

# Understanding Port Functions

As protocols were mentioned in this chapter, the default ports were also given. Each TCP/IP or application has at least one default port associated with it. When a communication is received, the target port number is checked to determine which protocol or service it is destined for. The request is then forwarded to that protocol or service. For example, consider HTTPS, whose assigned port number is 443. When a web browser forms a request for a secure web page, that request is sent to port 443 on the target system. When the target system receives the request, it examines the port number. When it sees that the port is 443, it forwards the request to the web server application.

TCP/IP has 65,535 ports available, with 0 to 1023 labeled as the well-known ports. Although a detailed understanding of the 65,535 ports is not necessary for the Network+ exam, you need to understand the numbers of some well-known ports. Network administration often requires you to specify port assignments when you work with applications and configure services. Table 2.5 shows some of the most common port assignments.

**ExamAlert**

You should concentrate on the information provided in Table 2.5 and apply it to any port-related questions you might receive on the exam. For example, the exam may present you with a situation in which you can't access a particular service; you may have to determine whether a port is open or closed on a firewall.

TABLE 2.5 **TCP/UDP Port Assignments for Commonly Used Protocols**

| Protocol | Port Assignment |
|---|---|
| *TCP Ports* | |
| FTP | 20/21 |
| SSH/SFTP | 22 |
| Telnet | 23 |
| SMTP | 25 |
| DNS | 53 |
| HTTP | 80 |
| POP3 | 110 |
| IMAP4 | 143 |
| LDAP | 389 |
| HTTPS | 443 |
| SMB | 445 |
| SMTP TLS | 587 |
| LDAPS | 636 |
| IMAP over SSL | 993 |
| POP3 over SSL | 995 |
| SQL Server | 1433 |
| SQLnet | 1521 |
| MySQL | 3306 |
| RDP | 3389 |
| SIP | 5060/5061 |
| *UDP Ports* | |
| DNS | 53 |
| DHCP (and BOOTP server) | 67 |
| DHCP (and BOOTP client) | 68 |

| Protocol | Port Assignment |
|---|---|
| TFTP | 69 |
| NTP | 123 |
| SNMP | 161/162 |
| Syslog | 514 |
| RDP | 3389 |
| SIP | 5060/5061 |

**ExamAlert**

The term *well-known ports* identifies the ports ranging from 0 to 1023. If/when an exam question refers to "well-known ports," this is what it refers to.

**Note**

You might have noticed in Table 2.5 that two ports are associated with FTP (and some other protocols, as well). With FTP, port 20 is considered the data port, and port 21 is considered the control port. In practical use, FTP connections use port 21. Port 20 is rarely used in modern implementations.

# Cram Quiz

1. TCP is an example of what kind of transport protocol?
   - ❍ **A.** Connection oriented
   - ❍ **B.** Connection reliant
   - ❍ **C.** Connection dependent
   - ❍ **D.** Connectionless

2. Which of the following are considered transport protocols? (Choose the two best answers.)
   - ❍ **A.** TCP
   - ❍ **B.** IP
   - ❍ **C.** UDP
   - ❍ **D.** THC

**3.** What is the function of NTP?

- ❍ **A.** It provides a mechanism for the sharing of authentication information.
- ❍ **B.** It is used to access shared folders on a Linux system.
- ❍ **C.** It is used to communicate utilization information to a central manager.
- ❍ **D.** It is used to communicate time synchronization information between systems.

**4.** Which of the following protocols offers guaranteed delivery?

- ❍ **A.** FTP
- ❍ **B.** POP
- ❍ **C.** IP
- ❍ **D.** TCP

**5.** By default, which protocol uses port 68?

- ❍ **A.** DHCP
- ❍ **B.** DNS
- ❍ **C.** SMB
- ❍ **D.** SMTP

**6.** What are SNMP databases called?

- ❍ **A.** HOSTS
- ❍ **B.** MIBs
- ❍ **C.** WINS
- ❍ **D.** Agents

**7.** What are logical groupings of SNMP systems known as?

- ❍ **A.** Communities
- ❍ **B.** Pairs
- ❍ **C.** Mirrors
- ❍ **D.** Nodes

**8.** What are two features supported in SNMPv3 and not previous versions?

- ❍ **A.** Authentication
- ❍ **B.** Dynamic mapping
- ❍ **C.** Platform independence
- ❍ **D.** Encryption

# Cram Quiz Answers

1. **A.** TCP is an example of a connection-oriented transport protocol. UDP is an example of a connectionless protocol. *Connection reliant* and *connection dependent* are not terms commonly associated with protocols.
2. **A and C.** Both TCP and UDP are transport protocols. IP is a network protocol, and THC is not a valid protocol.
3. **D.** NTP is used to communicate time-synchronization information between devices. Network File System (NFS) is a protocol typically associated with accessing shared folders on a Linux system. Utilization information is communicated to a central management system most commonly by using SNMP.
4. **D.** TCP is a connection-oriented protocol that guarantees delivery of data. FTP is a protocol used to transfer large blocks of data. POP stands for Post Office Protocol and is not the correct choice. IP is a network layer protocol responsible for tasks such as addressing and route discovery.
5. **A.** DHCP uses port 68 by default (along with 67). DNS uses port 53, SMB uses 445, and SMTP uses port 25.
6. **B.** SNMP uses databases of information called MIBs to define what parameters are accessible, which of the parameters are read-only, and which can be set.
7. **A.** SNMP communities are logical groupings of systems. When a system is configured as part of a community, it communicates only with other devices that have the same community name.
8. **A and D.** SNMPv3 supports authentication and encryption.

# Network Services

▶ **Explain the use and purpose of network services.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What is the name used for ranges of IP addresses available within DHCP?
2. What is the name of the packet on a system configured to use DHCP broadcasts when it comes onto the network?
3. What is dynamic DNS?
4. Within DNS, what is the domain name, along with any subdomains, called?

### Answers

1. Within DHCP, ranges of IP addresses are known as *scopes*.
2. When a system configured to use DHCP comes onto the network, it broadcasts a special packet that looks for a DHCP server. This packet is known as the DHCPDISCOVER packet.
3. Dynamic DNS is a newer system that enables hosts to be dynamically registered with the DNS server.
4. The domain name, along with any subdomains, is called the *fully qualified domain name (FQDN)* because it includes all the components from the top of the DNS namespace to the host.

Network services provide functionality enabling the network to operate. There are a plethora of services available, but three you need to know for the exam are DNS, DHCP, and NTP.

# Domain Name Service (DNS)

DNS performs an important function on TCP/IP-based networks. It resolves hostnames, such as www.quepublishing.com, to IP addresses, such as 209.202.161.67. Such a resolution system makes it possible for people to remember the names of and refer to frequently used hosts using easy-to-remember hostnames rather than hard-to-remember IP addresses. By default, DNS operates on port 53.

> **Note**
>
> Like other TCP/IP-based services, DNS is a platform-independent protocol. Therefore, it can be used on Linux, UNIX, Windows, and almost every other platform.

In the days before the Internet, the network that was to become the Internet used a text file called HOSTS to perform name resolution. The HOSTS file was regularly updated with changes and distributed to other servers. Following is a sample of some entries from a HOSTS file:

```
192.168.3.45 server1 s1 #The main file and print server
192.168.3.223 Mail mailserver #The email server
127.0.0.1 localhost
```

> **Note**
>
> A comment in the HOSTS file is preceded by a hash symbol (#).

As you can see, the host's IP address is listed, along with the corresponding hostname. You can add to a HOSTS file aliases of the server names, which in this example are **s1** and **mailserver**. All the entries must be added manually, and each system to perform resolutions must have a copy of the file.

Even when the Internet was growing at a relatively slow pace, such a mechanism was both cumbersome and prone to error. It was obvious that as the network grew, a more automated and dynamic method of performing name resolution was needed. DNS became that method.

> **Tip**
>
> HOSTS file resolution is still supported by most platforms. If you need to resolve just a few hosts that will not change often or at all, you can still use the HOSTS file for this.

DNS solves the problem of name resolution by offering resolution through servers configured to act as name servers. The name servers run DNS server software, which enables them to receive, process, and reply to requests from systems that want to resolve hostnames to IP addresses. Systems that ask DNS servers for a hostname-to-IP address mapping are called *resolvers* or *DNS clients*. Figure 2.5 shows the DNS resolution process. In this example, the client asks to reach the first server at mycoltd.com; the router turns to the DNS server for

an IP address associated with that server; and after the address is returned, the client can establish a connection.

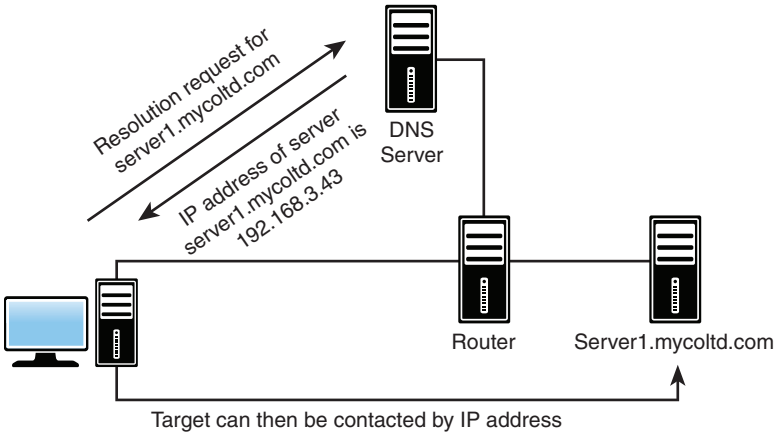



FIGURE 2.5 **The DNS resolution process**

Because the DNS namespace (which is discussed in the following section) is large, a single server cannot hold all the records for the entire namespace. As a result, there is a good chance that a given DNS server might not resolve the request for a certain entry. In this case, the DNS server asks another DNS server if it has an entry for the host.

**Note**

One of the problems with DNS is that, despite all its automatic resolution capabilities, entries and changes to those entries must still be manually performed. A strategy to solve this problem is to use *Dynamic DNS (DDNS)*, a newer system that enables hosts to be dynamically registered with the DNS server. When changes are made in real time to hostnames, addresses, and related information, there is less likelihood of not finding a server or site that has been recently added or changed.

**ExamAlert**

You might be asked to identify the difference between DNS and DDNS.

To speed up resolution, the client will often store the results of resolution locally (in the browser quite often) so that it does not have to query again if the same resolution needs to be done. This is known as *DNS caching*, and this is

also done by caching nameservers (also known as recursive nameservers). Since it is possible that values change (a different IP address issued to a host than it previously had), caches typically come with *TTL (time to live)* values and time out after a while.

# The DNS Namespace

DNS operates in the *DNS namespace*. This space has logical divisions *hierarchically* organized. At the top level are domains such as .com (commercial) and .edu (education), as well as domains for countries, such as .uk (United Kingdom) and .de (Germany). Below the top level are subdomains or second-level domains associated with organizations or commercial companies, such as Red Hat and Microsoft. Within these domains, hosts or other subdomains can be assigned. For example, the server ftp.redhat.com would be in the redhat.com domain. Figure 2.6 shows a DNS hierarchical namespace.

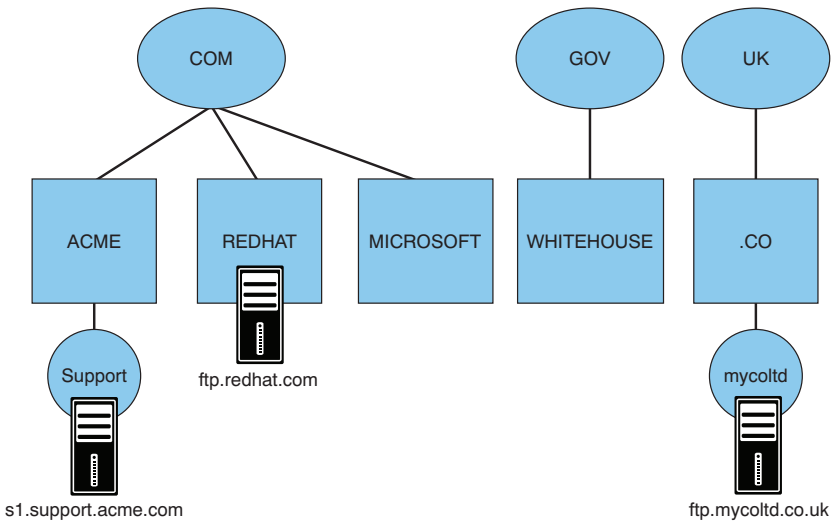



FIGURE 2.6 **A DNS hierarchical namespace**

**ExamAlert**

The domain name, along with any subdomains, is called the *fully qualified domain name (FQDN)* because it includes all the components from the top of the DNS namespace to the host.

**Note**

Many people refer to DNS as resolving FQDNs to IP addresses. An example of an FQDN is www.comptia.org, where www is the host, comptia is the second-level domain, and org is the top-level domain.

The lower domains are largely open to use in whatever way the domain name holder sees fit. However, the top-level domains are relatively closely controlled. Table 2.6 lists a selection of the most widely used top-level DNS domain names. Recently, a number of top-level domains were added, mainly to accommodate the increasing need for hostnames. While *root DNS servers* directly answer requests for records in the root zone, and answer other requests, they also return lists of the authoritative name servers for the top-level domain (TLD) being sought.

TABLE 2.6 **Selected Top-Level Domains in the DNS Namespace**

| Top-Level Domain Name | Intended Purpose |
|---|---|
| com | Commercial organizations |
| edu | Educational organizations/establishments |
| gov | U.S. government organizations/establishments |
| net | Network providers/centers |
| org | Not-for-profit and other organizations |
| mil | Military |
| arpa | Reverse DNS lookup |
| de | A country-specific domain—in this case, Germany* |

*In addition to country-specific domains, many countries have created subdomains that follow roughly the same principles as the original top-level domains (such as co.uk and gov.nz).

Although the assignment of domain names is supposed to conform to the structure shown in Table 2.6, the assignment of names is not as closely controlled as you might think. It's not uncommon for some domain names to be used for other purposes, such as .org or .net being used for business.

**Note**

Although the primary function of DNS is to resolve hostnames to IP addresses, you can also have DNS perform IP address-to-hostname resolution. This process is called *reverse lookup*, which is accomplished by using *pointer (PTR)* records.

ExamAlert

For the exam, know that PTR records are used for reverse lookup functions.

Two other words often used with DNS queries are *iterative* and *recursive*. An iterative lookup is one in which the client just keeps querying the server. A recursive lookup is one in which the server does not have the answer the client is looking for and forwards the request on to another DNS server in search of the answer. To use a silly analogy, an iterative lookup would be similar to asking your mother every five minutes if you can go outside and getting the same "no" answer over and over, while a recursive lookup would be her telling you to go ask your father.

# Types of DNS Entries

Although the most common entry in a DNS database is an A (address) record, which maps a hostname to an IP address, DNS can hold numerous other types of entries as well. Some are the MX record, which can map entries that correspond to mail exchanger systems, and CNAME (canonical record name), which can create alias records for a system. A system can have an A record and then multiple CNAME entries for its aliases. A DNS table with all these types of entries might look like this:

```
fileserve.mycoltd.com IN A 192.168.33.2
email.mycoltd.com IN A 192.168.33.7
fileprint.mycoltd.com IN CNAME fileserver.mycoltd.com
mailer.mycoltd.com IN MX 10 email.mycoltd.com
```

As you can see, rather than map to an actual IP address, the CNAME and MX record entries map to another host, which DNS in turn can resolve to an IP address.

# DNS Records

Each DNS name server maintains information about its *zone*, or domain, in a series of records, known as DNS resource records. There are several DNS resource records; each contains information about the DNS domain and the systems within it. These records are text entries stored on the DNS server. Some of the DNS resource records include the following:

- **Start of Authority (SOA):** This is a record of information containing data on DNS zones and other DNS records. A DNS zone is the part of a domain for which an individual DNS server is responsible. Each zone contains a single SOA record.

- **Name Server (NS):** This record stores information that identifies the name servers in the domain that store information for that domain.
- **Service Locator (SRV):** This is a generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX.
- **Canonical Name (CNAME):** This record stores additional hostnames, or aliases, for hosts in the domain. A CNAME specifies an alias or nickname for a canonical hostname record in a Domain Name Service (DNS) database. CNAME records give a single computer multiple names (aliases).
- **Pointer (PTR):** This record is a pointer to the canonical name, which is used to perform a reverse DNS lookup, in which case the name is returned when the query originates with an IP address.

ExamAlert

The most common type of DNS zone is the forward lookup zone, which allows DNS clients to obtain information such as IP addresses that correspond to DNS domain names. Remember that a reverse lookup zone maps from IP addresses back to DNS domain names.

- **IPv6 Address (AAAA):** This record stores information for IPv6 (128-bit) addresses. It is most commonly used to map hostnames to an IP address for a host.
- **IPv4 Address (A):** This record stores information for IPv4 (32-bit) addresses. It is most commonly used to map hostnames to an IP address for a host.
- **Text (TXT):** This field was originally created to carry human-readable text in a DNS record, but that purpose has long since passed. Today, it is more common that it holds machine-readable data, such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail).
- **Mail Exchange (MX):** This record stores information about where mail for the domain should be delivered.

ExamAlert

The exam objectives specifically list DNS records. You should expect to see a question about records A, MX, AAAA, CNAME, NS, SRV, TXT, or PTR.

# DNS in a Practical Implementation

In a real-world scenario, whether you use DNS is almost a nonissue. If you have Internet access, you will most certainly use DNS, but you are likely to use the DNS facilities of your *Internet service provider (ISP)* rather than have your own internal DNS server—this is known as *external DNS*. However, if you operate a large, complex, multiplatform network, you might find that internal DNS servers are necessary. The major network operating system vendors know that you might need DNS facilities in your organization, so they include DNS server applications with their offerings, making third-party/cloud-hosted DNS a possibility. Google, for example, offers Cloud DNS, which is "low latency, high availability and is a cost-effective way to make your applications and services available to your users" (for more information, see https://cloud.google.com/dns/).

It is common practice for workstations to be configured with the IP addresses of two DNS servers for fault tolerance (configured via the Alternate Configuration tab in Windows, for example). The importance of DNS, particularly in environments in which the Internet is heavily used, cannot be overstated. If DNS facilities are not accessible, the Internet effectively becomes unusable, unless you can remember the IP addresses of all your favorite sites.

Domain Name System Security Extensions (DNSSEC) is a suite of IETF specifications for securing certain kinds of information provided by DNS. As it was originally designed, DNS did not include any security features. DNSSEC not only adds security features to DNS but is also designed to be backward compatible.

## Windows Internet Name Service (WINS)

On Windows networks, you can use a system called WINS to enable Network Basic Input/Output System (NetBIOS) names to be resolved to IP addresses. NetBIOS name resolution is necessary on Windows networks so that systems can locate and access each other by using the NetBIOS computer name rather than the IP address. It's a lot easier for a person to remember a computer called *secretary* than to remember its IP address, 192.168.2.34. The NetBIOS name needs to be resolved to an IP address and subsequently to a MAC address (by ARP).

NetBIOS name resolution can be performed three ways on a network. The simplest way is to use a WINS server on the network that automatically performs the NetBIOS name resolution. If a WINS server is not available, NetBIOS name resolution can be performed statically using an LMHOSTS file. Using an LMHOSTS file requires that you manually configure at least one text file with the entries. As you can imagine, this can be a time-consuming process, particularly if the systems on the network frequently change. The third method, and the default, is that systems resolve NetBIOS names using broadcasts.

This approach has two problems. First, the broadcasts create additional network traffic, and second, the broadcasts cannot traverse routers unless the router is configured to forward them. This means that resolutions between network segments are impossible.

# Dynamic Host Configuration Protocol

One method to assign IP addresses to hosts is to use static addressing. This process involves manually assigning an address from those available to you and allowing the host to always use that address. The problems with this method include the difficulty in managing addresses for a multitude of machines and efficiently and effectively issuing them.

**ExamAlert**

Be sure to know the difference between static and dynamic IP addressing as you study for the Network+ exam.

DHCP, which is defined in RFC 2131, enables ranges of IP addresses, known as *scopes* or predefined groups of addresses within *address pools* to be defined on a system running a DHCP server application. When another system configured as a DHCP client is initialized, it asks the server for an address. If all things are as they should be, the server assigns an address from the scope to the client for a predetermined amount of time, known as the *lease* or *lease time*.

At various points during the TTL of the lease time (normally the 50 percent and 85 percent points), the client attempts to renew the lease from the server. If the server cannot perform a renewal, the lease expires at 100 percent, and the client stops using the address.

In addition to an IP address and the subnet mask, the DHCP server can supply many other pieces of information; however, exactly what can be provided depends on the DHCP server implementation. In addition to the address information, the default gateway is often supplied, along with DNS information.

In addition to having DHCP supply a random address from the scope, you can configure *scope options*, such as having it supply a specific address to a client. Such an arrangement is known as a *reservation* (see Figure 2.7). Reservations are a means by which you can still use DHCP for a system but at the same time guarantee that it always has the same IP address. When based on the MAC address, this is known as *MAC reservations.* DHCP can also be configured for exclusions, also called *IP exclusions*. In this scenario, certain IP addresses are not given out to client systems.

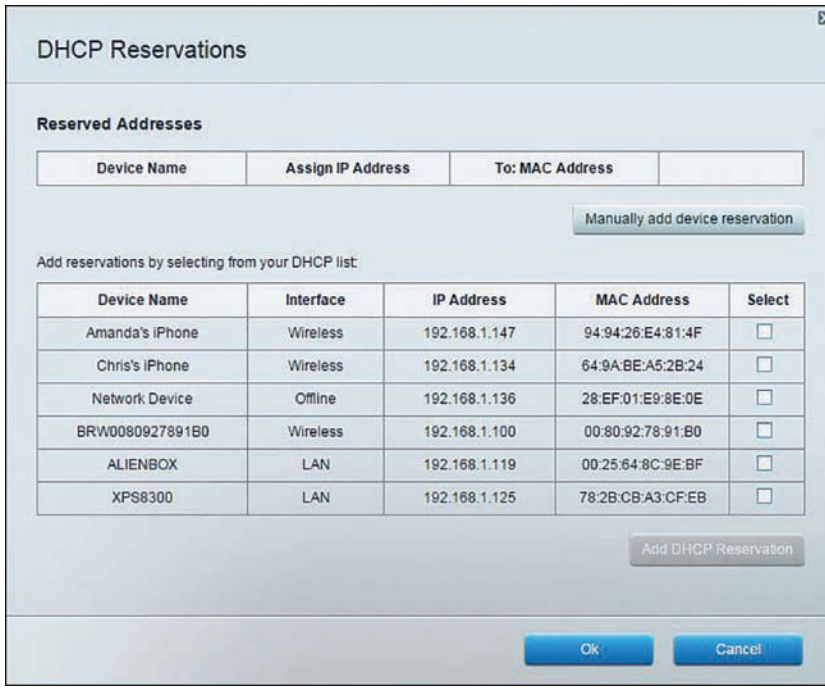



FIGURE 2.7 **DHCP reservations**

The advantages of using DHCP are numerous. First, administrators do not need to manually configure each system. Second, human error, such as the assignment of duplicate IP addresses, is eliminated. Third, DHCP removes the need to reconfigure systems if they move from one subnet to another, or if you decide to make a wholesale change in the IP addressing structure. The downsides are that DHCP traffic is broadcast based and thus generates network traffic—albeit a small amount. Finally, the DHCP server software must be installed and configured on a server, which can place additional processor load (again, minimal) on that system. From an administrative perspective, after the initial configuration, DHCP is about as maintenance-free as a service can get, with only occasional monitoring normally required.

**ExamAlert**

DHCP is a protocol-dependent service and is not platform dependent. This means that you can use, for instance, a Linux DHCP server for a network with Windows clients or with Linux clients. Although the DHCP server offerings in the various network operating systems might slightly differ, the basic functionality is the same across the board. Likewise, the client configuration for DHCP servers running on a different operating system platform is the same as for DHCP servers running on the same base operating system platform.

# The DHCP Process

To better understand how DHCP works, spend a few minutes looking at the processes that occur when a DHCP-enabled client connects to the network. When a system configured to use DHCP comes onto the network, it broadcasts a special packet that looks for a DHCP server. This packet is known as the DHCPDISCOVER packet. The DHCP server, which is always on the lookout for DHCPDISCOVER broadcasts, picks up the packet and compares the request with the scopes it has defined. If it finds that it has a scope for the network from which the packet originated, it chooses an address from the scope, reserves it, and sends the address, along with any other information, such as the lease duration, to the client. This is known as the DHCPOFFER packet. Because the client still does not have an IP address, this communication is also achieved via broadcast. By default, DHCP operates on ports 67 and 68.

**ExamAlert**

Remember that DHCP operates on ports 67 and 68.

When the client receives the offer, it looks at the offer to determine if it is suitable. If more than one offer is received, which can happen if more than one DHCP server is configured, the offers are compared to see which is best. *Best* in this context can involve a variety of criteria but normally is the length of the lease. When the selection process completes, the client notifies the server that the offer has been accepted, through a packet called a DHCPREQUEST packet. At this point the server finalizes the offer and sends the client an acknowledgment. This last message, which is sent as a broadcast, is known as a DHCPACK packet. After the client system receives the DHCPACK, it initializes the TCP/IP suite and can communicate on the network.

# DHCP and DNS Suffixes

In DNS, *suffixes* define the DNS servers to be used and the order in which to use them. DHCP settings can push a domain suffix search list to DNS clients. When such a list is specifically given to a client, the client uses only that list for name resolution. With Linux clients, this can occur by specifying entries in the resolve.conf file.

**ExamAlert**

Know that DHCP can provide DNS suffixes to clients.

# DHCP Relays and IP Helpers

On a large network, the DHCP server can easily get bogged down trying to respond to all the requests. To make the job easier, *DHCP relays* help make the job easier. A DHCP relay is nothing more than an agent on the router that acts as a go-between for clients and the server. This feature is useful when working with clients on different subnets, because a client cannot communicate directly with the server until it has the IP configuration information assigned to it.

One level above DHCP relay is *IP helper*. These two terms are often used as synonyms, but they are not; a better way to think of it is with IP helper being a superset DHCP relay. IP helper will, by default, forward broadcasts for DHCP/BOOTP, TFTP, DNS, TACACS/TACACS+, the time service, and the NetBIOS name/datagram service (ports 137–139). You can disable the additional traffic (or add more), but by default IP helper will do more than a DHCP relay.

**ExamAlert**

Know that an IP helper can do more than a DHCP relay agent.

# Network Time Protocol

*Network Time Protocol (NTP)* is one of the oldest Internet protocols in current use. It is the part of the TCP/IP protocol suite that facilitates the communication of time between systems. NTP operates over UDP port 123. The idea is that one system configured as a time provider transmits time information to other systems that can be both time receivers and time providers for other systems.

Time synchronization is important in today's IT environment because of the distributed nature of applications. Two good examples of situations in which time synchronization is important are email and directory services systems. In each of these cases, having time synchronized between devices is important because without it there would be no way to keep track of changes to data and applications.

NTP uses a hierarchical, semi-layered system of time sources wherein each level of the hierarchy is termed a *stratum*. Each stratum/level is assigned a number starting with zero for the reference clock at the top and incrementing from there with the number representing the distance from the reference clock: this means that a server synchronized to a stratum *n* server runs at stratum *n* + 1. This numbering is used to prevent cyclical dependencies in the hierarchy, but stratum is not always an indication of quality or reliability. It is possible to find a stratum server with a higher number (for example, 3) that is of higher quality than a stratum 2 time source.

In many environments, external time sources such as radio clocks, *Global Positioning System (GPS)* devices, and Internet-based time servers are used as sources of NTP time. In others, the system's BIOS clock is used. Regardless of what source is used, the time information is communicated between devices by using NTP.

**Note**

Specific guidelines dictate how NTP should be used. You can find these "rules of engagement" at http://support.ntp.org/bin/view/Servers/RulesOfEngagement. Note that the site uses HTTP, as opposed to HTTPS, and should not be considered secure.

**ExamAlert**

Remember that NTP is used for time synchronization and is implemented over UDP port 123.

NTP server and client software is available for a variety of platforms and devices. If you want a way to ensure time synchronization between devices, look to NTP as a solution.

# Cram Quiz

1. One of the programmers has asked that DHCP always issue his workstation the same IP address. What feature of DHCP enables you to accomplish this?

   - ❍ **A.** Stipulation
   - ❍ **B.** Rider
   - ❍ **C.** Reservation
   - ❍ **D.** Provision

2. Which of the following is *not* a common packet sent during the normal DHCP process?

   - ❍ **A.** DHCPACK
   - ❍ **B.** DHCPPROVE
   - ❍ **C.** DHCPDISCOVER
   - ❍ **D.** DHCPOFFER

3. During a discussion with your ISP's technical support representative, she mentions that you might have been using the wrong FQDN. Which TCP/IP-based network service is she referring to?

   - ❍ **A.** DHCP
   - ❍ **B.** WINS
   - ❍ **C.** SNMP
   - ❍ **D.** DNS

4. Which DNS record stores additional hostnames, or aliases, for hosts in the domain?

   - ❍ **A.** ALSO
   - ❍ **B.** ALIAS
   - ❍ **C.** CNAME
   - ❍ **D.** PTR

5. Which DNS record is most commonly used to map hostnames to an IP address for a host with IPv6?

   - ❍ **A.** A
   - ❍ **B.** AAAA
   - ❍ **C.** MX
   - ❍ **D.** PTR

## Cram Quiz Answers

1. **C.** Reservations are specific addresses reserved for clients.
2. **B.** DHCPPROVE is not a common packet. The other choices presented (DHCPACK, DHCPDISCOVER, and DHCPOFFER) are part of the normal process.
3. **D.** DNS is a system that resolves hostnames to IP addresses. The term *FQDN* is used to describe the entire hostname. None of the other services use FQDNs.
4. **C.** The CNAME record stores additional hostnames, or aliases, for hosts in the domain. There is not an ALSO record or ALIAS, and PTR is used for reverse lookups.
5. **B.** The AAAA record is most commonly used to map hostnames to an IP address for a host with IPv6. The A record is not used for this purpose. MX identifies the mail exchanger, and PTR is used for reverse lookup.

# What's Next?

The TCP/IP suite is the most widely implemented protocol on networks today. As such, it is an important topic on the Network+ exam. Chapter 3, "Addressing, Routing, and Switching," starts by discussing one of the more complex facets of TCP/IP: IP addresses.

CHAPTER 3

# Addressing, Routing, and Switching

**This chapter covers the following official Network+ objectives:**

- Given a scenario, configure a subnet and use appropriate IP addressing schemes.
- Compare and contrast routing technologies and bandwidth management concepts.
- Given a scenario, configure and deploy common Ethernet switching features.

This chapter covers CompTIA Network+ objectives 1.4, 2.2, and 2.3. For more information on the official Network+ exam topics, see the "About the Network+ Exam" section in the Introduction.

Without question, TCP/IP is the most widely implemented protocol suite on networks today. As such, it is an important topic on the Network+ exam. To pass the exam, you definitely need to understand the material presented in this chapter.

This chapter deals with the concepts that govern routing and switching. It starts, however, by discussing one of the more complex facets of TCP/IP: addressing.

# IP Addressing

- **Given a scenario, configure a subnet and use appropriate IP addressing schemes.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. How many octets does a Class A address use to represent the network portion?
2. What is the range that Class C addresses span in the first octet?
3. What are the reserved private IPv4 ranges for private networks?

### Answers

1. A Class A address uses only the first octet to represent the network portion, a Class B address uses two octets, and a Class C address uses three octets.
2. Class C addresses span from 192 to 223, with a default subnet mask of 255.255.255.0.
3. A private network is any network to which access is restricted. Reserved IP addresses are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.0.0, and 192.168.0.0 to 192.168.255.255.

IP addressing is one of the most challenging aspects of TCP/IP. It can leave even the most seasoned network administrators scratching their heads. Fortunately, the Network+ exam requires only a fundamental knowledge of IP addressing. The following sections look at how IP addressing works for both IPv4 and the newest version of IP: IPv6.

To communicate on a network using TCP/IP, each system must be assigned a unique address. The address defines both the number of the network to which the device is attached and the number of the node on that network. In other words, the IP address provides two pieces of information. It's a bit like a street name and house number in a person's home address.

### ExamAlert

A *node* or *host* is any device connected to the network. A node might be a client computer, a server computer, a printer, a router, or a gateway.

Each device on a logical network segment must have the same network address as all the other devices on the segment. All the devices on that network segment must then have different node (host) addresses.

In IP addressing, another set of numbers, called a subnet mask, defines which portion of the IP address refers to the network address and which refers to the node (host) address.

IP addressing is different in IPv4 and IPv6. The discussion begins by looking at IPv4.

# IPv4

An IPv4 address is composed of four sets of 8 binary bits, which are called *octets*. The result is that IP addresses contain 32 bits. Each bit in each octet is assigned a decimal value. The far-left bit has a value of 128, followed by 64, 32, 16, 8, 4, 2, and 1, left to right.

Each bit in the octet can be either a 1 or a 0. If the value is 1, it is counted as its decimal value, and if it is 0, it is ignored. If all the bits are 0, the value of the octet is 0. If all the bits in the octet are 1, the value is 255, which is 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1.

By using the set of 8 bits and manipulating the 1s and 0s, you can obtain any value between 0 and 255 for each octet.

Table 3.1 shows some examples of decimal-to-binary value conversions.

TABLE 3.1 **Decimal-to-Binary Value Conversions**

| Decimal Value | Binary Value | Decimal Calculation |
|---|---|---|
| 10 | 00001010 | 8 + 2 = 10 |
| 192 | 11000000 | 128 + 64 = 192 |
| 205 | 11001101 | 128 + 64 + 8 + 4 + 1 = 205 |
| 223 | 11011111 | 128 + 64 + 16 + 8 + 4 + 2 + 1 = 223 |

# IP Address Classes

IP addresses are grouped into logical divisions called *classes*. The IPv4 address space has five address classes (A through E); however, only three (A, B, and C) assign addresses to clients. Class D is reserved for multicast addressing, and Class E is reserved for future development and research.

Of the three classes available for address assignments, each uses a fixed-length subnet mask to define the separation between the network and the node (host) address. A Class A address uses only the first octet to represent the network portion; a Class B address uses two octets; and a Class C address uses the first three octets. The upshot of this system is that Class A has a small number of network addresses, but each Class A address has a large number of possible host addresses. Class B has a larger number of networks, but each Class B address has a smaller number of hosts. Class C has an even larger number of networks, but each Class C address has an even smaller number of hosts. The exact numbers are provided in Table 3.2.

Be prepared for questions asking you to identify IP class ranges, such as the IP range for a Class A network.

TABLE 3.2 **IPv4 Address Classes and the Number of Available Network/Host Addresses**

| Address Class | Range | Number of Networks | Number of Hosts Per Network | Binary Value of First Octet |
|---|---|---|---|---|
| A | 1 to 126 | 126 | 16,777,214 | 0xxxxxxx |
| B | 128 to 191 | 16,384 | 65,534 | 10xxxxxx |
| C | 192 to 223 | 2,097,152 | 254 | 110xxxxx |
| D | 224 to 239 | N/A | N/A | 1110xxxx |
| E | 240 to 255 | N/A | N/A | 1111xxxx |

**Note**

Notice in Table 3.2 that the network number 127 is not included in any of the ranges. The 127.0.0.1 network ID is reserved for the IPv4 local loopback. The local loopback is a function of the protocol suite used in the troubleshooting process.

**ExamAlert**

For the Network+ exam, be prepared to identify into which class a given address falls. Also be prepared to identify the IPv4 loopback address. The loopback address is 127.0.0.1.

# Subnet Mask Assignment

Like an IP address, a *subnet mask* is most commonly expressed in 32-bit dotted-decimal format. Unlike an IP address, though, a subnet mask performs just one function: it defines which parts of the IP address refers to the network address and which refers to the node (host) address. Each class of the IP address used for address assignment has a default subnet mask associated with it. Table 3.3 lists the default subnet masks.

TABLE 3.3 **Default Subnet Masks Associated with IP Address Classes**

| Address Class | Default Subnet Mask |
|---|---|
| A | 255.0.0.0 |
| B | 255.255.0.0 |
| C | 255.255.255.0 |

ExamAlert

You will likely see questions about address classes and the corresponding default subnet mask. Review Table 3.3 before taking the exam.

# Subnetting

Now that you have looked at how IPv4 addresses are used, you can learn the process of subnetting. *Subnetting* is a process by which the node (host) portions of an IP address create more networks than you would have if you used the default subnet mask.

To illustrate subnetting, for example, suppose that you have been assigned the Class B address 150.150.0.0. Using this address and the default subnet mask, you could have a single network (150.150) and use the rest of the address as node (host) addresses. This would give you a large number of possible node addresses, which in reality is probably not useful. With subnetting, you use bits from the node portion of the address to create more network addresses. Doing so reduces the number of nodes per network, but you probably will still have more than enough.

Following are two main reasons for subnetting:

- It enables you to more effectively use IP address ranges.
- It makes IP networking more secure and manageable by providing a mechanism to create multiple networks rather than having just one.

Using multiple networks confines traffic to the network that it needs to be on, which reduces overall network traffic levels. Multiple subnets also create more broadcast domains, which in turn reduces network-wide broadcast traffic. A difference exists between *broadcast domains* and *collision domains*: the latter is all the connected nodes, whereas the former is all the logical nodes that can reach each other. As such, collision domains are typically subsets of broadcast domains.

**ExamAlert**

Subnetting does not increase the number of IP addresses available. It increases the number of network IDs and, as a result, decreases the number of node IDs per network. It also creates more broadcast domains. Broadcasts are not forwarded by routers, so they are limited to the network on which they originate.

With *Variable Length Subnet Masking (VLSM)*, it is possible to use a different subnet mask for the same network number on different subnets. This way, a network administrator can use a long mask on networks with few hosts and a short mask on subnets with many hosts, thus allowing each subnet in a routed system to be correctly sized for the required size. The routing protocol used (EIGRP, OSPF, RIPv2, IS-IS, or BGP) must be able to advertise the mask for each subnet in the routing update, which means that it must be classless. Classless interdomain routing is discussed shortly.

# Identifying the Differences Between IPv4 Public and Private Networks

IP addressing involves many considerations, not the least of which are public and private networks:

- A public network is a network to which anyone can connect. The best (and perhaps only pure) example of such a network is the Internet.
- A private network is any network to which access is restricted. A corporate network and a network in a school are examples.

**Note**

The Internet Assigned Numbers Authority (IANA) is responsible for assigning IP addresses to public networks. However, because of the workload involved in maintaining the systems and processes to do this, IANA has delegated the assignment process to a number of regional authorities. For more information, visit www.iana.org/numbers.

The main difference between public and private networks, other than access—a private network is tightly controlled and access to a public network is not—is that the addressing of devices on a public network must be carefully considered. Addressing on a private network has a little more latitude.

As already discussed, for hosts on a network to communicate by using TCP/IP, they must have unique addresses. This number defines the logical network that each host belongs to and the host's address on that network. On a private network with, for instance, three logical networks and 100 nodes on each network, addressing is not a difficult task. On a network on the scale of the Internet, however, addressing is complex.

If you connect a system to the Internet, you need to get a valid registered IP address. Most commonly, you obtain this address from your *Internet service provider (ISP)*. Alternatively, if you want a large number of addresses, for example, you could contact the organization responsible for address assignment in your area. You can determine who the regional numbers authority for your area is by visiting the IANA website.

Because of the nature of their business, ISPs have large blocks of IP addresses that they can assign to their clients. If you need a registered IP address, getting one from an ISP is almost certainly a simpler process than going through a regional numbers authority. Some ISP plans include blocks of registered IP addresses, working on the principle that businesses want some kind of permanent presence on the Internet. However, if you discontinue your service with the ISP, you can no longer use the provided IP address.

## Private Address Ranges

To provide flexibility in addressing, and to prevent an incorrectly configured network from polluting the Internet, certain address ranges are set aside for private use. These address ranges are called *private ranges* because they are designated for use only on private networks. These addresses are special because Internet routers are configured to ignore any packets they see that use these addresses. This means that if a private network "leaks" onto the Internet, it won't get any farther than the first router it encounters. So a private address cannot be on the Internet because it cannot be routed to public networks.

Three ranges are defined in *RFC 1918*: one each from Classes A, B, and C. You can use whichever range you want; however, the Class A and B address ranges offer more addressing options than Class C. Table 3.4 defines the private address ranges for Class A, B, and C addresses.

TABLE 3.4 **Private Address Ranges**

| Class | Address Range | Default Subnet Mask |
|---|---|---|
| A | 10.0.0.0 to 10.255.255.255 | 255.0.0.0 |
| B | 172.16.0.0 to 172.31.255.255 | 255.255.0.0 |
| C | 192.168.0.0 to 192.168.255.255 | 255.255.255.0 |

**ExamAlert**

You can expect questions on RFC 1918, private IP address ranges, and their corresponding default subnet masks.

# Classless Interdomain Routing

*Classless interdomain routing (CIDR)* is an IPv4 method of assigning addresses outside the standard Class A, B, and C structure. Specifying the number of bits in the subnet mask offers more flexibility than the three standard class definitions.

Using CIDR, addresses are assigned using a value known as the *slash*. The actual value of the slash depends on how many bits of the subnet mask are used to express the network portion of the address. For example, a subnet mask that uses all 8 bits from the first octet and 4 from the second would be described as /12, or "slash 12." A subnet mask that uses all the bits from the first three octets would be called /24. Why the slash? In addressing terms, the CIDR value is expressed after the address, using a slash. So, the address 192.168.2.1/24 means that the node's IP address is 192.168.2.1, and the subnet mask is 255.255.255.0.

**Note**

You can find a great CIDR calculator that can compute values from ranges at www.subnet-calculator.com/.

**ExamAlert**

You will likely see IP addresses in their CIDR format on the exam. Be sure that you understand CIDR addressing and IPv4 notation for the exam.

# Default Gateways

Default gateways are the means by which a device can access hosts on other networks for which it does not have a specifically configured route.

Most workstation configurations default to using default gateways rather than having any static routes configured. This enables workstations to communicate with other network segments or with other networks, such as the Internet.

**ExamAlert**

You will be expected to identify the purpose and function of a default gateway. You may also be asked to place the IP address of the default gateway (or other specified system) in the correct location within a performance-based question.

When a system wants to communicate with another device, it first determines whether the host is on the local network or a remote network. If the host is on a remote network, the system looks in the routing table to determine whether it has an entry for the network on which the remote host resides. If it does, it uses that route. If it does not, the data is sent to the default gateway.

**Note**

Although it might seem obvious, it's worth mentioning that the default gateway must be on the same network as the nodes that use it.

In essence, the default gateway is simply the path out of the network for a given device. Figure 3.1 shows how a default gateway fits into a network infrastructure.

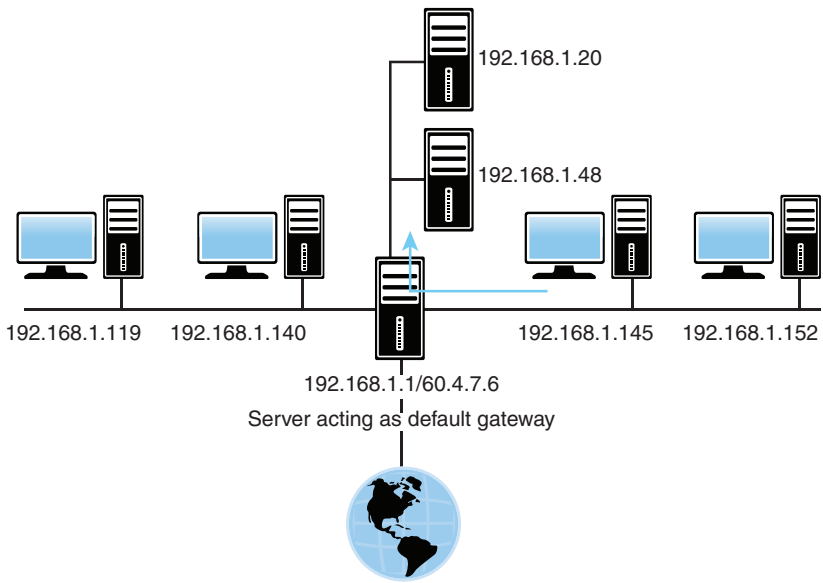



FIGURE 3.1 **The role of a default gateway**

On the network, a default gateway could be a router or a computer with network interfaces (multihomed) for all segments to which it is connected. These interfaces have local IP addresses for the respective segments. If a system is not configured with any static routes or a default gateway, it is limited to operating on its own network segment.

**ExamAlert**

For the exam, know that any system that does not have a default gateway or any static routes configured is limited to operating on its own network segment.

# Virtual IP

A *virtual IP address (VIP)* is an IP address assigned to multiple applications and is often used in high availability implementations. Data packets coming in are sent to the address and that routes them to the correct network interfaces. This allows hosting of different applications and virtual appliances on servers with only one (logical) IP address.

# IPv4 Address Types

IPv4 has three primary address types: unicast, broadcast, and multicast. You need to distinguish among these three types of IPv4 addresses.

## Unicast Address

With a *unicast address*, a single address is specified. Data sent with unicast addressing is delivered to a specific node identified by the address. It is a point-to-point, one-to-one, address link.

## Broadcast Address

A broadcast address is at the opposite end of the spectrum from a unicast address. A *broadcast address* is an IP address that you can use to target all systems on a subnet or network instead of single hosts. In other words, a broadcast message goes to everyone (one-to-all) on the network.

## Multicast

Multicasting is a mechanism by which groups of network devices can send and receive data between the members of the group at one time (one-to-many), instead of separately sending messages to each device in the group.

The multicast grouping is established by configuring each device with the same multicast IP address.

**ExamAlert**

Know the differences between unicast (one-to-one), broadcast (one-to-all), and multicast (one-to-many).

# IPv6 Addressing

Internet Protocol version 4 (IPv4) has served as the Internet's protocol for decades. When IPv4 was in development all those years ago, it would have been impossible for its creators to imagine or predict the future demand for IP devices and therefore IP addresses.

**Note**

There was an IPv5 after IPv4 and before IPv6, but it was an experimental protocol that never went anywhere.

## Where Have All the IPv4 Addresses Gone?

IPv4 uses a 32-bit addressing scheme. This gives IPv4 a total of 4,294,967,296 possible unique addresses that can be assigned to IP devices. More than 4 billion addresses might sound like a lot, and it is. However, the number of IP-enabled devices increases daily at a staggering rate. Not all these addresses can be used by public networks. Many of these addresses are reserved and are unavailable for public use. Reserving these addresses reduces the number of addresses that can be allocated as public Internet addresses.

The IPv6 project started in the mid-1990s, well before the threat of IPv4 limitations. Now network hardware and software are equipped for and ready to deploy IPv6 addressing. IPv6 offers a number of improvements. The most notable is its capability to handle growth in public networks. IPv6 uses a 128-bit addressing scheme, enabling a huge number of possible addresses:

340,282,366,920,938,463,463,374,607,431,768,211,456

## Identifying IPv6 Addresses

As previously discussed, IPv4 uses a dotted-decimal format: 8 bits converted to its decimal equivalent and separated by periods. An example of an IPv4 address is 192.168.2.1.

Because of the 128-bit structure of the IPv6 addressing scheme, it looks quite a bit different. An IPv6 address is divided along 16-bit boundaries, and each 16-bit block is converted into a four-digit hexadecimal number and separated by colons. The resulting representation is called colon hexadecimal. Now look at how it works. Figure 3.2 shows the IPv6 address 2001:0:4137:9e50:2811:34ff:3f57:febc from a Windows system.

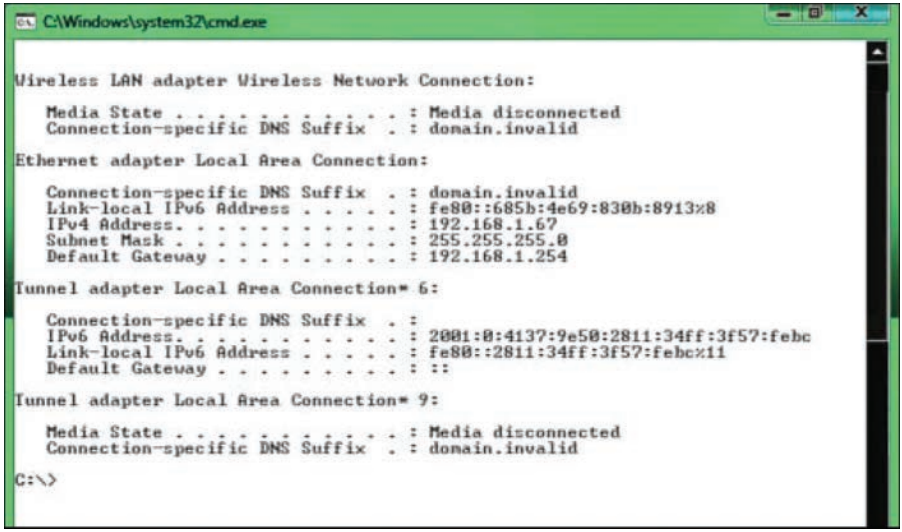



FIGURE 3.2 **An IPv6 address in a Windows dialog screen**

An IPv6 address can be simplified by removing the leading 0s within each 16-bit block. Not all the 0s can be removed, however, because each address block must have at least a single digit. Removing the 0 suppression, the address representation becomes

2001:0000:4137:9e50:2811:34ff:3f57:febc

Some of the IPv6 addresses you will work with have sequences of 0s. When this occurs, the number is often abbreviated to make it easier to read. In the preceding example you saw that a single 0 represented a number set in hexadecimal form. To further simplify the representation of IPv6 addresses, a contiguous sequence of 16-bit blocks set to 0 in colon hexadecimal format can be compressed to ::, known as the double colon.

For example, the IPv6 address of

2001:0000:0000:0000:3cde:37d1:3f57:fe93

can be compressed to

2001::3cde:37d1:3f57:fe93

However, there are limits on how the IPv6 0s can be reduced. Within the IPv6 address, 0s cannot be eliminated when they are not first in the number sequence. For instance, 2001:4000:0000:0000:0000:0000:0000:0003 cannot be compressed as 2001:4::3. This would actually appear as 2001:4000::3.

When you look at an IPv6 address that uses a double colon, how do you know exactly what numbers are represented? The formula is to subtract the number of blocks from 8 and then multiply that number by 16. For example, the address 2001:4000::3 uses three blocks: 2001, 4000, and 3. So the formula is as follows:

$$(8 - 3) \times 16 = 80$$

Therefore, the total number of bits represented by the double colon in this example is 80.

**Note**

You can remove 0s only once in an IPv6 address. Using a double colon more than once would make it impossible to determine the number of 0 bits represented by each instance of ::.

# IPv6 Address Types

Another difference between IPv4 and IPv6 is in the address types. IPv4 addressing was discussed in detail earlier. IPv6 addressing offers several types of addresses, as detailed in this section.

## Unicast IPv6 Addresses

As you might deduce from the name, a unicast address specifies a single interface. Data packets sent to a unicast destination travel from the sending host to the destination host. It is a direct line of communication. A few types of addresses fall under the unicast banner, as discussed next.

# Global Unicast Addresses

Global unicast addresses are the equivalent of IPv4 public addresses. These addresses are routable and travel throughout the network.

# Link-Local Addresses

*Link-local* addresses are designated for use on a single local network. Link-local addresses are automatically configured on all interfaces. This automatic configuration is comparable to the 169.254.0.0/16 APIPA automatically assigned IPv4 addressing scheme (discussed shortly). The prefix used for a link-local address is fe80::/64. On a single-link IPv6 network with no router, link-local addresses are used to communicate between devices on the link.

# Site-Local Addresses

Site-local addresses are equivalent to the IPv4 private address space (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16). As with IPv4, in which private address ranges are used in private networks, IPv6 uses site-local addresses that do not interfere with global unicast addresses. In addition, routers do not forward site-local traffic outside the site. Unlike link-local addresses, site-local addresses are not automatically configured and must be assigned through either stateless or stateful address configuration processes. The prefix used for the site-local address is feC0::/10.

## Multicast Addresses

As with IPv4 addresses, multicasting sends and receives data between groups of nodes. It sends IP messages to a group rather than to every node on the LAN (broadcast) or just one other node (unicast).

## Anycast Addresses

Anycast addresses represent the middle ground between unicast addresses and multicast addresses. Anycast delivers messages to any one node in the multicast group.

**Note**

You might encounter the terms *stateful* and *stateless* configuration. *Stateless* refers to IP autoconfiguration, in which administrators need not manually input configuration information. In a *stateful* configuration network, devices obtain address information from a server.

**ExamAlert**

Similar to stateful/stateless, *classful* and *classless* are address adjectives that are often used. Classful means that the address falls into one of the five IPv4 classes (A, B, C, D, or E), whereas classless uses the CIDR notation previously discussed.

**ExamAlert**

Earlier you read that IPv4 reserves 127.0.0.1 as the loopback address. IPv6 has the same reservation. IPv6 addresses 0:0:0:0:0:0:0:0 and 0:0:0:0:0:0:0:1 are reserved as the loopback addresses. 0:0:0:0:0:0:0:1 shortened is ::1. In CIDR format, the loopback address for IPv4 is 127.0. 0.1/8; for IPv6, it is ::1/128.

Remember that fe80:: is a private link-local address.

## Neighbor Discovery

IPv6 supports the Neighbor Discovery Protocol (NDP). Operating at the network layer, it is responsible for address autoconfiguration of nodes, discovery of other nodes on the link, determining the addresses of other nodes, duplicate address detection, finding available routers and DNS servers, address prefix discovery, and maintaining reachability information of other active neighbor nodes.

# Comparing IPv4 and IPv6 Addressing

Table 3.5 compares IPv4 and IPv6 addressing.

**Note**

Automatic Private IP Addressing (APIPA) appears in the table and is discussed in detail in the section "Automatic Private IP Addressing" later in this chapter.

TABLE 3.5 **Comparing IPv4 and IPv6 Addressing**

| Address Feature | IPv4 Address | IPv6 Address |
|---|---|---|
| Loopback address | 127.0.0.1 | 0:0:0:0:0:0:0:1 (::1) |
| Network-wide addresses | IPv4 public address ranges | Global unicast IPv6 addresses |
| Private network addresses | 10.0.0.0<br>172.16.0.0<br>192.168.0.0 | Site-local address ranges (feC0::) |
| Autoconfigured addresses | IPv4 automatic private IP addressing (169.254.0.0) | Link-local addresses of the fe80:: prefix |

**ExamAlert**

Make sure that you know the information provided in Table 3.5.

> **Note**
>
> IPv6 supports *dual stack*: this means that both IPv4 and IPv6 can run on the same network. This capability is extremely useful when transitioning from one to the other during the adoption and deployment phases. It also enables the network to continue to support legacy devices that may not be able to transition.

# Assigning IP Addresses

Now that you understand the need for each system on a TCP/IP-based network to have a unique address, the following sections examine how those systems receive their addresses.

## Static Addressing

*Static addressing* refers to the manual assignment of IP addresses to a system. This approach has two main problems:

- Statically configuring one system with the correct address is simple, but in the course of configuring, for instance, a few hundred systems, mistakes are likely. If the IP addresses are entered incorrectly, the system probably cannot connect to other systems on the network.
- If the IP addressing scheme for the organization changes, each system must again be manually reconfigured. In a large organization with hundreds or thousands of systems, such a reconfiguration could take a considerable amount of time. These drawbacks of static addressing are so significant that nearly all networks use dynamic IP addressing.

## Dynamic Addressing

*Dynamic addressing* refers to the automatic assignment of IP addresses. On modern networks, the mechanism used to do this is *Dynamic Host Configuration Protocol (DHCP)*. DHCP, part of the TCP/IP suite, enables a central system to provide client systems with IP addresses. Automatically assigning addresses with DHCP alleviates the burden of address configuration and reconfiguration that occurs with static IP addressing.

The basic function of the DHCP service is to automatically assign IP addresses to client systems. To do this, ranges of IP addresses, known as *scopes*, are defined on a system running a DHCP server application. When another system configured as a DHCP client is initialized, it asks the server for an address.

If all things are as they should be, the server assigns an address to the client for a predetermined amount of time, known as the *lease*, from the scope.

> **ExamAlert**
>
> As you study DHCP for the exam, make sure you know reservations, scopes, leases, options, and IP helper/DHCP relay. These topics were discussed in Chapter 2, "Models, Ports, Protocols, and Network Services."

A DHCP server typically can be configured to assign more than just IP addresses. It often is used to assign the subnet mask, the default gateway, and *Domain Name Service (DNS)* information.

Using DHCP means that administrators do not need to manually configure each client system with a TCP/IP address. This removes the common problems associated with statically assigned addresses, such as human error. The potential problem of assigning duplicate IP addresses is also eliminated. DHCP also removes the need to reconfigure systems if they move from one subnet to another, or if you decide to make a wholesale change in the IP addressing structure.

> **ExamAlert**
>
> Even when a network is configured to use DHCP, several mission-critical network systems continue to use static addressing: DHCP server, DNS server, web server, network printers, and more. They do not have dynamic IP addressing because their IP addresses can never change. If they do, client systems may be unable to access the resources from that server.

Configuring a client for TCP/IP can be relatively complex, or it can be simple. Any complexity involved is related to the possible need to manually configure TCP/IP. The simplicity is because TCP/IP configuration can occur automatically via DHCP or through APIPA. At the least, a system needs an IP address and subnet mask to log on to a network. The default gateway and DNS server IP information is optional, but network functionality is limited without them. The following list briefly explains the IP-related settings used to connect to a TCP/IP network, many of which are shown in Figure 3.3:

- **IP address:** This value is the unique address that each system must be assigned so that it can communicate on the network.
- **Subnet mask:** This value enables the system to determine what portion of the IP address represents the network address and what portion represents the node address.

- **Default gateway:** This value identifies the node on the network that enables the system to communicate on a remote network, without the need for explicit routes to be defined.
- **DNS server addresses:** This value identifies the server that is enabling dynamic hostname resolution to be performed. It is common practice to have two DNS server addresses defined so that if one server becomes unavailable, the other can be used.

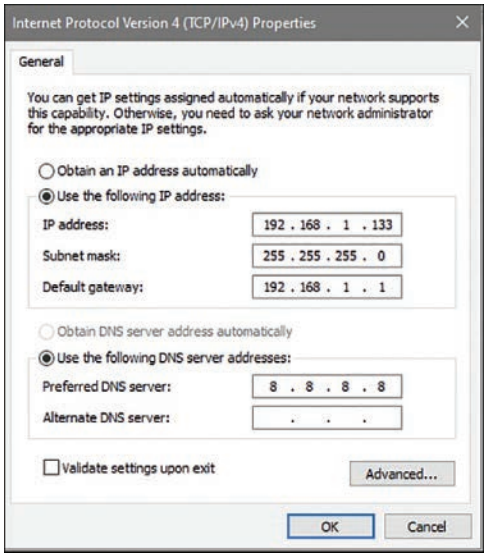



FIGURE 3.3 **Configuration options in Windows for TCP/IP**

**ExamAlert**

At the very minimum, an IP address and subnet mask are required to connect to a TCP/IP network. With this minimum configuration, connectivity is limited to the local segment, and DNS resolution is not possible.

*DHCP6* (or, more correctly, *DHCPv6*) is the IPv6 counterpart to DHCP. It issues the necessary configuration information for clients on IPv6-based networks. When it comes to assigning the addresses, the preferred method of assigning IP addresses in an IPv6 network is to use *Stateless Address Auto Configuration (SLAAC)*. With SLAAC, devices send the router a request for the network prefix, and the device then uses the prefix along with its own MAC address to create an IP address.

## BOOT Protocol (BOOTP)

BOOTP was originally created so that diskless workstations could obtain information needed to connect to the network, such as the TCP/IP address, subnet mask, and default gateway. Such a system was necessary because diskless workstations had no way to store the information.

When a system configured to use BOOTP is powered up, it broadcasts for a BOOTP server on the network. If such a server exists, it compares the MAC address of the system issuing the BOOTP request with a database of entries. From this database, it supplies the system with the appropriate information. It can also notify the workstation about a file that it must run on BOOTP.

In the unlikely event that you use BOOTP, you should be aware that, like DHCP, it is a broadcast-based system. Therefore, routers must be configured to forward BOOTP broadcasts.

## Automatic Private IP Addressing

Automatic Private IP Addressing (APIPA) was introduced with Windows 98 and has been included in all subsequent Windows versions. The function of APIPA is that a system can give itself an IP address if it is incapable of receiving an address dynamically from a DHCP server. Then APIPA assigns the system an address from the 169.254.0.0 address range and configures an appropriate subnet mask (255.255.0.0). However, it doesn't configure the system with a default gateway address. As a result, communication is limited to the local network. So, if you can connect to other devices on a local network but can't reach the Internet, for example, it is likely that your DHCP server is down and you are currently using an APIPA address.

**ExamAlert**

If a system that does not support APIPA cannot get an address from a DHCP server, it typically assigns itself an IP address of 0.0.0.0. Keep this in mind when troubleshooting IP addressing problems on non-APIPA platforms.

The idea behind APIPA is that systems on a segment can communicate with each other if DHCP server failure occurs. In reality, the limited usability of APIPA makes it little more than a last resort. For example, imagine that a system is powered on while the DHCP server is operational and receives an IP address of 192.168.100.2. Then the DHCP server fails. Now, if the other systems on the segment are powered on and cannot get an address from the DHCP server because it is down, they would self-assign addresses in the

169.254.0.0 address range via APIPA. The systems with APIPA addresses would talk to each other, but they couldn't talk to a system that received an address from the DHCP server. Likewise, any system that receives an IP address via DHCP cannot talk to systems with APIPA-assigned addresses. This, and the absence of a default gateway, is why APIPA is of limited use in real-world environments.

**ExamAlert**

Be prepared to answer APIPA questions. Know what it is and how you can tell whether you have been assigned an APIPA address and why.

# Identifying MAC Addresses

Many times this book refers to MAC addresses and how certain devices use them. However, it has not yet discussed why MAC addresses exist, how they are assigned, and what they consist of.

**Note**

A MAC address is sometimes called a physical address because it is physically embedded in the interface (network interface card).

A MAC address is a 6-byte (48-bit) hexadecimal address that enables a NIC to be uniquely identified on the network. The MAC address forms the basis of network communication, regardless of the protocol used to achieve network connection. Because the MAC address is so fundamental to network communication, mechanisms are in place to ensure that duplicate addresses cannot be used.

To combat the possibility of duplicate MAC addresses being assigned, the *Institute of Electrical and Electronics Engineers (IEEE)* took over the assignment of MAC addresses. But rather than be burdened with assigning individual addresses, the IEEE decided to assign each manufacturer an ID and then let the manufacturer further allocate IDs. The result is that in a MAC address, the first 3 bytes define the manufacturer, and the last 3 are assigned by the manufacturer.

For example, consider the MAC address of the computer on which this book is being written: 00:D0:59:09:07:51. The first 3 bytes (00:D0:59) identify the manufacturer of the card. Because only this manufacturer can use this address,

it is known as the *organizational unique identifier (OUI)*. The last 3 bytes (09:07:51) are called the *universal LAN MAC address*: they make this interface unique. You can find a complete listing of organizational MAC address assignments at http://standards-oui.ieee.org/oui.txt.

Because MAC addresses are expressed in hexadecimal, only the numbers 0 through 9 and the letters *A* through *F* can be used in them. If you get an exam question about identifying a MAC address and some of the answers contain letters and numbers other than 0 through 9 and the letters *A* through *F*, you can immediately discount those answers.

You can discover the NIC's MAC address in various ways, depending on what system or platform you work on (several of the ways can be found at https://carleton.ca/its/help-centre/how-to-find-your-mac-address/). Table 3.6 defines various platforms and methods you can use to view an interface's MAC address.

TABLE 3.6 **Methods of Viewing the MAC Addresses of NICs**

| Platform | Method |
|---|---|
| Windows | Enter **ipconfig /all** at a command prompt. |
| Linux/some UNIX | Enter the **ifconfig -a** command. |
| Cisco router | Enter the **sh int interface name** command. |

ExamAlert

Be sure that you know the commands used to identify the MAC address in various operating system formats.

Just as there was fear that there would not be enough IP addresses for all the devices needed to access the Internet if we stayed with IPv4, there has also been considerable fear that there are not enough MAC addresses to assign. To deal with this, 64-bit addresses are now available. The IEEE refers to 48-bit addresses as *EUI-48* (for *extended unique identifier*) and longer addresses as *EUI-64*. It is projected that there are a sufficient number of 48-bit addresses to last for quite some time, but the IEEE is encouraging the adoption of the 64-bit addressing as soon as possible. EUI-64 is used to automatically configure IPv6 host addresses by using the MAC address of its interface to generate a 64-bit interface ID. The MAC address is split in two and "FFFE" is inserted into the middle. Then the 7th bit of the interface ID is inverted and EUI-64 uses hyphens between number sets instead of colons. A good explanation/overview can be found at https://community.cisco.com/t5/networking-documents/understanding-ipv6-eui-64-bit-address/ta-p/3116953.

**ExamAlert**

Be sure that you know what EUI-64 is for the exam.

# NAT and PAT

This chapter has defined many acronyms and continues to do so with NAT and PAT. Since the technologies are related, and commonly used, SNAT and DNAT are also touched on.

## NAT

The basic principle of *Network Address Translation (NAT)* is that many computers can "hide" behind a single IP address. The main reason you need to do this (as pointed out earlier in the section "IP Addressing") is that there aren't enough IPv4 addresses to go around. Using NAT means that only one registered IP address is needed on the system's external interface, acting as the gateway between the internal and external networks. Figure 3.4 shows an example of enabling NAT on a SOHO router.

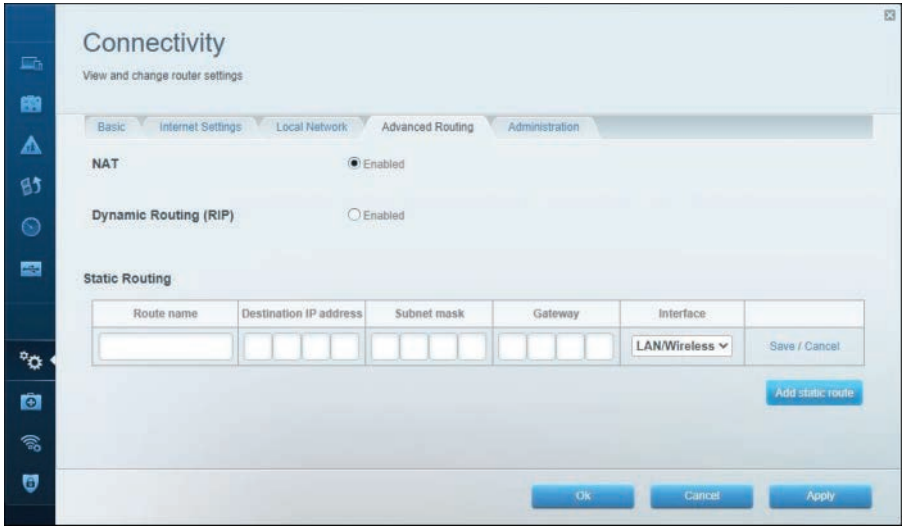



FIGURE 3.4 **NAT configuration on a SOHO router**

> **Note**
>
> Don't confuse NAT with proxy servers. The proxy service is different from NAT, but many proxy server applications do include NAT functionality.

NAT enables you to use whatever addressing scheme you like on your internal networks; however, it is common practice to use the private address ranges, which were discussed earlier.

When a system is performing NAT, it funnels the requests given to it to the Internet. To the remote host, the request looks like it is originating from a single address. The system performing the NAT function keeps track of who asked for what and makes sure that when the data is returned, it is directed to the correct system. Servers that provide NAT functionality do so in different ways. For example, you can statically map a specific internal IP address to a specific external one (known as the *one-to-one NAT method*) so that outgoing requests are always tagged with the same IP address. Alternatively, if you have a group of public IP addresses, you can have the NAT system assign addresses to devices on a first-come, first-served basis. Either way, the basic function of NAT is the same.

Tunneling can be used for transmitting packets of one type (such as IPv6) over another network (such as IPv4). *6to4* is one such tunneling technology, allowing IPv6 packets to be transmitted over an IPv4 network without having to create a complex tunnel. It is often used during the transition period when a network is being updated and is not intended to be a permanent solution. Its counterpart is *4to6*.

For a more long-term solution, there is a transition technology known as *Teredo* that gives full IPv6 connectivity for IPv6-capable hosts, which are on the IPv4 Internet but lack direct native connection to an IPv6 network. The distinguishing feature of Teredo is that it can do this from behind NAT devices (such as home routers). One of the most popular Teredo implementations is *Miredo*; it is a client designed to allow full IPv6 connectivity to systems that are strictly IPv4-based.

## PAT

NAT enables administrators to conserve public IP addresses and, at the same time, secure the internal network. *Port Address Translation (PAT)* is a variation on NAT. With PAT, all systems on the LAN are translated to the same IP address, but with a different port number assignment. PAT is used when multiple clients want to access the Internet. However, with not enough available public

IP addresses, you need to map the inside clients to a single public IP address. When packets come back into the private network, they are routed to their destination with a table within PAT that tracks the public and private port numbers.

When PAT is used, there is a typically only a single IP address exposed to the public network, and multiple network devices access the Internet through this exposed IP address. The sending devices, IP address, and port number are not exposed. For example, an internal computer with the IP address of 192.168.2.2 wants to access a remote web server at address 204.23.85.49. The request goes to the PAT router, where the sender's private IP and port number are modified, and a mapping is added to the PAT table. The remote web server sees the request coming from the IP address of the PAT router and not the computer actually making the request. The web server sends the reply to the address and port number of the router. When received, the router checks its table to see the packet's actual destination and forwards it.

**ExamAlert**

PAT enables nodes on a LAN to communicate with the Internet without revealing their IP address. All outbound IP communications are translated to the router's external IP address. Replies come back to the router, which then translates them back into the private IP address of the original host for final delivery.

## SNAT

*Static Network Address Translation (SNAT)* is a simple form of NAT. SNAT directly maps a private IP address to a static unchanging public IP address. This enables an internal system, such as a mail server, to have an unregistered (private) IP address and still be reachable over the Internet. For example, if a network uses a private address of 192.168.2.1 for a mail server, it can be statically linked to a public IP address such as 213.23.213.85.

## DNAT

To get more granular, *Destination Network Address Translation (DNAT)* can be implemented on any router to change the destination IP address on a packet (and do the inverse operation on replies). It is typically used between services located on a private network and IP addresses that are publicly accessible. It is more commonly referred to as *port forwarding*.

# Cram Quiz

1. What is the IPv6 equivalent of 127.0.0.1? (Choose two.)
   - ❍ **A.** 0:0:0:0:0:0:0:1
   - ❍ **B.** 0:0:0:0:0:0:0:24
   - ❍ **C.** ::1
   - ❍ **D.** ::24

2. Which of the following is a Class B address?
   - ❍ **A.** 129.16.12.200
   - ❍ **B.** 126.15.16.122
   - ❍ **C.** 211.244.212.5
   - ❍ **D.** 193.17.101.27

3. You are the administrator for a network with two Windows Server systems and 65 Windows desktop systems. At 10 a.m., three users call to report that they are experiencing network connectivity problems. Upon investigation, you determine that the DHCP server has failed. How can you tell that the DHCP server failure is the cause of the connectivity problems experienced by the three users?
   - ❍ **A.** When you check their systems, they have an IP address of 0.0.0.0.
   - ❍ **B.** When you check their systems, they have an IP address in the 192.168.x.x address range.
   - ❍ **C.** When you check their systems, they have a default gateway value of 255.255.255.255.
   - ❍ **D.** When you check their systems, they have an IP address from the 169.254.x.x range.

4. Which of the following address types are associated with IPv6? (Choose three.)
   - ❍ **A.** Broadcast
   - ❍ **B.** Multicast
   - ❍ **C.** Unicast
   - ❍ **D.** Anycast

5. Which of the following IP addresses is not from a private address range?
   - ❍ **A.** 192.168.200.117
   - ❍ **B.** 172.16.3.204
   - ❍ **C.** 127.45.112.16
   - ❍ **D.** 10.27.100.143

6. You have been assigned to set up a new network with TCP/IP. For the external interfaces, you decide to obtain registered IP addresses from your ISP, but for the internal network, you choose to configure systems by using one of the private address ranges. Of the following address ranges, which one would you not consider?
   - ❍ **A.** 192.168.0.0 to 192.168.255.255
   - ❍ **B.** 131.16.0.0 to 131.16.255.255
   - ❍ **C.** 10.0.0.0 to 10.255.255.255
   - ❍ **D.** 172.16.0.0 to 172.31.255.255

7. You ask your ISP to assign a public IP address for the external interface of your Windows server, which is running a proxy server application. In the email message that contains the information, the ISP tells you that you have been assigned the IP address 203.15.226.12/24. When you fill out the subnet mask field on the IP configuration dialog box on your system, what subnet mask should you use?
   - ❍ **A.** 255.255.255.255
   - ❍ **B.** 255.255.255.0
   - ❍ **C.** 255.255.240.0
   - ❍ **D.** 255.255.255.240

8. Examine the diagram shown here. What is the most likely reason that user Spencer cannot communicate with user Evan?

User: Evan
IP address: 192.168.1.121
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1

User: Spencer
IP address: 192.168.1.127
Subnet mask: 255.255.248.0
Default gateway: 192.168.1.1

   - ❍ **A.** The default gateways should have different values.
   - ❍ **B.** Spencer's IP address is not a loopback address.
   - ❍ **C.** The subnet values should be the same.
   - ❍ **D.** There is no problem identifiable by the values given.

# Cram Quiz Answers

1. **A and C.** The IPv4 address 127.0.0.1 is reserved as the loopback address, and IPv6 has the same reservation. IPv6 addresses 0:0:0:0:0:0:0:0 and 0:0:0:0:0:0:0:1 are reserved as the loopback addresses. The address 0:0:0:0:0:0:0:1 can be shown using the :: notation with the 0s removed, resulting in ::1.

2. **A.** Class B addresses fall into the range 128 to 191. Answer A is the only address listed that falls into that range. Answer B is a Class A address, and answers C and D are Class C IP addresses.
3. **D.** When a Windows desktop system that is configured to obtain an IP address via DHCP fails to obtain an address, it uses APIPA to assign itself an address from the 169.254.x.x address range. An address of 0.0.0.0 normally results from a system that does not support APIPA. APIPA does not use the 192.168.x.x address range. The IP address 255.255.255.255 is the broadcast address. A DHCP failure would not lead to a system assigning itself this address.
4. **B, C, and D.** A key difference between IPv4 and IPv6 is in the address types. IPv6 addressing has three main types of addresses: unicast, multicast, and anycast. IPv4 uses broadcast addressing, but IPv6 doesn't.
5. **C.** The 127.x.x.x network range is reserved for the loopback function. It is not one of the recognized private address ranges. The private address ranges as defined in RFC 1918 are 10.x.x.x, 172.16.x.x to 172.31.x.x, and 192.168.x.x.
6. **B.** The 131.16 range is from the Class B range and is not one of the recognized private IP address ranges. All the other address ranges are valid private IP address ranges.
7. **B.** In CIDR terminology, the number of bits to be included in the subnet mask is expressed as a slash value. If the slash value is 24, the first three octets form the subnet mask, so the value is 255.255.255.0.
8. **C.** The most likely problem, given the IP values for each user's workstation, is that the subnet value is not correct on Spencer's machine and should be 255.255.255.0.

# Managing Routing and Switching

- **Compare and contrast routing technologies and bandwidth management concepts.**
- **Given a scenario, configure and deploy common Ethernet switching features.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What are the most common distance-vector routing protocols?
2. What are the most common link-state protocols?
3. What is convergence?
4. What term is used when specific routes are combined into one route?
5. True or false: With the help of FSL, STP avoids or eliminates loops on Layer 2 bridges.

### Answers

1. Distance-vector routing protocols include RIP, RIPv2, and EIGRP. Of these, RIPv2 would be the most popular from the exam's perspective.
2. Link-state protocols include OSPF and IS-IS.
3. Convergence represents the time it takes routers to detect change on the network.
4. The term *route aggregation* applies when specific routes are combined into one route.
5. False. With the help of Spanning Tree Algorithm (STA), STP avoids or eliminates loops on a Layer 2 bridge.

Because today's networks branch out between interconnected offices all over the world, networks may have any number of separate physical network segments connected using routers. Routers are devices that direct data between networks. Essentially, when a router receives data, it must determine the destination for the data and send it there. To accomplish this, the network router uses two key pieces of information: the gateway address and the routing tables.

## The Default Gateway

A default gateway is the router's IP address, which is the pathway to any and all remote networks. To get a packet of information from one network to another,

the packet is sent to the default gateway, which helps forward the packet to its destination network. Computers that live on the other side of routers are said to be on remote networks. Without default gateways, Internet communication is not possible because your computer does not have a way to send a packet destined for any other network. On the workstation, it is common for the default gateway option to be configured automatically through DHCP configuration.

# Routing Tables

Before a data packet is forwarded, a chart is reviewed to determine the best possible path for the data to reach its destination. This chart is the computer's routing table. Maintaining an accurate routing table is essential for effective data delivery. Every computer on a TCP/IP network has a routing table stored locally. Figure 3.5 shows the routing table on a Windows system.

**Note**

You can use the **route print** command to view the routing table on a client system.

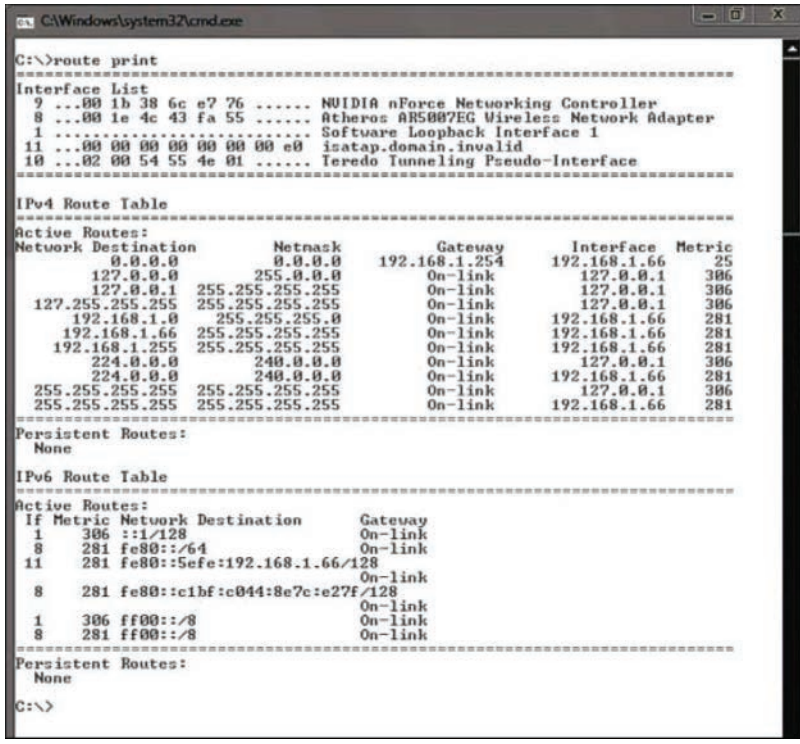



FIGURE 3.5 **The routing table on a Windows system**

As shown in Figure 3.5, the information in the routing table includes the following:

- **Network Destination:** The host IP address.
- **Netmask:** The subnet mask value for the destination parameter.
- **Gateway:** Where the IP address is sent. This may be a gateway server, a router, or another system acting as a gateway.
- **Interface:** The address of the interface that's used to send the packet to the destination.
- **Metric:** A measurement of the directness of a route. The lower the metric, the faster the route. If multiple routes exist for data to travel, the one with the lowest metric is chosen.

Routing tables play an important role in the network routing process. They are the means by which the data is directed through the network. For this reason, a routing table needs to be two things. It must be up to date and complete. The router can get the information for the routing table in two ways: through static routing or dynamic routing.

# Static Routing

In environments that use *static routing*, routes and route information are manually entered into the routing tables. Not only can this be a time-consuming task, but also errors are more common. In addition, when a change occurs to the network's layout, or topology, statically configured routers must be manually updated with the changes. Again, this is a time-consuming and potentially error-laden task. For these reasons, static routing is suited to only the smallest environments, with perhaps just one or two routers. A far more practical solution, particularly in larger environments, is to use dynamic routing.

You can add a static route to a routing table using the **route add** command. To do this, specify the route, the network mask, and the destination IP address of the network card your router will use to get the packet to its destination network.

The syntax for the **route add** command is as follows:

```
route add 192.168.2.1 mask (255.255.255.0) 192.168.2.4
```

Adding a static address is not permanent; in other words, it will most likely be gone when the system reboots. To make it persistent (the route is still in the routing table on boot), you can use the **-p** switch with the command.

ExamAlert

The **route add** command adds a static route to the routing table. The **route add** command with the **-p** switch makes the static route persistent. You might want to try this on your own before taking the Network+ exam.

*Distributed switching* is typically associated with telephone networks and is nothing more than an architecture in which multiple processor-controlled switching units are distributed. In this environment, there is usually a hierarchy of switches, with a centralized host switch working with remote switches located close to concentrations of users.

# Default Route

In environments that use dynamic routing, there is usually one static route defined that this known as the *default route*. The default route, sometimes called the route (or gateway) of last resort, specifies the path to be used if no other route is known (no next-hop host is available from the routing table or other routing mechanisms). All packets with unknown destination addresses are sent to the default route.

# Switching Methods

For systems to communicate on a network, the data needs a communication path or multiple paths on which to travel. To allow entities to communicate, these paths move the information from one location to another and back. This is the function of *switching*, which provides communication pathways between two endpoints and manages how data flows between them. Following are two of the more common switching methods used today:

- Packet switching
- Circuit switching

ExamAlert

You will be expected to identify the different switching features.

## Packet Switching

In packet switching, messages are broken into smaller pieces called *packets*. Each packet is assigned source, destination, and intermediate node addresses. Packets are required to have this information because they do not always use the same

path or route to get to their intended destination. Referred to as *independent routing*, this is one of the advantages of packet switching. Independent routing enables better use of available bandwidth by letting packets travel different routes to avoid high-traffic areas. Independent routing also enables packets to take an alternative route if a particular route is unavailable for some reason.

> **Note**
>
> Packet switching is the most popular switching method for networks and is used on most WANs.

In a packet-switching system, when packets are sent onto the network, the sending device is responsible for choosing the best path for the packet. This path might change in transit, and the receiving device can receive the packets in a random or nonsequential order. When this happens, the receiving device waits until all the data packets are received, and then it reconstructs them according to their built-in sequence numbers.

Two types of packet-switching methods are used on networks:

- **Virtual-circuit packet switching:** A logical connection is established between the source and the destination device. This logical connection is established when the sending device initiates a conversation with the receiving device. The logical communication path between the two devices can remain active for as long as the two devices are available or can be used to send packets once. After the sending process has completed, the line can be closed.
- **Datagram packet switching:** Unlike virtual-circuit packet switching, datagram packet switching does not establish a logical connection between the sending and transmitting devices. The packets in datagram packet switching are independently sent, meaning that they can take different paths through the network to reach their intended destination. To do this, each packet must be individually addressed to determine its source and destination. This method ensures that packets take the easiest possible routes to their destination and avoid high-traffic areas. Datagram packet switching is mainly used on the Internet.

## Circuit Switching

In contrast to the packet-switching method, circuit switching requires a dedicated physical connection between the sending and receiving devices. The most commonly used analogy to represent circuit switching is a telephone conversation in which the parties involved have a dedicated link between them

for the duration of the conversation. When either party disconnects, the circuit is broken, and the data path is lost. This is an accurate representation of how circuit switching works with network and data transmissions. The sending system establishes a physical connection, and the data is transmitted between the two. When the transmission is complete, the channel is closed.

Some clear advantages to the circuit-switching technology make it well suited for certain applications, such as *public switched telephone network (PSTN)* and *Integrated Services Digital Network (ISDN)*. The primary advantage is that after a connection is established, a consistent and reliable connection exists between the sending and receiving devices. This allows for transmissions at a guaranteed rate of transfer.

Like all technologies, circuit switching has its downsides. As you might imagine, a dedicated communication line can be inefficient. After the physical connection is established, it is unavailable to any other sessions until the transmission completes. Again, using the phone call analogy, this would be like a caller trying to reach another caller and getting a busy signal. Circuit switching therefore can be fraught with long connection delays.

## Comparing Switching Methods

Table 3.7 provides an overview of the various switching technologies.

TABLE 3.7 **Comparison of Switching Methods**

| Switching Method | Pros | Cons | Key Features |
|---|---|---|---|
| Packet switching | Packets can be routed around network congestion. Packet switching makes efficient use of network bandwidth. | Packets can become lost while taking alternative routes to the destination. Messages are divided into packets that contain source and destination information. | The two types of packet switching are datagram and virtual circuit. Datagram packets are independently sent and can take different paths throughout the network. Virtual circuit uses a logical connection between the source and destination devices. |
| Circuit switching | Circuit switching offers a dedicated transmission channel that is reserved until it is disconnected. | Dedicated channels can cause delays because a channel is unavailable until one side disconnects. Circuit switching uses a dedicated physical link between the sending and receiving devices. | Circuit switching offers the capability of storing messages temporarily to reduce network congestion. |

# Dynamic Routing

In a *dynamic routing* environment, routers use special routing protocols to communicate. The purpose of these protocols is simple: they enable routers to pass on information about themselves to other routers so that other routers can build routing tables. Two types of routing protocols are used: the older distance-vector protocols and the newer link-state protocols. A third type, hybrid, combines features of these two.

> **Note**
>
> The use of any routing protocol to advertise routes that have been learned (through another protocol, through static configuration, and so on) is known as *route redistribution*.

## Distance-Vector Routing

With distance-vector router communications, each router on the network communicates all the routes it knows about to the routers to which it is directly attached. In this way, routers communicate only with their router neighbors and are unaware of other routers that may be on the network.

The communication between distance-vector routers is known as *hops*. On the network, each router represents one hop, so a network using six routers has five hops between the first and last router.

The **tracert** command is used in a Windows environment to see how many hops a packet takes to reach a destination (the same functionality exists in macOS and Linux with the **traceroute** command). To try this at the command prompt, enter **tracert comptia.org**. Figure 3.6 shows an example of the output on a Windows workstation.

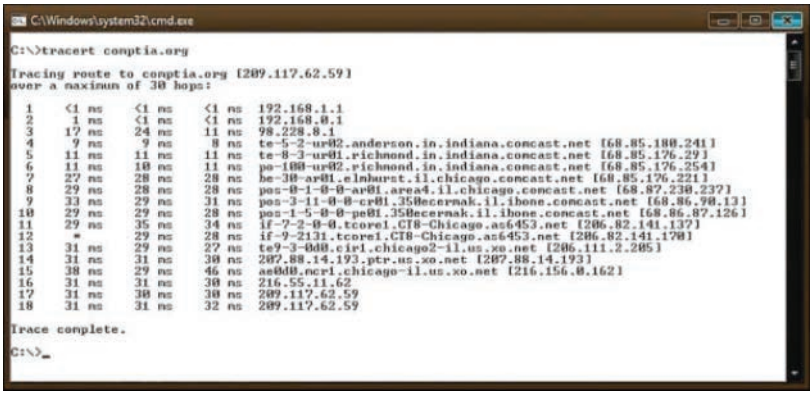



FIGURE 3.6 **The results of running tracert on a Windows system**

In addition to the **tracert** command in IPv4, you can get similar functionality in IPv6 with **tracert -6**, **traceroute6**, and **traceroute -6**.

Several distance-vector protocols are in use today, including Routing Information Protocol (RIP and RIPv2), and *Enhanced Interior Gateway Routing Protocol (EIGRP)*:

- **RIP:** As mentioned earlier, RIP is a distance-vector routing protocol. RIP is limited to a maximum of 15 hops. One of the downsides of the protocol is that the original specification required router updates to be transmitted every 30 seconds. On smaller networks this is acceptable; however, this can result in a huge traffic load on larger networks. The original RIP specification also did not support router authentication, leaving it vulnerable to attacks.
- **RIPv2:** The second version of RIP dealt with the shortcomings of the original design. Authentication was included to enable secure transmissions; also, it changed from a network-wide broadcast discovery method to a multicast method to reduce overall network traffic. However, to maintain compatibility with RIP, RIPv2 still supports a limit of 15 hops.
- **EIGRP:** This protocol enables routers to exchange information more efficiently than earlier network protocols. EIGRP uses its neighbors to help determine routing information. Routers configured to use EIGRP keep copies of their neighbors' routing information and query these tables to help find the best possible route for transmissions to follow. EIGRP uses *Diffusing Update Algorithm (DUAL)* to determine the best route to a destination.

**ExamAlert**

Be sure that you can identify the differences between the distance-vector protocols discussed here.

**Note**

Just as with DNS (discussed in Chapter 2), a TTL (time to live) value can be set with routing. In this case, the TTL value will equal the amount of time or number of hops that a packet can reach at a maximum before being discarded by a router.

Distance-vector routing protocols operate by having each router send updates about all the other routers it knows about to the routers directly connected to

it. The routers use these updates to compile their routing tables. The updates are sent automatically every 30 or 60 seconds. The interval depends on the routing protocol used. Apart from the periodic updates, routers can also be configured to send a *triggered update* if a change in the network topology is detected. The process by which routers learn of a change in the network topology is called *convergence*.

Routing loops can occur on networks with slow convergence. Routing loops occur when the routing tables on the routers are slow to update and a redundant communication cycle is created between routers. Two strategies can combat potential routing loops:

- **Split horizon:** Works by preventing the router from advertising a route back to the other router from which it was learned. This prevents two nodes from bouncing packets back and forth between them, creating a loop.
- **Poison reverse (also called split horizon with poison reverse):** Dictates that the route is advertised back on the interface from which it was learned, but it has a hop count of infinity, which tells the node that the route is unreachable.

**ExamAlert**

If a change in the routing is made, it takes some time for the routers to detect and accommodate this change. This is known as *convergence*.

Although distance-vector protocols can maintain routing tables, they have three problems:

- The periodic update system can make the update process slow.
- The periodic updates can create large amounts of network traffic—much of the time unnecessarily, because the network's topology should rarely change.
- Perhaps the most significant problem is that because the routers know about only the next hop in the journey, incorrect information can be propagated between routers, creating routing loops.

**ExamAlert**

Know that "next hop" in routing is the next closest router that a packet can go through.

## Link-State Routing

A router that uses a link-state protocol differs from a router that uses a distance-vector protocol because it builds a map of the entire network and then holds that map in memory. On a network that uses a link-state protocol, routers send *link-state advertisements (LSAs)* that contain information about the networks to which they connect. The LSAs are sent to every router on the network, thus enabling the routers to build their network maps.

When the network maps on each router are complete, the routers update each other at a given time, just like with a distance-vector protocol; however, the updates occur much less frequently with link-state protocols than with distance-vector protocols. The only other circumstance under which updates are sent is if a change in the topology is detected, at which point the routers use LSAs to detect the change and update their routing tables. This mechanism, combined with the fact that routers hold maps of the entire network, makes convergence on a link-state-based network quickly occur.

Although it might seem like link-state protocols are an obvious choice over distance-vector protocols, routers on a link-state-based network require more powerful hardware and more RAM than those on a distance-vector-based network. Not only do the routing tables need to be calculated, but they must also be stored. A router that uses distance-vector protocols need only maintain a small database of the routes accessible by the routers to which it is directly connected. A router that uses link-state protocols must maintain a database of all the routers in the entire network.

Link-state protocols include the following:

- **Open Shortest Path First (OSPF):** A link-state routing protocol based on the *shortest path first (SPF)* algorithm to find the least-cost path to any destination in the network. In operation, each router using OSPF sends a list of its neighbors to other routers on the network. From this information, routers can determine the network design and the shortest path for data to travel.
- **Intermediate System-to-Intermediate System (IS-IS):** A link-state protocol that discovers the shortest path for data to travel using the SPF algorithm. IS-IS routers distribute topology information to other routers, enabling them to make the best path decisions.

So, what's the difference between the two? OSPF (a network layer protocol) is more often used in medium to large enterprise networks because of its special tunneling features. IS-IS is more often used in large ISP networks because of its stability features and because it can support more routers.

### IGP Versus EGP

Now that routing protocols have been discussed, you need to understand the difference between *interior gateway protocols (IGPs)* and *exterior gateway protocols (EGPs)*. An IGP identifies the protocols used to exchange routing information between routers within a LAN or interconnected LANs. IGP is not a protocol itself but describes a category of link-state routing protocols that support a single, confined geographic area such as a LAN. IGPs fall into two categories: distance-vector protocols, which include RIPv2, and link-state protocols, which include OSPF and IS-IS.

Whereas IGPs are geographically confined, EGPs are used to route information outside the network, such as on the Internet. On the Internet, an EGP is required. An EGP is a distance-vector protocol commonly used between hosts on the Internet to exchange routing table information. *Border Gateway Protocol (BGP)* is an example of an EGP.

## Hybrid Routing Protocols

When you want the best of both worlds, distance vector and link state, you can turn to a hybrid protocol. The one hybrid protocol to know for this exam is the *Border Gateway Protocol (BGP)*. BGP can be used between gateway hosts on the Internet. BGP examines the routing table, which contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. BGP communicates between the routers using TCP. BGP supports the use of *autonomous system numbers (ASNs)*, which are globally unique numbers used by connected groups of IP networks that share the same routing policy.

ExamAlert

Be prepared to identify the link-state and distance-vector routing protocols used on TCP/IP networks, as well as the BGP hybrid.

## Network Traffic

Network access methods govern how systems access the network media and send data. Access methods are necessary to ensure that systems on the network can communicate with each other. Without an access method, two systems could communicate at the exclusion of every other system. Access methods ensure that everyone gets an opportunity to use the network.

Several access methods are used in networks; the most popular are CSMA/CD and CSMA/CA. Look at CSMA/CD first and then CSMA/CA.

*Carrier Sense Multiple Access/Collision Detection (CSMA/CD)*, which is defined in the IEEE 802.3 standard, is the most common media access method because it

is associated with 802.3 Ethernet networking, which is by far the most popular networking standard. CSMA/CD is a Media Access Control (MAC) protocol.

On a network that uses CSMA/CD, when a system wants to send data to another system, it first checks to see whether the network medium is free. It must do this because each piece of network medium used in a LAN can carry only one signal at a time. If the sending node detects that the medium is free, it transmits, and the data is sent to the destination. It seems simple.

Now, if it always worked like this, you wouldn't need the CD part of CSMA/CD. Unfortunately, in networking, as in life, things do not always go as planned. The problem arises when two systems attempt to transmit at the same time. It might seem unlikely that two systems would pick the same moment to send data, but you are dealing with communications that occur many times in a single second—and most networks have more than two machines. Imagine that 200 people are in a room. The room is silent, but then two people decide to say something at the same time. Before they start to speak, they check (listen) to see whether someone else is speaking; because no one else is speaking, they begin to talk. The result is two people speaking at the same time, which is similar to a network collision.

Collision detection works by detecting fragments of the transmission on the network media that result when two systems try to talk at the same time. The two systems wait for a randomly calculated amount of time before attempting to transmit again. This amount of time—a matter of milliseconds—is known as the *backoff* period or jam signal.

**ExamAlert**

Know that collisions do occur with CSMA. You can detect them (CD) or attempt to avoid them (CA).

When the backoff period has elapsed, the system attempts to transmit again. If the system does not succeed on the second attempt, it keeps retrying until it gives up and reports an error.

**ExamAlert**

CSMA/CD is known as a contention media access method because systems contend for access to the media.

The upside of CSMA/CD is that it has relatively low overhead, meaning that not much is involved in the workings of the system. The downside is that as

more systems are added to the network, more collisions occur, and the network becomes slower. The performance of a network that uses CSMA/CD degrades exponentially as more systems are added. Its low overhead means that CSMA/CD systems theoretically can achieve greater speeds than high-overhead systems. However, because collisions take place, the chance of all that speed translating into usable bandwidth is relatively low.

**ExamAlert**

On a network that uses CSMA/CD, every node has equal access to the network media.

Despite its problems, CSMA/CD is an efficient system. As a result, rather than replace it with some other technology, workarounds have been created that reduce the likelihood of collisions. One such strategy is the use of network switches that create multiple collision domains and therefore reduce the impact of collisions on performance.

Instead of collision detection, as with CSMA/CD, the *Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)* access method uses signal avoidance rather than detection. In a networked environment, CSMA/CA is the access mechanism used with the 802.11 wireless standards.

On CSMA/CA networks, each computer signals its intent to transmit data before any data is actually sent. When a networked system detects a potential collision, it waits before sending the transmission, allowing systems to avoid transmission collisions. The CSMA/CA access method uses a random backoff time that determines how long to wait before trying to send data on the network. When the backoff time expires, the system again "listens" to verify a clear channel on which to transmit. If the medium is still busy, another backoff interval is initiated that is less than the first. The process continues until the wait time reaches zero, and the medium is clear.

CSMA/CA uses a broadcast method to signal its intention to transmit data. Network broadcasts create a considerable amount of network traffic and can cause network congestion, which could slow down the entire network. Because CSMA/CD and CSMA/CA differ only in terms of detection and avoidance, they have similar advantages and disadvantages.

**ExamAlert**

CSMA/CA is the access mechanism used with the 802.11 wireless standards. Know that CSMA/CA uses broadcasts.

**Note**

The CSMA/CA access method uses a "listen before talking" strategy. Any system wanting to transmit data must first verify that the channel is clear before transmitting, thereby avoiding potential collisions.

# Routing Metrics

Following are several metrics related to routing that you should know for the exam:

- *Hop counts* are the number of hops necessary to reach a node. A hop count of infinity means the route is unreachable.
- The *maximum transmission unit (MTU)* defines the largest data unit that can be passed without fragmentation.
- *Bandwidth* specifies the maximum packet size permitted for Internet transmission.
- *Costs* are the numbers associated with traveling from point A to point B (often hops). The lower the total costs (the fewer links in the route), the more that route should be favored.
- *Administrative distance* is a numerical value assigned to a route based on its perceived quality. The number may be manually assigned, or assigned based on an algorithm employed by a routing protocol. The lower the number, the better the route is believed to be: 0 is the best and 255 is the worst.
- *Latency* is the amount of time it takes for a packet to travel from one location to another.

In the following section, we look at Spanning Tree Protocols, but before we do, it is important to point out here that they are being replaced by *shortest path bridging (SPB)*, based on IEEE 802.1aq. The big advantage of SPB is that it allows for multiple equal cost paths, leading to faster convergence times and improving the use of mesh topologies for increased bandwidth.

# Virtual Local-Area Networks

The word *virtual* is used a lot in the computing world—perhaps too often. For virtual local-area networks (VLANs), the word *virtual* does little to help explain the technology. Perhaps a more descriptive name for the VLAN concept might have been *segmented*. For now at least, use *virtual*.

**Tip**

802.1Q is the Institute of Electrical and Electronics Engineers (IEEE) specification developed to ensure interoperability of VLAN technologies from the various vendors.

VLANs are used for network segmentation, a strategy that significantly increases the network's performance capability, removes potential performance bottlenecks, and can even increase network security. A VLAN is a group of connected computers that act as if they are on their own network segment, even though they might not be. For instance, suppose that you work in a three-story building in which the advertising employees are spread over all three floors. A VLAN can enable all the advertising personnel to be combined and access network resources as if they were connected on the same physical segment. This virtual segment can be isolated from other network segments. In effect, it would appear to the advertising group that they were on a network by themselves.

**ExamAlert**

VLANs enable you to create multiple broadcast domains on a single switch. In essence, this is the same as creating separate networks for each VLAN.

VLANs offer some clear advantages. Logically segmenting a network gives administrators flexibility beyond the restrictions of the physical network design and cable infrastructure. VLANs enable easier administration because the network can be divided into well-organized sections. Furthermore, you can increase security by isolating certain network segments from others. For example, you can segment the marketing personnel from finance or the administrators from the students. VLANs can ease the burden on overworked routers and reduce broadcast storms. Table 3.8 summarizes the benefits of VLANs.

TABLE 3.8 **Benefits of VLANs**

| Advantage | Description |
|---|---|
| Increased security | With the creation of logical (virtual) boundaries, network segments can be isolated. |
| Increased performance | By reducing broadcast traffic throughout the network, VLANs free up bandwidth. |
| Organization | Network users and resources that are linked and that communicate frequently can be grouped in a VLAN. |
| Simplified administration | With a VLAN the network administrator's job is easier when moving users between LAN segments, recabling, addressing new stations, and reconfiguring switches and routers. |

*VLAN Trunking Protocol (VTP)*, a Cisco proprietary protocol, is used to reduce administration in the switched network. You can, for example, put all switches in the same VTP domain and reduce the need to configure the same VLAN everywhere.

*Trunking* falls under 802.1Q and a trunk port is one that is assigned to carry traffic for a specific switch (as opposed to an access port). The trunk port is usually fiber optic and used to interconnect switches to make a network, to interconnect LANs to make a WAN, and so on.

ExamAlert

IEEE 802.1Q also focuses on tagging and untagging in VLANs. *Tagging* means that the port will send out a packet with a header that has a tag number that matches its VLAN tag number. On any given port you can have just one *untagged* VLAN, and that will be the default port traffic will go to unless it is tagged to go elsewhere.

*Port binding* determines whether and how a port is bound. This can be done in one of three ways: static, dynamic, or ephemeral. Conversely, *port aggregation* is the combining of multiple ports on a switch, and it can be done in one of three ways: auto, desirable, or on.

The *Link Aggregation Control Protocol (LACP)* is a common aggregation protocol that enables multiple physical ports to be bound together. Most devices allow you to bind up to four, but some go up to eight.

## VLAN Membership

You can use several methods to determine VLAN membership or how devices are assigned to a specific VLAN. The following sections describe the common methods to determine how VLAN membership is assigned:

- **Protocol-based VLANs:** With protocol-based VLAN membership, computers are assigned to VLANs using the protocol in use and the Layer 3 address. For example, this method enables a particular IP subnet to have its own VLAN.

  The term *Layer 3 address* refers to one of the most important networking concepts, the Open Systems Interconnection (OSI) reference model. This conceptual model, created by the *International Organization for Standardization (ISO)* in 1978 and revised in 1984, describes a network architecture that enables data to be passed between computer systems. There are seven layers in total, which are discussed in detail in Chapter 2. In brief, Layer 3, known as the *network layer*, identifies the mechanisms

by which data can be moved between two networks or systems, such as transport protocols, which in the case of TCP/IP is IP.

Although VLAN membership may be based on Layer 3 information, this has nothing to do with routing or routing functions. The IP numbers are used only to determine the membership in a particular VLAN, not to determine routing.

- **Port-based VLANs:** Port-based VLANs require that specific ports on a network switch be assigned to a VLAN. For example, ports 1 through 4 may be assigned to marketing, ports 5 through 7 may be assigned to sales, and so on. Using this method, a switch determines VLAN membership by taking note of the port used by a particular packet. Figure 3.7 shows how the ports on a server could be used for port-based VLAN membership.

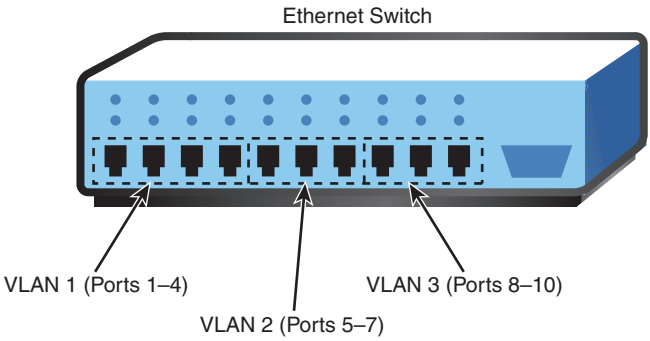



FIGURE 3.7 **Port-based VLAN membership**

- **MAC address-based VLANs:** The *Media Access Control (MAC)* address is a unique 12-digit hexadecimal number that is stamped into every network interface card. Every device used on a network has this unique address built in to it. It cannot be modified in any way. As you may have guessed, the MAC address type of a VLAN assigns membership according to the workstation's MAC address. To do this, the switch must keep track of the MAC addresses that belong to each VLAN. The advantage of this method is that a workstation computer can be moved anywhere in an office without needing to be reconfigured. Because the MAC address does not change, the workstation remains a member of a particular VLAN. Table 3.9 provides examples of the membership of MAC address-based VLANs.

TABLE 3.9 **MAC Address-Based VLANs**

| MAC Address | VLAN | Description |
|---|---|---|
| 44-45-53-54-00-00 | 1 | Sales |
| 44-45-53-54-13-12 | 2 | Marketing |
| 44-45-53-54-D3-01 | 3 | Administration |
| 44-45-53-54-F5-17 | 1 | Sales |

# VLAN Segmentation

The capability to logically segment a LAN provides a level of administrative flexibility, organization, and security. Whether the LAN is segmented using the protocol, MAC address, or port, the result is the same: the network is segmented. The segmentation is used for several reasons, including security, organization, and performance. To give you a better idea of how this works, Figure 3.8 shows a network that doesn't use a VLAN.

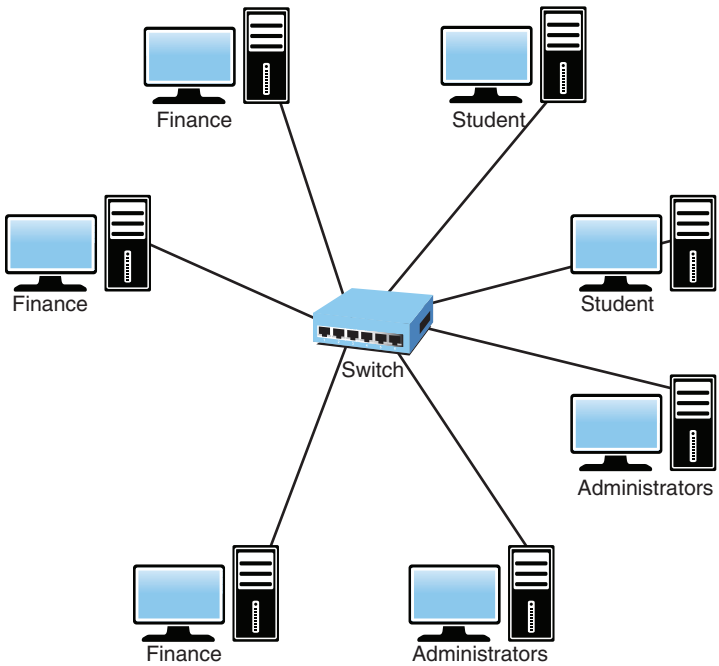



FIGURE 3.8 **Network configuration without using a VLAN**

In Figure 3.8, all systems on the network can see each other. That is, the students can see the finance and administrator computers. Figure 3.9 shows how this network may look using a VLAN.

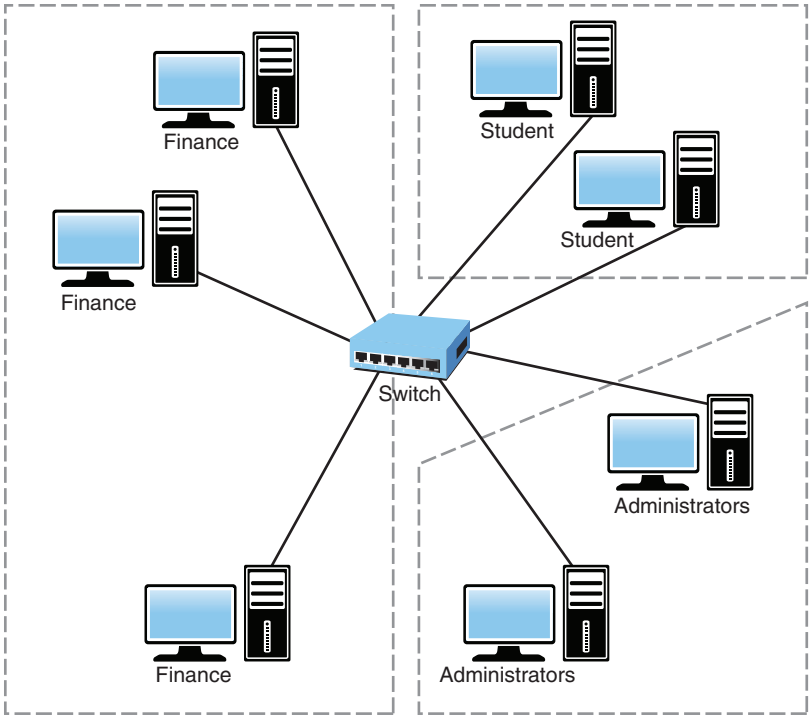



FIGURE 3.9 **Network configuration using a VLAN**

**ExamAlert**

Remember that one of the primary purposes of segmentation is to protect sensitive information from other hosts or the rest of the network in general.

# The Spanning Tree Protocol

An Ethernet network can have only a single active path between devices on a network. When multiple active paths are available, switching loops can occur. Switching loops are the result of having more than one path between two switches in a network. *Spanning Tree Protocol (STP)* is designed to prevent these loops from occurring.

STP is used with network bridges and switches. With the help of *Spanning Tree Algorithm (STA)*, STP avoids or eliminates loops on a Layer 2 bridge.

> **Note**
>
> As a heads up, talking about STP refers to Layer 2 of the OSI model. Both bridges and most switches work at Layer 2; routers work at Layer 3, as do Layer 3 switches.

STA enables a bridge or switch to dynamically work around loops in a network's topology. Both STA and STP were developed to prevent loops in the network and provide a way to route around any failed network bridge or ports. If the network topology changes, or if a switch port or bridge fails, STA creates a new spanning tree, notifies the other bridges of the problem, and routes around it. STP is the protocol, and STA is the algorithm STP uses to correct loops.

If a particular port has a problem, STP can perform a number of actions, including blocking the port, disabling the port, or forwarding data destined for that port to another port. It does this to ensure that no redundant links or paths are found in the spanning tree and that only a single active path exists between any two network nodes.

STP uses *bridge protocol data units (BPDUs)* to identify the status of ports and bridges across the network. BPDUs are simple data messages exchanged between switches. BPDUs contain information on ports and provide the status of those ports to other switches. If a BPDU message finds a loop in the network, it is managed by shutting down a particular port or bridge interface.

Redundant paths and potential loops can be avoided within ports in several ways:

- **Blocking:** A blocked port accepts BPDU messages but does not forward them.
- **Disabled:** The port is offline and does not accept BPDU messages.
- **Forwarding:** The port is part of the active spanning tree topology and forwards BPDU messages to other switches.
- **Learning:** In a learning state, the port is not part of the active spanning tree topology but can take over if another port fails. Learning ports receive BPDUs and identify changes to the topology when made.
- **Listening:** A listening port receives BPDU messages and monitors for changes to the network topology.

Most of the time, ports are in either a forwarding or blocked state. When a disruption to the topology occurs or a bridge or switch fails for some reason, listening and learning states are used.

**ExamAlert**

STP actively monitors the network, searching for redundant links. When it finds some, it shuts them down to prevent switching loops. STP uses STA to create a topology database to find and then remove the redundant links. With STP operating from the switch, data is forwarded on approved paths, which limits the potential for loops.

# Interface Configuration and Switch Management

Aside from VLAN trunking (802.1Q), binding, and a number of other possibilities previously discussed in this chapter, when you configure a switch interface, there are often other options that you can choose or tweak. They include the following:

- **Tag versus untag VLANs:** Tagging should be used if you are trunking. Because trunking combines VLANs, you need a way to identify which packet belongs to which VLAN; this is easily accomplished by placing a VLAN header (a *tag*) in the data packet. The only VLAN that is not tagged in a trunk is the *native VLAN*, and frames are transmitted to it unchanged.
- **Default VLAN:** The *default VLAN* is mandatory (cannot be deleted) and is used for communication between switches (such as configuring STP). In the Cisco world, the default VLAN is VLAN 1.
- **Flow control:** Ethernet provides a means of temporarily stopping the transmission of data to ensure zero packet loss in the presence of network congestion. This is accomplished using *flow control* and the pause frame. First appearing as a part of the IEEE 802.3x standard, it was further expanded upon in the IEEE 802.1Qbb standard.
- **Port mirroring:** Also known as port spanning, port mirroring is covered in more detail later in this chapter.
- **Port security:** Port security works at Layer 2 of the OSI model and allows an administrator to configure switch ports so that only certain MAC addresses can use the port. This essentially differentiates so-called

dumb switches from managed (or intelligent) switches. Three main areas of port security are (1) MAC limiting and filtering (limit access to the network to MAC addresses that are known, and filter out those that are not); (2) 802.1X (adding port authentication to MAC filtering takes security for the network down to the switch port level and increases your security exponentially); and (3) blocking unused ports (all ports not in use should be disabled).

- **Authentication, accounting, and authorization (AAA):** AAA overrides can also be configured for network security parameters as needed. AAA is the primary method for access control and often uses RADIUS, TACACS+, or Kerberos to accomplish integrated security.
- **Usernames/passwords:** It is possible to configure, without AAA, local username authentication using a configured username and password. This does not provide the same level of access control as AAA does and is not recommended.
- **Virtual consoles and terminals:** The console port (often called the *virtual console* or *VC*) is often a serial or parallel port, and it is possible for virtual ports to connect to physical ports. The *virtual terminal* (vt or vty) is a remote port connected to through Telnet or a similar utility and, as an administrator, you will want to configure an access list to limit who can use it.

ExamAlert

Know that the simplest way to protect a virtual terminal interface is to configure a username and password for it and prevent unauthorized logins.

- **Jumbo Frames:** One of the biggest issues with networking is that data of various sizes is crammed into packets and sent across the medium. Each time this is done, headers are created (more data to process), along with any filler needed, creating additional overhead. To get around this, the concept of *jumbo frames* is used to allow for very large Ethernet frames; by sending a lot of data at once, the number of packets is reduced, and the data sent is less processor intensive.
- **Other:** Other common configuration parameters include the speed, whether duplexing will be used or not, IP addressing, and the default gateway. Duplexing determines the direction in which data can flow through the network media and is discussed in Chapter 5, "Cabling Solutions and Issues."

# MDI-X

One technology that simplifies crossovers is the *auto-medium-dependent interface crossover (MDI-X* to friends). This technology expands on MDI (medium dependent interface) and enables ports on newer network interfaces to detect if the connection would require a crossover: if it would, then it automatically chooses the configuration (MDI or MDI-X) needed to match the other end of the link.

# Trunking

In computer networking, the term *trunking* refers to the use of multiple network cables or ports in parallel to increase the link speed beyond the limits of any one cable or port. Sound confusing? If you have network experience, you might have heard the term *link aggregation*, which is essentially the same thing. It is using multiple cables to increase the throughput. The higher-capacity trunking link is used to connect switches to form larger networks.

> **Note**
>
> *Aggregation* is a popular term any time multiples are combined. The term *route aggregation* applies when specific routes are combined into one route, and this is accomplished in BGP with the aggregate-address command.

*VLAN trunking* is the application of trunking to the virtual LAN—now common with routers, firewalls, VMware hosts, and wireless access points. VLAN trunking provides a simple and cheap way to offer a nearly unlimited number of virtual network connections. The requirements are only that the switch, the network adapter, and the OS drivers all support VLANs. The *VLAN Trunking Protocol (VTP)* is a proprietary protocol from Cisco for just such a purpose.

# Port Mirroring

You need some way to monitor network traffic and monitor how well a switch works. This is the function of *port mirroring*, also known as port spanning. Port mirroring copies the traffic from all ports to a single port and disallows bidirectional traffic on that port. There are a number of reasons why port mirroring can be used (duplicating the data for one port and sending it to another). One of the most common is to monitor the traffic. This can be done locally or remotely—the latter using a remote protocol such as Remote Switched Port Analyzer (RSPAN) instead of Switched Port Analyzer (SPAN).

To use port mirroring, administrators configure a copy of all inbound and outbound traffic to go to a certain port. A protocol analyzer examines the data sent to the port and therefore does not interrupt the flow of regular traffic.

ExamAlert

Port mirroring enables administrators to monitor the traffic outbound and inbound to the switch.

# Port Authentication

Port authentication is what it sounds like—authenticating users on a port-by-port basis. One standard that specifies port authentication is the 802.1X standard, often associated with wireless security. Systems that attempt to connect to a LAN port must be authenticated. Those who are authenticated can access the LAN; those who are not authenticated get no further.

# Power over Ethernet (PoE and PoE+)

The purpose of *Power over Ethernet (PoE)* is pretty much described in its name. Essentially, PoE is a technology defined by 802.3af that enables electrical power to transmit over twisted-pair Ethernet cable. This was enhanced/extended in 2009 by 802.3at, also known as *Power over Ethernet plus (PoE+)*, to be able to provide more power (increasing from 12.95W to 25.5W) and raising the maximum current (from 350mA to 600mA).

The electrical current sent, along with data, can provide power to remote devices. These devices may include remote switches, wireless access points, *voice over IP (VoIP)* equipment, and more.

One of the key advantages of PoE is the centralized management of power. For instance, without PoE, all remote devices need to be independently powered. In the case of a power outage, each of these devices requires an *uninterruptible power supply (UPS)* to continue operating. A UPS is a battery pack that enables devices to operate for a period of time. With PoE supplying power, a UPS is required only in the main facility. In addition, centralized power management enables administrators to power remote equipment up or down.

ExamAlert

Know that PoE and PoE+ enable electrical power to transmit over twisted-pair Ethernet cable.

# MAC Address Table

It was mentioned earlier that the MAC (Media Access Control) address is a unique 12-digit hexadecimal number that is stamped into every network interface card. This value can be used by a switch to "switch" frames between LAN ports efficiently. When the switch receives a frame, it associates the MAC address of the sending network device with the LAN port on which it was received and dynamically builds a *MAC address table* by using the source address of the frames received. Then, when the switch receives a frame for a MAC destination address not listed in its address table, it floods the frame to all LAN ports of the same VLAN except the port that received the frame.

When a destination station replies, the switch adds the MAC source address and port ID to this address table. Now that it knows the value, the switch can then forward all subsequent frames to a single LAN port without flooding all LAN ports.

**ExamAlert**

For the exam, know that all Ethernet switching ports maintain MAC address tables.

If there were a situation in which DHCP were not enabled on the management port of a switch and it was necessary to connect to it, then the IP address of that device would need to be known and used to establish a connection.

# Switch Management

Devices can be managed several ways: using *Simple Network Management Protocol (SNMP)*, *Windows Management Instrumentation (WMI)*, or *Intelligent Platform Management Interface (IPMI)*. If the monitoring of devices is done remotely, this is known as *out-of-band management*; otherwise, it is known as *in-band management*.

**ExamAlert**

For the exam, associate in-band management with local management (the most common method) and out-of-band management with remote.

# Managed and Unmanaged

If the switch has any configuration interface or options, it is said to be *managed*. If it does not have any configuration interface or options, it is said to be *unmanaged*. Although not always the case, it is generally such that unmanaged devices are less-expensive plug-and-play devices intended for a home or small office.

# Quality of Service

*Quality of service (QoS)* describes the strategies used to manage and increase the flow of network traffic. QoS features enable administrators to predict bandwidth use, monitor that use, and control it to ensure that bandwidth is available to the applications that need it. These applications generally can be broken into two categories:

- **Latency sensitive:** These applications need bandwidth for quick delivery where network lag time impacts their effectiveness. This includes voice and video transfer. For example, *voice over IP (VoIP)* would be difficult to use if there were a significant lag time in the conversation.
- **Latency insensitive:** Controlling bandwidth also involves managing latency-insensitive applications. This includes bulk data transfers such as huge backup procedures and *File Transfer Protocol Secure (FTPS)* transfers.

With bandwidth limited, and networks becoming increasingly congested, it becomes more difficult to deliver latency-sensitive traffic. If network traffic continues to increase and you cannot always increase bandwidth, the choice is to prioritize traffic to ensure timely delivery. This is where QoS comes into play. QoS ensures the delivery of applications, such as videoconferencing (and related video applications), VoIP telephony, and unified communications without adversely affecting network throughput. QoS achieves more efficient use of network resources by differentiating between latency-insensitive traffic such as fax data and latency-sensitive streaming media.

Two important components of QoS are DSCP and CoS. *Differentiated services code point (also known as Diffserv)* is an architecture that specifies a simple and coarse-grained mechanism for classifying and managing network traffic and providing QoS on modern networks. *Class of service (CoS)* is a parameter that is used in data and voice to differentiate the types of payloads being transmitted.

One important strategy for QoS is priority queuing. Essentially, traffic is placed in order based on its importance of delivery time. All data is given access, but the more important and latency-sensitive data is given higher priority.

**ExamAlert**

Be sure that you understand QoS and the methods used to ensure QoS on networks. Know that it is used with high-bandwidth applications such as VoIP, video applications, and unified communications.

# Traffic Shaping

The demand for bandwidth on networks has never been higher. Internet and intranet applications demand a large amount of bandwidth. Administrators must ensure that despite all these demands, adequate bandwidth is available for mission-critical applications while few resources are dedicated to spam or peer-to-peer downloads. To do this, you need to monitor network traffic to ensure that data flows as you need it to.

The term *traffic shaping* describes the mechanisms used to control bandwidth usage on the network. With this, administrators can control who uses network bandwidth, for what purpose, and what time of day bandwidth can be used. Traffic shaping establishes priorities for data traveling to and from the Internet and within the network.

A packet shaper essentially performs two key functions: monitoring and shaping. Monitoring includes identifying where usage is high and the time of day. After that information is obtained, administrators can customize or shape bandwidth usage for the best needs of the network.

# Access Control Lists

When it comes to computing, many things serve a similar function and go by the name of an *access control list (ACL)*. When it comes to websites, determining which ones users can or cannot access is usually done through a list of allowed or nonallowed websites. When it comes to routing and switching, an ACL provides rules that are applied to port numbers or IP addresses that are available on a host or other Layer 3 device, each with a list of hosts and/or networks permitted to use the service.

Although these two uses of ACL may seem disparate, in both cases, the ACL is the list of what is allowed by the entity trying to access. An alternative approach that can serve the same purpose is to reverse the situation and deny access to all entities (pages or ports, depending on the case) except those that appear in an "allowed" list. This approach has high administrative overhead and can greatly limit the productivity benefits available.

**ExamAlert**

Remember that the ACL is a list of allowed or nonallowed services, ports, websites, and the like.

# ARP and RARP

*Address Resolution Protocol (ARP)*, which is defined in RFC 826, is responsible for resolving IP addresses to *Media Access Control (MAC)* addresses. When a system attempts to contact another host, IP first determines whether the other host is on the same network it is on by looking at the IP address. If IP determines that the destination is on the local network, it consults the ARP cache to see whether it has a corresponding entry. The ARP cache is a table on the local system that stores mappings between data link layer addresses (the MAC address or physical address) and network layer addresses (IP addresses). Following is a sample of the ARP cache:

```
Interface: 192.168.1.66 --- 0x8
Internet Address    Physical Address    Type
192.168.1.65        00-1c-c0-17-41-c8   dynamic
192.168.1.67        00-22-68-cb-e2-f9   dynamic
192.168.1.254       00-18-d1-95-f6-02   dynamic
224.0.0.2           01-00-5e-00-00-02   static
239.255.255.250     01-00-5e-7f-ff-fa   static
```

If the ARP cache does not have an entry for the host, a broadcast on the local network asks the host with the target IP address to send back its MAC address. The communication is sent as a broadcast because without the target system's MAC address, the source system cannot communicate directly with the target system.

Because the communication is a broadcast, every system on the network picks it up. However, only the target system replies because it is the only device whose IP address matches the request. The target system, recognizing that the ARP request is targeted at it, replies directly to the source system. It can do this because the ARP request contains the MAC address of the system that sent it. If the destination host is determined to be on a different subnet than the sending host, the ARP process is performed against the default gateway and then repeated for each step of the journey between the sending and receiving host. Table 3.10 lists the common switches used with the **arp** command.

**ExamAlert**

ARP links IP addressing to Ethernet addressing (MAC addressing).

TABLE 3.10 **Commonly Used ARP Command Switches**

| Switch | Description |
|---|---|
| **-a** | Displays the entries in the ARP cache |
| **-s** | Manually adds a permanent entry to the ARP cache |
| **-d** | Deletes an entry from the ARP cache |

When you work with the ARP cache, you can dynamically or statically make entries. With dynamic entries, the ARP cache is automatically updated. The ARP cache is maintained with no intervention from the user. Dynamic entries are the ones most used. Static entries are configured manually using the **arp -s** command. The static entry becomes a permanent addition to the ARP cache until it is removed using the **arp -d** command.

*Reverse Address Resolution Protocol (RARP)* performs the same function as ARP, but in reverse. In other words, it resolves MAC addresses to IP addresses. RARP makes it possible for applications or systems to learn their own IP address from a router or *Domain Name Service (DNS)* server. Such a resolution is useful for tasks such as performing reverse lookups in DNS. RARP is defined in RFC 903.

Tip

The function of ARP is to resolve a system's IP address to the interface's MAC address on that system. Do not confuse ARP with DNS or WINS, which also perform resolution functions, but for different things.

# Cram Quiz

1. Which of the following best describes the function of the default gateway?
   - ❍ **A.** It provides the route for destinations outside the local network.
   - ❍ **B.** It enables a single Internet connection to be used by several users.
   - ❍ **C.** It identifies the local subnet and formulates a routing table.
   - ❍ **D.** It is used to communicate in a multiple-platform environment.

2. What is the term used for the number of hops necessary to reach a node?
   - ❍ **A.** Jump list
   - ❍ **B.** Link stops
   - ❍ **C.** Connections
   - ❍ **D.** Hop count

3. Which of the following enables administrators to monitor the traffic outbound and inbound to the switch?

   - ❍ **A.** Spanning Tree Algorithm
   - ❍ **B.** Trunking
   - ❍ **C.** HSRP
   - ❍ **D.** Port mirroring

4. Which of the following is the IEEE specification developed to ensure interoperability of VLAN technologies from the various vendors?

   - ❍ **A.** 802.1z
   - ❍ **B.** 802.1s
   - ❍ **C.** 802.1Q
   - ❍ **D.** 802.1X

5. Which of the following is a proprietary protocol from Cisco used to reduce administration in the switched network?

   - ❍ **A.** VTP
   - ❍ **B.** VNMP
   - ❍ **C.** VCPN
   - ❍ **D.** VNMC

6. In an Ethernet network, what technology is being implemented when a system wants to send data to another system and first checks to see whether the network medium is free?

   - ❍ **A.** QoS
   - ❍ **B.** MDI-X
   - ❍ **C.** Jumbo frames
   - ❍ **D.** CSMA/CD

7. Which of the following is PoE+ also known as?

   - ❍ **A.** 802.3aa
   - ❍ **B.** 802.3ac
   - ❍ **C.** 802.3af
   - ❍ **D.** 802.3at

8. What is the function of ARP?

   - ❍ **A.** It resolves MAC addresses to IP addresses.
   - ❍ **B.** It resolves NetBIOS names to IP addresses.
   - ❍ **C.** It resolves IP addresses to MAC addresses.
   - ❍ **D.** It resolves hostnames to IP addresses.

## Cram Quiz Answers

1. **A.** The default gateway enables systems on one local subnet to access those on another. Answer B does not accurately describe the role of the default gateway. Answers C and D do not describe the main function of a default gateway, which is to provide the route for destinations outside the local network.
2. **D.** The hop count is the number of hops necessary to reach a node.
3. **D.** Port mirroring enables administrators to monitor the traffic outbound and inbound to the switch.
4. **C.** 802.1Q is the IEEE specification developed to ensure interoperability of VLAN technologies from the various vendors.
5. **A.** *VLAN Trunking Protocol (VTP)* is used to reduce administration in the switched network.
6. **D.** On a network that uses CSMA/CD, when a system wants to send data to another system, it first checks to see whether the network medium is free. It must do this because each piece of network medium used in a LAN can carry only one signal at a time. QoS features enable administrators to predict bandwidth use, monitor that use, and control it to ensure that bandwidth is available to the applications that need it. MDI-X expands on MDI and allows ports on newer network interfaces to detect if the connection would require a crossover. Jumbo frames are used to allow for very large Ethernet frames; by sending a lot of data at once, the number of packets is reduced, and the data sent is less processor intensive.
7. **D.** IEEE 802.3at is more commonly known as PoE+.
8. **C.** ARP resolves IP addresses to MAC addresses. Answer A describes the function of RARP, answer B describes an unrelated process, and answer D describes the process of DNS resolution.

# What's Next?

Chapter 4, "Network Implementations," introduces you to commonly used networking architecture and devices. All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator and are requirements for a Network+ candidate.

CHAPTER 4

# Network Implementations

**This chapter covers the following official Network+ objectives:**

- Explain basic corporate and datacenter network architecture.
- Compare and contrast various devices, their features, and their appropriate placement on the network.

This chapter covers CompTIA Network+ objectives 1.7 and 2.1. For more information on the official Network+ exam topics, see the "About the Network+ Exam" section in the Introduction.

All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator and are requirements for a Network+ candidate.

This chapter introduces commonly used networking devices, and that is followed by a discussion of basic corporate and datacenter network architecture later in the chapter. You are not likely to encounter all the devices mentioned in this chapter on the exam, but you can expect to work with at least some of them.

# Common Networking Devices

- **Compare and contrast various devices, their features, and their appropriate placement on a network.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What is the difference between an active and a passive hub?
2. What is the major difference between a hub and a switch?
3. What are the types of ports found on hubs and switches?
4. What can distribute incoming data to specific application servers and help distribute the load?
5. True or false: A multilayer switch operates as both a router and a switch.
6. Your company is looking to add a hardware device to the network that can increase redundancy and data availability as it increases performance by distributing the workload. What use case might this sample technology apply to?

### Answers

1. Hubs can be either active or passive. Hubs are considered active when they regenerate a signal before forwarding it to all the ports on the device.
2. Rather than forwarding data to all the connected ports, a switch forwards data only to the port on which the destination system is connected.
3. Hubs and switches have two types of ports: *medium-dependent interface (MDI)* and *medium-dependent interface crossed (MDI-X)*.
4. A content switch can distribute incoming data to specific application servers and help distribute the load.
5. True. A multilayer switch operates as both a router and a switch.
6. A load balancer can be either a software or hardware component, and it increases redundancy and data availability as it increases performance by distributing the workload.

The best way to think about this chapter is as a catalog of networking devices. The first half looks at devices that you can commonly find in a network of any substantial size. The devices are discussed in objective order to simplify study and include everything from simple access points to VPN concentrators.

ExamAlert

Remember this objective begins with "Compare and contrast various devices." This means that you need to be able to distinguish one networking or networked device from another and know its appropriate placement on the network. What does it do? Where does it belong?

# Firewall

A *firewall* is a networking device, either hardware or software based, that controls access to your organization's network. This controlled access is designed to protect data and resources from an outside threat. To provide this protection, firewalls typically are placed at a network's entry/exit points—for example, between an internal network and the Internet. After it is in place, a firewall can control access into and out of that point.

Although firewalls typically protect internal networks from public networks, they are also used to control access between specific network segments within a network. An example is placing a firewall between the Accounts and Sales departments.

As mentioned, firewalls can be implemented through software or through a dedicated hardware device. Organizations implement software firewalls through *network operating systems (NOSs)* such as Linux/UNIX, Windows servers, and macOS servers. The firewall is configured on the server to allow or block certain types of network traffic. In small offices and for regular home use, a firewall is commonly installed on the local system and is configured to control traffic. Many third-party firewalls are available.

Hardware firewalls are used in networks of all sizes today. Hardware firewalls are often dedicated network devices that can be implemented with little configuration. They protect all systems behind the firewall from outside sources. Hardware firewalls are readily available and often are combined with other devices today. For example, many broadband routers and wireless access points have firewall functionality built in. In such a case, the router or AP might have a number of ports available to plug systems into. Figure 4.1 shows Windows Defender Firewall and the configured inbound and outbound rules.

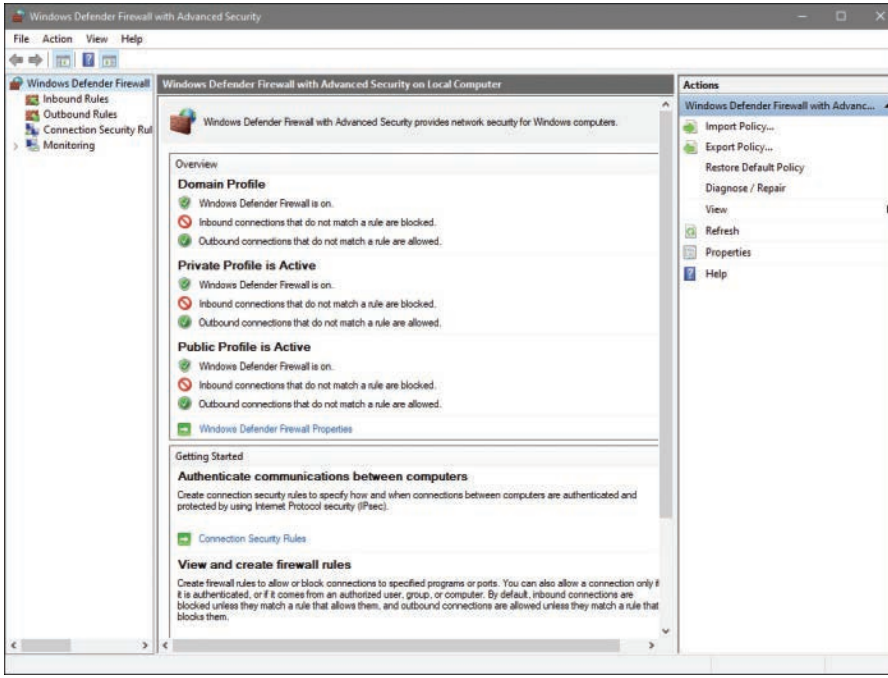



FIGURE 4.1 **Configuration of Windows Defender Firewall**

**ExamAlert**

Remember that a firewall uses inbound and outbound rules and can protect internal networks from public networks and control access between specific network segments.

# IDS/IPS

An *intrusion detection system (IDS)* is a passive detection system. The IDS can detect the presence of an attack and then log that information. It also can alert an administrator to the potential threat. The administrator then analyzes the situation and takes corrective measures if needed.

A variation on the IDS is the *intrusion prevention system (IPS)*, which is an active detection system. With IPS, the device continually scans the network, looking for inappropriate activity. It can shut down any potential threats. The IPS looks for any known signatures of common attacks and automatically tries to prevent those attacks. An IPS is considered an active/reactive security measure because it actively monitors and can take steps to correct a potential security threat.

Following are several variations on IDSs/IPSs:

- **Behavior based:** A *behavior-based system* looks for variations in behavior such as unusually high traffic, policy violations, and so on. By looking for deviations in behavior, it can recognize potential threats and quickly respond.
- **Signature based:** A signature-based system, also commonly known as *misuse-detection system (MD-IDS/MD-IPS)*, is primarily focused on evaluating attacks based on attack signatures and audit trails. Attack signatures describe a generally established method of attacking a system. For example, a TCP flood attack begins with a large number of incomplete TCP sessions. If the MD-IDS knows what a TCP flood attack looks like, it can make an appropriate report or response to thwart the attack. This IDS uses an extensive database to determine the signature of the traffic.
- **Network-based intrusion detection/prevention system (NIDS or NIPS):** The system examines all network traffic to and from network systems. If it is software, it is installed on servers or other systems that can monitor inbound traffic. If it is hardware, it may be connected to a hub or switch to monitor traffic.
- **Host-based intrusion detection/prevention system (HIDS or HIPS):** These applications are spyware or virus applications that are installed on individual network systems. The system monitors and creates logs on the local system.

ExamAlert

An intrusion detection system (IDS) can detect malicious activity and send alerting messages, but it does not prevent attacks. An intrusion prevention system (IPS) protects hosts and prevents against malicious attacks from the network layer up through the application layer.

# Router

In a common configuration, routers create larger networks by joining two network segments. A *small office/home office (SOHO)* router connects a user to the Internet. A SOHO router typically serves 1 to 10 users on the system. A router can be a dedicated hardware device or a computer system with more than one network interface and the appropriate routing software. All modern network operating systems include the functionality to act as a router.

> **Note**
>
> Routers normally create, add, or divide networks or network segments at the network layer of the OSI reference model because they normally are IP-based devices. Chapter 2, "Models, Ports, Protocols, and Network Services," covers the OSI reference model in greater detail.

A router derives its name from the fact that it can route data it receives from one network to another. When a router receives a packet of data, it reads the packet's header to determine the destination address. After the router has determined the address, it looks in its routing table to determine whether it knows how to reach the destination; if it does, it forwards the packet to the next hop on the route. The next hop might be the final destination, or it might be another router. Figure 4.2 shows, in basic terms, how a router works.

> **Note**
>
> You can find more information on network routing in Chapter 3, "Addressing, Routing, and Switching."

A router works at Layer 3 (the network layer) of the OSI model.

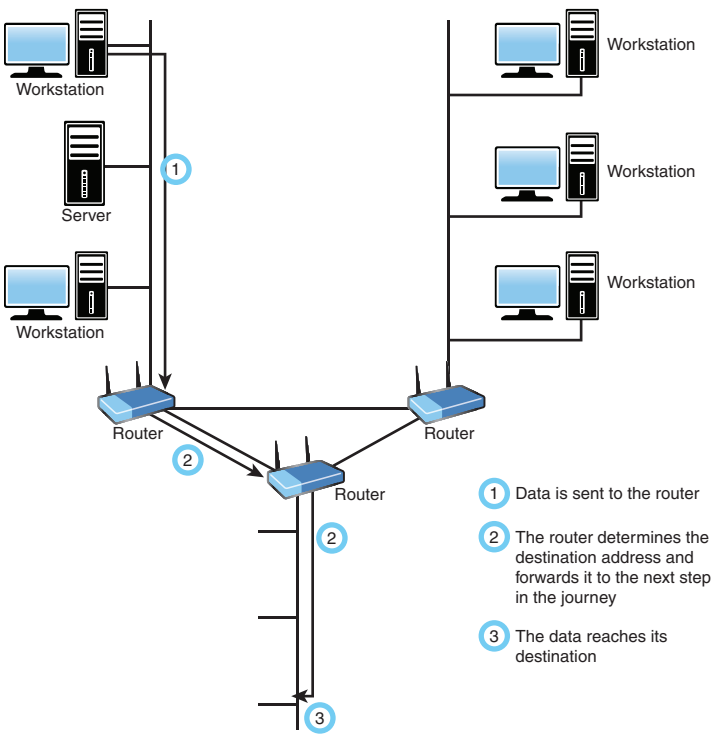



FIGURE 4.2 **How a router works**

# Switch

Like hubs, *switches* are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device. The difference between hubs and switches is in how the devices deal with the data they receive. Whereas a hub forwards the data it receives to all the ports on the device, a switch forwards it to only the port that connects to the destination device. It does this by the MAC address of the devices attached to it and then by matching the destination MAC address in the data it receives. Figure 4.3 shows how a switch works. In this case, it has learned the MAC addresses of the devices attached to it; when the workstation sends a message intended for another workstation, it forwards the message on and ignores all the other workstations.

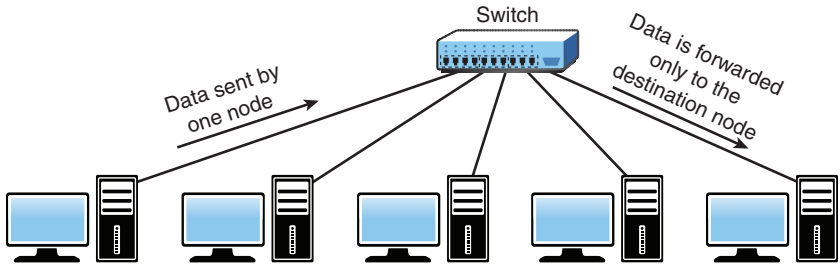



FIGURE 4.3 **How a switch works**

By forwarding data to only the connection that should receive it, the switch can greatly improve network performance. By creating a direct path between two devices and controlling their communication, the switch can greatly reduce the traffic on the network and therefore the number of collisions. As you might recall, collisions occur on Ethernet networks when two devices attempt to transmit at the same time. In addition, the lack of collisions enables switches to communicate with devices in full-duplex mode. In a full-duplex configuration, devices can send data to and receive data from the switch at the same time. Contrast this with half-duplex communication, in which communication can occur in only one direction at a time. Full-duplex transmission speeds are double that of a standard half-duplex connection. So, a 100 Mbps connection becomes 200 Mbps, and a 1000 Mbps connection becomes 2000 Mbps, and so on.

The net result of these measures is that switches can offer significant performance improvements over hub-based networks, particularly when network use is high.

Irrespective of whether a connection is at full or half duplex, the method of switching dictates how the switch deals with the data it receives. The following is a brief explanation of each method:

- **Cut-through:** In a cut-through switching environment, the packet begins to be forwarded as soon as it is received. This method is fast, but it creates the possibility of errors being propagated through the network because no error checking occurs.
- **Store-and-forward:** Unlike cut-through, in a store-and-forward switching environment, the entire packet is received and error-checked before being forwarded. The upside of this method is that errors are not propagated through the network. The downside is that the error-checking process takes a relatively long time, and store-and-forward switching is considerably slower as a result.
- **Fragment-free:** To take advantage of the error checking of store-and-forward switching, but still offer performance levels nearing that of cut-through switching, fragment-free switching can be used. In a fragment-free switching environment, enough of the packet is read so that the switch can determine whether the packet has been involved in a collision. As soon as the collision status has been determined, the packet is forwarded.

## Hub and Switch Cabling

In addition to acting as a connection point for network devices, hubs and switches can be connected to create larger networks. This connection can be achieved through standard ports with a special cable or by using special ports with a standard cable.

As you learned in Chapter 3, the ports on a hub, switch, or router to which computer systems are attached are called *medium-dependent interface crossed (MDI-X)*. The crossed designation is derived from the fact that two of the wires within the connection are crossed so that the send signal wire on one device becomes the receive signal of the other. Because the ports are crossed internally, a standard or straight-through cable can be used to connect devices.

Another type of port, called a *medium-dependent interface (MDI)* port, is often included on a hub or switch to facilitate the connection of two switches or hubs. Because the hubs or switches are designed to see each other as an extension of the network, there is no need for the signal to be crossed. If a hub or switch does not have an MDI port, hubs or switches can be connected

by using a cable between two MDI-X ports. The crossover cable uncrosses the internal crossing. Auto MDI-X ports on more modern network device interfaces can detect whether the connection would require a crossover, and automatically choose the MDI or MDI-X configuration to properly match the other end of the link.

**ExamAlert**

In a crossover cable, wires 1 and 3 and wires 2 and 6 are crossed.

A switch can work at either Layer 2 (the data link layer) or Layer 3 (the network layer) of the OSI model. When it filters traffic based on the MAC address, it is called a Layer 2 switch since MAC addresses exist at Layer 2 of the OSI model (if it operated only with IP traffic, it would be a Layer 3 switch).

## Multilayer Switch

It used to be that networking devices and the functions they performed were separate. Bridges, routers, hubs, and more existed but were separate devices. Over time, the functions of some individual network devices became integrated into a single device. This is true of *multilayer switches*.

A multilayer switch is one that can operate at both Layer 2 and Layer 3 of the OSI model, which means that the multilayer device can operate as both a switch and a router (by operating at more than one layer, it is living up to the name of being "multilayer"). Also called a Layer 3 switch, the multilayer switch is a high-performance device that supports the same routing protocols that routers do. It is a regular switch directing traffic within the LAN; in addition, it can forward packets between subnets.

**ExamAlert**

A multilayer switch operates as both a router (Layer 3 capable device) and a switch (Layer 2 switch).

A content switch is another specialized device. A content switch is not as common on today's networks, mostly due to cost. A content switch examines the network data it receives, decides where the content is intended to go, and forwards it. The content switch can identify the application that data is targeted for by associating it with a port. For example, if data uses the Simple Mail Transfer Protocol (SMTP) port, it could be forwarded to an SMTP server.

Content servers can help with load balancing because they can distribute requests across servers and target data to only the servers that need it, or distribute data between application servers. For example, if multiple mail servers are used, the content switch can distribute requests between the servers, thereby sharing the load evenly. This is why the content switch is sometimes called a load-balancing switch.

**ExamAlert**

A content switch can distribute incoming data to specific application servers and help distribute the load.

# Hub

At the bottom of the networking devices food chain, so to speak, are hubs. Hubs are used in networks that use Ethernet twisted-pair cabling to connect devices. Hubs also can be joined to create larger networks. *Hubs* are simple devices that direct data packets to all devices connected to the hub, regardless of whether the data package is destined for the device. This makes them inefficient devices and can create a performance bottleneck on busy networks.

In its most basic form, a hub does nothing except provide a pathway for the electrical signals to travel along. Such a device is called a *passive* hub. Far more common nowadays is an *active* hub, which, as well as providing a path for the data signals, regenerates the signal before it forwards it to all the connected devices. In addition, an active hub can buffer data before forwarding it. However, a hub does not perform any processing on the data it forwards, nor does it perform any error checking.

Hubs come in a variety of shapes and sizes. Small hubs with five or eight connection ports are commonly called *workgroup hubs*. Others can accommodate larger numbers of devices (normally up to 32). These are called *high-density devices*.

**ExamAlert**

Because hubs don't perform any processing, they do little except enable communication between connected devices. For today's high-demand network applications, something with a little more intelligence is required. That's where switches come in.

A basic hub works at Layer 1 (the physical layer) of the OSI model.

# Bridge

A *bridge*, as the name implies, connects two networks. Bridging is done at the first two layers (physical and data link layer) of the OSI model and differs from routing in its simplicity. With routing, a packet is sent to where it is intended to go, whereas with bridging, it is sent away from this network. In other words, if a packet does not belong on this network, it is sent across the bridge with the assumption that it belongs there rather than here.

If one or more segments of the bridged network are wireless, the device is known as a *wireless bridge*.

# DSL and Cable Modems

A traditional modem (short for modulator/demodulator) is a device that converts the digital signals generated by a computer into analog signals that can travel over conventional phone lines. The modem at the receiving end converts the signal back into a format that the computer can understand. While modems can be used as a means to connect to an ISP or as a mechanism for dialing up a LAN, they have faded in use in recent years in favor of faster technologies.

Modems can be internal add-in expansion cards or integrated with the motherboard, external devices that connect to a system's serial or USB port, or proprietary devices designed for use on other devices, such as portables and handhelds.

A *DSL modem* makes it possible for telephone lines to be used for high-speed Internet connections. Much faster than the old dial-up modems, DSL modems use the subscriber (dedicated) lines and send the data back and forth across them—translating them into signals the devices can use.

Similarly, a *cable modem* has a coaxial connection for connecting to the provider's outlet and an *unshielded twisted-pair (UTP)* connection for connecting directly to a system or to a hub, switch, or router. Cable providers often supply the cable modem, with a monthly rental agreement. Many cable providers offer free or low-cost installation of cable Internet service, which includes installing a network card in a PC. Some providers also do not charge for the network card. Figure 4.4 shows the results of a speed test from a cable modem.

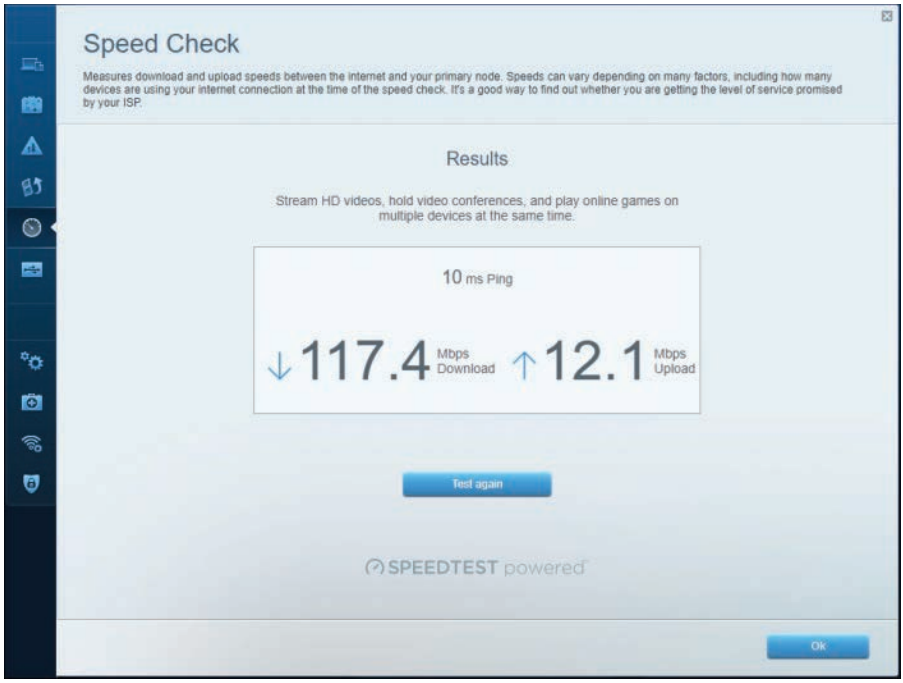



FIGURE 4.4 **Speed test results**

Most cable modems offer the capability to support a higher-speed Ethernet connection for the home LAN than is achieved. The actual speed of the connection can vary somewhat, depending on the utilization of the shared cable line in your area.

# Access Point

The term *access point (AP)* can technically be used for either a wired or wireless connection, but in reality it is almost always associated only with a wireless-enabling device. A *wireless access point (WAP)* is a transmitter and receiver (transceiver) device used to create a *wireless LAN (WLAN)*. WAPs typically are separate network devices with a built-in antenna, transmitter, and adapter. WAPs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. WAPs also usually have several ports, giving you a way to expand the network to support additional clients.

Depending on the size of the network, one or more WAPs might be required. Additional WAPs are used to allow access to more wireless clients and to expand the range of the wireless network. Each WAP is limited by a

transmission range—the distance a client can be from a WAP and still obtain a usable signal. The actual distance depends on the wireless standard used and the obstructions and environmental conditions between the client and the WAP.

**ExamAlert**

An AP or WAP can operate as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.

Saying that a WAP is used to extend a wired LAN to wireless clients does not give you the complete picture. A wireless AP today can provide different services in addition to just an access point. Today, the APs might provide many ports that can be used to easily increase the network's size. Systems can be added to and removed from the network with no effect on other systems on the network. Also, many APs provide firewall capabilities and *Dynamic Host Configuration Protocol (DHCP)* service. When they are hooked up, they give client systems a private IP address and then prevent Internet traffic from accessing those systems. So, in effect, the AP is a switch, DHCP server, router, and firewall.

APs come in all shapes and sizes. Many are cheaper and are designed strictly for home or small office use. Such APs have low-powered antennas and limited expansion ports. Higher-end APs used for commercial purposes have high-powered antennas, enabling them to extend how far the wireless signal can travel.

**Note**

APs are used to create a wireless LAN and to extend a wired network. APs are used in the infrastructure wireless topology.

An AP works at Layer 2 (the data link layer) of the OSI model.

# Media Converter

When you have two dissimilar types of network media, a *media converter* is used to allow them to connect. They are sometimes referred to as couplers. Depending on the conversion being done, the converter can be a small device, barely larger than the connectors themselves, or a large device within a sizable chassis.

Reasons for not using the same media throughout the network, and thus reasons for needing a converter, can range from cost (gradually moving from coax to fiber), disparate segments (connecting the office to the factory), or the need to run particular media in a setting (the need for fiber to reduce EMI problems in a small part of the building).

Figure 4.5 shows an example of a media converter. The one shown converts between 10/100/1000TX and 1000LX (with an SC-type connector).

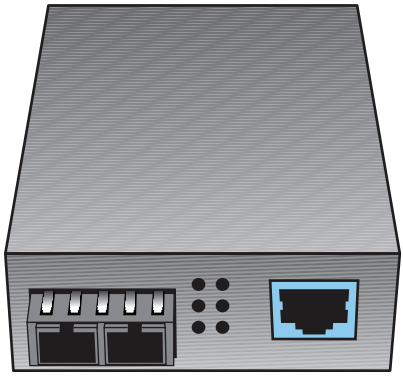


FIGURE 4.5 **A common media converter**

The following converters are commonly implemented and are ones that CompTIA has previously included on the Network+ exam.

**ExamAlert**

Make sure you know that the possibilities listed here exist:

- Single mode fiber to Ethernet
- Single mode to multimode fiber
- Multimode fiber to Ethernet
- Fiber to coaxial

# Voice Gateway

When telephone technology is married with information technology, the result is called telephony. There has been a massive move from landlines to *voice over IP (VoIP)* for companies to save money. One of the biggest issues with the administration of this is security. When both data and VoIP are on the same line, they are both vulnerable in the case of an attack. Standard telephone systems should be replaced with a securable *PBX*.

A *VoIP gateway*, also sometimes called a PBX gateway, can be used to convert between the legacy telephony connection and a VoIP connection using Session Initiation Protocol (SIP). This is referred to as a "digital gateway" because the voice media are converted in the process.

ExamAlert

Be sure that you know that by having both data and VoIP on the same line, they are both vulnerable in the case of an attack.

# Repeater

A *repeater* (also called a booster or wireless range extender) can amplify a wireless signal to make it stronger. This increases the distance that the client system can be placed from the access point and still be on the network. The extender needs to be set to the same channel as the AP for the repeater to take the transmission and repeat it. This is an effective strategy to increase wireless transmission distances.

ExamAlert

Carefully read troubleshooting question scenarios to be sure the transmission from the AP is getting to the repeater first, and then the repeater is duplicating the signal and passing it on.

# Wireless LAN Controller

*Wireless LAN controllers* are often used with branch/remote office deployments for wireless authentication. When an AP boots, it authenticates with a controller before it can start working as an AP. This is often used with *VLAN pooling*, in which multiple interfaces are treated as a single entity (usually for load balancing).

# Load Balancer

Network servers are the workhorses of the network. They are relied on to hold and distribute data, maintain backups, secure network communications, and more. The load of servers is often a lot for a single server to maintain. This is where load balancing comes into play. *Load balancing* is a technique in which the workload is distributed among several servers. This feature can take networks to the next level; it increases network performance, reliability, and availability.

**ExamAlert**

Remember that load balancing increases redundancy and therefore data availability. Also, load balancing increases performance by distributing the workload.

A load balancer can be either a hardware device or software specially configured to balance the load.

**Note**

Multilayer switches and DNS servers can serve as load balancers.

# Proxy Server

*Proxy servers* typically are part of a firewall system. They have become so integrated with firewalls that the distinction between the two can sometimes be lost.

However, proxy servers perform a unique role in the network environment—a role that is separate from that of a firewall. For the purposes of this book, a proxy server is defined as a server that sits between a client computer and the Internet and looks at the web page requests the client sends. For example, if a client computer wants to access a web page, the request is sent to the proxy server rather than directly to the Internet. The proxy server first determines whether the request is intended for the Internet or for a web server locally. If the request is intended for the Internet, the proxy server sends the request *as if it originated the request*. When the Internet web server returns the information, the proxy server returns the information to the client. Although a delay might be induced by the extra step of going through the proxy server, the process is largely transparent to the client that originated the request. Because each request a client sends to the Internet is channeled through the proxy server, the proxy server can provide certain functionality over and above just forwarding requests.

One of the most notable extra features is that proxy servers can greatly improve network performance through a process called *caching*. When a caching proxy server answers a request for a web page, the server makes a copy of all or part of that page in its cache. Then, when the page is requested again, the proxy server answers the request from the cache rather than going back to the Internet. For example, if a client on a network requests the web page www.comptia.org, the proxy server can cache the contents of that web page. When a second client computer on the network attempts to access the same site, that client can grab

it from the proxy server cache, and accessing the Internet is unnecessary. This greatly increases the response time to the client and can significantly reduce the bandwidth needed to fulfill client requests.

Nowadays, speed is everything, and the capability to quickly access information from the Internet is a crucial concern for some organizations. Proxy servers and their capability to cache web content accommodate this need for speed.

An example of this speed might be found in a classroom. If a teacher asks 30 students to access a specific *Uniform Resource Locator (URL)* without a proxy server, all 30 requests would be sent into cyberspace and subjected to delays or other issues that could arise. The classroom scene with a proxy server is quite different. Only one request of the 30 finds its way to the Internet; the other 29 are filled by the proxy server's cache. Web page retrieval can be almost instantaneous.

However, this caching has a potential drawback. When you log on to the Internet, you get the latest information, but this is not always so when information is retrieved from a cache. For some web pages, it is necessary to go directly to the Internet to ensure that the information is up to date. Some proxy servers can update and renew web pages, but they are always one step behind.

The second key feature of proxy servers is allowing network administrators to filter client requests. If a server administrator wants to block access to certain websites, a proxy server enables this control, making it easy to completely disallow access to some websites. This is okay, but what if it were necessary to block numerous websites? In this case, maintaining proxy servers gets a bit more complicated.

Determining which websites users can or cannot access is usually done through something called an *access control list (ACL)*. Chapter 3 discussed how an ACL can be used to provide rules for which port numbers or IP addresses are allowed access. An ACL can also be a list of allowed or nonallowed websites; as you might imagine, compiling such a list can be a monumental task. Given that millions of websites exist, and new ones are created daily, how can you target and disallow access to the "questionable" ones? One approach is to reverse the situation and deny access to all pages except those that appear in an "allowed" list. This approach has high administrative overhead and can greatly limit the productive benefits available from Internet access.

Understandably, it is impossible to maintain a list that contains the locations of all sites with questionable content. In fairness, that is not what proxy servers were designed to do. However, by maintaining a list, proxy servers can better provide a greater level of control than an open system. Along the way, proxy servers can make the retrieval of web pages far more efficient.

A *reverse proxy server* is one that resides near the web servers and responds to requests. These are often used for load-balancing purposes because each proxy can cache information from a number of servers.

# VPN Concentrators and Headends

A *VPN concentrator* can be used to increase remote-access security. This device can establish a secure connection (tunnel) between the sending and receiving network devices. VPN concentrators add an additional level to VPN security. They not only can create the tunnel but also can authenticate users, encrypt the data, regulate the data transfer, and control traffic.

The concentrator sits between the VPN client and the VPN server, creates the tunnel, authenticates users using the tunnel, and encrypts data traveling through the tunnel. When the VPN concentrator is in place, it can establish a secure connection (tunnel) between the sending and receiving network devices.

VPN concentrators add an additional level to VPN security. Depending on the exact concentrator, they can do the following:

- Create the tunnel.
- Authenticate users who want to use the tunnel.
- Encrypt and decrypt data.
- Regulate and monitor data transfer across the tunnel.
- Control inbound and outbound traffic as a tunnel endpoint or router.

The VPN concentrator invokes various standard protocols to accomplish these functions.

A *VPN headend* (or *head-end*) is a server that receives the incoming signal and then decodes/encodes it and sends it on.

# Networked Devices

One of the fastest areas of growth in networking isn't necessarily in adding more users, but in adding more devices. Each "smart" device has the ability to monitor or perform some task and report the status of the data it has collected, or itself, back. Most of these devices require IP addresses and function like normal nodes, but some network only through Bluetooth or NFC. Table 4.1 lists some of the devices commonly being added to the network today.

TABLE 4.1 **Commonly Networked Devices**

| Device | Description | Key Points |
|---|---|---|
| Telephones | Utilizing voice over IP (VoIP), the cost of traditional telephone service is reduced to a fraction of its old cost. | In the world of voice over IP (VoIP), an *endpoint* is any final destination for a voice call. |
| Printer | The printer was one of the first devices to be networked. Connecting the printer to the network makes it possible to share with all authorized users. | Networked printers need to be monitored for security concerns. Many high-speed printers spool print jobs, and the spooler can be a weakness for some unauthorized person looking for sensitive information. |
| Physical access control devices | These devices include door locks, gates, and other similar devices. | They greatly reduce the cost of manual labor, such as guards at every location. |
| Cameras | Cameras allow for monitoring areas remotely. | The capability to pan, tilt, and zoom (PTZ) is important in camera selection. |
| HVAC sensors | These devices provide heating, ventilation, and air conditioning. | Smart sensors for HVAC can work in conjunction with other sensors. For example, a smoke detector can go off and notify the furnace to immediately shut off the fan to prevent spreading smoke throughout the building. |
| IoT | Internet of Things (IoT) includes such devices as refrigerators, smart speakers, smart thermostats, and smart doorbells. | The acceptance—and adoption—of these items in the home market is predicted to grow so quickly that the number of sensors in use will outnumber the number of users within the next decade. |
| ICS/SCADA | Industrial Control Systems (ICS) is a catchall term for sensors and controls used in industry. A subset of this is SCADA (supervisory control and data acquisition), which refers to equipment often used to manage automated factory equipment, dams, power generators, and similar equipment. | When it comes to sensors and controls, an emerging area of growth is that of in-vehicle computing systems. Automobiles tend to have sophisticated systems, such as computers complete with hard drives and GPS devices. Similar devices to those always sensing the status of the vehicle are used in industrial environments for automation, safety, and efficiency. |

## ExamAlert

You will be expected to know the devices mentioned in this chapter. Review Table 4.1, and make sure that you understand each device and how and why it is used on the network.

# Cram Quiz

1. Users are complaining that the network's performance is unsatisfactory. It takes a long time to pull files from the server, and, under heavy loads, workstations can become disconnected from the server. The network is heavily used, and a new videoconferencing application is about to be installed. The network is a 1000BASE-T system created with Ethernet hubs. Which device are you most likely to install to alleviate the performance problems?
   - ❍ **A.** Switch
   - ❍ **B.** Router
   - ❍ **C.** Media converter
   - ❍ **D.** Firewall

2. Which of the following devices forwards data packets to all connected ports?
   - ❍ **A.** Router
   - ❍ **B.** Switch
   - ❍ **C.** Content filter
   - ❍ **D.** Hub

3. Which of the following devices passes data based on the MAC address?
   - ❍ **A.** Hub
   - ❍ **B.** Switch
   - ❍ **C.** MSAU
   - ❍ **D.** Router

4. Which of the following can serve as load balancers?
   - ❍ **A.** IDS and DNS servers
   - ❍ **B.** Multilayer switches and IPS
   - ❍ **C.** Multilayer switches and DNS servers
   - ❍ **D.** VoIP PBXs and UTM appliances

5. Which of the following is the best answer for a device that continually scans the network, looking for inappropriate activity?
   - ❍ **A.** IPS
   - ❍ **B.** NGFW
   - ❍ **C.** VCPN
   - ❍ **D.** AAA

# Cram Quiz Answers

1. **A.** Replacing Ethernet hubs with switches can yield significant performance improvements. Of the devices listed, switches are also the only ones that can be substituted for hubs. A router is used to separate networks, not as a connectivity point for workstations. A media converter is used to connect two dissimilar types of network media. A firewall is not a solution to the problem presented.
2. **D.** Hubs are inefficient devices that send data packets to all connected devices. Switches pass data packets to the specific destination device. This method significantly increases network performance.
3. **B.** When determining the destination for a data packet, the switch learns the MAC address of all devices attached to it and then matches the destination MAC address in the data it receives. None of the other devices listed passes data based solely on the MAC address.
4. **C.** Multilayer switches and DNS servers can serve as load balancers.
5. **A.** An intrusion prevention system (IPS) is a device that continually scans the network, looking for inappropriate activity.

# Networking Architecture

▶ **Explain basic corporate and datacenter network architecture.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then complete the Cram Quiz at the end of the section.

1. What is the term for the network architecture design in which servers, appliances, and other switches located within the same rack are connected to an in-rack network switch?
2. True or false: Traffic flows entering and leaving a datacenter are known as East-West traffic.
3. True or false: In the three-tiered architecture, the access/edge layer ensures data is delivered to edge/end devices.

### Answers

1. This is known as top-of-rack (ToR) switching.
2. False. Traffic flows entering and leaving a datacenter are known as North-South traffic.
3. True. The access/edge layer is the place where switches connect to and ensure data is delivered to edge/end devices.

The networking devices discussed previously in this chapter are used to build networks. For this particular objective, CompTIA wants you to be aware of some of the architecture and design elements of the network. Whether you're putting together a datacenter or a corporate office, planning should be involved, and no network should be allowed to haphazardly sprout without management and oversight.

## Three-Tiered Architecture

To improve system performance, as well as to improve security, it is possible to implement a *tiered* systems model. This is often referred to as an *n*-tiered model because the *n*- can be one of several different numbers.

If we were looking at database, for example, with a one-tier model, or single-tier environment, the database and the application exist on a single system. This is common on desktop systems running a standalone database. Early UNIX

implementations also worked in this manner; each user would sign on to a terminal and run a dedicated application that accessed the data. With two-tier architecture, the client workstation or system runs an application that communicates with the database that is running on a different server. This common implementation works well for many applications. With *three-tiered architecture*, security is enhanced. In this model, the end user is effectively isolated from the database by the introduction of a middle-tier server. This server accepts requests from clients, evaluates them, and then sends them on to the database server for processing. The database server sends the data back to the middle-tier server, which then sends the data to the client system. Becoming common in business today, this approach adds both capability and complexity.

While the examples are of database tiering, this same approach can be taken with devices such as routers, switches, and other servers. In a three-tiered model of routing and switching, the three tiers would be the core, the distribution/aggregation layer, and the access/edge. We walk through each of the layers present in this scenario.

## Core Layer

The *core* layer is the backbone: the place where switching and routing meet (switching ends, routing begins). It provides high-speed, highly redundant forwarding services to move packets between distribution-layer devices in different regions of the network. The core switches and routers would be the most powerful in the enterprise (in terms of their raw forwarding power,) and would be used to manage the highest-speed connections (such as 100 Gigabit Ethernet). Core switches also incorporate internal firewall capability as part of their features, helping with segmentation and control of traffic moving from one part of the network to another.

## Distribution/Aggregation Layer

The *distribution layer*, or *aggregation layer* (sometimes called the workgroup layer), is the layer in which management takes place. This is the place where QoS policies are managed, filtering is done, and routing takes place. Distribution layer devices can be used to manage individual branch-office WAN connections, and this is considered to be smart (usually offering a larger feature set than switches used at the access/edge layer). Lower latency and larger MAC address table sizes are important features for switches used at this level because they aggregate traffic from thousands of users rather than hundreds (as access/edge switches do).

## Access/Edge Layer

Switches that allow end users and servers to connect to the enterprise are called access switches or edge switches, and the layer where they operate in the three-tiered model is known as the *access layer*, or *edge layer*. Devices at this layer may or may not provide Layer 3 switching services; the traditional focus is on minimizing the cost of each provisioned Ethernet port (known as "cost-per-port") and providing high port density. Because the focus is on connecting client nodes, such as workstations to the network, this is sometimes called the desktop layer.

**ExamAlert**

Remember: The core layer is the backbone of the network (where the fastest routers and switches operate to manage separate networks), whereas the distribution/aggregation layer (between the access/edge and core layers) is the "boundary" layer where ACLs and Layer 3 switches operate to properly manage data between VLANs and subnetworks. The access/edge layer is the place where switches connect to and ensure data is delivered to edge/end devices, such as computers and servers.

# Software-Defined Networking

*Software-defined networking (SDN)* is a dynamic approach to computer networking intended to allow administrators to get around the static limitations of physical architecture associated with traditional networks. They can do so through the implementation of technologies such as the Cisco Systems Open Network Environment.

The goal of SDN is not only to add dynamic capabilities to the network but also to reduce IT costs through implementation of cloud architectures. SDN combines network and application services into centralized platforms that can automate provisioning and configuration of the entire infrastructure.

The SDN architecture, from the top down, consists of the application layer, control layer, and infrastructure layer. CompTIA also adds the management plane as an objective, and a discussion of each of these components follows.

## Application Layer

The *application layer* is the top of the SDN stack, and this is where load balancers, firewalls, intrusion detection, and other standard network applications are located. While a standard (non-SDN) network would use a specialized appliance for each of these functions, with an SDN network, an application is used in place of a physical appliance.

## Control Layer

The *control layer* is the place where the SDN controller resides; the controller is software that manages policies and the flow of traffic throughout the network. This controller can be thought of as the brains behind SDN, making it all possible. Applications communicate with the controller through a northbound interface, and the controller communicates with switching using southbound interfaces.

## Infrastructure Layer

The physical switch devices themselves reside at the *infrastructure layer*. This is also known as the control plane when breaking the architecture into "planes" because this is the component that defines the traffic routing and network topology.

## Management Plane

With SDN, the management plane allows administrators to see their devices and traffic flows and react as needed to manage data plane behavior. This can be done automatically through configuration apps that can, for example, add more bandwidth if it looks as if edge components are getting congested. The management plane manages and monitors processes across all layers of the network stack.

**ExamAlert**

A major benefit of SDN is that it replaces traditional dedicated hardware/services with virtual.

# Spine and Leaf

In an earlier section, we discussed the possibility of tiered models. A two-tier model that Cisco promotes for switches is the *spine and leaf* model. In this model, the spine is the *backbone* of the network, just as it would be in a skeleton and is responsible for interconnecting all the leaf switches in a full-mesh topology. Thanks to the mesh, every leaf is connected to every spine, and the path is randomly chosen so that the traffic load is evenly distributed among the top-tier switches. If one of the switches at the top tier were to fail, there would only be a slight degradation in performance throughout the datacenter.

Because of the design of this model, no matter which leaf switch is connected to a server, the traffic always has to cross the same number of devices to get to another server. This keeps latency at a steady level.

When *top-of-rack (ToR) switching* is incorporated into the network architecture, switches located within the same rack are connected to an in-rack network switch, which is connected to aggregation switches (usually via fiber cabling). The big advantage of this setup is that the switches within each rack can be connected with cheaper copper cabling and the cables to each rack are all that need be fiber.

**ExamAlert**

Remember that in a spine and leaf model the spine is the backbone of the network and is responsible for interconnecting all the leaf switches in a full-mesh topology.

# Traffic Flows

Traffic flows within a datacenter typically occur within the framework of one of two models: East-West or North-South. The names may not be the most intuitive, but the East-West traffic model means that data is flowing among devices within a specific datacenter while North-South means that data is flowing into the datacenter (from a system physically outside the datacenter) or out of it (to a system physically outside the datacenter).

The naming convention comes from the way diagrams are drawn: data staying within the datacenter is traditionally drawn on the same horizontal line (East-to-West), while data leaving or entering is typically drawn on a vertical line (North-to-South). With the increase in virtualization being implemented at so many levels, the East-West traffic has increased in recent years.

**ExamAlert**

East-West traffic is a concept referring to network traffic flow within a datacenter between servers. North-South refers to data transfers between the datacenter and that outside of the network.

# Datacenter Location Types

One of the biggest questions a network administrator today can face is where to store the data. At one point in time, this question was a no-brainer: servers

were kept close at hand so they could be rebooted and serviced regularly. Today, however, that choice is not such an easy one. The cloud, virtualization, software-defined networking, and many other factors have combined to offer several options in which cost often becomes one of the biggest components.

An *on-premises datacenter* can be thought of as the old, traditional approach: the data and the servers are kept in house. One alternative to this is to share a *colocation*. In this arrangement, several companies put their "servers" in a shared space. The advantage to this approach is that by renting space in a third-party facility, it is often possible to gain advantages associated with connectivity speed, and possibly technical support. When describing this approach, we placed "servers" in quotation marks because the provider will often offer virtual servers rather than dedicated machines for each client, thus enabling companies to grow without a reliance on physical hardware.

Incidentally, any remote and autonomous office, regardless of the number of users who may work from it, is known as a *branch office*. This point is important because it may be an easy decision to keep the datacenter on-premises at headquarters, but network administrators need to factor in how to best support branch offices as well. The situation could easily be that while on-premises works best at headquarters, all branch offices are supported by colocation sites.

## Storage-Area Networks

When it comes to data storage in the cloud, encryption is one of the best ways to protect it (keeping it from being of value to unauthorized parties), and VPN routing and forwarding can help. Backups should be performed regularly (and encrypted and stored in safe locations), and access control should be a priority.

The consumer retains the ultimate responsibility for compliance. Per NIST SP 800-144,

> The main issue centers on the risks associated with moving important applications or data from within the confines of the organization's computing center to that of another organization (i.e., a public cloud), which is readily available for use by the general public. The responsibilities of both the organization and the cloud provider vary depending on the service model. Reducing cost and increasing efficiency are primary motivations for moving towards a public cloud, but relinquishing responsibility for security should not be. Ultimately, the organization is accountable for the choice of public cloud and the security and privacy of the outsourced service.

For more information, see http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

Shared storage can be done on *storage-area networks (SANs)*, *network-attached storage (NAS)*, and so on; the virtual machine sees only a "physical disk." With clustered storage, you can use multiple devices to increase performance. A handful of technologies exist in this realm, and the following are those that you need to know for the Network+ exam.

> **Tip**
>
> Look to CompTIA's Cloud+ certification for more specialization in cloud and virtualization technologies.

## iSCSI

The *Small Computer Systems Interface (SCSI)* standard has long been the language of storage. *Internet Small Computer Systems Interface (iSCSI)* expands this through Ethernet, allowing IP to be used to send SCSI commands.

*Logical unit numbers (LUNs)* came from the SCSI world and carry over, acting as unique identifiers for devices. Both NAS and SAN use "targets" that hold up to eight devices.

Using iSCSI for a virtual environment gives users the benefits of a file system without the difficulty of setting up Fibre Channel. Because iSCSI works both at the hypervisor level and in the guest operating system, the rules that govern the size of the partition in the OS are used rather than those of the virtual OS (which are usually more restrictive).

The disadvantage of iSCSI is that users can run into IP-related problems if configuration is not carefully monitored.

## Fibre Channel and FCoE

Instead of using an older technology and trying to adhere to legacy standards, Fibre Channel (FC) is an option providing a higher level of performance than anything else. It utilizes FCP, the Fiber Channel Protocol, to do what needs to be done, and *Fibre Channel over Ethernet (FCoE)* can be used in high-speed (10 GB and higher) implementations.

The big advantage of Fibre Channel is its scalability. FCoE encapsulates FC over the Ethernet portions of connectivity, making it easy to add into an existing network. As such, FCoE is an extension to FC intended to extend the scalability and efficiency associated with Fibre Channel.

**ExamAlert**

Know that FCoE allows Fibre Channel to use 10 Gigabit Ethernet (or even higher) networks. This solves the problem of enterprises having to run parallel infrastructures for both LANs and SANs.

## Network-Attached Storage

Storage is always a big issue, and the best answer is always a storage-area network. Unfortunately, a SAN can be costly and difficult to implement and maintain. That is where *network-attached storage (NAS)* comes in. NAS is easier than SAN and uses TCP/IP. It offers file-level access, and a client sees the shared storage as a file server.

**Note**

On a VLAN, multipathing creates multiple paths to the storage resources and can be used to increase availability *and* add fault tolerance.

**ExamAlert**

For the exam, you should know the difference between NAS and SAN technologies and how to apply them.

# Cram Quiz

1. Logical unit numbers (LUNs) came from the SCSI world and use "targets" that hold up to how many devices?

   - ❍ **A.** 4
   - ❍ **B.** 6
   - ❍ **C.** 8
   - ❍ **D.** 128

2. What is the network architecture in which the database and the application exist on a single system?

   - ❍ **A.** *N*-tiered
   - ❍ **B.** One-tiered
   - ❍ **C.** Two-tiered
   - ❍ **D.** Three-tiered

3. On a VLAN, what creates multiple paths to the storage resources and can be used to increase availability and add fault tolerance?
   - ❍ **A.** FCoE
   - ❍ **B.** Adding a management plane
   - ❍ **C.** Colocating
   - ❍ **D.** Multipathing

4. What traffic pattern refers to data that travels outside the datacenter or enterprise?
   - ❍ **A.** East-to-West
   - ❍ **B.** North-to-South
   - ❍ **C.** On-premises
   - ❍ **D.** West-to-South

5. What layer in three-tiered network architecture is considered the backbone of a network?
   - ❍ **A.** Core layer
   - ❍ **B.** Distribution/aggregation layer
   - ❍ **C.** Access/edge layer
   - ❍ **D.** Application layer

# Cram Quiz Answers

1. **C.** LUNs came from the SCSI world and carry over, acting as unique identifiers for devices. Both NAS and SAN use “targets” that hold up to eight devices.
2. **B.** The network architecture in which the database and the application exist on a single system is called a one-tiered model.
3. **D**. On a VLAN, multipathing creates multiple paths to the storage resources and can be used to increase availability and add fault tolerance.
4. **B.** North-South refers to data transfers between the datacenter and that outside of the network. East-West traffic is a concept referring to network traffic flow within a datacenter between servers. On-premises can be thought of as the old, traditional approach: the data and the servers are kept in house. Although West-to-South is a direction, it is not a valid specified data path.
5. **A.** The core layer is the backbone of the network where the fastest routers and switches operate to manage separate networks. The distribution/aggregation layer is between the access/edge and core layers. This is the “boundary” layer where ACLs and Layer 3 switches operate. The access/edge layer is the place where switches connect to and ensure data is delivered to edge/end devices. The application layer is the seventh and top layer of the OSI reference model.

# What's Next?

For the Network+ exam, and for routinely working with an existing network or implementing a new one, you need to identify the characteristics of network media and their associated cabling. Chapter 5, "Cabling Solutions and Issues," focuses on the media and connectors used in today's networks and what you are likely to find in wiring closets.

*This page intentionally left blank*

CHAPTER 5

# Cabling Solutions and Issues

**This chapter covers the following official Network+ objectives:**

- Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
- Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This chapter covers CompTIA Network+ objectives 1.3 and 5.2. For more information on the official Network+ exam topics, see the "About the Network+ Exam" section in the Introduction.

When working with an existing network or implementing a new one, you need to identify the characteristics of network media and their associated cabling. This chapter focuses on the media and connectors used in today's networks and how they fit into wiring closets and beyond.

# General Media Considerations

▶ **Summarize the types of cables and connectors and explain which is the appropriate type for a solution.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What are the two main types of twisted-pair wiring used today?
2. What is the name of the wiring standard that offers a minimum of 500 MHz of bandwidth and specifies transmission distances up to 100 meters with 10 Gbps?
3. What is the difference between RJ-11 and RJ-45 connectors?
4. What are the two most common connectors used with fiber-optic cabling?
5. What are F-type connectors used for?

### Answers

1. The two main types of twisted-pair cabling in use today are unshielded twisted-pair (UTP) and shielded twisted-pair (STP).
2. Category 6a (Cat 6a) offers improvements over Category 6 (Cat 6) by offering a minimum of 500 MHz of bandwidth. It specifies transmission distances up to 100 meters with 10 Gbps networking speeds.
3. RJ-11 connectors are used with standard phone lines and are similar in appearance to RJ-45 connectors used in networking. However, RJ-11 connectors are smaller. RJ-45 connectors are used with UTP cabling.
4. Fiber-optic cabling uses a variety of connectors, but SC and ST are more commonly used than others. ST connectors offer a twist-type attachment, whereas SCs have a push-on connector. LC and MTRJ are other types of fiber-optic connectors. In environments where vibration can be a problem, FC connectors can be used and feature a threaded body.
5. F-type connectors are used to connect coaxial cable to devices such as Internet modems.

In addition to identifying the characteristics of network media and their associated cabling, the Network+ exam requires knowledge of some general terms and concepts that are associated with network media. Before you look at the individual media types, it is a good idea to first have an understanding of some general media considerations.

ExamAlert

Remember that this objective begins with "Summarize the types of cables and connectors." This means that you will need to be able to explain which is the appropriate cable or connector type for a solution.

# Broadband Versus Baseband Transmissions

Networks employ two types of signaling methods/modulation techniques:

- **Baseband transmissions:** Baseband transmissions use digital signaling over a single wire. Communication on baseband transmissions is bidirectional, enabling signals to be sent and received, but not at the same time. To send multiple signals on a single cable, baseband uses something called *time-division multiplexing (TDM)*. TDM divides a single channel into time slots. The key thing about TDM is that it does not change how baseband transmission works—only how data is placed on the cable.

ExamAlert

Most networks use baseband transmissions. (Notice the word *base*.) Examples are 1000BASE-T and 10GBASE-T.

- **Broadband transmissions:** In terms of LAN network standards, broadband transmissions use analog transmissions. For broadband transmissions to be sent and received, the medium must be split into two channels. (Alternatively, two cables can be used: one to send and one to receive transmissions.) Multiple channels are created using *frequency-division multiplexing (FDM)*. FDM enables broadband media to accommodate traffic going in different directions on a single medium at the same time.

# Simplex, Half-Duplex, and Full-Duplex Modes

Simplex, half-duplex, and full-duplex modes are referred to as *dialog modes*, and they determine the direction in which data can flow through the network media:

- Simplex mode enables one-way communication of data through the network, with the full bandwidth of the cable used for the transmitting signal. One-way communication is of little use on LANs, making it unusual at best for network implementations.

- Far more common is half-duplex mode, which accommodates transmitting and receiving on the network, but not at the same time. Many networks are configured for half-duplex communication.
- The preferred dialog mode for network communication is full-duplex mode. To use full-duplex, both the network card and the hub or switch must support full duplexing. Devices configured for full duplexing can simultaneously transmit and receive. This means that 100 Mbps network cards theoretically can transmit at 200 Mbps using full-duplex mode.

# Data Transmission Rates

One of the more important media considerations is the supported data transmission rate or speed. Different media types are rated to certain maximum speeds, but whether they are used to this maximum depends on the networking standard used and the network devices connected to the network.

> **Note**
>
> The transmission rate of media is sometimes incorrectly called the *bandwidth*. But the term *bandwidth* refers to the width of the range of electrical frequencies or the number of channels that the medium can support.

Transmission rates normally are measured by the number of data bits that can traverse the medium in a single second. In the early days of data communications, this measurement was expressed in bits per second (bps), but today's networks are measured in *megabits per second (Mbps)* and *gigabits per second (Gbps)*.

The different network media vary greatly in the transmission speeds they support. Many of today's application-intensive networks require more than the 10 Mbps or 100 Mbps offered by the older networking standards. In some cases, even 1 Gbps, which is found in many modern LANs, is not enough to meet current network needs. For this reason, many organizations now deploy 10 Gbps implementations.

# Types of Network Media

Whatever type of network is used, some type of network medium is needed to carry signals between computers. Two types of media are used in networks: cable-based media, such as twisted-pair, and the media types associated with wireless networking, such as radio waves.

In networks using cable-based media, there are two basic choices:

- Copper
- Fiber-optic

Copper wire is used with both twisted-pair and coaxial cables to conduct the signals electronically; fiber-optic cable uses a glass or plastic conductor and transmits the signals as light.

For many years, coaxial was the cable of choice for most LANs. Today, twisted-pair has proven to be the cable medium of choice, thus retiring coaxial to the confines of storage closets. Fiber-optic cable has seen a rise in popularity, but cost slowed its adoption to the home (although it is common today). It is widely used as a network backbone where segment length and higher speeds are needed and is common in server room environments as a server-to-switch connection method and in building-to-building connections in *metropolitan-area networks (MANs)*.

The following sections summarize the characteristics of each of these cable types.

## Twisted-Pair Cabling (Copper)

Twisted-pair cabling has been around for a long time. It was originally created for voice transmissions and has been widely used for telephone communication. Today, in addition to telephone communication, twisted-pair is the most widely used medium for networking.

The popularity of twisted-pair can be attributed to the fact that it is lighter, more flexible, and easier to install than coaxial or fiber-optic cable. It is also cheaper than other media alternatives and can achieve greater speeds than its coaxial competition. These factors make twisted-pair the ideal solution for most network environments.

Two main types of twisted-pair cabling are in use today: *unshielded twisted-pair (UTP)* and *shielded twisted-pair (STP)*. UTP is significantly more common than STP and is used for most networks. Shielded twisted-pair is used in environments in which greater resistance to EMI and attenuation is required. The greater resistance comes at a price, however. The additional shielding, plus the need to ground that shield (which requires special connectors), can significantly add to the cost of a cable installation of STP.

STP provides the extra shielding by using an insulating material that is wrapped around the wires within the cable. This extra protection increases the

distances that data signals can travel over STP but also increases the cost of the cabling. Figure 5.1 shows UTP and STP cabling.

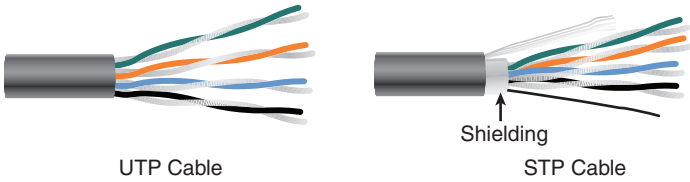



FIGURE 5.1 **UTP and STP cabling**

There are several categories of twisted-pair cabling. The early categories are most commonly associated with voice transmissions. The categories are specified by the *Electronic Industries Association/Telecommunications Industry Association (EIA/TIA)*. EIA/TIA is an organization that focuses on developing standards for electronic components, electronic information, telecommunications, and Internet security. These standards are important to ensure uniformity of components and devices.

> **Note**
>
> When learning about cabling, you need to understand the distinction between hertz and bits per second in relation to bandwidth. When you talk about bandwidth and a bits-per-second rating, you refer to a rate of data transfer.

EIA/TIA has specified a number of categories of twisted-pair cable, some of which are now obsolete. Those still in use today include the following:

- **Category 5:** This data-grade cable typically was used with Fast Ethernet operating at 100 Mbps with a transmission range of 100 meters. Although Category 5 was a popular media type, this cable is an outdated standard. Newer implementations use the 5e or greater standards. Category 5 provides a minimum of 100 MHz of bandwidth. Category 5, despite being used primarily for 10/100 Ethernet networking, can go faster. The IEEE 802.11ae standard specifies 1000 Mbps over Category 5 cable.
- **Category 5e:** This data-grade cable is used on networks that run at 10/100 Mbps and even up to 1000 Mbps. Category 5e cabling can be used up to 100 meters, depending on the implementation and standard used. Category 5e cable provides a minimum of 100 MHz of bandwidth.
- **Category 6:** This high-performance UTP cable can transmit data up to 10 Gbps. Category 6 has a minimum of 250 MHz of bandwidth and

specifies cable lengths up to 100 meters with 10/100/1000 Mbps transfer, along with 10 Gbps over shorter distances. Category 6 cable typically is made up of four twisted pairs of copper wire, but its capabilities far exceed those of other cable types. Category 6 twisted-pair uses a longitudinal separator, which separates each of the four pairs of wires from each other. This extra construction significantly reduces the amount of crosstalk in the cable and makes the faster transfer rates possible.

- **Category 6a:** Also called augmented 6, this cable offers improvements over Category 6 by offering a minimum of 500 MHz of bandwidth. It specifies transmission distances up to 100 meters with 10 Gbps networking speeds.
- **Category 7:** The big advantage to this cable is that shielding has been added to individual pairs and to the cable as a whole to greatly reduce crosstalk. It is rated for transmission of 600 MHz and is backward compatible with Category 5 and Category 6. Category 7 differs from the other cables in this group in that it is not recognized by the EIA/TIA and that it is shielded twisted pair, whereas all others listed as exam objectives are unshielded.
- **Category 8:** This standard was created for use where distances are short (such as between switches and servers in a datacenter). While it was not specifically intended for general office use (primarily due to cost), it will work great if used in a SOHO network because it can obtain speeds up to 40 Gbps at 2000 MHz and only for distances up to 30 meters (approximately 98 feet).

**ExamAlert**

On the exam, you might see these as Cat 5, Cat 5e, Cat 6, Cat 6a, Cat 7, and Cat 8. Remember their characteristics, such as cable length, speed, and bandwidth.

**Tip**

If you work on a network that is a few years old, you might need to determine which category of cable it uses. The easiest way to do this is to read the cable. The category number should be clearly printed on it.

Table 5.1 summarizes the categories and the speeds they support in common network implementations.

TABLE 5.1 **Twisted-Pair Cable Categories**

| Category | Common Application |
|---|---|
| 5 | 100 Mbps |
| 5e | 1000 Mbps (1 Gbps) |
| 6 | 10/100/1000 Mbps plus 10 Gbps |
| 6a | 10 Gbps and beyond networking |
| 7 | 10 Gbps and beyond networking |
| 8 | Up to 40 Gbps |

**Note**

The numbers shown in Table 5.1 refer to speeds these cables are commonly used to support. Ratified standards for these cabling categories might actually specify lower speeds than those listed, but cable and network component manufacturers are always pushing the performance envelope in the quest for greater speeds. The ratified standards define minimum specifications. For more information on cabling standards, visit the TIA website at www.tiaonline.org/.

# Coaxial Cables

*Coaxial cable*, or *coax* as it is commonly called, has been around for a long time. Coax found success in both TV signal transmission and network implementations. As shown in Figure 5.2, coax is constructed with a copper core at the center (the main wire) that carries the signal, insulation (made of plastic), ground (braided metal shielding), and insulation on the outside (an outer plastic covering).

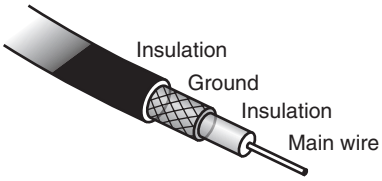



FIGURE 5.2 **Coaxial cabling**

Coaxial cable is constructed in this way to add resistance to *attenuation* (the loss of signal strength as the signal travels over distance), *crosstalk* (the degradation of a signal caused by signals from other cables running close to it), and EMI.

Two types of coax are used in networking: thin coax, also known as thinnet or 10BASE2, and thick coax, also known as *thicknet*. Neither is particularly popular anymore, but you are most likely to encounter thin coax. Thick coax was used primarily for backbone cable. It could be run through plenum spaces because it offered significant resistance to EMI and crosstalk and could run in lengths up to 500 meters. Thick coax offers speeds up to 10 Mbps, far too slow for today's network environments.

Thin coax is much more likely to be seen than thick coax in today's networks, but it isn't common. Thin coax is only 0.25 inch in diameter, making it fairly easy to install. Unfortunately, one of the disadvantages of all thin coax types is that they are prone to cable breaks, which increase the difficulty when installing and troubleshooting coaxial-based networks.

Several types of thin coax cable exist, each of which has a specific use. Table 5.2 summarizes these categories.

**ExamAlert**

For the exam, you should focus on RG-6 and know the difference between it and RG-59.

TABLE 5.2 **Thin Coax Categories**

| Cable Type | Description |
|---|---|
| RG-59 | Used to generate low-power video connections. The RG-59 cable cannot be used over long distances because of its high-frequency power losses. In such cases, RG-6 cables are used instead. |
| RG-6 | Often used for cable TV and cable modems. |

## Twinaxial Cables

*Twinaxial cable*, or *twinax*, is like coaxial but with two inner conductors instead of one. As shown in Figure 5.3, twinax is constructed with two wires at the center, insulation, ground (braided metal shielding), and insulation on the outside (an outer plastic covering). These cables are commonly used for short distances (7 meters or less) and are popular with SFP (Small Form Factor Pluggable) use with transceivers (discussed a bit later).

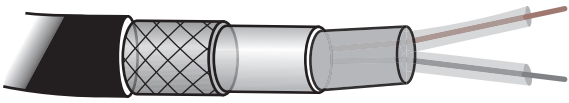


FIGURE 5.3 **Twinaxial cabling**

## Fiber-Optic Cables

In many ways, fiber-optic media addresses the shortcomings of copper-based media. Because fiber-based media use light transmissions instead of electronic pulses, threats such as EMI, crosstalk, and attenuation become nonissues. Fiber is well suited for the transfer of data, video, and voice transmissions. In addition, fiber-optic is the most secure of all cable media. Anyone trying to access data signals on a fiber-optic cable must physically tap into the medium. Given the composition of the cable, this is a particularly difficult task.

Unfortunately, despite the advantages of fiber-based media over copper, it still does not enjoy the popularity of twisted-pair cabling. The moderately difficult installation and maintenance procedures of fiber often require skilled technicians with specialized tools. Furthermore, the cost of a fiber-based solution limits the number of organizations that can afford to implement it. Another sometimes hidden drawback of implementing a fiber solution is the cost of retrofitting existing network equipment. Fiber is incompatible with most electronic network equipment. This means you have to purchase fiber-compatible network hardware.

**ExamAlert**

Fiber-optic cable, although still more expensive than other types of cable, is well suited for high-speed data communications. It eliminates the problems associated with copper-based media, such as near-end crosstalk, EMI, and signal tampering.

As shown in Figure 5.4, fiber-optic cable is composed of a core (glass fiber) that is surrounded by *cladding* (silica). A silicone coating is next, followed by a buffer jacket. There are strength members next, and then a protective sheath (polyurethane outer jacket) surrounds everything.

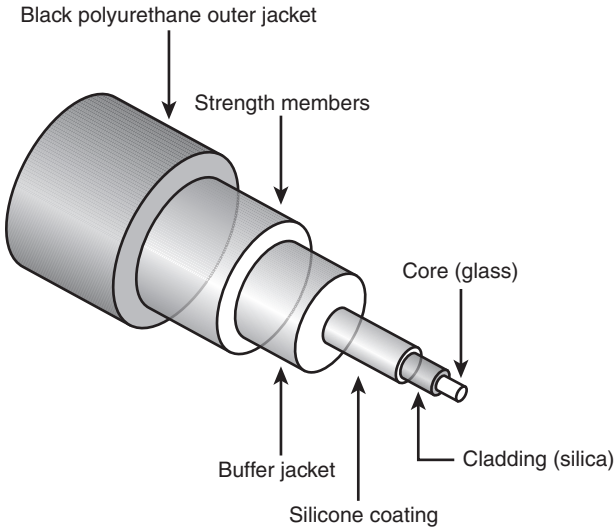



FIGURE 5.4 **Fiber-optic cabling**

Two types of fiber-optic cable are available:

- **Multimode fiber:** Many beams of light travel through the cable, bouncing off the cable walls. This strategy actually weakens the signal, reducing the length and speed at which the data signal can travel.
- **Single-mode fiber:** This type uses a single direct beam of light, thus allowing for greater distances and increased transfer speeds.

Some common types of fiber-optic cable include the following:

- 62.5-micron core/125-micron cladding multimode
- 50-micron core/125-micron cladding multimode
- 8.3-micron core/125-micron cladding single mode

In the ever-increasing search for bandwidth that can keep pace with the demands of modern applications, fiber-optic cables are sure to continue to play a key role.

ExamAlert

Understanding the types of fiber optics available focusing on single-mode and multimode, as well as their advantages and limitations, is important for real-world applications as well as the Network+ exam.

## Plenum Versus PVC Cables

A plenum is the mysterious space that resides between the false, or drop, ceiling and the true ceiling. This space typically is used for air conditioning and heating ducts. It might also hold a myriad of cables, including telephone, electrical, and networking. The cables that occupy this space must be plenum-rated rather than the standard PVC cables. Plenum cables are coated with a nonflammable material, often Teflon or Kynar, and they do not give off toxic fumes if they catch fire. As you might imagine, plenum-rated cables cost more than regular (PVC-based) cables, but they are mandatory when cables are not run through a conduit. As a bonus, plenum-rated cables suffer from less attenuation than nonplenum cables.

ExamAlert

Cables run through the plenum areas must have two important characteristics: They must be fire resistant, and they must not produce toxic fumes if exposed to intense heat.

# Types of Media Connectors

Various connectors are used with the associated network media. Media connectors attach to the transmission media and allow the physical connection into the computing device. For the Network+ exam, you need to identify the connectors associated with a specific medium. The following sections describe the connectors and associated media.

## BNC Connectors

BNC connectors are associated with coaxial media and 10BASE2 networks. BNC connectors are not as common as they previously were, but they still are used on some networks, older network cards, and older hubs. Common

BNC connectors include a barrel connector, T-connector, and terminators. Figure 5.5 shows two terminators (top and bottom) and two T-connectors (left and right).

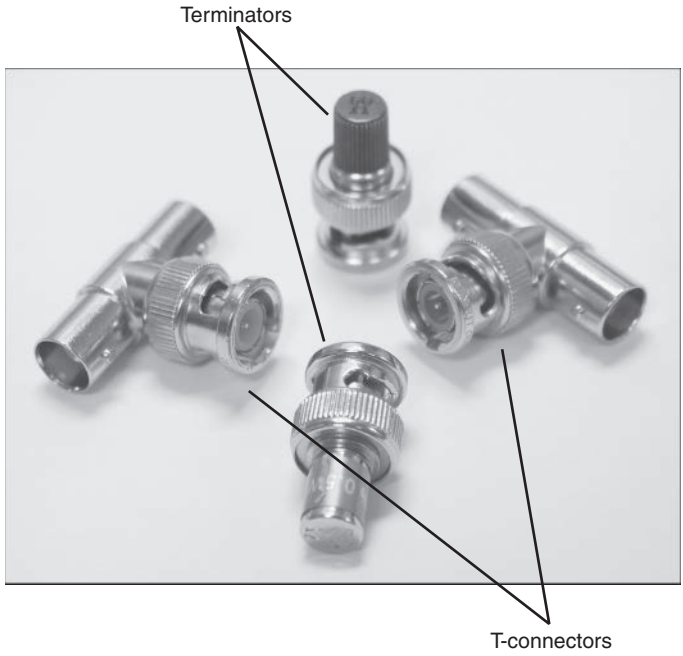



FIGURE 5.5 **BNC connectors**

ExamAlert

*Connectors* are sometimes referred to as *couplers*. For exam purposes, consider the two words to be synonyms.

## RJ-11 Connectors

*RJ-11 (Registered Jack)* connectors are small plastic connectors used on telephone cables. They have capacity for six small pins. However, in many cases, not all the pins are used. For example, a standard telephone connection uses only two pins, and a cable used for a *digital subscriber line (DSL)* modem connection uses four.

RJ-11 connectors are somewhat similar to RJ-45 connectors, which are discussed next, although they are a little smaller. Both RJ-11 and RJ-45 connectors have a small plastic flange on top of the connector to ensure a secure connection. Figure 5.6 shows two views of an RJ-11 connector.

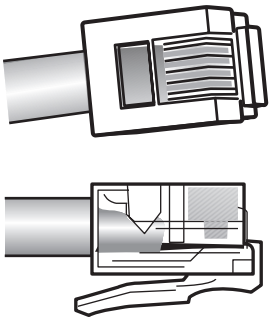


FIGURE 5.6 **RJ-11 connectors**

## RJ-45 Connectors

RJ-45 connectors, as shown in Figure 5.7, are the ones you are most likely to encounter in your network travels. RJ-45 connectors are used with twisted-pair cabling, the most prevalent network cable in use today. RJ-45 connectors resemble the aforementioned RJ-11 phone jacks, but they support up to eight wires instead of the six supported by RJ-11 connectors. RJ-45 connectors are also larger than RJ-11 connectors.

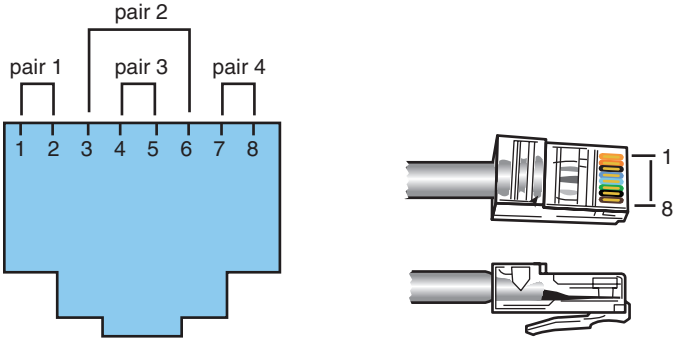



FIGURE 5.7 **RJ-45 connectors**

## F-Type Connectors and RG-59 and RG-6 Cables

F-type connectors, as shown in Figure 5.8, are screw-on connections used to attach coaxial cable to devices. This includes RG-59 and RG-6 cables. In the world of modern networking, F-type connectors are most commonly associated with connecting Internet modems to equipment from a cable or satellite *Internet service provider (ISP)*. However, F-type connectors are also used to connect to some proprietary peripherals.

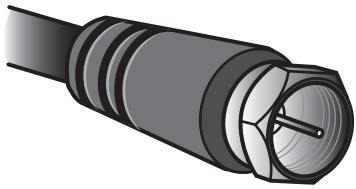


FIGURE 5.8 **F-type connector**

F-type connectors have a "nut" on the connection that provides something to grip as the connection is tightened by hand. If necessary, this nut can also be lightly gripped with pliers to aid disconnection.

**ExamAlert**

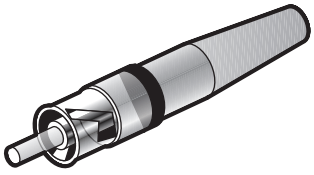
For the Network+ exam, you will be expected to identify the connectors discussed in this chapter by their appearance.

## Fiber Connectors

A variety of connectors are associated with fiber cabling, and there are several ways of connecting them. They include bayonet, snap-lock, and push-pull connectors. Figure 5.9 shows the fiber connectors identified in the Network+ objectives.

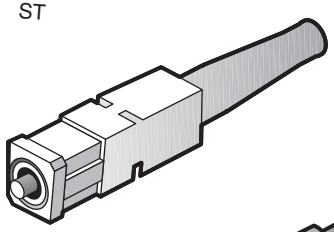
**ExamAlert**

As with the other connectors discussed in this section, be prepared to identify fiber connectors by their appearance and by how they are physically connected.



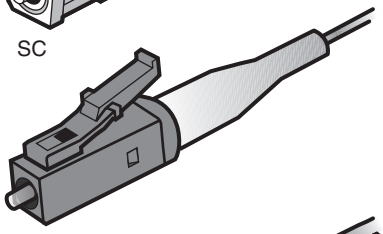
ST

The ST connector uses a half-twist bayonet type of lock.



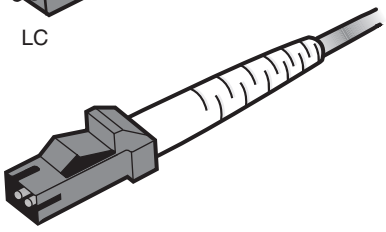
SC

The SC uses a push-pull connector similar to common audio and video plugs and sockets.



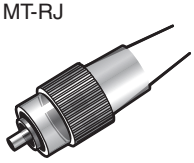
LC

LC connectors have a flange on top, similar to an RJ-45 connector, that aids secure connection.



MT-RJ

MT-RJ is a popular connector for two fibers in a very small form factor.



FC

FC connectors have a threaded body and are used in environments where vibration is a problem.

FIGURE 5.9 **Fiber connectors**

Within the various types of connectors (ST, SC, LC, MT-RJ, and so on), you can choose to purchase ones that are either *angled physical contact (APC)* or *ultra-physical contact (UPC)*. The biggest difference between these two is the "angle" present in APC. UPC connectors have an endface polished at a zero-degree angle (flat), whereas APC is eight degrees. As a general rule, the more polished (UPC) gives less insertion loss.

MT-RJ (standing for either Mechanical Transfer Registered Jack or Media Termination Recommended Jack) is popular for duplex multimode connections.

It is often written with the dash between the letters, but CompTIA prefers to use MTRJ in their objectives and on the exam.

## Transceivers

On routers, *small form-factor pluggable (SFP)* modules and *gigabit interface converter (GBIC)* modules are often used to link a gigabit Ethernet port with a fiber network (often 1000BASE-X). Both SFPs and GBICs exist for technologies other than fiber (Ethernet and SONET/SDH are usual), but connecting to fiber has become the most common use.

> **Note**
>
> *SFP+* is an enhanced small form-factor pluggable module; it is a newer version of SFP that supports data rates up to 16 Gbps. Quad Small Form-factor Pluggable (QSFP) is a different transceiver that is both compact and hot-pluggable; it has been jointly developed by many networking vendors. Similarly, *Enhanced QSFP+* is an evolution of QSFP that supports four channels.

Fiber transceivers are *bidirectional* and capable of operating in *duplex* mode. With either an SFP or GBIC, there is a *receiver port (RX)* and *transmitter port (TX)*. These devices are static-sensitive as well as dust-sensitive, and dirty connectors can cause intermittent problems. Care should be taken to not remove them more often than absolutely necessary to keep from shortening their life. After a module goes bad, they can be swapped for a new one to resolve the problem.

> **Note**
>
> Cisco has a great post on the care and maintenance of SFPs at www.cisco.com/en/US/products/hw/modules/ps4999/products_tech_note09186a00807a30d6.shtml.

Signal loss can occur not only from unclean connectors, but also from *connector mismatch*. Improper alignment and differences in core diameters contribute to signal loss.

When troubleshooting an SFP or GBIC, you should make sure that you do not have a *cable mismatch* or a *bad cable/transceiver*. As simple as it may sound, it is important to verify that you are using a single-mode fiber with a single-mode interface and a multimode fiber cable for a multimode interface. Such a *fiber type mismatch* can cause the physical link to go completely down but does not always do so, thus making troubleshooting it difficult.

# Media Couplers/Converters

When you have two dissimilar types of network media, a *media converter* is used to allow them to connect. They are sometimes referred to as *couplers*. Depending on the conversion being done, the converter can be a small device barely larger than the connectors themselves or a large device within a sizable chassis.

Reasons for not using the same media throughout the network, and thus reasons for needing a converter, can range from cost (gradually moving from coax to fiber), disparate segments (connecting the office to the factory), or needing to run a particular media in a setting (the need for fiber to reduce EMI problems in a small part of the building).

Figure 5.10 shows an example of a media converter. The one shown converts between 10/100/1000TX and SFP.

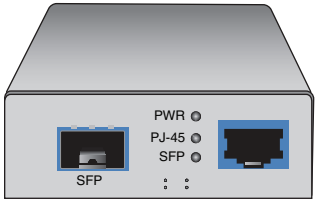



FIGURE 5.10 **A common media converter**

The following converters are commonly implemented and ones that CompTIA includes on the Network+ exam.

**ExamAlert**

Make sure you know that the possibilities listed here exist.

- Single mode fiber to Ethernet
- Single mode to multimode fiber
- Multimode fiber to Ethernet
- Fiber to coaxial

# TIA/EIA 568A and 568B Wiring Standards

568A and 568B are telecommunications standards from TIA and EIA. These 568 standards specify the pin arrangements for the RJ-45 connectors on UTP or STP cables. The number 568 refers to the order in which the wires within the cable are terminated and attached to the connector.

The *TIA/EIA 568A* and *568B* standards (often referred to as *T568A* and *T568B* for termination standard) are similar; the difference is the order in which the pins are terminated. The signal is the same for both. Both are used for patch cords in an Ethernet network.

**ExamAlert**

The only notable difference between T568A and T568B is that pairs 2 and 3 (orange and green) are swapped.

Network media might not always come with connectors attached, or you might need to make custom length cables. This is when you need to know something about how these standards actually work. Before you can crimp on the connectors, you need to know in which order the individual wires will be attached to the connector. Figure 5.11 shows the pin number assignments for the T568A and T568B standards.

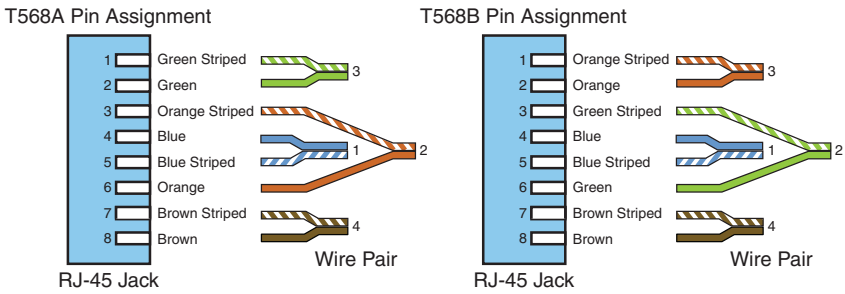



FIGURE 5.11 **Pin assignments for the T568A and T568B standards**

# Straight-Through Versus Crossover Cables

Two types of cables are used to connect devices to hubs and switches: crossover cables and straight-through cables. The difference between the two types is that in a crossover cable, two of the wires are crossed; in a straight-through cable, all the wires run straight through.

Specifically, in a crossover cable, wires 1 and 3 and wires 2 and 6 are crossed. Wire 1 at one end becomes wire 3 at the other end, wire 2 at one end becomes wire 6 at the other end, and vice versa in both cases. You can see the differences between the two cables in Figures 5.12 and 5.13. Figure 5.12 shows the pinouts for a straight-through cable, and Figure 5.13 shows the pinouts for a crossover cable.

## ExamAlert

The crossover cable can be used to directly network two PCs without using a hub or switch. This is done because the cable performs the function of the switch.

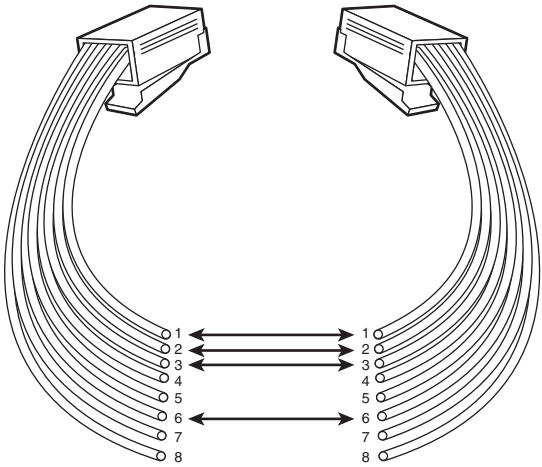



FIGURE 5.12 **Pinouts for a straight-through twisted-pair cable**

## Note

Auto MDI-X ports on newer interfaces detect whether the connection requires a crossover and automatically choose the MDI or MDI-X configuration to match the other end of the link.

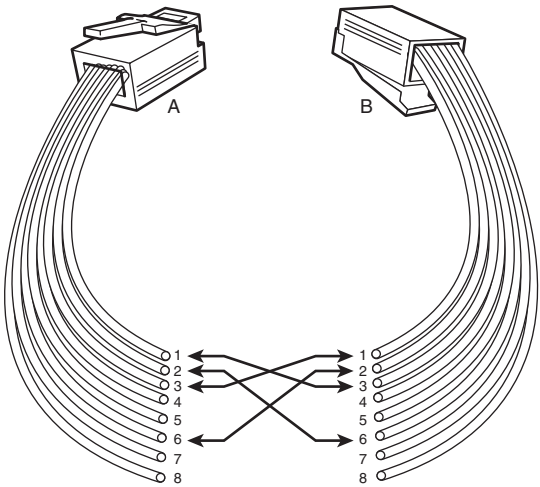



FIGURE 5.13 **Pinouts for a crossover twisted-pair cable**

To make a crossover Ethernet cable, you need to use both the 568A and 568B standards. One end of the cable can be wired according to the 568A standard and the other with the 568B standard.

A T1 crossover cable, the pinouts of which are shown in Figure 5.14, is used to connect two T1 CSU/DSU devices in a back-to-back configuration. RJ-45 connectors are used on both ends.

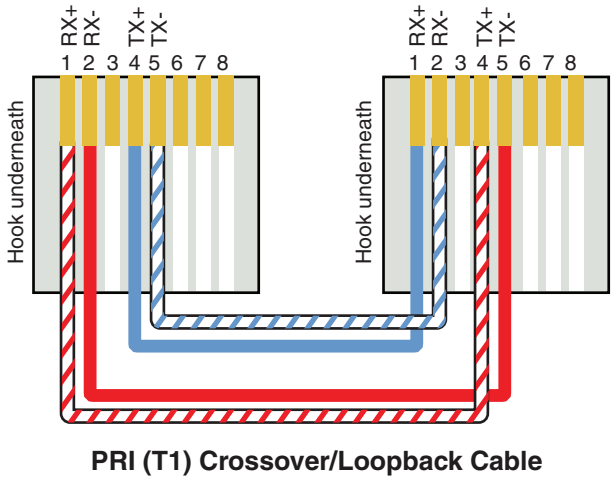



FIGURE 5.14 **Pinouts for a T1 crossover cable**

# Rollover and Loopback Cables

The rollover cable is a Cisco proprietary cable used to connect a computer system to a router or switch console port. The rollover cable resembles an Ethernet UTP cable; however, it is not possible to use it on anything but Cisco equipment. Like UTP cable, the rollover cable has eight wires inside and an RJ-45 connector on each end that connects to the router and the computer port.

As far as pinouts are concerned, pin 1 on one end of the rollover cable connects to pin 8 at the other end of the cable. Similarly, pin 2 connects to pin 7, and so on. The ends are simply reversed. As soon as one end of the rollover cable is connected to the PC and the other to the Cisco terminal, the Cisco equipment can be accessed from the computer system using a program such as PuTTY.

**ExamAlert**

Remember that the rollover cable is a proprietary cable used to connect a PC to a Cisco router.

A loopback cable, also known as a *plug*, is used to test and isolate network problems. If made correctly, the loopback plug causes the link light on a device such as a *network interface card (NIC)* to come on. This is a quick and cheap way to test simple network cabling problems. The loopback plug redirects outgoing data signals to the system. The system then believes that it is both sending and receiving data.

The loopback cable is basically a troubleshooting tool used to test the device to see if it is sending and receiving properly. It uses UTP cable and RJ-45 connectors.

ExamAlert

Know that a loopback cable is a basic troubleshooting tool.

# Components of Wiring Distribution

So far, this chapter has examined various types of media and the associated connectors. This section looks at wiring in the closet, the place in networks where you connect the cables and networking devices. These rooms have many names, including the wiring closet, the telecommunications room, and the *network operations center (NOC)*. These telecommunications rooms contain the key network devices, such as the hubs, routers, switches, and servers. These rooms also contain the network media, such as patch cables that connect network devices to horizontal cables and the rest of the network.

## Network Cross-Connects

The cable that runs throughout a network can be divided into two distinct sections:

- **Horizontal cabling:** Connects client systems to the network
- **Vertical (backbone) cabling:** Runs between floors to connect different locations on the network

Both of these cable types have to be consolidated and distributed from a location—a wiring closet.

Following are three types of cable distribution:

- **Vertical or main cross-connect:** The location where outside cables enter the building for distribution. This can include Internet and phone cabling.
- **Horizontal cross-connect:** The location where the vertical and horizontal connections meet.
- **Intermediate cross-connect:** A type typically used in larger networks. It provides an intermediate cross-connect between the main and horizontal cross-connects.

The term *cross-connect* refers to the point where the cables running throughout the network meet and are connected.

## Horizontal Cabling

Within the telecommunications room, horizontal cabling connects the telecommunications room to the end user, as shown in Figure 5.15. Specifically, the horizontal cabling extends from the telecommunications outlet, or a network outlet with RJ-45 connectors, at the client end. It includes all cable from that outlet to the telecommunications room to the horizontal cross-connect—the distribution point for the horizontal cable. The horizontal cross-connect includes all connecting hardware, such as patch panels and patch cords. The horizontal cross-connect is the termination point for all network horizontal cables.

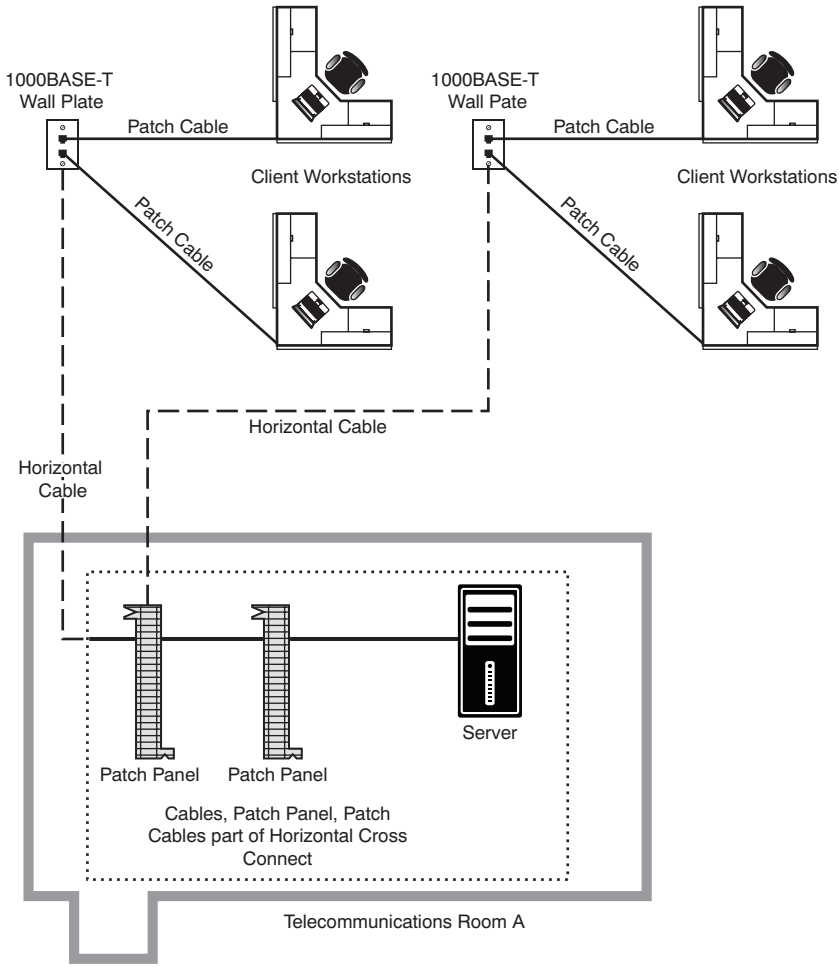



FIGURE 5.15 **Horizontal cabling**

Horizontal cabling runs within walls and ceilings and therefore is called *permanent cable* or *structure cable*. The length of cable running from the horizontal connects and the telecommunication outlet on the client side should not exceed 90 meters. Patch cables used typically should not exceed 5 meters because of the 100-meter distance limitation of most UTP cable.

**Note**

Horizontal wiring includes all cabling run from the wall plate or network connection to the telecommunications closet. The outlets, cable, and cross-connects in the closet are all part of the horizontal wiring, which gets its name because the cable typically runs horizontally above ceilings or along the floor.

## Vertical Cables

*Vertical cable*, or backbone cable, refers to the media used to connect telecommunications rooms, server rooms, and remote locations and offices. Vertical cable may be used to connect locations outside the local LAN that require high-speed connections. Therefore, vertical cable is often fiber-optic cable or high-speed UTP cable. Figure 5.16 shows the relationship between horizontal cable and vertical cable.

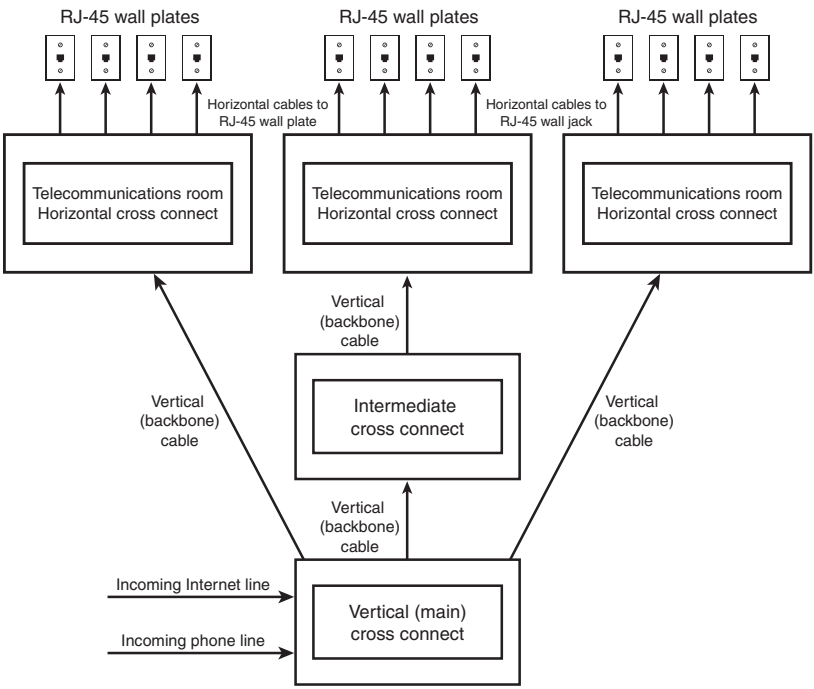



FIGURE 5.16 **Vertical and horizontal cabling**

## Patch Panels

If you have ever looked in a telecommunications room, you have probably seen a distribution block, more commonly called a patch panel. A *patch panel* is a freestanding or wall-mounted unit with a number of RJ-45 port connections on the front. In a way, it looks like a wall-mounted hub without the *light-emitting diodes (LEDs)*. The patch panel provides a connection point between network equipment, such as hubs and switches, and the ports to which PCs are connected, which normally are distributed throughout a building.

> **Note**
>
> Not all environments use patch panels. In some environments, cables run directly between systems and a hub or switch. This is an acceptable method of connectivity, but it is not as easy to make tidy as a structured cabling system that uses a patch panel system and wall or floor sockets.

Also found in a wiring closet is the punchdown block. The wires from a telephony or UTP cable are attached to the punchdown block using a *punchdown tool*. To use the punchdown tool, you place the wires in the tip of the tool and push it into the connectors attached to the punchdown block. The wire insulation is stripped, and the wires are firmly embedded into the metal connector. Because the connector strips the insulation on the wire, it is known rather grandiosely as an *insulation displacement connector (IDC)*. Figure 5.17 shows a punchdown tool used for placing wires into a patch panel.

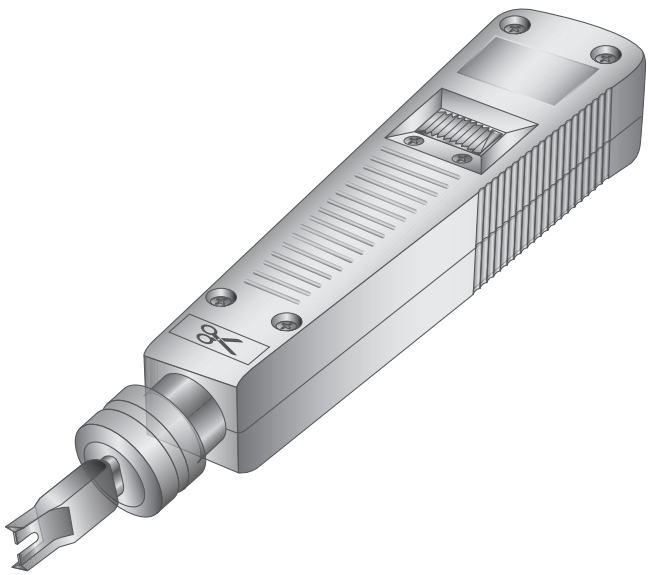


FIGURE 5.17 **Punchdown tool**

Using a punchdown tool is much faster than using wire strippers to prepare each individual wire and then twisting the wire around a connection pole or tightening a screw to hold the wire in place. In many environments, cable tasks are left to a specialized cable contractor. In others, the administrator is the one who must connect wires to a patch panel.

**ExamAlert**

Punchdown tools are used to attach twisted-pair network cable to connectors within a patch panel. Specifically, they connect twisted-pair wires to the IDC.

## Fiber Distribution Panels

Just as a patch panel is used to provide a connection point between network equipment, so too is a *fiber distribution panel (FDP)*. The difference between the two is that the FDP is a cabinet intended to provide space for termination, storage, and splicing of fiber connections.

**ExamAlert**

As you study for the exam, make sure you can identify the following exam objectives discussed here and the following: termination points, 66 block, 110 block, patch panel, and fiber distribution panel.

## 66 and 110 Blocks (T568A, T568B)

Two main types of punchdown blocks are used: type 66 and type 110. Type 66 is an older design used to connect wiring for telephone systems and other low-speed network systems and is not as widely used as type 110. The 66 block has 50 rows of IDC contacts to accommodate 25-pair twisted-pair cable. Block 66 was used primarily for voice communication. Although it was approved for Category 5 and greater, it is not really suitable for anything greater than 10BASE-T due to crosstalk problems. However, specialized certified blocks are available that do meet Cat 5e or Cat T6 termination standards.

In the network wiring closet, the 110 block is used to connect network cable to patch panels. The 110 connections can also be used at the other end of the network cable at the RJ-45 wall jack. The 110 blocks are preferred over the older 66 blocks because the 110 block improves on the 66 block by supporting higher frequencies and less crosstalk. Therefore, it supports higher-speed networks and higher-grade twisted-pair cable. The termination will be T568A or T568B, depending on which wiring standard is used.

In addition to 66 and 110 blocks, *Krone* and *Bix* blocks also exist. These two require different blades in the punchdown tools (Krone, for example, requires a separate scissor-like mechanism for trimming the wire) to work with them. Bix (Building Industry Cross-connect) is certified for Cat 5e and Cat 6. Bix is popular in older implementations and Krone is more popular internationally.

## MDF and IDF Wiring Closets

The preceding section looked at wiring closets. Two types of wiring closets are *main distribution frame (MDF)* and *intermediate distribution frame (IDF)*. The main wiring closet for a network typically holds the majority of the network gear, including routers, switches, wiring, servers, and more. This is also typically the wiring closet where outside lines run into the network. This main wiring closet is known as the MDF. One of the key components in the MDF is a primary patch panel. The network connector jacks attached to this patch panel lead out to the building for network connections.

In some networks, multiple wiring closets are used. When this is the case, the MDF connects to these secondary wiring closets, or IDFs, using a backbone cable. This backbone cable may be UTP, fiber, or even coaxial. In today's high-speed networks, UTP Gigabit Ethernet or high-speed fiber are the media of choice. Figure 5.18 shows the relationship between the MDF and the IDF.

**ExamAlert**

Be prepared to identify the difference between an IDF and an MDF. They are addressed in objective 3.2 and covered in Chapter 8, "Network Operations."

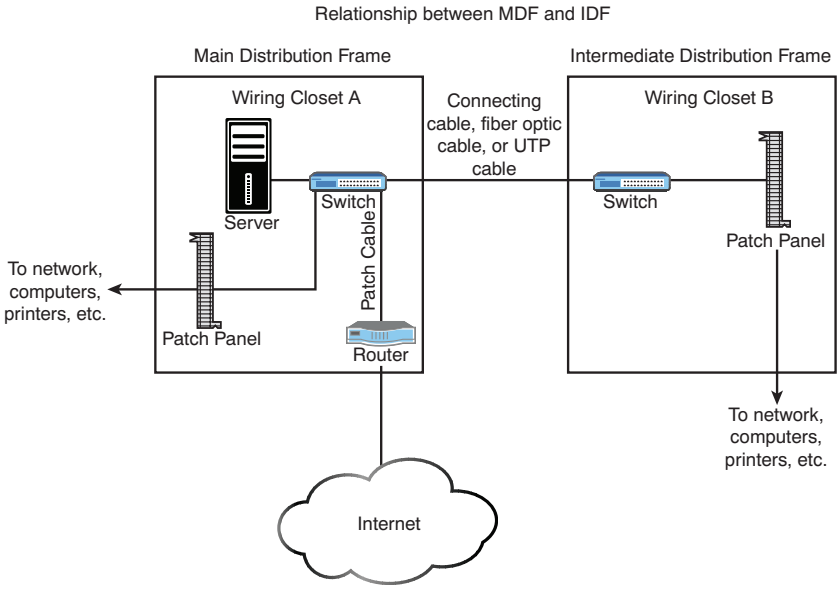



FIGURE 5.18 **The relationship between MDFs and IDFs**

# Ethernet Copper and Fiber Standards

A number of IEEE standards relate to networking and cover everything from implementation to security. The 802.3 standards relate to Ethernet deployment, and many of the early ones have become outdated. Make sure that you are familiar with the information that follows for the most popular standards presently before you take the Network+ exam.

## 10BASE-T

The 10BASE-T standard specifies an Ethernet network that commonly uses unshielded twisted-pair cable. In some implementations that require a greater resistance to interference and attenuation, STP can be used because it has extra shielding and is more able to combat interference.

**ExamAlert**

Hyphens have no meaning when it comes to wiring standards; 10BASE-T is the same as 10BaseT. Because CompTIA uses the hyphen in this round of objectives, this book does as well. Know that both notations mean the same thing.

The 10BASE-T standard uses broadband transmission and has a maximum physical segment length of 100 meters. Repeaters are sometimes used to extend the maximum segment length, although the repeating capability is now

often built into networking devices used in twisted-pair networks. 10BASE-T specifies transmission speeds of 10 Mbps and can use several categories of UTP cable with RJ-45 connectors. The maximum number of computers supported on a 10BASE-T network is 1,024.

## 100BASE-TX

At one time, 10 Mbps networks were considered fast enough, but those days are long gone. Today, companies and home users alike demand more bandwidth than that, and 100BASE-TX transmits network data at speeds up to 100 Mbps. 100BASE-TX is most often implemented with UTP cable, but it can use STP; therefore, it suffers from the same 100-meter distance limitations as other UTP-based networks. 100BASE-TX uses Category 5, or higher, UTP cable, and it uses independent transmit and receive paths and therefore can support full-duplex operation. 100BASE-TX is the most common implementation of the Fast Ethernet (802.3u) standard.

> **Tip**
>
> Repeaters are sometimes needed when you connect segments that use 100BASE-TX or 100BASE-FX.

A counterpart to 100BASE-TX is 100BASE-FX, which is the IEEE standard for running Fast Ethernet over fiber-optic cable. Due to the expense of fiber implementations, 100BASE-FX is largely limited to use as a network backbone. 100BASE-FX can use two-strand multimode fiber or single-mode fiber media. The maximum segment length for half-duplex multimode fiber is 412 meters, but this maximum increases to an impressive 10,000 meters for full-duplex single-mode fiber. 100BASE-FX often uses SC or ST fiber connectors. Table 5.3 summarizes the characteristics of the 802.3u Fast Ethernet specifications.

TABLE 5.3 **Summary of 802.3u Fast Ethernet Characteristics**

| Characteristic | 100BASE-TX | 100BASE-FX |
|---|---|---|
| Transmission method | Baseband | Baseband |
| Speed | 100 Mbps | 100 Mbps |
| Distance | 100 meters | 412 meters (multimode half duplex); 10,000 meters (single-mode full duplex) |
| Cable type | Category UTP, STP | Fiber-optic |
| Connector type | RJ-45 | SC, ST |

An additional fiber option, 100BASE-SX, is considered a lower-cost alternative to 100BASE-FX. It uses LEDs instead of lasers and can be used for shorter distances (up to 300 meters).

# 1000BASE-T

The Gigabit Ethernet standard 1000BASE-T, or 1000BASE-TX, is given the IEEE 802.3ab designation. The 802.3ab standard specifies Gigabit Ethernet over Category 5 or better UTP cable. The standard allows for full-duplex transmission using the four pairs of twisted cable. To reach speeds of 1000 Mbps over copper, a data transmission speed of 250 Mbps is achieved over each pair of twisted-pair cable. Table 5.4 summarizes the characteristics of 1000BASE-T.

TABLE 5.4 **Summary of 1000BASE-T Characteristics**

| Characteristic | Description |
|---|---|
| Transmission method | Baseband |
| Speed | 1000 Mbps |
| Total distance/segment | 75 meters |
| Cable type | Category 5 or better |
| Connector type | RJ-45 |

# 10GBASE-T

The 802.3an standard brings 10-gigabit speed to regular copper cabling. Although transmission distances may not be that of fiber, it allows a potential upgrade from 1000 Mbps networking to 10 Gbps networking using the current wiring infrastructure.

The 10GBASE-T standard specifies 10 Gbps transmissions over UTP or STP twisted-pair cables. The standard calls for a cable specification of Category 6 or Category 6a. With Category 6, the maximum transmission range is 55 meters; with the augmented Category 6a cable, transmission range increases to 100 meters. Category 6 and 6a cables are specifically designed to reduce attenuation and crosstalk, making 10 Gbps speeds possible. The 802.3an standard specifies regular RJ-45 networking connectors. Table 5.5 outlines the characteristics of this standard.

TABLE 5.5 **Summary of 802.3an Characteristics**

| Characteristic | Descriptions |
|---|---|
| Transmission method | Baseband |
| Speed | 10 Gbps |
| Total distance/segment | 100 meters Category 6a cable; 55 meters Category 6 cable |
| Cable type | Category 6, 6a UTP or STP |
| Connector | RJ-45 |

# 40GBASE-T

The 40GBASE-T standard provides for 4-pair balanced (40 Gbps on 4-twisted pairs cable) twisted-pair Category 8 copper cabling up to 30 meters. It is defined in the IEEE 802.3bq standard it is expected to be used primarily within datacenters.

Table 5.6 outlines the characteristics of the 802.3bq standard.

TABLE 5.6 **Summary of 802.3bq Characteristics**

| Characteristic | Descriptions |
|---|---|
| Transmission method | Baseband |
| Speed | 40 Gbps |
| Total distance/segment | 30 meters Category 8 cable |
| Cable type | Category 8 |
| Connector | RJ-45 |

# 1000BASE-LX and 1000BASE-SX

Both 1000BASE-LX and 1000BASE-SX are Gigabit Ethernet standards for fiber.

As a fiber standard for Gigabit Ethernet, 1000BASE-LX utilizes single-mode fiber. It can also run over multimode fiber with a maximum segment length of 550m.

The 1000BASE-SX standard is intended for use with multimode fiber and has a maximum length of 220 meters for default installations (550 meters is possible with the right optics and terminations). This standard is popular for intrabuilding links in office buildings.

## 10GBASE-LR and 10GBASE-SR

The 10GBASE-LR standard is easy to remember in that the *LR* stands for long range: the maximum fiber length is 10 kilometers, but it varies greatly depending on the type of single-mode fiber used. 10GBASE-SR is a multimode fiber intended for the short range (up to 400 meters): it is considered the lowest cost, lowest power, and smallest form factor optical option available at this speed.

# Multiplexing Options

Virtual circuits establish a bidirectional communication link between devices and use it for their communication links. Multiplexing was discussed earlier in the "Broadband Versus Baseband Transmissions" section, but you should know that bidirectional wavelength division multiplexing (WDM) is the transmission of optical channels on a fiber propagating simultaneously in both directions.

Several types of WDM multiplexing can be employed during these links. One form of multiplexing optical signals is *dense wavelength-division multiplexing (DWDM)*. This method replaces SONET/SDH regenerators and can amplify the signal and enable it to travel a greater distance. The main components of a DWDM system include the following:

- Terminal multiplexer
- Line repeaters
- Terminal demultiplexer

**ExamAlert**

Make sure that you understand that DWDM works with SONET/SDH.

An alternative to DWDM is *coarse wavelength-division multiplexing (CWDM)*. This method is commonly used with television cable networks. The main thing to know about it is that it has relaxed stabilization requirements; thus, you can have vastly different speeds for download than upload.

**ExamAlert**

Make sure that you associate CWDM with television cabling.

# Cram Quiz

1. Which of following connectors is commonly used with fiber cabling?
   - ❍ **A.** RJ-45
   - ❍ **B.** BNC
   - ❍ **C.** SC
   - ❍ **D.** RJ-11

2. What kind of cable would you associate with an F-type connector?
   - ❍ **A.** Fiber-optic
   - ❍ **B.** UTP
   - ❍ **C.** Coaxial
   - ❍ **D.** STP

3. Which of the following is not a type of fiber-optic connector used in network implementations?
   - ❍ **A.** MTRJ
   - ❍ **B.** SC
   - ❍ **C.** BNC
   - ❍ **D.** LC

4. Which of the following fiber connectors uses a twist-type connection method?
   - ❍ **A.** ST
   - ❍ **B.** SC
   - ❍ **C.** BNC
   - ❍ **D.** SA

5. Which of the following is a fiber standard for Gigabit Ethernet that utilizes single-mode fiber?
   - ❍ **A.** 1000BASE-SX
   - ❍ **B.** TIA/EIA 568a
   - ❍ **C.** RG-6
   - ❍ **D.** 1000BASE-LX

6. In a crossover cable, which wire is wire 1 crossed with?
   - ❍ **A.** 2
   - ❍ **B.** 3
   - ❍ **C.** 4
   - ❍ **D.** 5

7. What are the main types of punchdown blocks? (Choose two.)
   - ❍ **A.** 110
   - ❍ **B.** 220
   - ❍ **C.** 66
   - ❍ **D.** 12

8. Which of the following are cables that are specifically coated with a nonflammable material and do not give off toxic fumes if they catch fire?
   - ❍ **A.** SFP and GBIC
   - ❍ **B.** Cat 5e, Cat 6, Cat 6a
   - ❍ **C.** FDP
   - ❍ **D.** Plenum-rated

# Cram Quiz Answers

1. **C.** SC connectors are used with fiber-optic cable. RJ-45 connectors are used with UTP cable, BNC is used for thin coax cable, and RJ-11 is used for regular phone connectors.
2. **C.** F-type connectors are used with coaxial cables. They are not used with fiber-optic, unshielded twisted-pair (UTP), or shielded twisted-pair (STP) cabling.
3. **C.** BNC is a connector type used with coaxial cabling. It is not used as a connector for fiber-optic cabling. MTRJ, SC, and LC are all recognized types of fiber-optic connectors.
4. **A.** ST fiber connectors use a twist-type connection method. SC connectors use a push-type connection method. The other choices are not valid fiber connectors.
5. **D.** The 1000BASE-LX fiber standard for Gigabit Ethernet utilizes single-mode fiber. 1000BASE-SX is intended for use with multimode fiber and has a maximum length of 220 meters for default installations. TIA/EIA 568A (and 568B) are telecommunications standards that specify the pin arrangements for the RJ-45 connectors on UTP or STP cables. RG-6 is a common type of coaxial cable often used for cable TV and cable modems.
6. **B.** In a crossover cable, wires 1 and 3 and wires 2 and 6 are crossed.
7. **A, C.** The two main types of punchdown blocks are type 66 and type 110. Type 66 is an older design used to connect wiring for telephone systems and other low-speed network systems and is not as widely used as type 110.
8. **D.** Plenum-rated cables are coated with a nonflammable material, often Teflon or Kynar, and they do not give off toxic fumes if they catch fire. On routers, SFP modules and GBIC modules are often used to link a gigabit Ethernet port with a fiber network. Cat 5, Cat 5e, Cat 6, Cat 6a, and also Cat 7 and Cat 8 are general categories of twisted-pair cabling. FDP is an acronym for fiber distribution panel, which is a cabinet intended to provide space for termination, storage, and splicing of fiber connections.

# Troubleshooting Common Cable Connectivity Issues

- **Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What is the correct term for delay time on a satellite-based network?
2. What are two types of crosstalk?
3. What tools are used to attach twisted-pair network cable to connectors within a patch panel?
4. What are the two parts of a toner probe?

### Answers

1. Latency is the time of the delay.
2. Two types of crosstalk are near-end (NEXT) and far-end crosstalk (FEXT).
3. Punchdown tools are used to attach twisted-pair network cable to connectors within a patch panel.
4. A toner probe has two parts: the tone generator, or toner, and the tone locator, or probe.

### ExamAlert

Remember that this objective begins with "Given a scenario." This means that you may receive a drag and drop, matching, or "live OS" scenario where you have to click through to complete a specific objective-based task.

When administering a wired network, you should be aware of a number of performance issues and common connectivity problems. Some of the topics lumped within this objective are more knowledge/definitions than actionable items, but make sure you are familiar with them all the same. We first look at some limitations, considerations, and issues. Following that, we discuss some of the common tools used by network technicians.

# Limitations, Considerations, and Issues

Specifications and issues abound when trying to optimize a network and keep it up and running. It is very rare for resource demands to lessen over time, and they only seem to grow. Keeping up with that growth requires taking a lot into consideration and knowing the limitations of each technology. In the sections that follow, we look at some of the specifications/limitations and common issues associated with them.

## Throughput, Speed, and Distance

There must be enough bandwidth to serve all users, and you need to be alert for bandwidth hogs. You want to look for top talkers (those that transmit the most) and top listeners (those that receive the most) and figure out why they are so popular.

In the networking world, *throughput* refers to the rate of data delivery over a communication channel. In this case, throughput testers test the rate of data delivery over a network. Throughput is measured in *bits per second (bps)*. Testing throughput is important for administrators to make them aware of exactly what the network is doing. With throughput testing, you can tell whether a high-speed network is functioning close to its expected throughput.

A throughput tester is designed to quickly gather information about network functionality—specifically, the average overall network throughput. Many software-based throughput testers are available online—some for free and some for a fee.

As you can see, throughput testers do not need to be complicated to be effective. A throughput tester tells you how long it takes to send data to a destination point and receive an acknowledgment that the data was received. To use the tester, enter the beginning point and then the destination point. The tester sends a predetermined number of data packets to the destination and then reports on the throughput level. The results typically display in *kilobits per second (Kbps)*, *megabits per second (Mbps)*, or *gigabits per second (Gbps)*. Table 5.7 shows the various data rate units.

TABLE 5.7 **Data Rate Units**

| Data Transfer | Abbreviation | Speed |
|---|---|---|
| Kilobits per second | Kbps or Kbit/s | 1,000 bits per second |
| Megabits per second | Mbps or Mbit/s | 1,000,000 bits per second |
| Gigabits per second | Gbps or Gbit/s | 1,000,000,000 bits per second |
| Kilobytes per second | KBps | 1,000 bytes per second, or 8 kilobits per second |
| Megabytes per second | MBps | 1,000,000 bytes per second, or 8 megabits per second |
| Gigabytes per second | GBps | 1,000,000,000 bytes per second, or 8 gigabits per second |

Administrators and techs can periodically conduct throughput tests and keep them on file to create a picture of network performance. If you suspect a problem with the network functioning, you can run a test to compare with past performance to see exactly what is happening.

One thing worth mentioning is the difference between throughput and bandwidth. These terms are often used interchangeably, but they have different meanings. When talking about measuring throughput, you measure the amount of data flow under real-world conditions—measuring with possible electromagnetic interference (EMI) influences, heavy traffic loads, improper wiring, and even network collisions. Take all this into account, take a measurement, and you have the network throughput. Bandwidth, in contrast, refers to the maximum amount of information that can be sent through a particular medium under ideal conditions.

**Note**

Be sure that you know the difference between throughput and bandwidth/speed.

# Cabling Specifications/Limitations

Earlier in this chapter, we discussed the cabling types (Cat 7, Cat 8, etc.) that are available. Each of those categories of cables comes with its own limitations for throughput, speed, and distance—the three variables that a network administrator must so often juggle and balance.

Two types of websites that can be invaluable when it comes to networking are *speed test sites* and *looking-glass sites*. Speed test sites, as the name implies, are *bandwidth speed testers* that report the speed of the connection that you have to them and can be helpful in determining if you are getting the rate your ISP has promised.

Looking-glass sites are servers running *looking-glass (LG)* software that enables you to see routing information. The servers act as a read-only portal giving information about the backbone connection. Most of these servers will show **ping** information, trace (**tracert/traceroute**) information, and Border Gateway Protocol (BGP) information.

# Cabling Considerations

When you're considering what cabling option to go with, money is almost always a factor. While the best option is always to use the best cabling and best devices, financial officers often insist that everything be done with in budgetary constraints that prohibit always using the best. This means that you often have to work with what you have and try to keep it up and running cost-efficiently when things go wrong.

Damaged or bad wiring could be a patch cable (easy to replace) or the in-wall wiring (more difficult to replace). If you suspect wiring to be the faulty component, you can diagnose rather quickly by taking the device that is having trouble connecting to another location and/or bringing a working machine to this environment. You can use a multifunction cable tester to troubleshoot most wiring problems. You must check for cable continuity, as well as for shorts.

> **Note**
>
> Never assume that the cable you use is good until you test it and confirm that it is good. Sometimes cables break, and bad media can cause network problems.

Bent pins on a network cable or socket can result in very little or no contact being made on those connections. If the problem is with the cable, you can replace the cable. If the problem is with the client machine, it can be difficult

to fix because most Ethernet ports are soldered directly to the motherboard. Often, the solution is to abandon that port and use a USB/Ethernet adapter to allow the client to continue to connect to the network.

# Cabling Applications

Cabling can be used for many different scenarios; three common ones are as a crossover cable (used to connect any two devices of the same type), a rollover cable (used to connect a computer terminal to a router's console port), and a Power over Ethernet (PoE) cable (described in Chapter 3, "Addressing, Routing, and Switching").

An incorrect cable type—using a crossover cable instead of a standard cable, for instance—will keep the host from being able to communicate on the network. A cable tester can be used to diagnose individual cabling issues, and the solution is to swap the incorrect cable with one suited for the purpose you are intending to use it for.

# Attenuation and dB Loss

*Attenuation* refers to the weakening of data signals as they travel through a medium. Network media vary in their resistance to attenuation. Coaxial cable generally is more resistant than *unshielded twisted-pair (UTP)*; *shielded twisted-pair (STP)* is slightly more resistant than UTP; and fiber-optic cable does not suffer from attenuation. That's not to say that a signal does not weaken as it travels over fiber-optic cable, but the correct term for this weakening is *chromatic dispersion* rather than attenuation.

You must understand attenuation or chromatic dispersion and the maximum distances specified for network media. Exceeding a medium's distance without using repeaters can cause hard-to-troubleshoot network problems. A repeater is a network device that amplifies data signals as they pass, enabling them to travel farther. Most attenuation-related or chromatic dispersion-related difficulties on a network require using a network analyzer to detect them.

All media have recommended lengths at which the cable can be run. The reason is that data signals weaken as they travel farther from the point of origin. If the signal travels far enough, it can weaken so much that it becomes unusable. The weakening of data signals as they traverse the medium is called attenuation. The measurement of it is done in decibels; thus, attenuation is also known as *dB loss*.

All copper-based cabling is particularity susceptible to attenuation. When cable lengths have to be run farther than the recommended lengths, signal repeaters can be used to boost the signal as it travels. If you work on a network with intermittent problems, and you notice that cable lengths are run too far, attenuation may be the problem.

**ExamAlert**

For the Network+ objective referencing cable problems associated with distance, think of attenuation.

# Interference

Depending on where network cabling (commonly called *media*) is installed, *interference* can be a major consideration. Two types of media interference can adversely affect data transmissions over network media: *electromagnetic interference (EMI)* and crosstalk (discussed earlier).

EMI is a problem when cables are installed near electrical devices, such as air conditioners or fluorescent light fixtures. If a network medium is placed close enough to such a device, the signal within the cable might become corrupt. Network media vary in their resistance to the effects of EMI. Standard *unshielded twisted-pair (UTP)* cable is susceptible to EMI, whereas fiber cable, with its light transmissions, is resistant to EMI. When deciding on a particular medium, consider where it will run and the impact EMI can have on the installation.

EMI can reduce or corrupt signal strength. This can happen when cables are run too close to everyday office fixtures, such as computer monitors, fluorescent lights, elevators, microwaves, and anything else that creates an electromagnetic field. Again, the solution is to carefully run cables away from such devices. If they have to be run through EMI areas, shielded cabling or fiber cabling is needed.

# Incorrect Pinout

Most splits in a cable are intentional—enabling you to run the wiring in multiple directions with the use of a splitter. Depending on the type of cabling in question, it is not uncommon for each split to reduce the strength of the signal. It is also not uncommon for splitters to go bad. You should split the cable as few times as possible and check the splitter if a problem in a run that was normally working suddenly occurs.

If the split is unintentional, you are often dealing with an open/short, which is discussed later.

# Bad Ports

On the router, the port configuration dictates what traffic is allowed to flow through. The router can be configured to enable individual port traffic in, out, or both and is referred to as *port forwarding*. If a port is blocked (such as 80 for HTTP or 21 for FTP), the data will not be allowed through, and users will be affected.

**ExamAlert**

Think of port configuration and port forwarding as the same when it comes to the router.

A condition known as a *black hole* can occur when a router does not send back an expected message that the data has been received. It is known as a black hole from the view that data is being sent, but is essentially being lost.

This condition occurs when the packet the router receives is larger than the configured size of the *maximum transmission unit (MTU)* and the Don't Fragment flag is configured on that packet. When this condition occurs, the router is supposed to send a "Destination Unreachable" message back to the host. If the packet is not received, the host does not know that the packet did not go through.

Although there are several solutions to this problem, the best is to verify whether a mismatch has occurred between the maximum size packet that clients can send and that the router can handle. You can use **ping** to check that packets of a particular size can move through the router by using the **-l** parameter to set a packet size and the **-f** parameter to set the Do Not Fragment bit.

# Open/Short

In addition to the common issue of miswiring, other problems that can occur with cables (and that can be checked with a multifunction cable tester) include *open/short* faults. An open fault means that the cables are not making a full circuit; this can be due to a cut in the cable (across all or some of the wires). A short fault means that the data attempts to travel on wires other than those for which it is intended; this can be caused by miswiring or a twist in the cabling at a cut allowing the bare wires to touch.

ExamAlert

You should expect questions asking you what tool can be used to identify an open/short fault.

# LED Status Indicators

Hubs and switches provide light-emitting diodes (LEDs) that provide information on the port status. For instance, by using the LEDs, you can determine whether there is a jabbering network card, whether there is a proper connection to the network device, and whether there are too many collisions on the network.

# Incorrect Transceivers

When troubleshooting an SFP or GBIC, you should make sure that you do not have a bad, or mismatched, transceiver. As simple as this advice may sound, it is important to verify that you are using a single-mode fiber with a single-mode interface and a multimode fiber cable for a multimode interface. Such a fiber type mismatch can cause the physical link to go completely down but does not always do so, thus making troubleshooting it difficult.

# Duplexing Issues

When configuring a client for the network, you must be aware of two settings: port speed and duplex settings. They are adjusted in Windows in the Network Properties area. Speed and duplex mismatches can slow data rates to a crawl and prevent high-bandwidth applications (such as voice or streaming video) from being possible.

You have several choices for port speed and duplex settings as Figure 5.19 illustrates. You can choose Auto Negotiation to detect the setting that the network uses. You also can choose one of the other settings to match the network configuration, such as 100 Mbps Half Duplex. If you work with a client system that is unable to log on to a network, you might need to ensure that the duplex setting and port speeds are correctly set for the network.

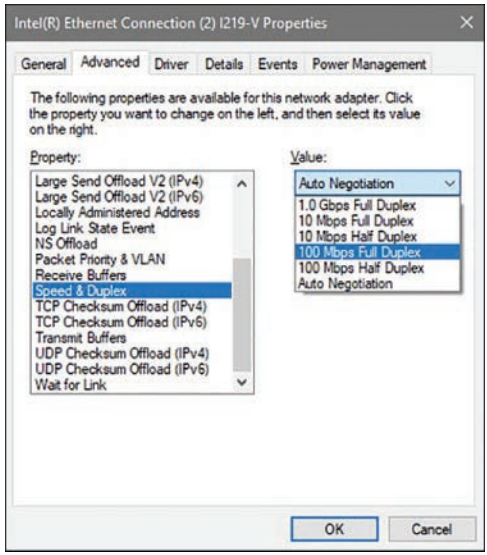



FIGURE 5.19 **Configuring speed and duplex options**

# TX/RX Reversed

Two primary types of cables can be used in an Ethernet network: a straight-through cable (as the name implies, all wires run straight through and are the same on both ends) and a crossover cable. In a crossover cable, two pairs of the wires are reversed; these are the TX and RX pairs (transmit and receive).

A crossover cable is intended to be used in specific applications only (such as to directly network two PCs without using a hub or switch) and will cause problems when used where a straight-through cable is called for (as a general rule, in all fixed wiring).

# Dirty Optical Cables

Dirty fiber cables—or, more commonly, connector—can cause a slowdown in traffic due to the need to be able to clearly transmit light. The "dirty" can be caused by exposure to liquids, dust, or other contaminants. Isopropyl alcohol can be used if wet cleaning is necessary (where it is not possible to simply blow away the dust).

# Common Tools

A large part of network administration involves having the right tools for the job and knowing when and how to use them. Selecting the correct tool for a networking job sounds like an easy task, but network administrators can choose from a mind-boggling number of tools and utilities.

Given the diverse range of tools and utilities available, it is unlikely that you will encounter all the tools available—or even all those discussed in this chapter. For the Network+ exam, you are required to have general knowledge of the tools available and what they are designed to do.

Until networks become completely wireless, network administrators can expect to spend some of their time using a variety of media-related troubleshooting and installation tools. Some of these tools (such as the tone generator and locator) may be used to troubleshoot media connections, and others (such as wire crimpers and punchdown tools) are used to create network cables and connections.

### The Basic Tools

Although many are costly, specialized networking tools and devices are available to network administrators and techs. The most widely used tools cost only a few dollars: the standard screwdrivers we use on almost a daily basis. As a network administrator or tech, you can expect with amazing regularity to take the case off a system to replace a network interface card (NIC) or perhaps remove the cover from a hub or switch to replace a fan. Advanced cable testers and other specialized tools will not help you when a screwdriver is needed.

## Cable Crimpers, Strippers, and Snips/Cutters

Wire crimpers, also known as cable crimpers, are tools you might regularly use. Like many things, making your own cables can be fun at first, but the novelty soon wears off. Basically, a wire crimper is a tool that you use to attach media connectors to the ends of cables. For instance, you use one type of wire crimper to attach RJ-45 connectors on unshielded twisted-pair (UTP) cable. You use a different type of wire crimper to attach British Naval Connectors/Bayonet Neill-Concelman (BNCs) to coaxial cabling.

> **Tip**
>
> When making cables, always order more connectors than you need; a few mishaps will probably occur along the way.

In a sense, you can think of a wire crimper as a pair of special pliers. You insert the cable and connector separately into the crimper, making sure that the wires in the cable align with the appropriate connectors. Then, by squeezing the crimper's handles, you force metal connectors through the cable's wires, making the connection between the wire and the connector.

When you crimp your own cables, you need to be sure to test them before putting them on the network. It takes only a momentary lapse to make a mistake when creating a cable, and you can waste time later trying to isolate a problem in a faulty cable.

Two other commonly used wiring tools are strippers and snips/cutters. Wire strippers come in a variety of shapes and sizes. Some are specifically designed to strip the outer sheathing from coaxial cable, and others are designed to work best with UTP cable. All strippers are designed to cleanly remove the sheathing from wire to make sure a clean contact can be made.

Many administrators do not have specialized wire strippers unless they do a lot of work with copper-based wiring. However, standard wire strippers are good things to have on hand.

Wire snips, also known as wire cutters, are tools designed to cleanly cut the cable. Sometimes network administrators buy cable in bulk and use wire snips to cut the cable into desired lengths. The wire strippers are then used to prepare the cable for the attachment of the connectors.

## Punchdown Tools

As discussed in the section titled "Patch Panels" earlier in this chapter, punchdown tools are used to attach twisted-pair network cable to connectors within a patch panel. Specifically, they connect twisted-pair wires to the insulation displacement connector (IDC).

# Tone Generator

A *toner probe* is a device that can save a network installer many hours of frustration. This device has two parts: the *tone generator*, or toner, and the *tone locator*, or probe. The toner sends the tone, and at the other end of the cable, the probe receives the toner's signal. This tool makes it easier to find the beginning and end of a cable. You might hear the tone generator and tone locator referred to as the *fox and hound*.

As you might expect, the purpose of the tone probe is to generate a signal that is transmitted on the wire you are attempting to locate. At the other end, you press the probe against individual wires. When it makes contact with the wire that has the signal on it, the locator emits an audible signal or tone.

The tone locator probe is a useful device, but it does have some drawbacks. First, it often takes two people to operate: one at each end of the cable. Of course, one person could just keep running back and forth, but if the cable is run over great distances, this can be a problem. Second, using the toner probe is time consuming because it must be attached to each cable independently.

**Note**

Many problems that can be discovered with a tone generator are easy to prevent by taking the time to properly label cables. If the cables are labeled at both ends, you will not need to use such a tool to locate them.

**Note**

Toner probes are specifically used to locate cables hidden in floors, ceilings, or walls and to track cables from the patch panels to their destinations.

# Loopback Adapter

A number of items fall under the loopback umbrella, and all of them serve the same purpose: they allow you to test a device/configuration/connectivity component using a dummy. The most popular loopback is the address used with ping (discussed later in this chapter), but Windows also includes a *loopback adapter*, which is a dummy network card (no hardware) used for testing a virtual network environment.

Various loopback adapters—actual hardware—can be purchased and used to test Ethernet jacks, fiber jacks, and so on.

# OTDR

A *time-domain reflectometer (TDR)* is a device used to send a signal through a particular medium to check the cable's continuity. Good-quality TDRs can locate many types of cabling faults, such as a severed sheath, damaged conductors, faulty crimps, shorts, loose connectors, and more. Although network administrators will not need to use a tool such as this every day, it could significantly help in the troubleshooting process. TDRs help ensure that data sent across the network is not interrupted by poor cabling that may cause faults in data delivery.

> **Note**
>
> TDRs work at the physical layer of the OSI model, sending a signal through a length of cable, looking for cable faults.

Because the majority of network cabling is copper based, most tools designed to test cabling are designed for copper-based cabling. However, when you test fiber-optic cable, you need an optical tester.

An optical cable tester performs the same basic function as a wire media tester, but on optical media. The most common problem with an optical cable is a break in the cable that prevents the signal from reaching the other end. Due to the extended distances that can be covered with fiber-optic cables, degradation is rarely an issue in a fiber-optic LAN environment.

Ascertaining whether a signal reaches the other end of a fiber-optic cable is relatively easy, but when you determine that there is a break, the problem becomes locating the break. That's when you need a tool called an *optical time-domain reflectometer (OTDR)*. By using an OTDR, you can locate how far along in the cable the break occurs. The connection on the other end of the cable might be the source of the problem, or perhaps there is a break halfway along the cable. Either way, an OTDR can pinpoint the problem.

Unless you work extensively with fiber-optic cable, you are unlikely to have an OTDR or even a fiber-optic cable tester in your toolbox. Specialized cabling contractors will have them, though, so knowing they exist is important.

You can use a *light meter* to certify and troubleshoot fiber. A light source is placed on one end, and the light meter is used at the opposite end to measure loss.

# Multimeter

One of the simplest cable-testing devices is a *multimeter*. By using the continuity setting, you can test for shorts in a length of coaxial cable. Or if you know the correct cable pinouts and have needlepoint probes, you can test twisted-pair cable.

A basic multimeter combines several electrical meters into a single unit that can measure voltage, current, and resistance. Advanced models can also measure temperature.

A multimeter has a display, terminals, probes, and a dial to select various measurement ranges. A digital multimeter has a numeric digital display, and an analog has a dial display. Inside a multimeter, the terminals are connected to different resistors, depending on the range selected.

Network multimeters can do much more than test electrical current:

- **Ping specific network devices:** A multimeter can ping and test response times of key networking equipment, such as routers, DNS servers, DHCP servers, and more.
- **Verify network cabling:** You can use a network multimeter to isolate cable shorts, split pairs, and other faults.
- **Locate and identify cable:** Quality network multimeters enable administrators to locate cables at patch panels and wall jacks using digital tones.
- **Documentation ability:** Multimeter results can be downloaded to a PC for inspection. Most network multimeters provide a means such as USB ports to link to a PC.

# Cable Tester

A media tester, also called a *cable tester*, defines a range of tools designed to test whether a cable properly works. Any tool that facilitates the testing of a cable can be deemed a cable tester. However, a specific tool called a *media tester* enables administrators to test a segment of cable, looking for shorts, improperly attached connectors, or other cable faults. All media testers tell you whether the cable works correctly and where the problem in the cable might be.

Generically, the phrase *line tester* can be used for any device that tests a media line. Although products are available that are Ethernet line testers, fiber line testers, and so on, most often a "line tester" is used to check telephone wiring and usually includes RJ-11 plugs as well as alligator clips.

A *cable certifier* is a type of tester that enables you to certify cabling by testing it for speed and performance to see that the implementation will live up to the ratings. Most stress and test the system based on noise and error testing. You need to know that the gigabit cable you think you have run is actually providing that speed to the network.

## Wire Map

A *wire map* (sometimes called a wiremap, without the space between the words) is a test (when run, called wire mapping) to see that all Ethernet wiring is correct and there are no opens, shorts, or wires reversed on one end.

## Tap

A *tap* is used to connect drop cables to a distribution cable much like a splitter. The difference between a tap and a splitter is that the splitter sends the incoming signal out to all paths equally, whereas a tap can apply a different amount of loss to each output path individually. This way, if you have one short path and one long path coming off the tap, the strength of the signal received by the host at the end of each path can be close to the same.

## Fusion Splicer

A *fusion splicer* is an expensive tool used to join two optical cables. The splicing is typically done by an electric arc but could also be a laser or a flame. It is important that the splice be as undetectable as possible in order to keep from scattering or reflecting light as it passes through the splice and reducing the quality of the transmission.

## Spectrum Analyzer

A *spectrum analyzer* measures the magnitude of an input signal versus frequency within the full frequency range of the instrument and can be used for a wide range of signals. Today, they are commonly used with Wi-Fi to reveal Wi-Fi hotspots and detect wireless network access with LED visual feedback. Such devices can be configured to scan specific frequencies. When working with 802.11b/g/n/ac/ax networks, you will most certainly require scanning for 2.4 GHz or 5 GHz RF signals.

Such devices can be used in the troubleshooting process to see where and how powerful RF signals are. Given the increase in wireless technologies, RF detectors are sure to continue to increase in popularity.

## Fiber Light Meter

A *fiber light meter* measures the light moving through an optical fiber to look for problems with a cable. To use the meter, you connect one end of the fiber to a light source and put the meter on the other end. The meter reads the light it receives and determines the amount of signal loss, if any.

# Cram Quiz

1. Which of the following describes the loss of signal strength as a signal travels through a particular medium?
   - ❍ **A.** Attenuation
   - ❍ **B.** Crosstalk
   - ❍ **C.** EMI
   - ❍ **D.** Chatter

2. A user calls to report that he is experiencing periodic problems connecting to the network. Upon investigation, you find that the cable connecting the user's PC to the switch is close to a fluorescent light fixture. What condition is most likely causing the problem?
   - ❍ **A.** Crosstalk
   - ❍ **B.** EMI
   - ❍ **C.** Attenuation
   - ❍ **D.** Faulty cable

3. Which of the following is similar to latency but differs in that the length of the delay between received packets differs?
   - ❍ **A.** Slack
   - ❍ **B.** Jitter
   - ❍ **C.** Stretch
   - ❍ **D.** Lax

**4.** With a crossover cable, which two pairs are reversed?

- ❍ **A.** RX and SX
- ❍ **B.** TX and RX
- ❍ **C.** SX and TX
- ❍ **D.** SX and CX

**5.** While you were away, an air conditioning unit malfunctioned in a server room, and some equipment overheated. Which of the following would have alerted you to the problem?

- ❍ **A.** Multimeter
- ❍ **B.** Environmental monitor
- ❍ **C.** TDR
- ❍ **D.** OTDR

**6.** What tool would you use when working with an IDC?

- ❍ **A.** Wire crimper
- ❍ **B.** Media tester
- ❍ **C.** OTDR
- ❍ **D.** Punchdown tool

**7.** As a network administrator, you work in a wiring closet where none of the cables have been labeled. Which of the following tools are you most likely to use to locate the physical ends of the cable?

- ❍ **A.** Toner probe
- ❍ **B.** Wire crimper
- ❍ **C.** Punchdown tool
- ❍ **D.** **ping**

**8.** You are installing a new system into an existing star network, and you need a cable that is 45 feet long. Your local vendor does not stock cables of this length, so you are forced to make your own. Which of the following tools do you need to complete the task?

- ❍ **A.** Optical tester
- ❍ **B.** Punchdown tool
- ❍ **C.** Crimper
- ❍ **D.** UTP splicer

## Cram Quiz Answers

1. **A.** The term used to describe the loss of signal strength for media is *attenuation*. Crosstalk refers to the interference between two cables, EMI is electromagnetic interference, and chatter is not a valid media interference concern.
2. **B.** EMI is a type of interference that is often seen when cables run too close to electrical devices. Crosstalk is when two cables interfere with each other. Attenuation is a loss of signal strength. Answer D is incorrect also. It may be that a faulty cable is causing the problem. However, the question asked for the most likely cause. Because the cable is running near fluorescent lights, the problem is more likely associated with EMI.
3. **B.** Jitter is when the length of the delay between received packets differs.
4. **B.** In a crossover cable, two pairs of the wires are reversed; these are the TX and RX pairs (transmit and receive).
5. **B.** Environmental monitors are used in server and network equipment rooms to ensure that the temperature does not fluctuate too greatly. In the case of a failed air conditioner, the administrator is alerted to the drastic changes in temperature. Multimeters, TDRs, and OTDRs are used to work with copper-based media.
6. **D.** You use a punchdown tool when working with an IDC. All the other tools are associated with making and troubleshooting cables; they are not associated with IDCs.
7. **A.** The toner probe tool, along with the tone locator, can be used to trace cables. Crimpers and punchdown tools are not used to locate a cable. The **ping** utility would be of no help in this situation.
8. **C.** When you're attaching RJ-45 connectors to UTP cables, the wire crimper is the tool you use. None of the other tools listed are used in the construction of UTP cable.

# What's Next?

This chapter focused on wiring solutions. Chapter 6, "Wireless Solutions and Issues," looks at wireless solutions. Client systems communicate with a wireless access point using wireless LAN adapters. Such adapters are built into or can be added to laptops, handhelds, desktop computers, and even IoT devices. Wireless LAN adapters provide the communication point between the client system and the airwaves via an antenna.

CHAPTER 6

# Wireless Solutions and Issues

**This chapter covers the following official Network+ objectives:**

- Given a scenario, install and configure the appropriate wireless standards and technologies.
- Given a scenario, troubleshoot common wireless connectivity issues.

This chapter covers CompTIA Network+ objectives 2.4 and 5.4. For more information on the official Network+ exam topics, see the "About the Network+ Exam" section in the Introduction.

One of the bigger changes in the networking world since the Network+ exam first came into being is in wireless networking technologies. Networks of all shapes and sizes incorporate wireless segments into their networks. Home wireless networking has also grown significantly in the past few years.

Wireless networking enables users to connect to a network using radio waves instead of wires. Network users within range of a wireless *access point (AP)* can move around an office or any other location within range of a hotspot freely, without needing to plug into a wired infrastructure. The benefits of wireless networking clearly have led to its continued growth.

This chapter explores the many facets of wireless networking, starting with some of the concepts and technologies that make wireless networking possible.

# Understanding Wireless Basics

- **Given a scenario, install and configure the appropriate wireless standards and technologies.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. How many nonoverlapping channels are supported by 802.11a?
2. What are the ranges the 802.11b and 802.11g standards operate in?
3. True or false: Linux users can use the **iwconfig** command to view the state of their wireless network.
4. What does WPA3-Personal enable which replaces pre-shared key (PSK) in WPA2-Personal?

### Answers

1. The 802.11a standard supports up to eight nonoverlapping channels.
2. The 802.11b and 802.11g standards operate in the 2.4 to 2.497 GHz range.
3. True. Linux users can use the **iwconfig** command to view the state of their wireless network.
4. For better password protection, WPA3-Personal uses Simultaneous Authentication of Equals (SAE), which replaces pre-shared key (PSK) in WPA2-Personal.

### ExamAlert

Remember that this objective begins with "Given a scenario." This means that you may receive a drag-and-drop, matching, or "live OS" scenario where you have to click through to complete a specific objective-based task.

# Wireless Channels and Frequencies

*Radio frequency (RF)* channels are an important part of wireless communication. A *channel* is the band of RF used for the wireless communication. Each IEEE wireless standard specifies the channels that can be used. The 802.11a standard specifies radio frequency ranges between 5.15 and 5.875 GHz. In contrast, 802.11b and 802.11g standards operate in the 2.4 to 2.497 GHz range. 802.11n (known as *Wi-Fi 4*) can operate in either 2.4 GHz or 5 GHz ranges, and

802.11ac (known as *Wi-Fi 5*) operates in the 5 GHz range, while 802.11ax (known as *Wi-Fi 6*) can use 2.4 GHz or 5 GHz ranges. There has been much discussion about Wi-Fi congestion and the need for regulatory intervention, particularly in the 2.4 GHz range, but the *regulatory impact* of such intervention has largely prevented attempts to limit the use of these channels.

**Note**

As of this writing, a standard for Wi-Fi 6e (the *e* is for extended) has been designated to support the higher 6 GHz standard, but it is not yet in use.

**Note**

*Hertz (Hz)* is the standard of measurement for radio frequency. Hertz is used to measure the frequency of vibrations and waves, such as sound waves and electromagnetic waves. One hertz is equal to one cycle per second. RF is measured in *kilohertz (KHz)*, one thousand cycles per second; *megahertz (MHz)*, one million cycles per second; or *gigahertz (GHz)*, one billion cycles per second.

As far as channels are concerned, 802.11a has a wider frequency band, enabling more channels and therefore more data throughput. As a result of the wider band, 802.11a supports up to eight nonoverlapping channels. 802.11b/g standards use the smaller band and support only up to three nonoverlapping channels.

It is recommended that nonoverlapping channels be used for communication. In the United States, 802.11b/g standards use 11 channels for data communication, as mentioned; three of these—channels 1, 6, and 11—are nonoverlapping. Most manufacturers set their default channel to one of the nonoverlapping channels to avoid transmission conflicts. With wireless devices you can select which channel your WLAN operates on to avoid interference from other wireless devices that operate in the 2.4 GHz frequency range.

When troubleshooting a wireless network, be aware that overlapping channels can disrupt the wireless communications. For example, in many environments, APs are inadvertently placed close together—perhaps two APs in separate offices located next door to each other or between floors. Signal disruption results if channel overlap exists between the APs. The solution is to try to move the AP to avoid the overlap problem, or to change channels to one of the other nonoverlapping channels. For example, you could switch from channel 6 to channel 11.

Typically, you would change the channel of a wireless device only if it overlapped with another device. If a channel must be changed, it must be changed to another, nonoverlapping channel. Table 6.1 shows the channel ranges for 802.11b/g wireless standards. Table 6.2 shows the channel ranges for 802.11a. 802.11n added the option of using both channels used by 802.11a and b/g and operating at 2.4 GHz/5 GHz. As such, you can think of 802.11n as an amendment that improved upon the previous 802.11 standards by adding *multiple input*, *multiple output (MIMO)* antennas and a huge increase in the data rate. 802.11n devices are still available, but they have largely been superseded today by 802.11ac, which became an approved standard in January 2014, and 802.11ax (which uses MU-MMO and is discussed later). Both 802.11ac and 802.11ax can be thought of as extensions of 802.11n.

**ExamAlert**

When troubleshooting a wireless problem in Windows, you can use the **ipconfig** command to see the status of IP configuration. Similarly, the **ifconfig** command can be used in Linux. In addition, Linux users can use the **iwconfig** command to view the state of your wireless network. Using **iwconfig**, you can view such important information as the link quality, AP MAC address, data rate, and encryption keys, which can be helpful in ensuring that the parameters in the network are consistent.

**Note**

IEEE 802.11b/g wireless systems communicate with each other using radio frequency signals in the band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. Applying two channels that allow the maximum channel separation decreases the amount of channel crosstalk and provides a noticeable performance increase over networks with minimal channel separation.

Tables 6.1 and 6.2 outline the available wireless channels. When you're deploying a wireless network, it is recommended that you use channel 1, grow to use channel 6, and add channel 11 when necessary, because these three channels do not overlap.

**ExamAlert**

The 802.11n, 802.11ac, and 802.11ax standards are the most common today, and you will be hard-pressed to purchase (or even find) older technologies. It is, however, recommended that you know the older technologies for the exam.

TABLE 6.1 **RF Channels for 802.11b/g/n/ax**

| Channel | Frequency Band |
|---|---|
| 1 | 2412 MHz |
| 2 | 2417 MHz |
| 3 | 2422 MHz |
| 4 | 2427 MHz |
| 5 | 2432 MHz |
| 6 | 2437 MHz |
| 7 | 2442 MHz |
| 8 | 2447 MHz |
| 9 | 2452 MHz |
| 10 | 2457 MHz |
| 11 | 2462 MHz |

**Note**

When looking at Table 6.1, remember that the RF channels listed (2412 for channel 1, 2417 for 2, and so on) are actually the center frequency that the transceiver within the radio and AP uses. There is only a 5 MHz separation between the center frequencies, and an 802.11b signal occupies approximately 30 MHz of the frequency spectrum. As a result, data signals fall within about 15 MHz of each side of the center frequency and overlap with several adjacent channel frequencies. This leaves you with only three channels (channels 1, 6, and 11 for the United States) that you can use without causing interference between APs.

TABLE 6.2 **RF Channels for 802.11a/ac/ax**

| Channel | Frequency |
|---|---|
| 36 | 5180 MHz |
| 40 | 5200 MHz |
| 44 | 5220 MHz |
| 48 | 5240 MHz |
| 52 | 5260 MHz |
| 56 | 5280 MHz |
| 60 | 5300 MHz |
| 64 | 5320 MHz |

As mentioned, channels 1, 6, and 11 do not overlap. On a non-MIMO setup (such as with 802.11a, b, or g), always try to use one of these three channels. Similarly, if you use 802.11n/ac/ax with 20 MHz channels, stay with channels 1, 6, and 11 to be safe even though 802.11ac and ax channels can be 20 MHz, 40 MHz, 80 MHz, and 160 MHz wide.

**ExamAlert**

Understand the importance of channels 1, 6, and 11 as you study for the exam.

**ExamAlert**

For the exam, you should know the values in Table 6.2.

It is important to note that 802.11ac operates in the 5 GHz range only, while 802.11ax operates in both the 2.4 GHz and 5 GHz ranges (which no other standard had done since 802.11n) and is, thus, compatible with 802.11a/b/g/n/ac. Operating in both ranges creates more available channels (early chipsets, for example, support eight channels in the 5 GHz and four channels in the 2.4 GHz range for a total of twelve available channels). With 802.11ac, MU-MIMO is limited to only downlink transmissions while 802.11ax creates MU-MIMO connections so a downlink MU-MIMO access point can transmit concurrently to multiple receivers and an uplink MU-MIMO endpoint can simultaneously receive from multiple transmitters.

The 802.11ax standard will support up to eight MU-MIMO transmissions at a time (an increase from the four available with 802.11ac). Orthogonal frequency-division multiple access (OFDMA) is new with 802.11ax (and discussed in the upcoming section on channel bonding), as are several other technologies (including trigger-based random access, dynamic fragmentation, and spatial frequency reuse) enabling it to have a theoretical maximum speed of 10 Gbps. New with 802.11ax is the use of 1024-QAM (quadrature amplitude modulation) to encode (modulate/demodulate) a larger number of data bits and increase throughput.

A subcategory of 802.11ax, known as Wi-Fi 6e (Wi-Fi 6 extended), is expected to be available and adopted soon and will also work in the 6 GHz frequency: devices that are compatible will be able to operate on the 2.4, 5, and 6 GHz frequencies and benefit from less congested bands.

# Cellular Technology Access

One reason why cellular access is an important topic from the perspective of this exam is that when devices (smartphones, tablets, etc.) are accessing the network outside of a Wi-Fi connection, they are often doing so through a cellular network and that cellular network becomes the WAN. As a network administrator, you are dependent upon the cellular network your users are using (and the security, or lack thereof, inherent in it) to protect your data and resources.

The *Global System for Mobile Communications (GSM)* initially used *time-division multiple access (TDMA)* to provide multiuser access by chopping up the channel into sequential time slices. Each user of the channel takes turns to transmit and receive signals and, ideally, this happens so quickly that the user is unaware of it. TDMA was replaced in later implementations by *code-division multiple access (CDMA)* which (instead of splitting the channel into time slices) uses different frequencies for each user to provide various means of cell phone coverage.

The individual methods that can be used for cellular access include 5G, LTE/4G, or 3G, and they represent enhancements to the technology over time—each generation represents new frequency bands and higher data rates. The original GSM access (with both TDMA and CDMA) was labeled 2G. As standards that became available focused on increasing speeds and enabling sending of images, this morphed into 3G (which, initially, was more marketing hype than anything else). 4G added the capability to implement mobile broadband Internet access (not just for smartphones but also laptops with wireless modems and other similar devices). LTE (Long-Term Evolution) was based on EDGE (Enhanced Data rates for GSM Evolution) and HSPA (high-speed packet access) technologies, which increased the capacity and speed by using a different radio interface together with core network improvements. The newest iteration, 5G, not only provides faster speeds but is also needed to meet the needs of Internet of Things (IoT) sensors and other communication-intensive devices.

For purposes of comparison, a typical download speed of basic 3G would be 0.0375 Mbps; 4G would be 150 Mbps; LTE would be approximately 600 Mbps; and 5G is estimated to be between 1–10 Gbps.

# Speed, Distance, and Bandwidth

When talking about wireless transmissions, you need to distinguish between *throughput* and *data rate*. From time to time these terms are used interchangeably, but technically speaking, they are different. As shown later

in this chapter, each wireless standard has an associated speed. For instance, 802.11n lists a theoretical speed of up to 600 Mbps, and 802.11ax has a theoretical maximum speed of a whopping 10 Gbps. This represents the speed at which devices using this standard can send and receive data. However, in network data transmissions, many factors prevent the actual speeds from reaching this end-to-end theoretical maximum. For instance, data packets include overhead such as routing information, checksums, and error recovery data. Although this might all be necessary, it can impact overall speed.

The number of clients on the network can also impact the data rate; the more clients, the more collisions. Depending on the network layout, collisions can have a significant impact on end-to-end transmission speeds. Wireless network signals degrade as they pass through obstructions such as walls or doors; the signal speed deteriorates with each obstruction.

All these factors leave you with the actual throughput of wireless data transmissions. Goodput represents the actual speed to expect from wireless transmissions (what is often thought of as throughput). In practical applications, wireless transmissions are approximately one-half or less of the data rate. Depending on the wireless setup, the transmission rate could be much less than its theoretical maximum.

**ExamAlert**

*Data rate* refers to the theoretical maximum of a wireless standard, such as the 600 Mbps for 802.11n or the 10 Gbps for 802.11ax. *Throughput* refers to the actual speeds achieved after all implementation and interference factors.

**Note**

Speed is always an important factor in the design of any network, and *high throughput (ht)* is a goal that has been around for a while. A number of the 802.11 standards offer a high throughput connection type, such as *802.11a-ht* and *802.11g-ht*. Although these implementations are better with the ht than without, it is true that today you will achieve better results with 802.11ax.

# Channel Bonding

With channel bonding, you can use two channels at the same time. As you might guess, the ability to use two channels at once increases performance. Bonding can help increase wireless transmission rates with 802.11n from a maximum of 40 MHz up to 80 or even 160 MHz (for speed increases of

117 or 333 percent, respectively). 802.11n uses the orthogonal frequency-division multiplexing (OFDM) transmission strategy.

Whereas 802.11n stopped at four spatial streams, 802.11ac goes to eight (for another 100 percent speed increase). 802.11ax replaces OFDM with OFDMA, a multi-user version of OFDM that uses a digital modulation scheme. The multiple access is achieved by assigning subsets of subcarriers to individual users.

**ExamAlert**

If it seems as if 802.11ax keeps coming up in each discussion, the reason is that it is important to know this standard for the exam. Know that it works in both bands (2.4 and 5 GHz), utilizes multiuser MIMO (downlink and uplink), OFDMA (downlink and uplink), and higher data rates (thanks to 1024-QAM).

# MIMO/MU-MIMO/Directional/Omnidirectional

A wireless antenna is an integral part of overall wireless communication. Antennas come in many shapes and sizes, with each one designed for a specific purpose. Selecting the right antenna for a particular network implementation is a critical consideration, and one that could ultimately decide how successful a wireless network will be. In addition, using the right antenna can save you money on networking costs because you need fewer antennas and APs.

**ExamAlert**

*Multiple input, multiple output (MIMO)* and *multiuser multiple input, multiple output (MU-MIMO)* are advanced antenna technologies that are key in wireless standards such as 802.11n, 802.11ac, 802.11ax, and LTE.

Many small home network adapters and APs come with a nonupgradable antenna, but higher-grade wireless devices require you to choose an antenna. Determining which antenna to select takes careful planning and requires an understanding of what range and speed you need for a network. The antenna is designed to help wireless networks do the following:

- Work around obstacles
- Minimize the effects of interference
- Increase signal strength
- Focus the transmission, which can increase signal speed

The following sections explore some of the characteristics of wireless antennas.

## Antenna Ratings

When a wireless signal is low and is affected by heavy interference, it might be possible to upgrade the antenna to create a more solid wireless connection. To determine an antenna's strength, refer to its *gain value*. But how do you determine the gain value?

**ExamAlert**

For the exam, know that an antenna's strength is its gain value.

Suppose that a huge wireless tower is emanating circular waves in all directions. If you could see these waves, you would see them forming a sphere around the tower. The signals around the antenna flow equally in all directions, including up and down. An antenna that does this has a 0 dBi gain value and is called an *isotropic antenna*. The isotropic antenna rating provides a base point for measuring actual antenna strength.

**Note**

The *dB* in dBi stands for decibels, and the *i* stands for the hypothetical isotropic antenna.

An antenna's gain value represents the difference between the 0dBi isotropic and the antenna's power. For example, a wireless antenna advertised as 15dBi is 15 times stronger than the hypothetical isotropic antenna. The higher the decibel figure, the higher the gain.

When looking at wireless antennas, remember that a higher gain value means stronger send and receive signals. In terms of performance, the general rule is that every 3dB of gain added doubles an antenna's effective power output.

## Antenna Coverage

When selecting an antenna for a particular wireless implementation, you need to determine the type of coverage the antenna uses. In a typical configuration, a wireless antenna can be either *omnidirectional* or *directional* (also called unidirectional). Which one you choose depends on the wireless environment.

An omnidirectional antenna is designed to provide a 360-degree dispersed wave pattern. This type of antenna is used when coverage in all directions from the antenna is required. Omnidirectional antennas are advantageous when a broad-based signal is required. For example, if you provide an even signal in all directions, clients can access the antenna and its associated AP from various locations. Because of the dispersed nature of omnidirectional antennas, the signal is weaker overall and therefore accommodates shorter signal distances. Omnidirectional antennas are great in an environment that has a clear line of sight between the senders and receivers. The power is evenly spread to all points, making omnidirectional antennas well suited for home and small office applications.

Directional antennas are designed to focus the signal in a particular direction (which is why they are often referred to as unidirectional). This focused signal enables greater distances and a stronger signal between two points. The greater distances enabled by directional antennas give you a viable alternative for connecting locations, such as two offices, in a point-to-point configuration.

Directional antennas are also used when you need to tunnel or thread a signal through a series of obstacles. This arrangement concentrates the signal power in a specific direction and enables you to use less power for a greater distance than an omnidirectional antenna. Table 6.3 compares omnidirectional and directional wireless antennas.

TABLE 6.3 **Comparing Omnidirectional and Directional Antennas**

| Characteristic | Omnidirectional | Directional | Advantage/Disadvantage |
|---|---|---|---|
| Wireless area coverage | General coverage area | Focused coverage area | Omnidirectional allows 360-degree coverage, giving it a wide coverage area. Directional provides a targeted path for signals to travel. |
| Wireless transmission range | Limited | Long point-to-point range | Omnidirectional antennas provide a 360-degree coverage pattern and, as a result, far less range. Directional antennas focus the wireless transmission; this focus enables greater range. |
| Wireless coverage shaping | Restricted | The directional wireless range can be increased and decreased. | Omnidirectional antennas are limited to their circular pattern range. Directional antennas can be adjusted to define a specific pattern, wider or more focused. |

**Note**

In the wireless world, *polarization* refers to the direction in which the antenna radiates wavelengths. This direction can be vertical, horizontal, or circular. Today, vertical antennas are perhaps the most common. As far as the configuration is concerned, the sending and receiving antennas should be set to the same polarization.

**ExamAlert**

Omnidirectional antennas provide wide coverage but weaker signal strength in any one direction than a directional antenna.

# Establishing Communications Between Wireless Devices

When you work with wireless networks, you must have a basic understanding of the communication that occurs between wireless devices. If you use an infrastructure wireless network design, the network has two key parts: the wireless client, also known as the *station (STA)*, and the AP. The AP acts as a *bridge* (or wireless bridge) between the STA and the wired network.

**ExamAlert**

When a single AP is connected to the wired network and to a set of wireless stations, it is called a *basic service set (BSS)*. An *extended service set (ESS)* describes the use of multiple BSSs that form a single subnetwork. Ad hoc mode is sometimes called an *independent basic service set (IBSS)*.

As with other forms of network communication, before transmissions between devices can occur, the wireless AP and the client must begin to talk to each other. In the wireless world, this is a two-step process involving *association* and *authentication*.

The association process occurs when a wireless adapter is turned on. The client adapter immediately begins scanning the wireless frequencies for wireless APs or, if using ad hoc mode, other wireless devices. When the wireless client is configured to operate in infrastructure mode, the user can choose a wireless AP with which to connect. This process may also be automatic, with the AP selection based on the SSID, signal strength, and frame error rate. Finally, the wireless adapter switches to the assigned channel of the selected wireless AP and negotiates the use of a port.

If at any point the signal between the devices drops below an acceptable level, or if the signal becomes unavailable for any reason, the wireless adapter initiates another scan, looking for an AP with stronger signals. When the new AP is located, the wireless adapter selects it and associates with it. This is known as *reassociation*.

**ExamAlert**

The 802.11 standards enable a wireless client to roam between multiple APs. An AP transmits a beacon signal every so many milliseconds. It includes a time stamp for client synchronization and an indication of supported data rates. A client system uses the beacon message to identify the strength of the existing connection to an AP. If the connection is too weak, the *roaming* client attempts to associate itself with a new AP. This association enables the client system to roam between distances and APs.

With the association process complete, the authentication process begins. After the devices associate, keyed security measures are applied before communication can take place. On many APs, authentication can be set to either *shared key authentication* or *open authentication*. The default setting for older APs typically is open authentication. Open authentication enables access with only the SSID and/or the correct WEP key for the AP. The problem with open authentication is that if you do not have other protection or authentication mechanisms in place, your wireless network is totally open to intruders. When set to shared key mode, the client must meet security requirements before communication with the AP can occur.

After security requirements are met, you have established IP-level communication. This means that wireless standard requirements have been met, and Ethernet networking takes over. There is basically a switch from 802.11 to 802.3 standards. The wireless standards create the physical link to the network, enabling regular networking standards and protocols to use the link. This is how the physical cable is replaced, but to the networking technologies there is no difference between regular cable media and wireless media.

Several components combine to enable wireless communications between devices. Each of these must be configured on both the client and the AP:

- **Service set identifier (SSID):** Whether your wireless network uses infrastructure mode or ad hoc mode, an SSID is required. The SSID is a configurable client identification that enables clients to communicate with a particular base station. Only client systems configured with the same SSID as the AP can communicate with it. SSIDs provide a simple password arrangement between base stations and clients in a BSS network. ESSIDs are used for the ESS wireless network.

- **Wireless channel:** As stated earlier in the chapter, RF channels are an important part of wireless communications. A channel is the frequency band used for the wireless communication. Each standard specifies the channels that can be used. The 802.11a standard specified radio frequency ranges between 5.15 GHz and 5.875 GHz. In contrast, the 802.11b and 802.11g standards operate in the 2.4 GHz to 2.497 GHz ranges. 802.11n and 802.11ax can operate in either the 2.4 GHz or 5 GHz range, and 802.11ac is at 5 GHz. Fourteen channels are defined in the IEEE 802.11 channel set, 11 of which are available in North America.
- **Security features:** IEEE 802.11 provides security using two methods: authentication and encryption. Authentication verifies the client system. In infrastructure mode, authentication is established between an AP and each station. Wireless encryption services must be the same on the client and the AP for communication to occur.

**ExamAlert**

Wireless devices ship with default SSIDs, security settings, channels, passwords, and usernames. To protect yourself, it is strongly recommended that you change these default settings. Today, many Internet sites list the default settings used by manufacturers with their wireless devices. This information is used by people who want to gain unauthorized access to your wireless devices.

# Configuring the Wireless Connection

Wireless connection configuration is fairly straightforward. Figure 6.1 shows an example of a simple wireless router. In addition to providing wireless access, it also includes a four-port wired switch.


FIGURE 6.1 **A wireless broadband router for a small network**

Most of the broadband routers similar to the one shown in Figure 6.1 differ based upon the following features:

- **Wireless bands:** The routers can provide only 2.4 GHz, only 5 GHz, or be either selectable (choosing one of the two) or simultaneous (using both).

- **Switch speed:** The ports on the switch can usually support either Fast Ethernet (10/100 Mbps) or Gigabit Ethernet (10/100/1000 Mbps).
- **Security supported:** The SSID, security mode, and passphrase may be configurable for each band, and some routers include a push-button feature for accessing setup. Some enable you to configure MAC address filtering and guest access, such as the one shown in Figure 6.2. MAC address filtering enables you to limit access to only those specified hosts. Guest access uses a different password and network name and enables visitors to use the Internet without having access to the rest of the network (thus avoiding your data and computers).

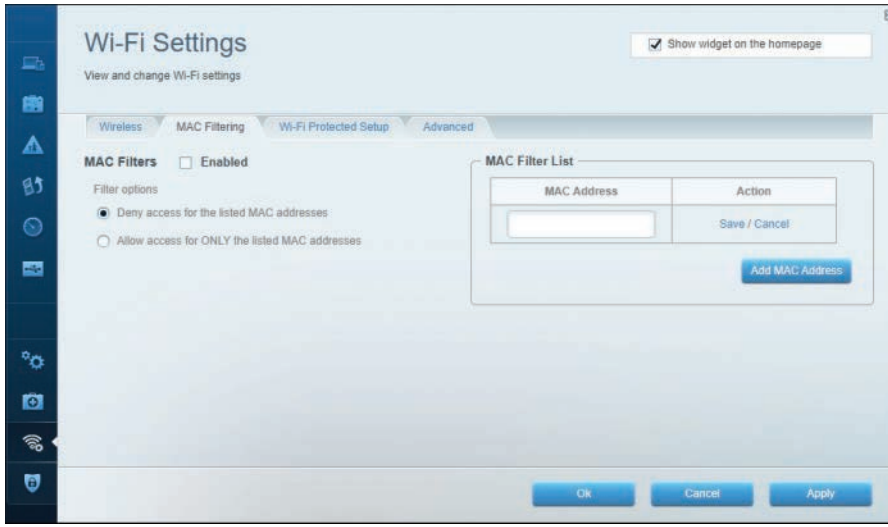



FIGURE 6.2 **Configuring MAC address filtering on a SOHO router**

**ExamAlert**

Make sure that you understand the purpose of MAC address filtering.

- **Antenna:** The antenna may be a single external pole, two poles or even more, or be entirely internal. The model shown in Figure 6.1 uses an internal antenna, as shown in Figure 6.3.

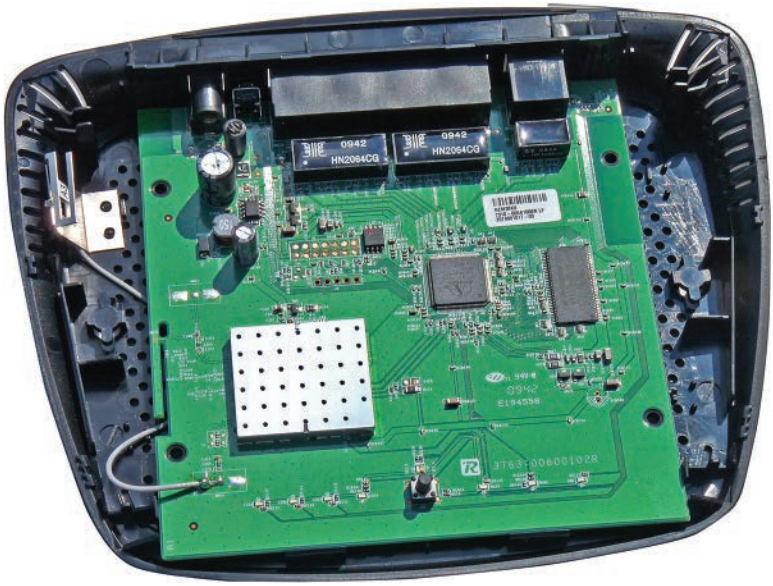



FIGURE 6.3 **The antenna is the wire and metal component on the left**

> **Note**
>
> The wireless antenna for a laptop, all-in-one desktop system, or mobile device is often built in to the areas around the screen.

The settings for a wireless router are typically clearly laid out. You can adjust many settings for troubleshooting or security reasons. For example, most newer *small office/home office (SOHO)* wireless routers offer useful configuration setup screens for administering firewall, demilitarized zone (DMZ), apps and gaming, parental controls, guest access, and diagnostic settings (as illustrated in Figure 6.4). Following are some of the basic settings that can be adjusted on a wireless AP:

- **SSID:** This name is used for anyone who wants to access the Internet through this wireless AP. The SSID is a configurable client identification that enables clients to communicate with a particular base station. In an application, only clients configured with the same SSID can communicate with base stations having the same SSID. SSID provides a simple password arrangement between base stations and clients.

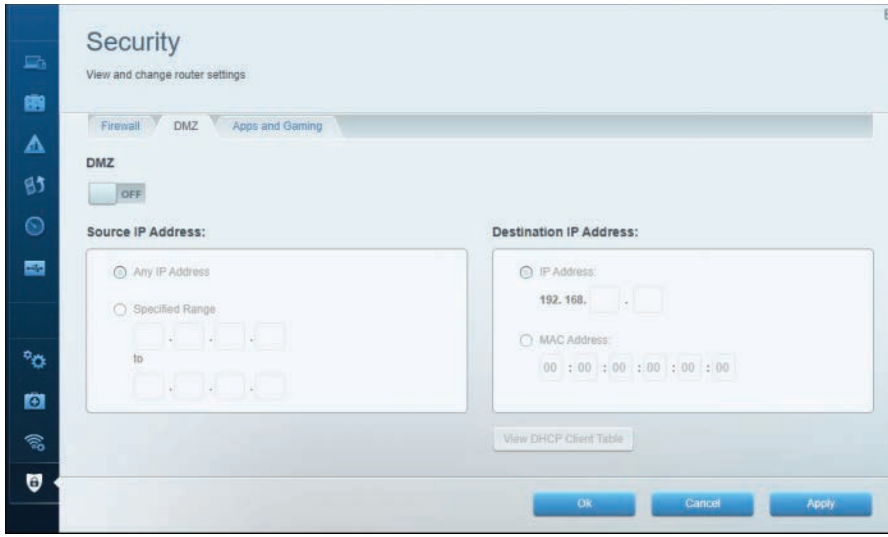



FIGURE 6.4 **Common security configuration parameters for a wireless router**

- As far as troubleshooting is concerned, if a client cannot access a base station, you need to ensure that both use the same SSID. Incompatible SSIDs are sometimes found when clients move computers, such as laptops or other mobile devices, between different wireless networks. They obtain an SSID from one network. If the system is not rebooted, the old SSID does not enable communication with a different base station.
- **Channel:** To access this network, all systems must use this channel. If needed, you can change the channel using the drop-down menu. The menu lists channels 1 through 11.
- **SSID broadcast:** In their default configuration, wireless APs typically broadcast the SSID name into the air at regular intervals. This feature is intended to allow clients to easily discover the network and roam between WLANs. The problem with SSID broadcasting is that it makes it a little easier to get around security. SSIDs are not encrypted or protected in any way. Anyone can snoop and get a look at the SSID and attempt to join the network if not secured.

**Note**

For SOHO use, *roaming* is not needed. This feature can be disabled for home use to improve the security of your WLAN. As soon as your wireless clients are manually configured with the right SSID, they no longer require these broadcast messages.

- **Authentication:** When configuring authentication security for the AP, you have several options depending on the age of the AP. At the lower (older) end, choices often include WEP-Open, WEP-Shared, and WPA-PSK. WEP-Open is the simplest of the authentication methods because it does not perform any type of client verification. It is a weak form of authentication because it requires no proof of identity. WEP-Shared requires that a WEP key be configured on both the client system and the AP. This makes authentication with WEP-Shared mandatory, so it is more secure for wireless transmission. To strengthen WEP encryption, a *Temporal Key Integrity Protocol (TKIP)* was employed. This protocol placed a 128-bit wrapper around the WEP encryption with a key that is based on things such as the MAC address of the destination device and the serial number of the packet. TKIP was designed as a backward-compatible replacement to WEP, and it could work with all existing hardware. Without the use of TKIP, WEP was considered weak. It is worth noting, however, that even TKIP has been broken.
- *Wi-Fi Protected Access with Pre-Shared Key (WPA-PSK)* is a stronger form of encryption in which keys are automatically changed and authenticated between devices after a specified period of time, or after a specified number of packets have been transmitted.
- On newer APs, the choices usually include WPA3, WPA Personal, WPA Enterprise, WPA2 Personal, and WPA2 Enterprise. Other choices can include WPA2/WPA Mixed Mode and RADIUS. Although WPA mandates the use of TKIP, WPA2 requires *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)*. CCMP uses 128-bit AES encryption with a 48-bit initialization vector. With the larger initialization vector, it increases the difficulty in cracking and minimizes the risk of a replay attack. WPA3 (shown as an option in Figure 6.5) uses Simultaneous Authentication of Equals (SAE), which replaces pre-shared key (PSK) used in WPA2-Personal and is resistant to offline dictionary attacks. When given as a choice, WPA3-Personal adds more protection for individual users as a result of the password-based authentication even when the passwords that users choose are not all that complex.

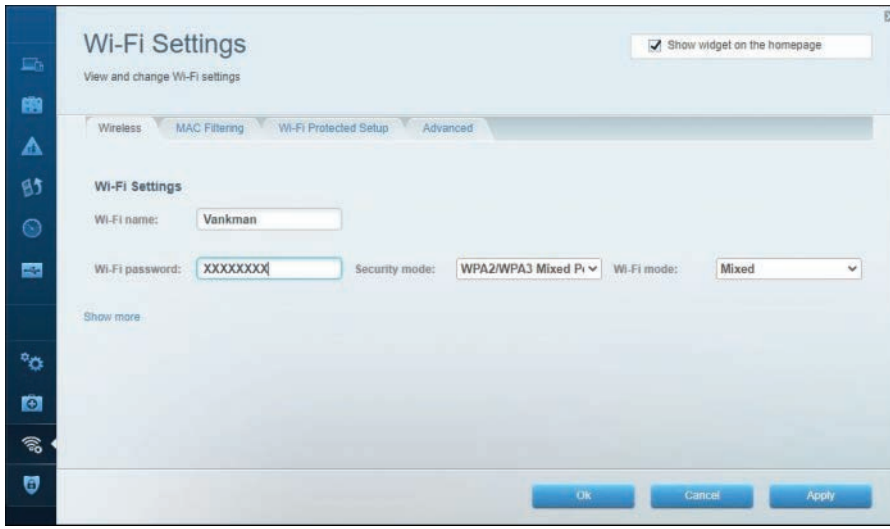



FIGURE 6.5 **Newer wireless routers offer WPA2/WPA3 Mixed Personal mode as a security option**

**ExamAlert**

Know that WPA3 helps prevent offline password attacks by using Simultaneous Authentication of Equals. SAE allows users to choose easier-to-remember passwords and, through forward secrecy, does not compromise traffic already transmitted even if the password becomes compromised.

- **Wireless mode:** To access the network, the client must use the same wireless mode as the AP. Today, most users configure the network for 802.11ac or 802.11ax for faster speeds.
- **DTIM period (seconds):** Wireless transmissions can broadcast to all systems—that is, they can send messages to all clients on the wireless network. Multiple broadcast messages are known as *multicast* or *broadcast traffic*. *Delivery Traffic Indication Message (DTIM)* is a feature used to ensure that when the multicast or broadcast traffic is sent, all systems are awake to hear the message. The DTIM setting specifies how often the DTIM is sent within the beacon frame. For example, if the DTIM setting by default is 1, this means that the DTIM is sent with every beacon. If the DTIM is set to 3, the DTIM is sent every three beacons as a DTIM wake-up call.

- **Maximum connection rate:** The transfer rate typically is set to Auto by default. This setting enables the maximum connection speed. However, it is possible to decrease the speed to increase the distance that the signal travels and boost signal strength caused by poor environmental conditions.
- **Network type:** This is where the network can be set to use the ad hoc or infrastructure network design.

It is easy to fall into the trap of thinking of wireless devices as being laptops connecting to the AP. Over the years, however, the number and type of mobile devices that need to connect to the network has expanded tremendously. In addition to the laptops and tablets, gaming devices, media devices, cell phones, and IoT devices now all connect for wireless access. Although they might all seem different, they require the same information to connect.

Unfortunately, they all bring security concerns as well. *Bring-your-own-device (BYOD)* policies are highly recommended for every organization. Administrators can implement *mobile device management (MDM)* and *mobile application management (MAM)* products to help with the management and administration issues with these devices.

**ExamAlert**

Know that devices on networks today include such things as PCs, cell phones, laptops, tablets, gaming devices, media, and IoT devices.

## Cram Quiz

1. Which of the following wireless protocols can operate at 2.4 GHz? (Choose four.)
   - ❍ **A.** 802.11a
   - ❍ **B.** 802.11b
   - ❍ **C.** 802.11g
   - ❍ **D.** 802.11n
   - ❍ **E.** 802.11ac
   - ❍ **F.** 802.11ax

2. Under what circumstance would you change the default channel on an access point?

   - ❍ **A.** When channel overlap occurs between APs
   - ❍ **B.** To release and renew the SSID
   - ❍ **C.** To increase WPA2 security settings
   - ❍ **D.** To decrease WPA2 security settings

3. A client on your network has had no problems accessing the wireless network in the past, but recently she moved to a new office. Since the move, she cannot access the network. Which of the following is most likely the cause of the problem?

   - ❍ **A.** The SSIDs on the client and the AP are different.
   - ❍ **B.** The SSID has been erased.
   - ❍ **C.** The client has incorrect broadcast settings.
   - ❍ **D.** The client system has moved too far from the AP.

4. You are installing a wireless network solution, and you require a standard that can operate using either 2.4 GHz or 5 GHz frequencies. Which of the following standards could you choose? (Choose two.)

   - ❍ **A.** 802.11a
   - ❍ **B.** 802.11b
   - ❍ **C.** 802.11g
   - ❍ **D.** 802.11n
   - ❍ **E.** 802.11ac
   - ❍ **F.** 802.11ax

5. You are installing a wireless network solution that uses a feature known as MU-MIMO. Which wireless networking standards are you possibly using? (Choose two.)

   - ❍ **A.** 802.11a
   - ❍ **B.** 802.11b
   - ❍ **C.** 802.11n
   - ❍ **D.** 802.11ac
   - ❍ **E.** 802.11ax

# Cram Quiz Answers

1. **B, C, D, and F.** Wireless standards specify an RF range on which communications are sent. The 802.11b and 802.11g standards use the 2.4 GHz range. 802.11a and 802.11ac use the 5 GHz range. 802.11n can operate at 2.4 GHz and 5 GHz. 802.11ax operates in both the 2.4 GHz and 5 GHz ranges.
2. **A.** Ordinarily, the default channel used with a wireless device is adequate; however, you might need to change the channel if overlap occurs with another nearby AP. The channel should be changed to another, nonoverlapping channel. Changing the channel would not impact the WPA2 security settings.
3. **D.** An AP has a limited distance that it can send data transmissions. When a client system moves out of range, it cannot access the AP. Many strategies exist to increase transmission distances, including RF repeaters, amplifiers, and buying more powerful antennas or wireless APs. The problem is not likely related to the SSID or broadcast settings, because the client had access to the network before, and no settings were changed.
4. **D and F.** The IEEE standards 802.11n and 802.11ax can use either the 2.4 GHz or 5 GHz radio frequencies. Given a choice today, you should choose 802.11ax. 802.11a uses 5 GHz, and 802.11b and 802.11g use 2.4 GHz. 802.11ac operates at 5 GHz.
5. **D and E.** MU-MIMO is used by the 802.11ac and 802.11ax standards and makes multiuser MIMO possible (increasing the range and speed of wireless networking). MIMO, itself, enables the transmission of multiple data streams traveling on different antennas in the same channel at the same time.

# Troubleshooting Wireless Issues

▶ **Given a scenario, troubleshoot common wireless connectivity issues.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. You have noticed that connections between nodes on one network are inconsistent and suspect there may be another network using the same channel. What should you try first?
2. True or false: Weather conditions should not have a noticeable impact on wireless signal integrity.
3. True or false: When a client connects to an AP, it is said to associate with that AP, and disassociation is the process of it no longer associating with that AP.

### Answers

1. If connections are inconsistent, try changing the frequency channel to another, nonoverlapping channel.
2. False. Weather conditions can have a huge impact on wireless signal integrity.
3. True. When a client connects to an AP, it is said to associate with that AP, and disassociation is the process of it no longer associating with that AP. Disassociation can happen any time the AP thinks it no longer needs to communicate with the client.

### ExamAlert

Remember that this objective begins with "Given a scenario." This means that you may receive a drag and drop, matching, or "live OS" scenario where you have to click through to complete a specific objective-based task.

Poor communication between wireless devices has many different potential causes. Some of these problems, such as latency and jitter, are similar to those that exist with wired connections and were discussed in the previous chapter. Others are characteristic only of wireless connectivity and are discussed in the following sections.

To put a lot of information into a format that is coherent, the discussion starts with a review checklist of wireless troubleshooting and then moves into some individual topics:

- **Signal loss:** The cause of signal loss, known as *attenuation*, can be anything from distance to obstacles to interference. The *signal-to-noise ratio* should be examined to measure the desired signal against the background noise interfering with it. Look for signs of saturation with either the device or the bandwidth.

ExamAlert

Signal-to-noise ratio can be used to measure that which the name implies.

- **Wireless enabled:** Some laptops make it incredibly easy to turn wireless on and off. A user may accidentally press a button that he is not aware of and then suddenly not be able to access the network. Although this is a simple problem to fix, it is one that you need to identify as quickly as possible. Figure 6.6 shows the wireless light on an HP laptop. This light is also a button that toggles wireless on and off. When the light is blue, wireless is enabled, and when it is not blue (orange), it is disabled.

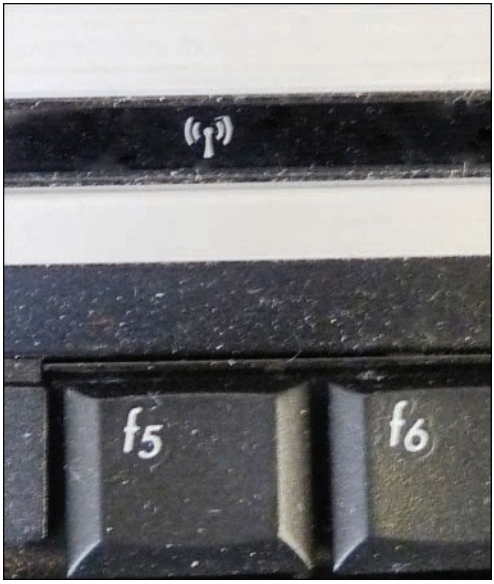



FIGURE 6.6 **A light also serves as a button, enabling wireless to be quickly turned on and off**

- **Untested updates:** Never apply untested updates to the network. This is especially true with AP updates, which should always be tested in nonproduction environments before being applied to live machines.
- **Wrong wireless standard:** Make sure that the standard you are using supports the rates and attributes you are striving for. This is particularly important in terms of throughput, frequency, distance, and channels.
- **Auto transfer rate:** By default, wireless devices are configured to use the strongest, fastest signal. If you experience connectivity problems between wireless devices, try using the lower transfer rate in a fixed mode to achieve a more stable connection. For example, you can manually choose the wireless transfer rate. Also, instead of using the highest transfer rate available, try a lesser speed. The higher the transfer rate, the shorter the connection distance.
- **AP placement and configuration:** If signal strength is low, try moving the AP to a new location. Moving it just a few feet can make a difference. You can also try to *bounce* a signal, as needed, off reflective surfaces. The configuration of the AP should take into account the use of *Lightweight Access Point Protocol (LWAPP)*, which can allow you to monitor the network and reduce the amount of time needed to configure and troubleshoot it—and whether the authentication/configuration will be done at the AP (known as *thick*) or it will be passed on up (known as *thin*).
- Within the 802.11 standard, signal strength is measured in terms of *Received Signal Strength Indication (RSSI)*. This value is an indicator of the power level being received by the receiving host after any antenna or cable loss. The greater the RSSI value, the stronger the signal.

> **Note**
>
> Anytime an AP is doing key functions—authentication, filtering, QoS enforcement, and so on—it is said to be *thick*. If it is not doing these key functions—even though it might be doing others—it is usually said to be *thin*. Although there is no 100 percent sure method of distinguishing what a vendor will label thick or thin, one good rule is to question whether the AP is dependent on another device (thin) or not (thick).

- **Antenna:** The default antenna shipped with wireless devices may not be powerful enough for a particular client system. Better-quality antennas can be purchased for some APs, which can boost the distance the signal can go. Make sure you do not use the wrong antenna type or have other incompatibilities.

- *Effective Isotropic Radiated Power (EIRP)* is used to measure the combination of the power emitted by the transmitter and the ability of the antenna to direct that power in a given direction. It is the total power—expressed in watts—that would need to be radiated by a half-wave dipole antenna to give the same signal strength as the actual source antenna at a distant receiver located in the direction of the antenna's strongest beam.
- **Environmental obstructions:** Wireless RF communications are weakened if they have to travel through obstructions such as metal studs, window film, and concrete walls. Wireless site surveys can be performed to troubleshoot RF signal loss issues as well as assist in planning optimal locations for new wireless networks.
- **Conflicting devices:** Any device that uses the same frequency range as the wireless device can cause interference. For example, 2.4 GHz phones, appliances, or Bluetooth devices can cause interference with devices using the 802.11g or single-band 802.11n wireless standards.
- **Wireless channels:** If connections are inconsistent, try changing the channel to another, nonoverlapping channel. Make certain you do not have mismatched channels between devices.
- **Protocol issues:** If an IP address is not assigned to the wireless client, a wrong SSID or incorrect WEP/WPA/WPA2/WPA3 settings can prevent a system from obtaining IP information.
- **SSID:** The SSID number used on the client system must match the one used on the AP. You might need to change it if you are switching a laptop or other wireless device between different WLANs.
- **Encryption type:** If encryption is enabled on the connecting system, the encryption type must match what is set in the AP. For example, if the AP uses WPA2/WPA3-AES, the connecting system must also use WPA2/WPA3-AES.
- **Captive portal issues:** Most public networks, including Wi-Fi hotspots, use a *captive portal*, which is a web page that requires users to agree to some condition before they use the network or Internet. The condition could be to agree to the acceptable use policy (AUP), payment charges for the time they are using the network, and so forth. Security vulnerabilities have been reported with captive portals, so administrators should be on the alert for any new problems that are reported.

- **Client disassociation issues:** When a client connects to an AP, it is said to associate with that AP, and disassociation is the process of it no longer associating with that AP. Disassociation can happen any time the AP thinks it no longer needs to communicate with the client—due to going into hibernation mode, powering down, leaving the building, and so on. Most unintentional disassociations can be traced to weak signals, but relocating the AP (or boosting the signal) can often help.

**ExamAlert**

Captive portals are common in public places such as airports and coffee shops. The user simply clicks Accept, views an advertisement, provides an email address, or performs some other required action. The network then grants access to the user and no longer holds the user captive to that portal.

Most router configuration interfaces allow you to run basic diagnostics through them, as illustrated in Figure 6.7. You can also usually change the security settings and configure the firewall, as shown in Figure 6.8.

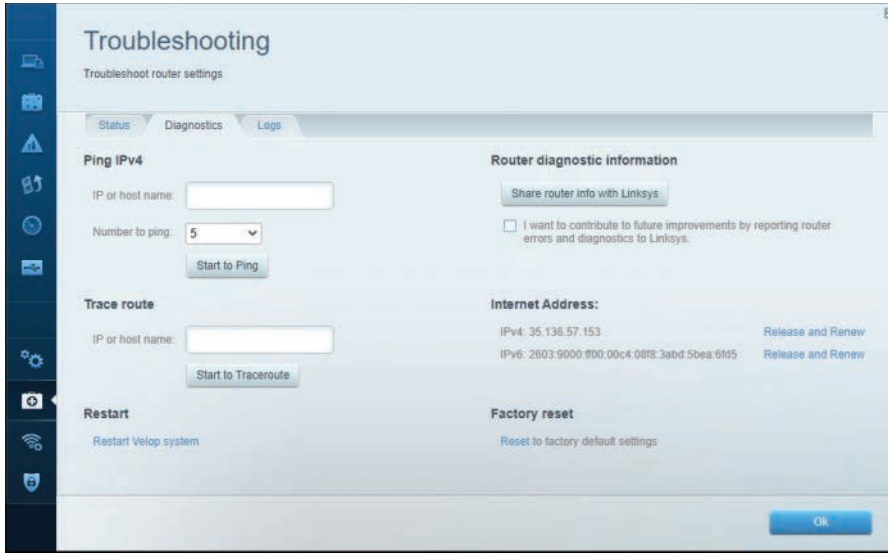



FIGURE 6.7 **Wireless router diagnostic options**

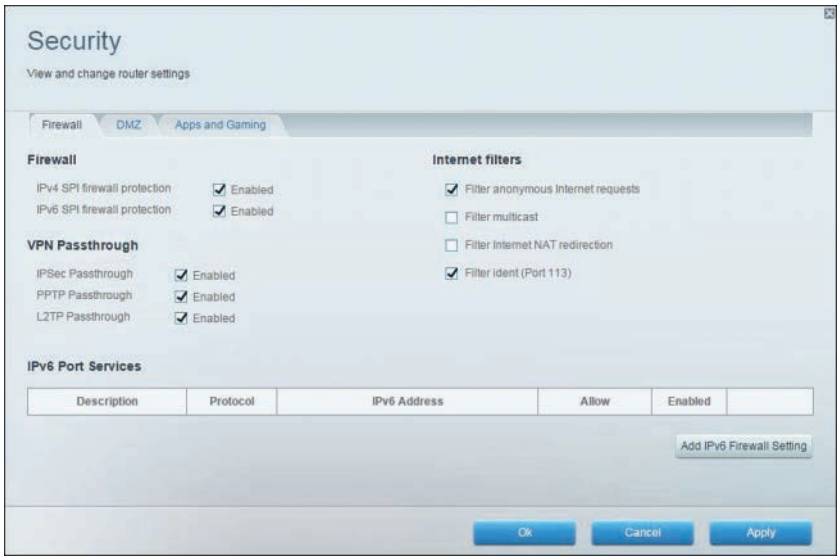



FIGURE 6.8 **Configuring security settings**

# Site Surveys

As more networks go wireless, you need to pay special attention to issues associated with them. Wireless survey tools can be used to create heat maps showing the quantity and quality of wireless network coverage in areas. They can also allow you to see access points (including rogues) and security settings. These tools can be used to help you design and deploy an efficient network, and they can also be used (by you or others) to find weaknesses in your existing network (often marketed for this purpose as wireless analyzers).

# Factors Affecting Wireless Signals

Because wireless signals travel through the atmosphere, they are susceptible to different types of interference than are standard wired networks. Interference weakens wireless signals and therefore is an important consideration when working with wireless networking.

## Interference

Wireless interference is an important consideration when you plan a wireless network. Interference is, unfortunately, inevitable, but the trick is to minimize the levels of interference. Wireless LAN communications typically are based on radio frequency signals that require a clear and unobstructed transmission path.

The following factors can cause interference:

- **Physical objects:** Trees, masonry, buildings, and other physical structures are some of the most common sources of interference. The *density* of the materials used in a building's construction determines the number of walls the RF signal can pass through and still maintain adequate coverage. Concrete and steel walls are particularly difficult for a signal to pass through. These structures weaken or at times completely prevent wireless signals.

ExamAlert

Be sure that you understand that physical objects are a common source of interference. A wireless site survey can be used to test for interference.

- **Radio frequency interference:** Wireless technologies such as 802.11n can use an RF range of 2.4 GHz, and so do many other devices, such as cordless phones, microwaves, Bluetooth devices, and so on. Devices that share the channel can cause noise and weaken the signals.
- **Electrical interference:** Electrical interference comes from devices such as computers, refrigerators, fans, lighting fixtures, or any other motorized devices. The impact that electrical interference has on the signal depends on the proximity of the electrical device to the wireless AP. Advances in wireless technologies and in electrical devices have reduced the impact that these types of devices have on wireless transmissions.
- **Environmental factors:** Weather conditions can have a huge impact on wireless signal integrity. Lightning, for example, can cause electrical interference, and fog can weaken signals as they pass through.

## Reflection, Refraction, and Absorption

The line differentiating between interference and reflection can be blurry when it comes to wireless networking. The key difference between them is that *interference* is a conflict with something else (usually another signal), whereas *reflection* is a problem caused by a bouncing of the same signal off an object. A subset of this is refraction, which involves a change in direction of the wave as a result of its traveling at different speeds at different points. Put in simple terms, reflection happens when the signal hits a piece of metal and cannot pass through, and refraction happens when the signal goes through a body of water.

If the wave is completely swallowed by the object it hits (not reflected, or refracted), then it is said to be absorbed. Where security is concerned, items

known to absorb wireless signals can be used to prevent the signal from traveling beyond an established perimeter. Shielding paint (sometimes called RF paint) can be used for this purpose, as can copper plates and aluminum sheets.

Many wireless implementations are found in the office or at home. Even when outside interference such as weather is not a problem, every office has plenty of wireless obstacles. Table 6.4 highlights a few examples to be aware of when implementing a wireless network indoors.

TABLE 6.4 **Wireless Obstacles Found Indoors**

| Obstruction | Obstacle Severity | Sample Use |
|---|---|---|
| Wood/wood paneling | Low | Inside a wall or hollow door |
| Drywall | Low | Inside walls |
| Furniture | Low | Couches or office partitions |
| Clear glass | Low | Windows |
| Tinted glass | Medium | Windows |
| People | Medium | High-volume traffic areas that have considerable pedestrian traffic |
| Ceramic tile | Medium | Walls |
| Concrete blocks | Medium/high | Outer wall construction |
| Mirrors | High | Mirror or reflective glass |
| Metals | High | Metal office partitions, doors, metal office furniture |
| Water | High | Aquariums, rain, fountains |

ExamAlert

Be sure that you understand the severity of obstructions given in Table 6.4.

# Troubleshooting AP Coverage

Like any other network medium, APs have a limited transmission distance. This limitation is an important consideration when you decide where an AP should be placed on the network. When troubleshooting a wireless network, pay close attention to how far the client systems are from the AP.

ExamAlert

*Distance limitations* from the AP are among the first things to check when troubleshooting AP coverage.

When faced with a problem in which client systems cannot consistently access the AP, you could try moving the AP to better cover the area, but then you may disrupt access for users in other areas. So what can be done to troubleshoot AP coverage?

Depending on the network environment, the quick solution may be to throw money at the problem and purchase another access point, cabling, and other hardware to expand the transmission area. However, you can try a few things before installing another wireless AP. The following list starts with the least expensive solution and progresses to the most expensive:

- **Increase transmission power:** Some APs have a setting to adjust the transmission power output (power levels). By default, most of these settings are set to the maximum output; however, this is worth verifying just in case. You can decrease the transmission power if you are trying to reduce the dispersion of radio waves beyond the immediate network. Increasing the power gives clients stronger data signals and greater transmission distances.
- **Relocate the AP:** When wireless client systems suffer from connectivity problems, the solution may be as simple as relocating the AP. You could relocate it across the room, a few feet away, or across the hall. Finding the right location will likely take a little trial and error.
- **Adjust or replace antennas:** If the AP distance is insufficient for some network clients, you might need to replace the default antenna used with both the AP and the client with higher-end antennas. Upgrading an antenna can make a big difference in terms of transmission range. Unfortunately, not all APs have replaceable antennas.
- **Tweak the signal amplification:** *Radio frequency (RF)* amplifiers add significant distance to wireless signals. An RF amplifier increases the strength and readability of the data transmission. The amplifier improves both the received and transmitted signals, resulting in an increase in wireless network performance.
- **Use a repeater:** Before installing a new AP, you might want to think about a wireless repeater. When set to the same channel as the AP, the repeater takes the transmission and repeats it. So, the AP transmission gets to the repeater, and then the repeater duplicates the signal and passes it on. This is an effective strategy to increase wireless transmission distances.

**ExamAlert**

Be prepared to answer questions on AP coverage and possible reasons to relocate or replace APs.

# Cram Quiz

1. You purchase a new wireless AP that uses no security by default. You change the security settings to use 128-bit encryption. How must the client systems be configured?

   - ❍ **A.** All client systems must be set to 128-bit encryption.
   - ❍ **B.** The client system inherits security settings from the AP.
   - ❍ **C.** Wireless security does not support 128-bit encryption.
   - ❍ **D.** The client wireless security settings must be set to autodetect.

2. You experience connectivity problems with your SOHO network. What can you change in an attempt to solve this problem?

   - ❍ **A.** Shorten the SSID.
   - ❍ **B.** Remove all encryption.
   - ❍ **C.** Lower the transfer rate.
   - ❍ **D.** Raise the transfer rate.

3. Which of the following is a web page that is first launched when a user is connecting through a network that usually requires some type of interaction before the user is allowed access to other network resources or Internet sites?

   - ❍ **A.** EIRP
   - ❍ **B.** RSSI
   - ❍ **C.** Captive portal
   - ❍ **D.** SSID

4. Your organization is doing upfront planning for proper AP placement to ensure coverage and address security concerns. Which of the following would help you most with this endeavor? (Choose two.)

   - ❍ **A.** Site survey
   - ❍ **B.** Yagi
   - ❍ **C.** MU-MIMO
   - ❍ **D.** Heat map

## Cram Quiz Answers

1. **A.** On a wireless connection between an AP and the client, each system must be configured to use the same wireless security settings. In this case, they must both be configured to use 128-bit encryption.
2. **C.** If you experience connectivity problems between wireless devices, try using the lower transfer rate in a fixed mode to achieve a more stable connection. For example, you can manually choose the wireless transfer rate. The higher the transfer rate, the shorter the connection distance.
3. **C.** A captive portal is a web page that is first launched when a user is connecting through a network that usually requires some type of interaction before the user is allowed access to other network resources or Internet sites. EIRP (Effective Isotropic Radiated Power) is used to measure the combination of the power emitted by the transmitter and the ability of the antenna to direct that power in a given direction. RSSI (Received Signal Strength Indication) is an indicator of the power level being received by the receiving host after any antenna or cable loss. The greater the RSSI value, the stronger the signal. The SSID number used on the client system must match the one used on the AP. You might need to change it if you are switching a laptop or other wireless device between different WLANs.
4. **A and D.** Professional site surveys for wireless network installations and proper access point (AP) placement are used to ensure coverage area and security concerns. Site surveys use Wi-Fi and other wireless analyzers to understand and map out the wireless infrastructure. One output is a wireless heat map. A Yagi antenna is an example of a directional antenna, and multiuser multiple input, multiple output (MU-MIMO) antennas take advantage of multipath signal reflections.

# What's Next?

Chapter 7, "Cloud Computing Concepts and Options," focuses on the definitions of cloud computing at the level you need to know for the Network+ exam.

*This page intentionally left blank*

CHAPTER 7

# Cloud Computing Concepts and Options

**This chapter covers the following official Network+ objectives:**

- Summarize cloud concepts and connectivity options.

This chapter covers CompTIA Network+ objective 1.8. For more information on the official Network+ exam topics, see the "About the Network+ Exam" section in the Introduction.

The term *cloud computing* is used everywhere these days, even by those who have no idea what it means. It is important for you, as a Network+ candidate, to be versed in the definitions of cloud computing and able to discuss it with others using a common vernacular.

This chapter focuses on the definitions of cloud computing at the level you need to know for the Network+ exam. If you want to go further with the technology, consider the Cloud+ certification from CompTIA.

# Cloud Concepts

▶ **Summarize cloud concepts and connectivity options.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. In which cloud delivery model are resources owned by the organization, and what organization acts as both the provider and the consumer?
2. With which cloud service model can consumers deploy, but not manage or control, any of the underlying cloud infrastructure (but they can have control over the deployed applications)?
3. What are some of the characteristics of cloud computing?
4. What cloud deployment model can be managed and operated by one or more organizations in the community, a third party, or some combination of them, and may exist on or off premises?

### Answers

1. In a private cloud model, the cloud is owned by the organization, and it acts as both the provider and the consumer.
2. With the platform as a service (PaaS) cloud service model, consumers can deploy, but not manage or control, any of the underlying cloud infrastructure (but they can have control over the deployed applications).
3. Regardless of the service model used, the characteristics include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.
4. A community cloud may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

The best way to think about this chapter is as an introduction to cloud computing and an agreement on the definition of what the terms associated with it really mean. The *National Institute of Standards and Technology (NIST)* defines three service models in Special Publication 800-145: Software as a Service (SaaS); Platform as a Service (PaaS); and Infrastructure as a Service (IaaS). It also defines four possible delivery models: private, public, community, and hybrid.

This chapter looks at each of these terms and what they mean as defined by the NIST and agreed upon by the computing community. Know that it is possible to mix and match the service models with the platform models so that you can have public IaaS, or private PaaS, and so on and that you utilize a Cloud Access Security Broker (CASB)—a software program—to sit between the cloud service users and cloud applications to monitor activity and enforce established security policies.

> **Note**
>
> The CASB can offer services beyond just monitoring users' actions, but must always be able to enforce compliance with security policies.

# Service Models

In addition to the three service models defined by NIST (SaaS, PaaS, and IaaS), CompTIA also adds Desktop as a Service (DaaS) to the mix. In the sections that follow, we walk through each of the four models and compare the key elements of each.

# Software as a Service

According to the NIST, Software as a Service (SaaS) is defined as follows: "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

The words used are significant and the ones to focus on in this definition are that consumers can *use* the provider's applications and that they do not *manage or control* any of the underlying cloud infrastructure. Figure 7.1 depicts the responsibility of each party in the SaaS model.

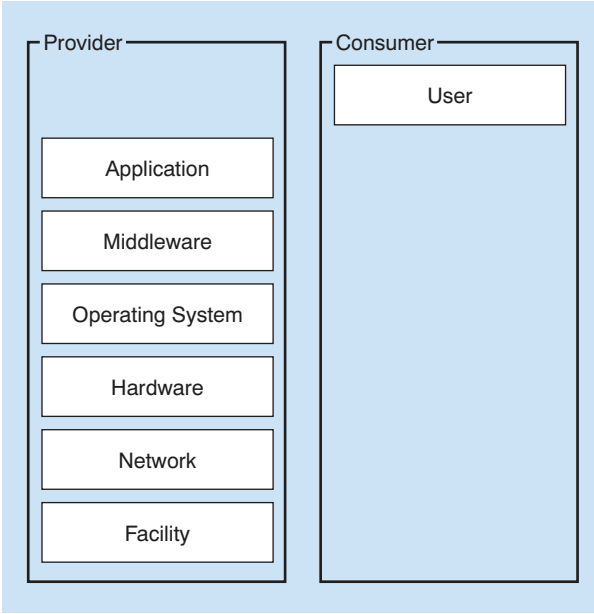



FIGURE 7.1 **The SaaS service model**

**ExamAlert**

For the exam, know Software as a Service (SaaS) involves delivering a licensed application to customers over the Web for use as a service on demand.

# Platform as a Service

According to the NIST, *Platform as a Service (PaaS)* is defined as follows: "The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possible configuration settings for the application-hosting environment."

The important words to focus on in this definition are that consumers can *deploy*, that they do not *manage or control* any of the underlying cloud infrastructure, but they can have *control over the deployed applications*. Figure 7.2 depicts the responsibility of each party in the PaaS model.

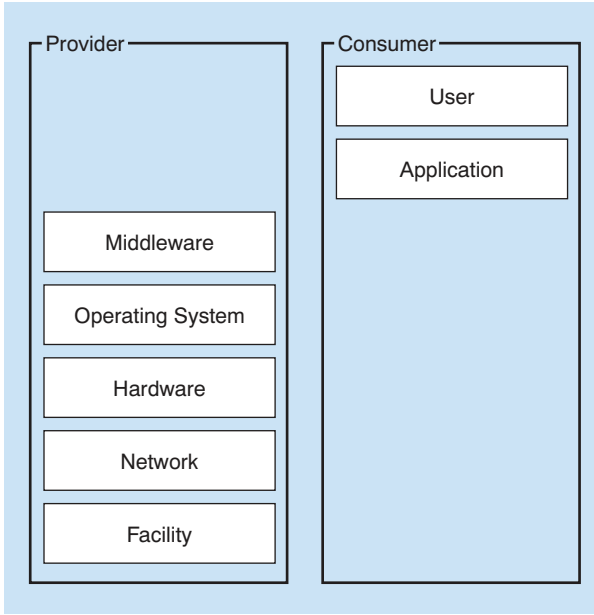



FIGURE 7.2 **The PaaS service model**

**ExamAlert**

Know that Platform as a Service (PaaS) involves delivering a platform to develop applications over the Internet, without downloads or installation.

# Infrastructure as a Service

According to the NIST, *Infrastructure as a Service (IaaS)* is defined as follows: "The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possible limited control of select networking components (e.g., host firewalls)."

The words to focus on are that the consumer can *provision*, is able to *deploy and run*, but still does not *manage or control* the underlying cloud infrastructure, but now can be responsible for some aspects. Figure 7.3 depicts the responsibility of each party in the IaaS model.

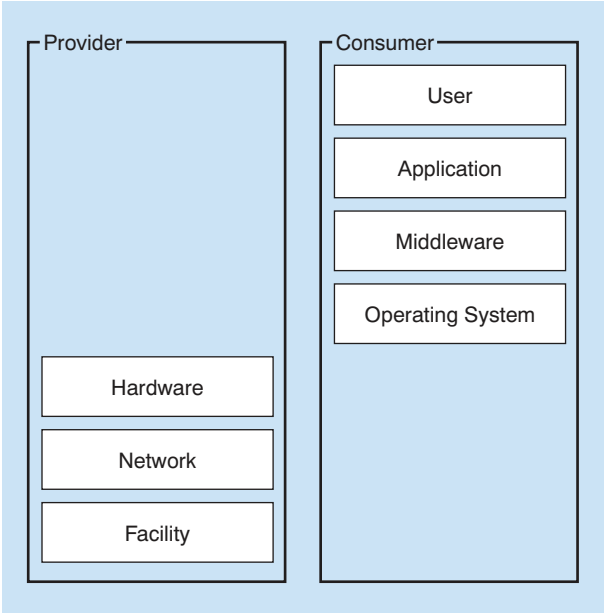



FIGURE 7.3 **The IaaS service model**

**ExamAlert**

Know that Infrastructure as a Service (IaaS) involves delivering the computer infrastructure in a hosted service model over the Internet.

# Desktop as a Service

IaaS, PaaS, and SaaS are the most popular models in use today, but virtually anything can have "aaS" tacked to the end of it and its subscription referenced "as a Service." *Desktop as a Service (DaaS)* is an implementation of desktop virtualization that does not require you to build and manage your own infrastructure. It is important to note that this is a business model and not one of the three recognized service models by NIST. Other similar business models, as opposed to service models, include Communication as a Service (CaaS)—outsourced communications leased from a vendor(s) such as voice over IP (VoIP), videoconferencing apps, and Everything as a Service (XaaS).

**Note**

Regardless of the service model used, the characteristics of each of them are that they include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

After you have a service model selected, both CompTIA and NIST recognize the different delivery models, which are discussed next.

**ExamAlert**

For the exam, know that there are three possible cloud service models: IaaS, PaaS, and SaaS. DaaS, along with other models that are always labeled with "aaS," are for mostly marketing purposes.

# Deployment Models

Cloud deployment can be done in various ways. It is possible to isolate the cloud (a private model), make it widely available (a public model), or do something in between (a community model or hybrid model). In the discussion that follows, we look at deployment models and move into discussing cloud-based features.

# Private Cloud

A *private cloud* is defined as follows: "The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises."

Under most circumstances, a private cloud is owned by the organization, and it acts as both the provider and the consumer. It has a security-related advantage in not needing to put its data on the Internet.

# Public Cloud

A *public cloud* is defined as follows: "The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider."

Under most circumstances, a public cloud is owned by the cloud provider, and it uses a pay-as-you-go model. A good example of a public cloud is webmail or online document sharing/collaboration.

# Hybrid and Community Clouds

A *hybrid cloud* is defined as follows: "The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)."

A hybrid can be any combination of other delivery models. Not only are public and private listed in the definition, but also community. A community cloud is defined as follows: "The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises."

For real-world purposes, you should know that the key to distinguishing between a community cloud and other types of cloud delivery is that it serves a *similar* group. There must be joint interests and limited enrollment.

**Note**

A common reason for using cloud computing is to be able to offload traffic to resources from a cloud provider if your own servers become too busy. This is known as *cloud bursting*, and it requires load-balancing/prioritizing technologies such as *quality of service (QoS)* protocols to make it possible.

**ExamAlert**

For the exam, you should know that the most deployed cloud delivery models are private, public, community, and hybrid.

# Infrastructure as Code

Infrastructure as Code (IaC) involves using virtual machines and bare-metal servers to provision and manage data centers via machine-readable definition files (as opposed to physical hardware configuration). Those definitions

are within a version control system and can either use scripts or declarative definitions. The two methods are known as push and pull: with the pull method, the server pulls its configuration from the controlling server, while the controlling server with the push method "pushes" the configuration to the destination.

With infrastructure automation, faster execution is possible as is increased visibility that can help other teams across the enterprise work quickly and more efficiently. The automation removes risks that can come from human error, thus decreasing downtime and increasing reliability. These outcomes can help the enterprise implement a DevOps culture combining development and operations. Complementing this, orchestration allows IaC to be arranged or coordinated across multiple systems: allowing a distributed application, or a set of services, to span multiple machines.

## Connectivity Options

Most cloud providers offer a number of methods that clients can employ to connect to them. It is important, before making an investment in infrastructure, to check with your provider and see what methods it recommends and supports. One of the most common is to use an IPSec, hardware virtual private network (VPN) connection between your network(s) and the cloud provider. This method offers the capability to have a managed VPN endpoint that includes automated multidata center redundancy and failover.

A dedicated direct connection, known as a private-direct connection, is another, simpler, method. You can combine the dedicated network connection(s) with the hardware VPN to create a combination that offers an IPSec-encrypted private connection while also reducing network costs.

Amazon Web Services (AWS) is one of the most popular cloud providers on the market. It allows the two connectivity methods discussed (calling the dedicated connection "AWS Direct Connect") and a number of others that are variations, or combinations, of these two.

> **Note**
>
> Virtual private cloud (VPC) endpoint allows the VPC to be connected with other services without the need for additional technologies like a VPN connection or Internet gateway. Resources within the VPC must make any requests because the connected services are not able to initiate requests via the VPC endpoint.

# Multitenancy

One of the ways cloud computing is able to obtain cost efficiencies is by putting data from various clients on the same machines. This "multitenant" nature, known as multitenancy, means that workloads from different clients can be on the same system, and a flaw in implementation could compromise security. In theory, a security incident could originate with another customer at the cloud provider and bleed over into your data. Therefore, data needs to be protected from other cloud consumers and from the cloud provider as well.

# Elasticity

According to NIST, one of the five essential characteristics of the cloud is not just elasticity, but rapid elasticity. This characteristic is defined as follows: "Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time." The key words to focus on in this definition are *provisioned and released*, *scale*, and *appear to be unlimited*.

# Scalability

Another feature that makes cloud computing valuable is scalability. According to NIST, "Performance can potentially be scaled to meet conditions of anticipated or real-world demand, within the parameters of a cloud service agreement." To be able to scale, elasticity is required, and autonomic autoscaling of resources is critical.

**ExamAlert**

For the exam, you should know the differences between *multitenancy*, *elasticity*, and *scalability* cloud concepts and be able to summarize them.

# Security Implications

Security is one of the most important issues to discuss with your cloud provider. Cloud computing holds great promise when it comes to scalability, cost savings, rapid deployment, and empowerment. As with any technology where so much is removed from your control, though, risks are involved. Each risk should be considered carefully to identify ways to help mitigate it. Naturally, the

responsibilities of both the organization and the cloud provider vary depending on the service model chosen, but ultimately the organization is accountable for the security and privacy of the outsourced service.

Software and services not necessary for the implementation should be removed or at least disabled. Patches and firmware updates should be kept current, and log files should be carefully monitored. You should find the vulnerabilities in the implementation before others do and work with your service provider(s) to close any holes.

When it comes to data storage on the cloud, encryption is one of the best ways to protect it (keeping it from being of value to unauthorized parties), and VPN routing and forwarding can help. Backups should be performed regularly (and encrypted and stored in safe locations), and access control should be a priority.

> **Note**
>
> For a good discussion of cloud computing and data protection, visit https://cloud.google.com/security/transparency/data-protection.

## The Relationship Between Resources

Just as the cloud holds such promise for running applications, balancing loads, and a plethora of other options, it also offers the capability to store more and more data on it and to let a provider worry about scaling issues instead of local administrators. From an economic perspective, this can be a blessing. From an administrative point of view, though, it can present some issues. Redundancy that occurs from having data in more than one location (local and remote) can be wonderful when you need to recover data, but problematic when you want to make sure you are always working with the most recent version. To minimize problems, be sure that files are kept current, and synchronization between local and remote files is always running.

## Cram Quiz

1. With which cloud service model can consumers use the provider's applications but not manage or control any of the underlying cloud infrastructure?

   - ❍ **A.** SaaS
   - ❍ **B.** PaaS
   - ❍ **C.** IaaS
   - ❍ **D.** GaaS

2. Which of the following involves offloading traffic to resources from a cloud provider if your own servers become too busy?
   - ❍ **A.** Ballooning
   - ❍ **B.** Cloud bursting
   - ❍ **C.** Bridging
   - ❍ **D.** Harvesting

3. Which of the following does the NIST define as a composition of two or more distinct cloud infrastructures?
   - ❍ **A.** Private cloud
   - ❍ **B.** Public cloud
   - ❍ **C.** Community cloud
   - ❍ **D.** Hybrid cloud

4. "To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time." Which cloud concept does this statement BEST describe?
   - ❍ **A.** Scalability
   - ❍ **B.** AWS Direct Connect
   - ❍ **C.** CSAB
   - ❍ **D.** Elasticity

5. Which of the following means that workloads from different clients can be on the same system, and a flaw in implementation could compromise security?
   - ❍ **A.** VPC
   - ❍ **B.** IaC
   - ❍ **C.** Multitenancy
   - ❍ **D.** DaaS

# Cram Quiz Answers

1. **A.** With the SaaS cloud service model, consumers are able to use the provider's applications, but they do not manage or control any of the underlying cloud infrastructure.
2. **B.** A common reason for using cloud computing is to be able to offload traffic to resources from a cloud provider if your own servers become too busy. This is known as cloud bursting.
3. **D.** The hybrid cloud delivery model is a composition of two or more distinct cloud infrastructures (public, private, and so on).

4. **D.** The statement describes elasticity. The key words to focus on in this definition are *provisioned and released*, *scale*, and *appear to be unlimited*.
5. **C.** With multitenancy, a security incident could originate with another customer at the cloud provider and bleed over into your data. Therefore, data needs to be protected from other cloud consumers and from the cloud provider as well.

# What's Next?

Chapter 8, "Network Operations," focuses on several important topics: network availability, organizational documents and policies, and disaster recovery technologies/techniques.

*This page intentionally left blank*

CHAPTER 8

# Network Operations

**This chapter covers the following official Network+ objectives:**

- Given a scenario, use the appropriate statistics and sensors to ensure network availability.
- Explain the purpose of organizational documents and policies.
- Explain high availability and disaster recovery concepts and summarize which is the best solution.

This chapter covers CompTIA Network+ objectives 3.1, 3.2, and 3.3. For more information on the official Network+ exam topics, see the "About the Network+ Exam" section in the Introduction.

This chapter examines two important parts of the role of a network administrator: documentation and the tools to use to monitor or optimize connectivity. Documentation, although not glamorous, is an essential part of the job. This chapter also looks at ensuring high availability, using statistics appropriately, and disaster recover concepts.

# Organizational Documents and Policies

▶ **Explain the purpose of organizational documents and policies.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. Which network topology focuses on the direction in which data flows within the physical environment?
2. In computing, what are historical readings used as a measurement for future calculations referred to as?
3. True or false: Both logical and physical network diagrams provide an overview of the network layout and function.
4. True or false: Acceptable use policies define what controls are required to implement and maintain the security of systems, users, and networks.

### Answers

1. The logical network refers to the direction in which data flows on the network within the physical topology. The logical diagram is not intended to focus on the network hardware but rather on how data flows through that hardware.
2. An essential part of the administrator's role is keeping and reviewing baselines.
3. True. Both logical and physical network diagrams provide an overview of the network layout and function.
4. False. Security policies define what controls are required to implement and maintain the security of systems, users, and networks. *Acceptable use policies (AUPs)* describe how the employees in an organization can use company systems and resources: both software and hardware.

## ExamAlert

Remember that this objective begins with "Explain the purpose." This means that you need to know and appreciate the role organizational documents and policies play in keeping a business up and running.

Administrators have several daily tasks, and new ones often crop up. In this environment, tasks such as documentation sometimes fall to the background. It's important that you understand why administrators need to spend valuable time writing and reviewing documentation. Having a well-documented network offers a number of advantages:

- **Troubleshooting:** When something goes wrong on the network, including the wiring, up-to-date documentation is a valuable reference to guide the troubleshooting effort. The documentation saves you money and time in isolating potential problems.
- **Training new administrators/technicians:** In many network environments, new administrators are hired, and old ones leave. In this scenario, documentation is critical. New administrators do not have the time to try to figure out where cabling is run, what cabling is used, potential trouble spots, and more. Up-to-date information helps new administrators quickly see the network layout.
- **Working with contractors and consultants:** Consultants and contractors occasionally may need to visit the network to make recommendations for the network or to add wiring or other components. In such cases, up-to-date documentation is needed. If documentation is missing, it would be much more difficult for these people to do their jobs, and more time and money would likely be required.
- **Inventory management:** Knowing what you have, where you have it, and what you can turn to in the case of an emergency is both constructive and helpful.

Quality network documentation does not happen by accident; rather, it requires careful planning. When creating network documentation, you must keep in mind who you are creating the documentation for and that it is a communication tool. Documentation is used to take technical information and present it in a manner that someone new to the network can understand. When planning network documentation, you must decide what you need to document.

> **Note**
>
> Imagine that you have just taken over a network as administrator. What information would you like to see? This is often a clear gauge of what to include in your network documentation.

All networks differ and so does the documentation required for each network. However, certain elements are always included in quality documentation:

- **Floor plan:** This diagram need not be complicated; it should simply show where everything is. It is a layout of the area and what would be found in each location. A good way to think of this plan is that it would be a useful tool to hand to new junior administrators on their first day at work to familiarize them with where resources can be found.
- **Network topology:** Networks can be complicated. If someone new is looking over the network, it is critical to document the entire topology. This includes both the wired and wireless topologies used on the network. Network topology documentation typically consists of a diagram or series of diagrams labeling all critical components used to create the network. These diagrams utilize common symbols for components such as firewalls, hubs, routers, and switches. Figure 8.1, for example, shows standard figures for, from left to right, a firewall, a hub, a router, and a switch.

FIGURE 8.1 **Diagram symbols for a firewall, a hub, a router, and a switch**

- **Wiring layout and rack diagrams:** Network wiring can be confusing. Much of it is hidden in walls and ceilings, making it hard to know where the wiring is and what kind is used on the network. Therefore, it is critical to keep documentation on network wiring up to date. Diagram what is on each rack and any unusual configurations that might be employed.
- **IDF/MDF documentation:** It is not enough to show that there is an intermediate distribution frame (IDF) and/or main distribution frame (MDF) in your building. You need to thoroughly document any and every free-standing or wall-mounted rack and the cables running between them and the end-user devices.
- **Server configuration:** A single network typically uses multiple servers spread over a large geographic area. Documentation must include schematic drawings of where servers are located on the network and the services each provides. This includes server function, server IP address, operating system (OS), software information, and more. Essentially, you need to document all the information you need to manage or administer the servers.

- **Network equipment:** The hardware used on a network is configured in a particular way—with protocols, security settings, permissions, and more. Trying to remember them would be a difficult task. Having up-to-date documentation makes it easier to recover from a failure.
- **Network configuration, performance baselines, and key applications:** Documentation also includes information on all current network configurations, performance baselines taken, and key applications used on the network, such as up-to-date information on their updates, vendors, install dates, and more.
- **Detailed account of network services:** Network services are a key ingredient in all networks. Services such as Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP), and more are an important part of documentation. You should describe in detail which server maintains these services, the backup servers for these services, maintenance schedules, how they are structured, and so on.
- **Site survey report:** A *site survey* is typically associated with wireless networking and used to identify access points and security settings. These surveys can be used to help you design and deploy an efficient network.
- **Audit and assessment report:** An *audit and assessment report* is used to see how well your operations/settings match what you intended them to. For more information, see "Network Device Logs" later in this chapter.
- **Standard operating procedures/work instructions:** Finally, documentation should include information on network policy and procedures. This information includes many elements, ranging from who can and cannot access the server room, to network firewalls, protocols, passwords, physical security, cloud computing use, mobile device use, and so on.

ExamAlert

Be sure that you know the types of information that should be included in network documentation.

# Wiring and Port Locations

Network wiring schematics are an essential part of network documentation, particularly for midsize to large networks, where the cabling is certainly complex. For such networks, it becomes increasingly difficult to visualize network cabling and even harder to explain it to someone else. A number of software tools exist to help administrators clearly document network wiring in detail.

Several types of wiring schematics exist. They can be general, as shown in Figure 8.2, or they can be very specific, indicating the actual type of wiring used, the operating system on each machine, and so on. The more generalized they are, the less they need updating, whereas very specific schematics often need to be changed regularly. Table 8.1 represents another way of documenting data.

**ExamAlert**

For the exam, be familiar with the look of a general wiring schematic such as the one shown in Figure 8.2.

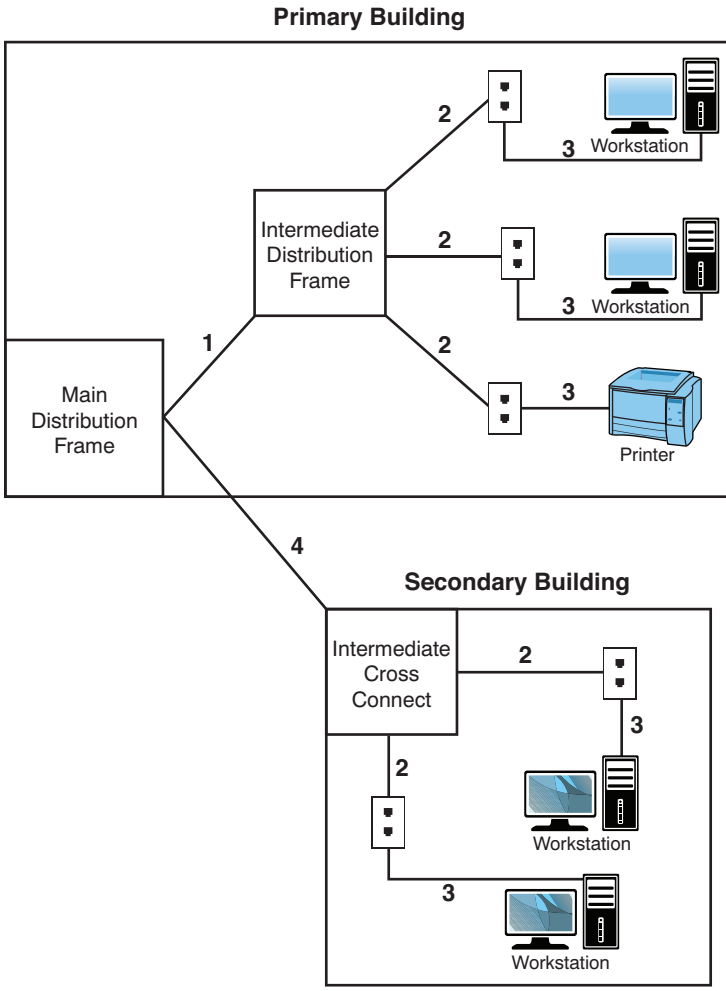



FIGURE 8.2 **A general wiring schematic**

TABLE 8.1 **Wiring Details**

| Cable | Description | Installation Notes |
|---|---|---|
| 1 | Category 6 plenum-rated cable | Cable runs 50 feet from the MDF to IDF. Cable placed through the ceiling and through a mechanical room. Cable was installed 02/26/2019, upgrading a nonplenum Category 5e cable. |
| 2 | Category 6a plenum cable | Horizontal cable runs 45 feet to 55 feet from IDF to wall jack. Replaced Category 5 cable February 2019. Section of cable run through the ceiling and over fluorescent lights. |
| 3 | Category 6 UTP cable | All patch cable connectors were attached in-house. Patch cable connecting the printer runs 45 feet due to printer placement. |
| 4 | 8.3-micron core/ 125-micron cladding single mode | Connecting fiber cable runs 2 kilometers between the primary and secondary buildings. |

Figure 8.2 provides a simplified look at network wiring schematics. Imagine how complicated these diagrams would look on a network with 1,000, 2,000, or even 6,000 computers. Quality network documentation software makes this easier; however, the task of network wiring can be a large one for administrators. Administrators need to ensure that someone can pick up the wiring documentation diagrams and have a good idea of the network wiring.

**Caution**

Reading schematics and determining where wiring runs are an important part of the administrator's role. Expect to see a schematic on your exam.

Port locations should be carefully recorded and included in the documentation as well. SNMP can be used directly to map ports on switches and other devices; it is much easier, however, to use software applications that incorporate SNMP and use it to create ready-to-use documentation. A plethora of such programs are available; some are free and many are commercial products.

## Troubleshooting Using Wiring Schematics

Some network administrators do not take the time to maintain quality documentation. This failure to keep updated information will haunt them when it comes time to troubleshoot some random network problems. Without any network wiring schematics, the task will be frustrating and time-consuming. The information shown in Figure 8.2 might be simplified, but you could use that documentation to evaluate the network and make recommendations.

**Caution**

When looking at a wiring schematic, pay close attention to where the cable is run and the type of cable used if the schematic indicates this information. If a correct cable is not used, a problem could occur.

**Note**

Network wiring schematics are a work in progress. Although changes to wiring do not happen daily, they do occur when the network expands or old cabling is replaced. It is imperative to remember that when changes are made to the network, the schematics and their corresponding references must be updated to reflect the changes. Out-of-date schematics can be frustrating to work with.

# Physical and Logical Network Diagrams

In addition to the wiring schematics, documentation should include diagrams of the physical and logical network design. Recall from Chapter 1, "Network Technologies, Topologies, and Types," that network topologies can be defined on a physical or a logical level. The *physical topology* refers to how a network is physically constructed—how it looks. The *logical topology* refers to how a network looks to the devices that use it—how it functions.

Network infrastructure documentation isn't reviewed daily; however, this documentation is essential for someone unfamiliar with the network to manage or troubleshoot the network. When it comes to documenting the network, you need to document all aspects of the infrastructure. This includes the physical hardware, physical structure, protocols, and software used.

**ExamAlert**

You should be able to identify a physical and logical diagram. You need to know the types of information that should be included in each diagram.

The physical documentation of the network should include the following elements:

- **Cabling information:** A visual description of all the physical communication links, including all cabling, cable grades, cable lengths, WAN cabling, and more.
- **Servers:** The server names and IP addresses, types of servers, and domain membership.

- **Network devices:** The location of the devices on the network. This information includes the printers, hubs, switches, routers, gateways, and more.
- **Wide-area network:** The location and devices of the WAN and components.
- **User information:** Some user information, including the number of local and remote users.

As you can see, many elements can be included in the physical network diagram. Figure 8.3 shows a physical segment of a network.

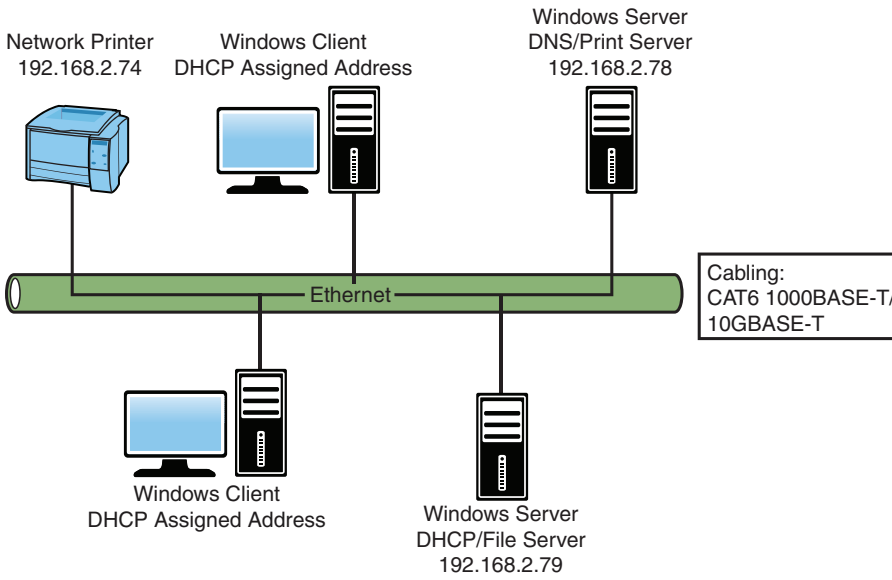



FIGURE 8.3 **A physical network diagram**

**Caution**

You should recognize the importance of maintaining documentation that includes network diagrams, asset management, IP address utilization, vendor documentation, and internal operating procedures, policies, and standards.

Networks are dynamic, and changes can happen regularly, which is why the physical network diagrams also must be updated. Networks have different

policies and procedures on how often updates should occur. Best practice is that the diagram should be updated whenever significant changes to the network occur, such as the addition of a switch or router, a change in protocols, or the addition of a new server. These changes impact how the network operates, and the documentation should reflect the changes.

**Caution**

There are no hard-and-fast rules about when to change or update network documentation. However, most administrators want to update whenever functional changes to the network occur.

The logical network refers to the direction in which data flows on the network within the physical topology. The logical diagram is not intended to focus on the network hardware but rather on how data flows through that hardware. In practice, the physical and logical topologies can be the same. In the case of the bus physical topology, data travels along the length of the cable from one computer to the next. So, the diagram for the physical and logical bus would be the same.

This is not always the case. For example, a topology can be in the physical shape of a star, but data is passed in a logical ring. The function of data travel is performed inside a switch in a ring formation. So the physical diagram appears to be a star, but the logical diagram shows data flowing in a ring formation from one computer to the next. Simply put, it is difficult to tell from looking at a physical diagram how data is flowing on the network.

In today's network environments, the star/hub-and-spoke topology is a common network implementation. Ethernet uses a physical star topology but a logical bus topology. In the center of the physical Ethernet star topology is a switch. It is what happens inside the switch that defines the logical bus topology. The switch passes data between ports as if they were on an Ethernet bus segment.

In addition to data flow, logical diagrams may include additional elements, such as the network domain architecture, server roles, protocols used, and more. Figure 8.4 shows how a logical topology may look in the form of network documentation.

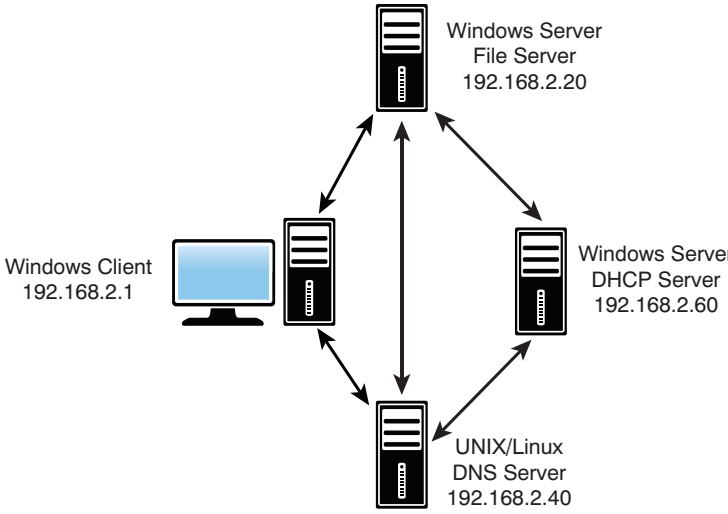



FIGURE 8.4 **A logical topology diagram**

**Caution**

The logical topology of a network identifies the logical paths that data signals travel over the network.

# Baseline Configurations

Baselines play an integral part in network documentation because they let you monitor the network's overall performance. In simple terms, a *baseline* is a measure of performance that indicates how hard the network is working and where network resources are spent. The purpose of a baseline is to provide a basis of comparison. For example, you can compare the network's performance results taken in March to results taken in June, or from one year to the next. More commonly, you would compare the baseline information at a time when the network is having a problem to information recorded when the network was operating with greater efficiency. Such comparisons help you determine whether there has been a problem with the network, how significant that problem is, and even where the problem lies.

To be of any use, baselining is not a one-time task; rather, baselines should be taken periodically to provide an accurate comparison. You should take an initial baseline after the network is set up and operational, and then again when major

changes are made to the network. Even if no changes are made to the network, periodic baselining can prove useful as a means to determine whether the network is still operating correctly.

All *network operating systems (NOSs)*, including Windows, macOS, UNIX, and Linux, have built-in support for network monitoring. In addition, many third-party software packages are available for detailed network monitoring. These system-monitoring tools provided in an NOS give you the means to take performance baselines, either of the entire network or for an individual segment within the network. Because of the different functions of these two baselines, they are called a system baseline and a component baseline.

To create a network baseline, network monitors provide a graphical display of network statistics. Network administrators can choose a variety of network measurements to track. They can use these statistics to perform routine troubleshooting tasks, such as locating a malfunctioning network card, a downed server, or a *denial-of-service (DoS)* attack.

**Note**

*Graphing*, and the process of seeing data visually, can be much more helpful in identifying trends than looking at raw data and log files.

Collecting network statistics is a process called *capturing*. Administrators can capture statistics on all elements of the network. For baseline purposes, one of the most common statistics to monitor is bandwidth usage. By reviewing bandwidth statistics, administrators can see where the bulk of network bandwidth is used. Then they can adapt the network for bandwidth use. If too much bandwidth is used by a particular application, administrators can actively control its bandwidth usage. Without comparing baselines, however, it is difficult to see what is normal network bandwidth usage and what is unusual.

**Caution**

Remember that baselines need to be taken periodically and under the same conditions to be effective. They are used to compare current performance with past performance to help determine whether the network is functioning properly or if troubleshooting is required.

# Policies, Procedures, Configurations, and Regulations

Well-functioning networks are characterized by documented policies, procedures, configurations, and regulations. Because they are unique to every network, policies, procedures, configurations, and regulations should be clearly documented.

## Policies

By definition, policies refer to an organization's documented rules about what is to be done, or not done, and why. Policies dictate who can and cannot access particular network resources, server rooms, backup media, and more.

Although networks might have different policies depending on their needs, some common policies include the following:

- **Network usage policy:** This policy defines who can use network resources such as PCs, printers, scanners, mobile devices, and remote connections. In addition, the usage policy dictates what can be done with these resources after they are accessed. No outside systems will be networked without permission from the network administrator.
- **Internet usage policy:** This policy specifies the rules for Internet use on the job. Typically, usage should be focused on business-related tasks. Incidental personal use is allowed during specified times.
- **Bring-your-own-device (BYOD) policy:** *Bring-your-own-device (BYOD)* policies define what personally owned mobile devices (laptops, tablets, and smartphones) employees are allowed to bring to their workplace and use. *Mobile device management (MDM)* and *mobile application management (MAM)* systems can be used to help enterprises manage and secure the use of those mobile devices in the workplace and to interact with privileged company information and applications. Two things the policy needs to address are onboarding and offboarding. *Onboarding* the mobile device is the set of procedures gone through to get it ready to go on the network (scanning for viruses, adding certain apps, and so forth). *Offboarding* is the process of removing company-owned resources when it is no longer needed (often done with a wipe or factory reset).

**ExamAlert**

For the exam, be familiar with onboarding and offboarding.

- **Email usage policy:** Email must follow the same code of conduct as expected in any other form of written or face-to-face communication. All emails are company property and can be accessed by the company. Personal emails should be immediately deleted.
- **Personal software policy:** No outside software should be installed on network computer systems. All software installations must be approved by the network administrator. No software can be copied or removed from a site. Licensing restrictions must be adhered to.
- **Password policy:** Detail how often passwords must be changed and the minimum level of security for each (number of characters, use of alphanumeric character set, longer phrases, and so on).
- **Acceptable use policy (AUP):** *Acceptable use policies (AUPs)* describe how the employees in an organization can use company systems and resources, both software and hardware. This policy should also outline the consequences for misuse. In addition, the policy (also known as a *use policy*) should address installation of personal software on company computers and the use of personal hardware, such as USB devices.
- **User account policy:** All users are responsible for keeping their password and account information secret. All staff are required to log off and sometimes lock their systems after they finish using them. Attempting to log on to the network with another user account is considered a serious violation.
- **International export controls:** A number of laws and regulations govern what can and cannot be exported when it comes to software and hardware to various countries. Employees should take every precaution to make sure they are adhering to the letter of the law.
- **Data loss prevention (DLP):** Losses from employees can quickly put a company in the red. All employees should understand that it is their responsibility to make sure all preventable losses are prevented.
- **Incident response plan:** When an incident occurs, all employees should understand it is their responsibility to be on the lookout for it and report it immediately to the appropriate party.
- **Disaster recovery plan:** Just as you should have a plan in place for responding to incidents, so, too, do you need one for disasters. This topic is explored in further detail in the section "High Availability and Disaster Recovery" later in this chapter.

- **Business continuity plan (BCP):** When an incident occurs, it is too late to consider policies and procedures then; this must be done well ahead of time. *Business continuity* should always be of the utmost concern. Business continuity is primarily concerned with the processes, policies, and methods that an organization follows to minimize the impact of a system failure, network failure, or the failure of any key component needed for operation. *Business continuity planning (BCP)* is the process of implementing policies, controls, and procedures to counteract the effects of losses, outages, or failures of critical business processes. BCP is primarily a management tool that ensures that *critical business functions (CBFs)* can be performed when normal business operations are disrupted.
- **Nondisclosure agreements (NDAs):** NDAs are the oxygen that many companies need to thrive. Employees should understand the importance of them to continued business operations and agree to follow them to the letter, and spirit, of the law.
- **Service-level agreements (SLAs):** A *service-level agreement (SLA)* is an agreement between you or your company and a service provider, typically a technical support provider. SLAs are also usually part of network availability and other agreements. They stipulate the performance you can expect or demand by outlining the expectations a vendor has agreed to meet. They define what is possible to deliver and provide the contract to make sure what is delivered is what was promised.
- **Memorandum of understanding (MOU):** A *memorandum of understanding (MOU)* is an agreement between two or more parties that indicates what the relationship is between the parties. It is sometimes a precursor to a contract, but is often used in place of it when a contract would not do (such as defining the relationship between departments of the same organization).
- **Safety procedures and policies:** Safety is everyone's business, and all employees should know how to do their job in the safest manner while also looking out for other employees and customers alike.
- **Ownership policy:** The company owns all data, including users' email, voice mail, and Internet usage logs, and the company reserves the right to inspect them at any time. Some companies even go so far as controlling how much personal data can be stored on a workstation or mobile device.

This list is just a snapshot of the policies that guide the behavior for administrators and network users. Network policies should be clearly documented and available to network users. Often, these policies are reviewed with new staff

members or new administrators. As they are updated, they are rereleased to network users. Policies are regularly reviewed and updated.

> **Note**
>
> You might be asked about network policies. Network policies dictate network rules and provide guidelines for network conduct. Policies are often updated and reviewed and are changed to reflect changes to the network and perhaps changes in business requirements.

# Password-Related Policies

Although biometrics and smartcards are becoming more common, they still have a long way to go before they attain the level of popularity that username and password combinations enjoy. Usernames and passwords do not require any additional equipment, which practically every other method of authentication does; the username and password process is familiar to users, easy to implement, and relatively secure. For that reason, they are worthy of more detailed coverage than the other authentication systems previously discussed.

> **Note**
>
> Biometrics are not as ubiquitous as username/password combinations, but they are coming up quickly. Some smartphones, for example, offer the ability to use a fingerprint scanner and/or gestures to access the system instead of username and password. Features such as these are expected to become more common with future releases.

Passwords are a relatively simple form of authentication in that only a string of characters can be used to authenticate the user. However, how the string of characters is used and which policies you can put in place to govern them make usernames and passwords an excellent form of authentication.

## Password Policies

All popular network operating systems include password policy systems that enable the network administrator to control how passwords are used on the system. The exact capabilities vary between network operating systems. However, generally they enable the following:

- **Minimum length of password:** Shorter passwords are easier to guess than longer ones. Setting a minimum password length does not prevent a user from creating a longer password than the minimum; however, each network operating system has a limit on how long a password can be.

- **Password expiration:** Also known as the maximum password age, password expiration defines how long the user can use the same password before having to change it. A general practice is that a password be changed every 30 days. In high-security environments, you might want to make this value shorter, but you should generally not make it any longer. Having passwords expire periodically is a crucial feature because it means that if a password is compromised, the unauthorized user will not indefinitely have access.
- **Prevention of password reuse:** Although a system might cause a password to expire and prompt the user to change it, many users are tempted to use the same password again. A process by which the system remembers the last 10 passwords, for example, is most secure because it forces the user to create completely new passwords. This feature is sometimes called enforcing password history.
- **Prevention of easy-to-guess passwords:** Some systems can evaluate the password provided by a user to determine whether it meets a required level of complexity. Enabling this function prevents users from having passwords such as *password*, *12345678*, their name, or their nickname.

Figure 8.5 shows an example of configuring a security policy in Windows for password complexity.

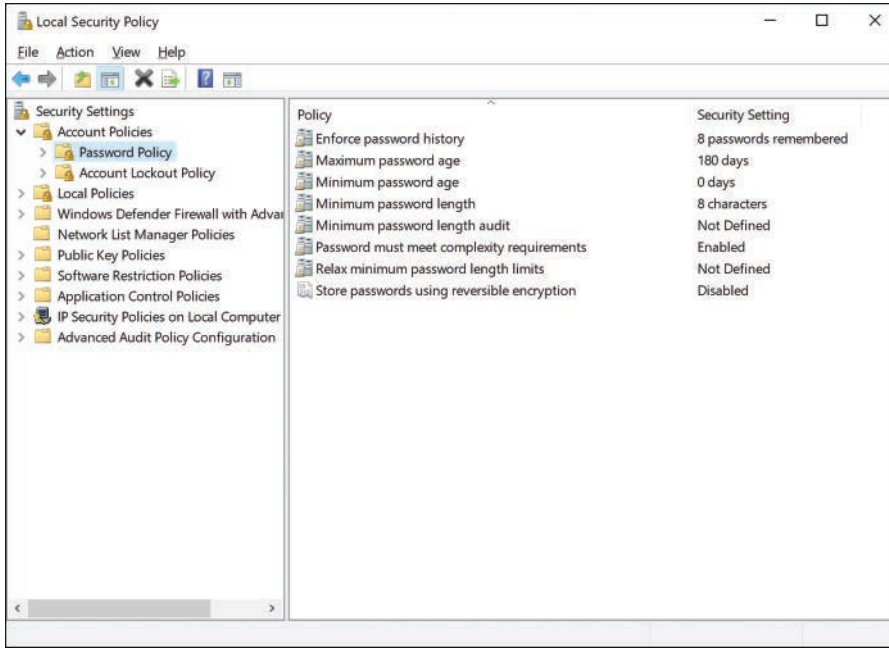



FIGURE 8.5 **Configuring a password security policy.**

ExamAlert

You must identify an effective password policy. For example, a robust password policy would include forcing users to change their passwords on a regular basis.

## Password Strength

No matter how good a company's password policy, it is only as effective as the passwords created within it. A password that is hard to guess, or strong, is more likely to protect the data on a system than one that is easy to guess, or weak.

If you are using only numbers and letters—and the OS is not case sensitive—36 possible combinations exist for each entry, and the total number of possibilities is $36^6$. That might seem like a lot, but to a password-cracking program, it's not much security. A password that uses eight case-sensitive characters, with letters, numbers, and special characters, has so many possible combinations that a standard calculator cannot display the actual number.

There has always been a debate over how long a password should be. It should be sufficiently long that it is hard to break but sufficiently short that the user can easily remember it (and type it). In a normal working environment, passwords of 8 characters are sufficient. Certainly, they should be no fewer than 6 characters. In environments in which security is a concern, passwords should be 10 characters or more.

Users should be encouraged to use a password that is considered strong. A strong password has at least eight characters; has a combination of letters, numbers, and special characters; uses mixed case; and does not form a proper word. Examples are 3Ecc5T0h and e1oXPn3r. Such passwords might be secure, but users are likely to have problems remembering them. For that reason, a popular strategy is to use a combination of letters and numbers to form phrases or long words. Examples include d1eTc0La and tAb1eT0p. These passwords might not be quite as secure as the preceding examples, but they are still strong and a whole lot better than the name of the user's pet.

The National Institute of Standards and Technology (NIST) offers both requirements and recommendations when it comes to passwords. Their requirements include an eight-character minimum length, and changing passwords only if there is evidence of compromise. They also recommend that new passwords be screened against a list of known compromised passwords, password hints and knowledge-based security questions be skipped, and a limit placed on the number of failed authentication attempts that are allowed. Their recommendations, on the other hand, increase the password length to at least 64 characters,

suggest character composition rules be skipped (they are an unnecessary burden for end-users), printable ASCII characters be allowed in addition to UNICODE characters (to now include emojis), and copy/paste functionality be enabled in password fields to facilitate the use of password managers.

## Procedures

Network procedures differ from policies in that they describe how tasks are to be performed. For example, each network administrator has backup procedures specifying the time of day backups are done, how often they are done, and where they are stored. A network is full of a number of procedures for practical reasons and, perhaps more important, for security reasons.

Administrators must be aware of several procedures when on the job. The number and exact type of procedure depend on the network. The network's overall goal is to ensure uniformity and ensure that network tasks follow a framework. Without this procedural framework, different administrators might approach tasks differently, which could lead to confusion on the network.

Network procedures might include the following:

- **Backup procedures:** Backup procedures specify when they are to be performed, how often a backup occurs, who does the backup, what data is to be backed up, and where and how it will be stored. Network administrators should carefully follow backup procedures.
- **Procedures for adding new users:** When new users are added to a network, administrators typically have to follow certain guidelines to ensure that the users have access to what they need to do their job, but no more. This is called the *principle of least privilege*.
- **Privileged user agreement:** Administrators and authorized users who have the ability to modify secure configurations and perform tasks such as account setup, account termination, account resetting, auditing, and so on need to be held to high standards.
- **Security procedures:** Some of the more critical procedures involve security. Security procedures are numerous but may include specifying what the administrator must do if security breaches occur, security monitoring, security reporting, and updating the OS and applications for potential security holes.
- **Network monitoring procedures:** The network needs to be constantly monitored. This includes tracking such things as bandwidth usage, remote access, user logons, and more.

- **Software procedures/*system life cycle*:** All software must be periodically monitored and updated. Documented procedures dictate when, how often, why, and for whom these updates are done. When assets are disposed of, asset disposal procedures should be followed to properly document and log their removal.
- **Procedures for reporting violations:** Users do not always follow outlined network policies. This is why documented procedures should exist to properly handle the violations. This might include a verbal warning upon the first offense, followed by written reports and account lockouts thereafter.
- **Remote-access policy and network admission procedures:** Many workers remotely access the network. This remote access is granted and maintained using a series of defined procedures. These procedures might dictate when remote users can access the network, how long they can access it, and what they can access. *Network admission control (NAC)*—also referred to as *network access control*—determines who can get on the network and is usually based on 802.1X guidelines.

## Change Management Documentation

Change management procedures might include the following:

- **Document reason for a change:** Before making any change at all, the first question to ask is *why*. A change requested by one user may be based on a misunderstanding of what technology can do, may be cost prohibitive, or may deliver a benefit not worth the undertaking.
- **Change request:** An official request should be logged and tracked to verify what is to be done and what has been done. Within the realm of the change request should be the configuration procedures to be used, the rollback process that is in place, potential impact identified, and a list of those who need to be notified.
- **Approval process:** Changes should not be approved on the basis of who makes the most noise, but rather who has the most justified reasons. An official process should be in place to evaluate and approve changes prior to actions being undertaken. The approval can be done by a single administrator or a formal committee based on the size of your organization and the scope of the change being approved.
- **Maintenance window:** After a change has been approved, the next question to address is when it is to take place. Authorized downtime should be used to make changes to production environments.

- **Notification of change:** Those affected by a change should be notified after the change has taken place. The notification should not be just of the change but should include any and all impacts to them and identify whom they can turn to with questions.
- **Documentation:** One of the last steps is always to document what has been done. This documentation should include information on network configurations, additions to the network, and physical location changes.

These procedures represent just a few of the ones that administrators must follow on the job. It is crucial that all these procedures are well documented, accessible, reviewed, and updated as needed to be effective.

## Configuration Documentation

One other critical form of documentation is configuration documentation. Many administrators believe they could never forget the configuration of a router, server, or switch, but it often happens. Although it is often a thankless, time-consuming task, documenting the network hardware and software configurations is critical for continued network functionality.

Two primary types of network configuration documentation are required: software documentation and hardware documentation. Both include all configuration information so that should a computer or other hardware fail, both the hardware and software can be replaced and reconfigured as quickly as possible. The documentation is important because often the administrator who configured the software or hardware is unavailable, and someone else has to re-create the configuration using nothing but the documentation. To be effective in this case, the documentation must be as current as possible. Older configuration information might not help.

> **Note**
>
> Organizing and completing the initial set of network documentation are huge tasks, but they are just the beginning. Administrators must constantly update all documentation to keep it from becoming obsolete. Documentation is perhaps one of the less-glamorous aspects of the administrator's role, but it is one of the most important.

## Regulations

The terms *regulation* and *policy* are often used interchangeably; however, there is a difference. As mentioned, policies are written by an organization for its employees. Regulations are actual legal restrictions with legal consequences.

These regulations are set not by the organizations but by applicable laws in the area. Improper use of networks and the Internet can certainly lead to legal violations and consequences. The following is an example of network regulation from an online company:

> Transmission, distribution, uploading, posting or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, material kept in violation of state laws or industry regulations such as social security numbers or credit card numbers, and material that is obscene, defamatory, libelous, unlawful, harassing, abusive, threatening, harmful, vulgar, constitutes an illegal threat, violates export control laws, hate propaganda, fraudulent material or fraudulent activity, invasive of privacy or publicity rights, profane, indecent or otherwise objectionable material of any kind or nature. You may not transmit, distribute, or store material that contains a virus, 'Trojan Horse,' adware or spyware, corrupted data, or any software or information to promote or utilize software or any of Network Solutions services to deliver unsolicited email. You further agree not to transmit any material that encourages conduct that could constitute a criminal offense, gives rise to civil liability or otherwise violates any applicable local, state, national or international law or regulation.

**ExamAlert**

For the exam and for real-life networking, remember that regulations often are enforceable by law.

# Labeling

One of the biggest problems with documentation is the time needed to do it. To shorten this time, users, through human nature, take shortcuts and use code or shorthand when labeling devices, maps, reports, and the like. Although these shortcuts can save time initially, they can render the labels useless if a person other than the one who created the labels looks at them or if a long period of time has passed since they were created and the author cannot remember what the label now means.

To prevent this dilemma, it is highly recommended that each organization create standard labeling rules and enforce them at all levels.

# Cram Quiz

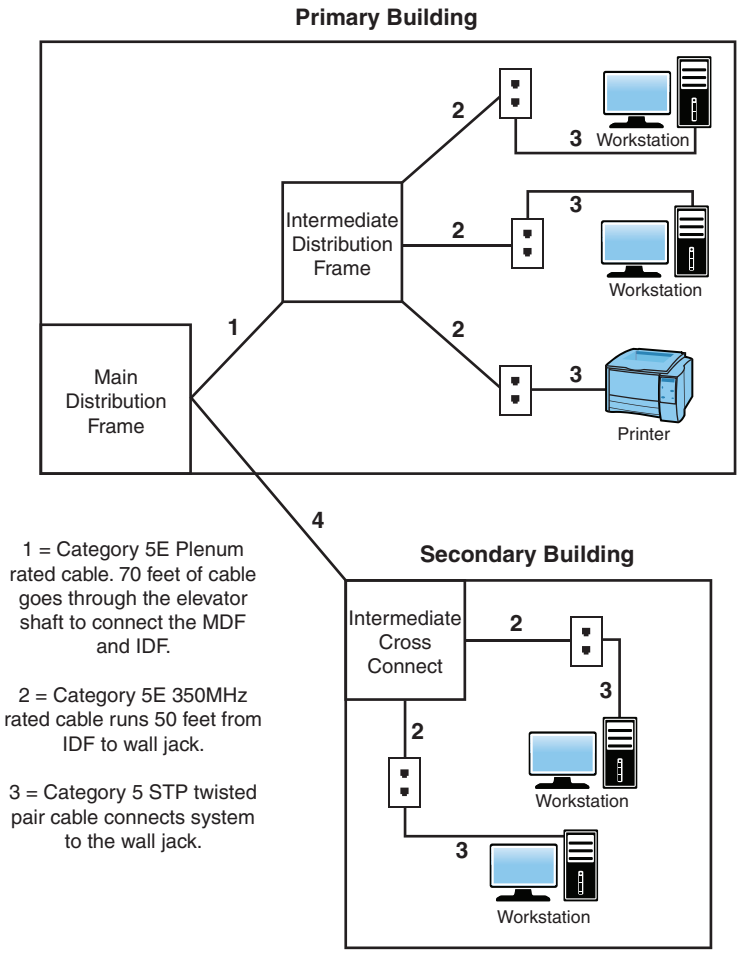
You have been given a physical wiring schematic that shows the following:

| Description | Installation Notes |
|---|---|
| Category 5E 350 MHz plenum-rated cable | Cable runs 50 feet from the MDF to the IDF.<br>Cable placed through the ceiling and through a mechanical room.<br>Cable was installed 01/15/2018, upgrading a nonplenum cable. |
| Category 5E 350 MHz nonplenum cable | Horizontal cable runs 45 feet to 55 feet from the IDF to a wall jack.<br>Cable 6 replaced Category 5e cable February 2018.<br>Section of cable run through ceiling and over fluorescent lights. |
| Category 6a UTP cable | Patch cable connecting printer runs 15 feet due to printer placement. |
| 8.3-micron core/125-micron | Connecting fiber cable runs 2 kilometers cladding single mode between the primary and secondary buildings. |

**1.** Given this information, what cable recommendation might you make, if any?

- ❍ **A.** Nonplenum cable should be used between the IDF and MDF.
- ❍ **B.** The horizontal cable run should use plenum cable.
- ❍ **C.** The patch cable connecting the printer should be shorter.
- ❍ **D.** Leave the network cabling as is.

**2.** You have been called in to inspect a network configuration. You are given only one network diagram, shown in the following figure. Using the diagram, what recommendation might you make?




- ❍ **A.** Cable 1 does not need to be plenum rated.
- ❍ **B.** Cable 2 should be STP cable.
- ❍ **C.** Cable 3 should be STP cable.
- ❍ **D.** None. The network looks good.

3. The head of HR is complaining that the network cabling in her office is outdated and should be changed. What should she do to have the cabling evaluated and possibly changed?
   - ❍ **A.** Tell her supervisor that IT needs to get on the ball.
   - ❍ **B.** Tell your supervisor that IT needs to get on the ball.
   - ❍ **C.** Purchase new cabling at the local electronics store.
   - ❍ **D.** Complete a change request.

4. What stipulates the performance you can expect or demand by outlining the expectations a vendor has agreed to meet?
   - ❍ **A.** SLA
   - ❍ **B.** MOU
   - ❍ **C.** NDA
   - ❍ **D.** BCP

# Cram Quiz Answers

1. **B.** In this scenario, a section of horizontal cable runs through the ceiling and over fluorescent lights. This cable run might be a problem because such devices can cause electromagnetic interference (EMI). Alternatively, plenum cable is used in this scenario. Shielded twisted-pair (STP) may have worked as well.
2. **B.** In this diagram, Cable 1 is plenum rated and should be fine. Cable 3 is patch cable and does not need to be STP rated. Cable 2, however, goes through walls and ceilings. Therefore, it would be recommended to have a better grade of cable than regular UTP. STP provides greater resistance to EMI.
3. **D.** An official change request should be logged and tracked to verify what is to be done and what has been done. Within the realm of the change request should be the configuration procedures to be used, the rollback process that is in place, the potential impact identified, and a list of those that need to be notified.
4. **A.** A service-level agreement (SLA) is an agreement between you or your company and a service provider, typically a technical support provider. SLAs are also usually part of network availability and other agreements. They stipulate the performance you can expect or demand by outlining the expectations a vendor has agreed to meet.

# High Availability and Disaster Recovery

- **Explain high availability and disaster recovery concepts and summarize which is the best solution.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What is the difference between an incremental backup and a differential backup?
2. True or false: A brownout is total failure of the power supplied to the server.
3. What are hot, warm, and cold sites used for?
4. True or false: The MTTR is the measurement of the anticipated or predicted incidence of failure of a system or component between inherent failures, whereas the MTBF is the measurement of how long it takes to repair a system or component after a failure occurs.
5. What is the concept of simultaneous management and utilization of multiple available paths for the transmission of streams of data called?

### Answers

1. With incremental backups, all data that has changed since the last full or incremental backup is backed up. The restore procedure requires several backup iterations: the media used in the latest full backup and all media used for incremental backups since the last full backup. An incremental backup uses the archive bit and clears it after a file is saved to disk. With a differential backup, all data changed since the last full backup is backed up. The restore procedure requires the latest full backup media and the latest differential backup media. A differential backup uses the archive bit to determine which files must be backed up but does not clear it.
2. False. A total failure of the power supplied to the server is called a blackout.
3. Hot, warm, and cold sites are designed to provide alternative locations for network operations if a disaster occurs.
4. False. The MTBF is the measurement of the anticipated or predicted incidence of failure of a system or component between inherent failures, whereas the MTTR is the measurement of how long it takes to repair a system or component after a failure occurs.
5. Multipathing is the concept of simultaneous management and utilization of multiple available paths for the transmission of streams of data.

Even the most fault-tolerant networks can fail, which is an unfortunate fact. When those costly and carefully implemented fault-tolerance strategies fail, you are left with disaster recovery.

Disaster recovery can take many forms. In addition to disasters such as fire, flood, and theft, many other potential business disruptions can fall under the banner of disaster recovery. For example, the failure of the electrical supply to your city block might interrupt the business functions. Such an event, although not a disaster per se, might invoke the disaster recovery methods.

The cornerstone of every disaster recovery strategy is the preservation and recoverability of data. When talking about preservation and recoverability, you must talk about backups. Implementing a regular backup schedule can save you a lot of grief when fault tolerance fails or when you need to recover a file that has been accidentally deleted. When it's time to design a backup schedule, you can use three key types of backups: full, differential, and incremental.

# Backups

Backups are equivalent to an insurance policy for a server, workstation, or any other data-containing device. Most of the time, they are nothing but time-/resource-consuming entities that make you wonder why you are wasting your time doing them. When disaster happens, however, you realize immediately their worth and kick yourself for not doing them with even more frequency.

## Full Backups

The preferred method of backup is the *full backup* method, which copies all files and directories from the hard disk to the backup media. There are a few reasons why doing a full backup is not always possible. First among them is likely the time involved in performing a full backup.

> **ExamAlert**
>
> During a recovery operation, a full backup is the fastest way to restore data of all the methods discussed here, because only one set of media is required for a full restore.

Depending on the amount of data to be backed up, however, full backups can take an extremely long time when you are backing up and can use extensive system resources. Depending on the configuration of the backup hardware,

completing this backup can considerably slow down the network. In addition, some environments have more data than can fit on a single medium. Therefore, doing a full backup is awkward because someone might need to be there to change the media.

The main advantage of full backups is that a single set of media holds all the data you need to restore. If a failure occurs, that single set of media should be all that is needed to get all data and system information back. The upshot of all this is that any disruption to the network is greatly reduced.

Unfortunately, its strength can also be its weakness. A single set of media holding an organization's data can be a security risk. If the media were to fall into the wrong hands, all the data could be restored on another computer. Using passwords on backups and using a secure offsite and onsite location can minimize the security risk.

## Differential Backups

Companies that don't have enough time to complete a full backup daily can use the *differential backup*. Differential backups are faster than a full backup because they back up only the data that has changed since the last full backup. This means that if you do a full backup on a Saturday and a differential backup on the following Wednesday, only the data that has changed since Saturday is backed up. Restoring the differential backup requires the last full backup and the latest differential backup.

Differential backups know what files have changed since the last full backup because they use a setting called the archive bit. The archive bit flags files that have changed or have been created and identifies them as ones that need to be backed up. Full backups do not concern themselves with the archive bit because all files are backed up, regardless of date. A full backup, however, does clear the archive bit after data has been backed up to avoid future confusion. Differential backups notice the archive bit and use it to determine which files have changed. The differential backup does not reset the archive bit information.

## Incremental Backups

Some companies have a finite amount of time they can allocate to backup procedures. Such organizations are likely to use *incremental backups* in their backup strategy. Incremental backups save only the files that have changed since the last full or incremental backup. Like differential backups, incremental backups use the archive bit to determine which files have changed since the last full or

incremental backup. Unlike differentials, however, incremental backups clear the archive bit, so files that have not changed are not backed up.

**ExamAlert**

Both full and incremental backups clear the archive bit after files have been backed up.

The faster backup time of incremental backups comes at a price—the amount of time required to restore. Recovering from a failure with incremental backups requires numerous sets of media—all the incremental backup media sets and the one for the most recent full backup. For example, if you have a full backup from Sunday and an incremental for Monday, Tuesday, and Wednesday, you need four sets of media to restore the data. Each set in the rotation is an additional step in the restore process and an additional failure point. One damaged incremental media set means that you cannot restore the data. Table 8.2 summarizes the various backup strategies.

TABLE 8.2 **Backup Strategies**

| Backup Type | Advantage | Disadvantage | Data Backed Up | Archive Bit |
|---|---|---|---|---|
| Full | Backs up all data on a single media set. Restoring data requires the fewest media sets. | Depending on the amount of data, full backups can take a long time. | All files and directories are backed up. | Does not use the archive bit, but resets it after data has been backed up. |
| Differential | Faster backups than a full backup. | The restore process takes longer than just a full backup.<br>A differential backup uses more media sets than a full backup. | All files and directories that have changed since the last full backup. | Uses the archive bit to determine the files that have changed, but does not reset the archive bit. |
| Incremental | Faster backup times | An incremental backup requires multiple disks; restoring data takes more time than the other backup methods. | The files and directories that have changed since the last full or incremental backup. | Uses the archive bit to determine the files that have changed, and resets the archive bit. |

ExamAlert

Review Table 8.2 before taking the Network+ exam.

## Snapshots

In addition to the three types of backups previously discussed, there are also *snapshots*. Whereas a backup can take a long time to complete, the advantage of a snapshot—an image of the state of a system at a particular point in time—is that it is an instantaneous copy of the system. This snapshot is often accomplished by splitting a mirrored set of disks or by creating a copy of a disk block when it is written to preserve the original and keep it available.

Snapshots are popular with virtual machine implementations. You can take as many snapshots as you want (provided you have enough storage space) to be able to revert a machine to a "saved" state. Snapshots contain a copy of the virtual machine settings (hardware configuration), information on all virtual disks attached, and the memory state of the machine at the time of the snapshot. This makes the snapshots additionally useful for virtual machine cloning, allowing the machine to be copied once—or multiple times—for testing.

ExamAlert

Think of a snapshot as a photograph, which is where the name came from, of a moment in time of any system.

# Backup Best Practices

Many details go into making a backup strategy a success. The following are issues to consider as part of your backup plan:

- **Offsite storage:** Consider storing backup media sets offsite so that if a disaster occurs in a building, a current set of media is available offsite. The offsite media should be as current as any onsite and should be secure.
- **Label media:** The goal is to restore the data as quickly as possible. Trying to find the media you need can prove difficult if it is not marked. Furthermore, labeling can prevent you from recording over something you need to keep.
- **Verify backups:** Never assume that the backup was successful. Seasoned administrators know that checking backup logs and performing periodic test restores are part of the backup process.
- **Cleaning:** You need to occasionally clean the backup drive. If the inside gets dirty, backups can fail.

ExamAlert

A backup strategy must include offsite storage to account for theft, fire, flood, or other disasters.

# Using Uninterruptible Power Supplies

No discussion of fault tolerance can be complete without a look at power-related issues and the mechanisms used to combat them. When you design a fault-tolerant system, your planning should definitely include *uninterruptible power supplies (UPSs)*. A UPS serves many functions and is a major part of server consideration and implementation.

On a basic level, a UPS, also known as a *battery backup*, is a box that holds a battery and built-in charging circuit. During times of good power, the battery is recharged; when the UPS is needed, it's ready to provide power to the server. Most often, the UPS is required to provide enough power to give the administrator time to shut down the server in an orderly fashion, preventing any potential data loss from a dirty shutdown.

## Why Use a UPS?

Organizations of all shapes and sizes need UPSs as part of their fault-tolerance strategies. A UPS is as important as any other fault-tolerance measure. Three key reasons make a UPS necessary:

- **Data availability:** The goal of any fault-tolerance measure is data availability. A UPS ensures access to the server if a power failure occurs—or at least as long as it takes to save a file.
- **Protection from data loss:** Fluctuations in power or a sudden power-down can damage the data on the server system. In addition, many servers take full advantage of caching, and a sudden loss of power could cause the loss of all information held in cache.
- **Protection from hardware damage:** Constant power fluctuations or sudden power-downs can damage hardware components within a computer. Damaged hardware can lead to reduced data availability while the hardware is repaired.

## Power Threats

In addition to keeping a server functioning long enough to safely shut it down, a UPS safeguards a server from inconsistent power. This inconsistent power

can take many forms. A UPS protects a system from the following power-related threats:

- **Blackout:** A total failure of the power supplied to the server.
- **Spike:** A short (usually less than 1 second) but intense increase in voltage. Spikes can do irreparable damage to any kind of equipment, especially computers.
- **Surge:** Compared to a spike, a surge is a considerably longer (sometimes many seconds) but usually less intense increase in power. Surges can also damage your computer equipment.
- **Sag:** A short-term voltage drop (the opposite of a spike). This type of voltage drop can cause a server to reboot.
- **Brownout:** A drop in voltage that usually lasts more than a few minutes.

Many of these power-related threats can occur without your knowledge; if you don't have a UPS, you cannot prepare for them. For the cost, it is worth buying a UPS, if for no other reason than to sleep better at night.

## Beyond the UPS

Power management is not limited only to the use of UPSs. In addition, to these devices, you should employ *power generators* to be able to keep your systems up and running when the electrical provider is down for an extended period of time. *Redundant circuits* and *dual power supplies* should also be used for key equipment.

Any device fitted with multiple outputs that is specifically designed to distribute electric power is known as a *power distribution unit (PDU)*, and they are often plentiful in datacenters for supplying power to racks. The two main types of PDUs are "Basic" and "Intelligent"; the latter is any that is networked (allowing for remote management of power metering, toggling an outlet on/off, and so on).

You want to make sure that power can stay up and running in the event of a crisis, so two other areas to pay attention to are the heating, ventilation, and air conditioning (HVAC) and the fire suppression system. It will do little good to keep the computers and servers running if you cannot keep the temperature within an operating range and provide safety in the event a fire occurs. Redundant systems should be considered for both of these crucial areas and regularly maintained.

# Cold, Warm, Hot, and Cloud Sites

A disaster recovery plan might include the provision for a recovery site that can be quickly brought into play. These sites fall into three categories: hot, warm, and cold. The need for each of these types of sites depends largely on the business you are in and the funds available. Disaster recovery sites represent the ultimate in precautions for organizations that need them. As a result, they do not come cheaply.

The basic concept of a disaster recovery site is that it can provide a base from which the company can be operated during a disaster. The disaster recovery site normally is not intended to provide a desk for every employee. It's intended more as a means to allow key personnel to continue the core business functions.

In general, a cold recovery site is one that can be up and operational in a relatively short amount of time, such as a day or two. Provision of services, such as telephone lines and power, is taken care of, and the basic office furniture might be in place. But there is unlikely to be any computer equipment, even though the building might have a network infrastructure and a room ready to act as a server room. In most cases, cold sites provide the physical location and basic services.

Cold sites are useful if you have some forewarning of a potential problem. Generally, cold sites are used by organizations that can weather the storm for a day or two before they get back up and running. If you are the regional office of a major company, it might be possible to have one of the other divisions take care of business until you are ready to go. But if you are the only office in the company, you might need something a little hotter.

For organizations with the dollars and the desire, hot recovery sites represent the ultimate in fault-tolerance strategies. Like cold recovery sites, hot sites are designed to provide only enough facilities to continue the core business function, but hot recovery sites are set up to be ready to go at a moment's notice.

A hot recovery site includes phone systems with connected phone lines. Data networks also are in place, with any necessary routers and switches plugged in and turned on. Desks have installed and waiting desktop PCs, and server areas are equipped with the necessary hardware to support business-critical functions. In other words, within a few hours, the hot site can become a fully functioning element of an organization.

The issue that confronts potential hot-recovery site users is that of cost. Office space is expensive in the best of times, but having space sitting idle 99.9 percent of the time can seem like a tremendously poor use of money. A popular strategy to get around this problem is to use space provided in a disaster recovery

facility, which is basically a building, maintained by a third-party company, in which various businesses rent space. Space is usually apportioned according to how much each company pays.

Sitting between the hot and cold recovery sites is the warm site. A warm site typically has computers but is not configured ready to go. This means that data might need to be upgraded or other manual interventions might need to be performed before the network is again operational. The time it takes to get a warm site operational lands right in the middle of the other two options, as does the cost.

**ExamAlert**

A hot site mirrors the organization's production network and can assume network operations at a moment's notice. Warm sites have the equipment needed to bring the network to an operational state but require configuration and potential database updates. A cold site has the space available with basic services but typically requires equipment delivery.

One of the newer types of sites being marketed is a *cloud site*. Similar to a warm site, a cloud site is available when needed. The difference between the cloud site and the warm site is that the warm site is often dedicated to the company while a cloud site is controlled by a provider who may market availability of it to many different companies (like an insurance policy) knowing that the odds are good that only one will need it at a time.

# High Availability and Recovery Concepts

Critical business functions refer to those processes or systems that must be made operational immediately when an outage occurs. The business can't function without them, and many are information intensive and require access to both technology and data. When you evaluate your business's sustainability, realize that disasters do indeed happen. If possible, build infrastructures that don't have a *single point of failure (SPOF)* or connection. If you're the administrator for a small company, it is not uncommon for the SPOF to be a router/gateway, but you must identify all *critical nodes* and *critical assets*. The best way to remove an SPOF from your environment is to add in redundancy.

Know that every piece of equipment can be rated in terms of mean time between failures (MTBF) and mean time to recovery (MTTR). The MTBF is the measurement of the anticipated or predicted incidence of failure of a system or component between inherent failures, whereas the MTTR is the measurement of how long it takes to repair a system or component after a failure occurs.

The *recovery time objective (RTO)* is the maximum amount of time that a process or service is allowed to be down and the consequences still considered acceptable. Beyond this time, the break in business continuity is considered to affect the business negatively. The *recovery point objective (RPO)* is the maximum time in which transactions could be lost from a major incident—how much you are willing to walk away from in order to get everything up and running again. Both RTO and RPO have to be balanced in coming up with a policy for how to deal with incidents.

ExamAlert

For the exam, make sure you know the differences between MTBF, MTTR, RTO, and RPO. Know what the acronyms stand for and what they mean.

Some technologies that can help with availability are the following:

- **Fault tolerance** is the capability to withstand a fault (failure) without losing data. This can be accomplished through the use of RAID, backups, and similar technologies. Popular fault-tolerant RAID implementations include RAID 1, RAID 5, and RAID 10.
- **Load balancing** is a technique in which the workload is distributed among several servers. This feature can take networks to the next level; it increases network performance, reliability, and availability. A load balancer can be either a hardware device or software specially configured to balance the load.

ExamAlert

Remember that load balancing increases redundancy and therefore data availability. Also, load balancing increases performance by distributing the workload.

- **Multipathing** is the concept of simultaneous management and utilization of multiple available paths for the transmission of streams of data. By increasing the available paths that data can take, often by introducing redundancy, it is possible to decrease the likelihood of a path's failure bringing operations down.
- **Redundant hardware** is a key component of making sure systems have a chance of staying up in the event of a failure of any one component. Redundancy can apply to switches, routers, firewalls, and literally any other piece of hardware that network operations are dependent upon.

- **Network interface card (NIC) teaming** is the process of combining multiple network cards for performance and redundancy (fault tolerance) reasons. This can also be called bonding, balancing, or aggregation.
- **Port aggregation** is the combining of multiple ports on a switch; it can be done one of three ways: auto, desirable, or on.
- **Clustering** is a method of balancing loads and providing fault tolerance.

Use *vulnerability scanning* and *penetration testing* to find the weaknesses in your systems before others do. Make sure that *end user awareness and training* are priorities when it comes to identifying problems and that you stress *adherence to standards and policies*. Those policies should include the following:

- **Network policies:** Similar to AUPs, these policies describe acceptable uses for the network resources.
- **Security policies:** *Security policies* define what controls are required to implement and maintain the security of systems, users, and networks. These policies should be used as guides in system implementations and evaluations. One of particular note is a *consent to monitoring policy* in which employees and other network users acknowledge that they know they're being monitored and consent to it.

ExamAlert

As you study for the exam, three topics to pay attention to are adherence to standards and policies, vulnerability scanning, and penetration testing.

All these policies are important, but those that relate to first responders and deal with data breaches are of elevated importance.

# Active-Active Versus Active-Passive

When it comes to high availability, solutions fall into two types of approaches: active-active and active-passive. The difference between the two is pretty straightforward: if the devices to be used in the event of a failure are in use normally, that is *active-active* because they are both currently active. An example would be nodes in a cluster: they are all currently in use and can carry on in the event of a failure.

If, on the other hand, a device is not is use currently but becomes activated by a failure (a failover), that is *active-passive*. An example would be having multiple phone carriers or Internet service providers (ISPs) able to provide service to a

facility and using only one unless their service goes out, in which case the others are activated.

Redundancy and availability can be contracted with multiple ISPs to create diverse paths and make sure you can stay up in the event an ISP experiences a failure. You can also use redundancy with routers through the use of Virtual Router Redundancy Protocol (VRRP) and First Hop Redundancy Protocol (FHRP).

The *Virtual Router Redundancy Protocol (VRRP)* is used to automatically assign routers to hosts. It creates virtual routers (abstract representations of multiple routers) that act as a group. The default gateway on a host is configured to the virtual router rather than a physical router, and so if the physical router fails, a redundant choice is already built in to the group.

There are several *First Hop Redundancy Protocols (FHRP)*; one of the more popular is the Hot Standby Router Protocol (HSRP) that is exclusive to Cisco. All work by allowing a default router address to be configured to be used in the event that the primary router fails.

**ExamAlert**

For the exam, be able to explain the differences between VRRP and FHRP.

## Cram Quiz

1. Which two types of backup methods clear the archive bit after the backup has been completed? (Choose two.)
   - ❍ **A.** Full
   - ❍ **B.** Differential
   - ❍ **C.** Incremental
   - ❍ **D.** GFS

2. You come to work on Thursday morning to find that the server has failed and you need to restore the data from backup. You finished a full backup on Sunday and incremental backups on Monday, Tuesday, and Wednesday. How many media sets are required to restore the backup?
   - ❍ **A.** Four
   - ❍ **B.** Two
   - ❍ **C.** Three
   - ❍ **D.** Five

**3.** Which of the following recovery sites might require the delivery of computer equipment and an update of all network data?

- ❍ **A.** Cold site
- ❍ **B.** Warm site
- ❍ **C.** Hot site
- ❍ **D.** None of the above

**4.** As part of your network administrative responsibilities, you have completed your monthly backups. As part of backup best practices, where should the media be stored?

- ❍ **A.** In a secure location in the server room
- ❍ **B.** In a secure location somewhere in the building
- ❍ **C.** In an offsite location
- ❍ **D.** In a secure offsite location

**5.** As network administrator, you have been tasked with designing a disaster recovery plan for your network. Which of the following might you include in a disaster recovery plan?

- ❍ **A.** RAID 5
- ❍ **B.** Offsite media storage
- ❍ **C.** Mirrored hard disks
- ❍ **D.** UPS

**6.** Which type of recovery site mirrors the organization's production network and can assume network operations on a moment's notice?

- ❍ **A.** Warm site
- ❍ **B.** Hot site
- ❍ **C.** Cold site
- ❍ **D.** Mirrored site

**7.** Which of the following are used to find weaknesses in your systems before others do? (Choose two.)

- ❍ **A.** Data breachers
- ❍ **B.** Vulnerability scanners
- ❍ **C.** Penetration testers
- ❍ **D.** First responders

8. Which of the following is a type of policy in which employees and other network users give consent to be monitored?
   - ❍ **A.** Consent to monitoring
   - ❍ **B.** Acceptable use
   - ❍ **C.** Memorandum of understanding
   - ❍ **D.** Service-level agreement

9. Which device is fitted with multiple outputs and is specifically designed to distribute electric power?
   - ❍ **A.** Port aggregator
   - ❍ **B.** Cluster
   - ❍ **C.** RTO
   - ❍ **D.** PDU

10. Which of the following is used to automatically assign routers to hosts and creates virtual routers that act as a group?
    - ❍ **A.** VRRP
    - ❍ **B.** RAID 5
    - ❍ **C.** RAID 10
    - ❍ **D.** NIC teaming

# Cram Quiz Answers

1. **A and C.** The archive bit is reset after a full backup and an incremental backup. Answer B is incorrect because the differential backup does not reset the archive bit. Answer D is wrong because GFS is a rotation strategy, not a backup method.
2. **A.** Incremental backups save all files and directories that have changed since the last full or incremental backup. To restore, you need the latest full backup and all incremental media sets. In this case, you need four sets of media to complete the restore process.
3. **A.** A cold site provides an alternative location but typically not much more. A cold site often requires the delivery of computer equipment and other services. A hot site has all network equipment ready to go if a massive failure occurs. A warm site has most equipment ready but still needs days or weeks to have the network up and running.
4. **D.** Although not always done, it is a best practice to store backups in a secure offsite location in case of fire or theft. Answer A is incorrect because if the server room is damaged by fire or flood, the backups and the data on the server can be compromised by the same disaster. Similarly, answer B is incorrect because storing the backups onsite does not eliminate the threat of a single disaster destroying the data on the server and backups. Answer C is incorrect because of security reasons. The offsite media sets must be secured.

5. **B.** Offsite storage is part of a disaster recovery plan. The other answers are considered fault-tolerance measures because they are implemented to ensure data availability.
6. **B.** A hot site mirrors the organization's production network and can assume network operations at a moment's notice. Answer A is incorrect because warm sites have the equipment needed to bring the network to an operational state but require configuration and potential database updates. Answer C is incorrect because cold sites have the space available with basic services but typically require equipment delivery. Answer D is incorrect because a mirrored site is not a valid option.
7. **B and C.** Use vulnerability scanning and penetration testing to find the weaknesses in your systems before others do. Answer A is incorrect because data breaches are invalid. Answer D is incorrect because first responders are typically those who are first on the scene after an incident.
8. **A.** A consent to monitoring policy is one in which employees and other network users acknowledge that they know they're being monitored and consent to it. Answer B is incorrect because acceptable use policies describe how the employees in an organization can use company systems and resources. Answers C and D are incorrect because a memorandum of understanding and service-level agreements are standard business documents.
9. **D.** A device fitted with multiple outputs that is specifically designed to distribute electric power is known as a power distribution unit (PDU), and these devices are often plentiful in datacenters for suppling power to racks. Port aggregation is the combining of multiple ports on a switch; it can be done one of three ways: auto, desirable, or on. Clustering is a method of balancing loads and providing fault tolerance. The recovery time objective (RTO) is the maximum amount of time that a process or service is allowed to be down and the consequences still considered acceptable.
10. **A.** The Virtual Router Redundancy Protocol (VRRP) is used to automatically assign routers to hosts. It creates virtual routers (abstract representations of multiple routers) that act as a group. Popular fault-tolerant RAID implementations include RAID 1, RAID 5, and RAID 10. NIC teaming is the process of combining multiple network cards for performance and redundancy (fault tolerance) reasons.

# Monitoring Network Performance

- **Given a scenario, use the appropriate statistics and sensors to ensure network availability.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What can be used to capture network data?
2. True or false: Port scanners detect open and often unsecured ports.
3. True or false: Interface monitoring tools can be used to create "heat maps" showing the quantity and quality of wireless network coverage in areas.
4. True or false: Always test updates on a lab machine before rolling out on production machines.
5. What is it known as when you roll a system back to a previous version of a driver or firmware?

### Answers

1. Packet sniffers can be used by both administrators and hackers to capture network data.
2. True. Port scanners detect open and often unsecured ports.
3. False. Wireless survey tools can be used to create heat maps showing the quantity and quality of wireless network coverage in areas.
4. True. Always test updates on a lab machine before rolling out on production machines.
5. Rolling a system back to a previous version is known as *downgrading* and is often necessary when dealing with legacy systems and implementations.

### ExamAlert

Remember that this objective begins with "Given a scenario." This means that you may receive a drag and drop, matching, or "live OS" scenario where you have to click through to complete a specific objective-based task.

When networks were smaller and few stretched beyond the confines of a single location, network management was a simple task. In today's complex, multisite, hybrid networks, however, the task of maintaining and monitoring network devices and servers has become a complicated but essential part of the network administrator's role. Nowadays, the role of network administrator often stretches beyond the physical boundary of the server room and reaches every node and component on the network. Whether an organization has 10 computers on a single segment or a multisite network with several thousand devices attached, the network administrator must monitor all network devices, protocols, and usage—preferably from a central location.

Given the sheer number and diversity of possible devices, software, and systems on any network, it is clear why network management is such a significant consideration. Although a robust network management strategy can improve administrator productivity, increase *uptime*, and reduce *downtime*, many companies choose to neglect network management because of the time involved in setting up the system or because of the associated costs. If these companies understood the potential savings, they would realize that neglecting network management provides false economies.

Network management and network monitoring are essentially methods to control, configure, and monitor devices on a network. Imagine a scenario in which you are a network administrator working out of your main office in Spokane, Washington, and you have satellite offices in New York, Dallas, Vancouver, and London. Network management allows you to access systems in the remote locations or have the systems notify you when something goes awry. In essence, network management is about seeing beyond your current boundaries and acting on what you see.

Network management is not one thing. Rather, it is a collection of tools, systems, and protocols that, when used together, enables you to perform tasks such as reconfiguring a network card in the next room or installing an application in the next state.

# Common Performance Metrics

The capabilities demanded from network management vary somewhat among organizations, but essentially, several key types of information and functionality are required, such as fault detection and performance monitoring. Some of the

types of information and functions that network management tools can provide include the following:

- **Temperature:** You should make certain that devices are running within the acceptable range. Usually, the biggest problem is heat, so you need to get rid of it to keep systems from overheating or encountering chip creep.
- **Utilization:** Once upon a time, it was not uncommon for a network to have to limp by with scarce resources. Administrators would constantly have to trim logs and archive files to keep enough storage space available to service print jobs. Those days are gone, and any such hint of those conditions would be unacceptable today. For you to keep this from happening, one of the keys is to manage utilization and stay on top of problems before they escalate. Several areas of utilization to monitor are as follows:
  - **Bandwidth/throughput:** There must be enough bandwidth to serve all users, and you need to be alert for bandwidth hogs. You want to look for top talkers (those that transmit the most) and top listeners (those that receive the most) and figure out why they are so popular. *NetFlow data* can be used to ascertain this information and allow you to decide how to best respond. NetFlow is a network protocol analyzer developed by Cisco.
  - **Storage space:** Free space needs to be available for all users, and quotas may need to be implemented.
  - **Network device CPU:** Just as a local machine will slow when the processor is maxed out, so will the network.
  - **Network device memory:** It is next to impossible to have too much memory. You should balance loads to optimize the resources you have to work with.
  - **Wireless channel utilization:** Akin to bandwidth utilization is channel utilization in the wireless realm. As a general rule, a wireless network starts experiencing performance problems when channel utilization reaches 50 percent of the channel capacity.
- **Latency:** One of the biggest problems with satellite access is trouble with latency (the time lapse between sending or requesting information and the time it takes to return). Satellite communication experiences high latency due to the distance it has to travel as well as weather conditions. While latency is not restricted solely to satellites, it is one of the easiest forms of transmission to associate with it. In reality, latency can occur with almost any form of transmission.

- **Jitter:** Closely tied to latency, jitter differs in that the length of the delay between received packets differs. While the sender continues to transmit packets in a continuous stream and space them evenly apart, the delay between packets received varies instead of remaining constant. This issue can be caused by network congestion, improper queuing, or configuration errors.
- **Fault detection:** One of the most vital aspects of network management is knowing if anything is not working or is not working correctly. Network management tools can detect and report on a variety of faults on the network. Given the number of possible devices that constitute a typical network, determining faults without these tools could be an impossible task. In addition, network management tools might not only detect the faulty device but also shut it down. This means that if a network card is malfunctioning, you can remotely disable it. When a network spans a large area, fault detection becomes even more invaluable because it enables you to be alerted to network faults and to manage them, thereby reducing downtime.

ExamAlert

Most of this discussion involves your being alerted to some condition. Those alerts can generally be sent to you through email or Short Message Service (SMS) to any mobile device.

- **Performance monitoring:** Another feature of network management is the ability to monitor network performance. Performance monitoring is an essential consideration that gives you some crucial information. Specifically, performance monitoring can provide network usage statistics and user usage trends. This type of information is essential when you plan network capacity and growth. Monitoring performance also helps you determine whether there are any performance-related concerns, such as whether the network can adequately support the current user base.
- **Security monitoring:** Good server administrators have a touch of paranoia built in to their personality. A network management system enables you to monitor who is on the network, what they are doing, and how long they have been doing it. More important, in an environment in which corporate networks are increasingly exposed to outside sources, the ability to identify and react to potential security threats is a priority. Reading log files to learn of an attack is a poor second to knowing that an attack is in progress and being able to react accordingly. One thing to look for is changes in raw data values; these changes can be identified through comparisons of *cyclic redundancy check (CRC)* values. Look for CRC errors, as

well as *giants* (packets that are discarded because they exceed the medium's maximum packet size), *runts* (packets that are discarded because they are smaller than the medium's minimum packet size), and *encapsulation errors*.

- **Link state status:** You should regularly monitor link status to make sure that connections are up and functioning (or down, if expected to be). Breaks should be found and identified as quickly as possible to repair them or find workarounds. A number of link status monitors exist for the purpose of monitoring connectivity, and many can reroute (per a configured script file) when a down condition occurs.
- **Interface monitoring:** Just as you want to monitor for a link going down, you also need to know when an interface has problems. Particular problems to watch for include errors, utilization problems (unusually high, for example), discards, packet drops, resets, and problems with speed/duplex. An *interface monitoring tool* is invaluable for troubleshooting problems here.
- **Maintenance and configuration:** Want to reconfigure or shut down the server located in Australia? Reconfigure a local router? Change the settings on a client system? Remote management and configuration are key parts of the network management strategy, enabling you to centrally manage huge multisite locations.
- **Environmental monitoring:** It is important to monitor the server room, and other key equipment, for temperature and humidity conditions. Humidity control prevents the buildup of static electricity and reduces the chances of electronic components becoming vulnerable to damage from electrostatic shock; not only can very low humidity lead to increased static electricity, but it can also contribute to health problems, such as skin irritation. *Environmental monitoring tools* can alert you to any dangers that arise here. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommends that relative humidity be maintained below 60 percent and the relative humidity should be greater than 30 percent.

ExamAlert

For the exam, recognize the role humidity plays in controlling electrostatic shock.

- **Power monitoring:** A consistent flow of reliable energy is needed to keep a network up and running. A wide array of *power monitoring tools* are available to help identify and log problems that you can then begin to resolve.

- **Wireless monitoring:** As more networks go wireless, you need to pay special attention to issues associated with them. *Wireless survey tools* can be used to create heat maps showing the quantity and quality of wireless network coverage in areas. They can also allow you to see access points (including rogues) and security settings. These can be used to help you design and deploy an efficient network, and they can also be used (by you or others) to find weaknesses in your existing network (often marketed for this purpose as *wireless analyzers*).

Many tools are available to help monitor the network and ensure that it is properly functioning. Some tools, such as a packet sniffer, can be used to monitor traffic by administrators and those who want to obtain data that does not belong to them. The following sections look at several monitoring tools.

# SNMP Monitors

An SNMP management system is a computer running a special piece of software called a *network management system (NMS)*. These software applications can be free, or they can cost thousands of dollars. The difference between the free applications and those that cost a great deal of money normally boils down to functionality and support. All NMS applications, regardless of cost, offer the same basic functionality. Today, most NMS applications use graphical maps of the network to locate a device and then query it. The queries are built into the application and are triggered by pointing and clicking. You can actually issue SNMP requests from a command-line utility, but with so many tools available, this is unnecessary.

> **Note**
>
> Some people call SNMP managers or NMSs *trap managers*. This reference is misleading, however, because an NMS can do more than just accept trap messages from agents.

Using SNMP and an NMS, you can monitor all the devices on a network, including switches, hubs, routers, servers, and printers, as well as any device that supports SNMP, from a single location. Using SNMP, you can see the amount of free disk space on a server in Jakarta or reset the interface on a router in Helsinki—all from the comfort of your desk in San Jose. Such power, though, brings with it some considerations. For example, because an NMS

enables you to reconfigure network devices, or at least get information from them, it is common practice to implement an NMS on a secure workstation platform, such as a Linux or Windows server, and to place the NMS PC in a secure location.

## Management Information Base (MIB)

SNMP uses databases of information called MIBs to define what parameters are accessible, which of the parameters are read-only, and which can be set. MIBs are available for thousands of devices and services, covering every imaginable need. *Object identifiers (OIDs)* uniquely identify managed objects within an MIB hierarchy. Quite simply, an OID is an address used to identify each node in a tree structure. The addresses are integers separated by periods, corresponding to the path from the root through the series of ancestor nodes, to the node. Each node in the tree is controlled by an assigning authority who can create child nodes and delegate assigning authority for the child nodes.

To ensure that SNMP systems offer cross-platform compatibility, MIB creation is controlled by the *International Organization for Standardization (ISO)*. An organization that wants to create MIBs can apply to the ISO. The ISO then assigns the organization an ID under which it can create MIBs as it sees fit. The assignment of numbers is structured within a conceptual model called the *hierarchical name tree*.

**ExamAlert**

When studying for the Network+ exam, be sure that you know SNMP and its use of traps, object identifiers (OIDs), and management information bases (MIBs).

# Network Performance, Load, and Stress Testing

To test the network, administrators often perform three distinct types of tests:

- Performance tests
- Load tests
- Stress tests

These test names are sometimes used interchangeably. Although some overlap exists, they are different types of network tests, each with different goals.

## Performance Tests

A *performance test* is, as the name suggests, all about measuring the network's current performance level. The goal is to take ongoing performance tests and evaluate and compare them, looking for potential bottlenecks. For performance tests to be effective, they need to be taken under the same type of network load each time, or the comparison is invalid. For example, a performance test taken at 3 a.m. will differ from one taken at 3 p.m.

> **Note**
>
> The goal of performance testing is to establish baselines for the comparison of network functioning. The results of a performance test are meaningless unless you can compare them to previously documented performance levels.

## Load Tests and Send/Receive Traffic

Load testing has some overlap with performance testing. Sometimes called *volume* or *endurance testing*, load tests involve artificially placing the network under a larger workload. For example, the network traffic might be increased throughout the entire network. After this is done, performance tests can be done on the network with the increased load. Load testing is sometimes done to see if bugs exist in the network that are not currently visible but that may become a problem as the network grows. For example, the mail server might work fine with current requirements. However, if the number of users in the network grew by 10 percent, you would want to determine whether the increased load would cause problems with the mail server. Load tests are all about finding a potential problem before it happens.

Performance tests and load tests are actually quite similar; however, the information outcomes are different. Performance tests identify the current level of network functioning for measurement and benchmarking purposes. Load tests are designed to give administrators a look into the future of their network load and to see whether the current network infrastructure can handle it.

> **Note**
>
> Performance tests are about network functioning today. Load tests look forward to see whether performance may be hindered in the future by growth or other changes to the network.

## Stress Tests

Whereas load tests do not try to break the system under intense pressure, stress tests sometimes do. They push resources to the limit. Although these tests are not done often, they are necessary and—for administrators, at least—entertaining. Stress testing has two clear goals:

- It shows you exactly what the network can handle. Knowing a network's breaking point is useful information when you consider network expansion.
- It enables you to test your backup and recovery procedures. If a test knocks out network resources, you can verify that your recovery procedures work. Stress testing enables you to observe network hardware failure.

Stress tests assume that someday something will go wrong, and you will know exactly what to do when it happens.

## Performance Metrics

Whether the testing being done is related to performance, load, or stress, you have to choose the metrics you want to monitor and focus on. Although a plethora of options are available, the most common four are the following:

- **Error rate:** This metric identifies the frequency of errors.
- **Utilization:** This metric shows the percentage of resources being utilized.
- **Packet drops:** This metric shows how many packets of data on the network fail to reach their destination.
- **Bandwidth/throughput:** This metric involves the capability to move data through a channel as related to the total capability of the system to identify bottlenecks, throttling, and other issues.

# Network Device Logs

In a network environment, all NOSs and most firewalls, proxy servers, and other network components have logging features. These logging features are essential for network administrators to review and monitor. Many types of logs can be used. The following sections review some of the most common log file types.

On a Windows Server system, as with the other operating systems, events and occurrences are logged to files for later review. Windows Server and desktop systems use Event Viewer to view many of the key log files. The logs in Event Viewer can be used to find information on, for example, an error on the system or a security incident. Information is recorded into key log files; however, you will also see additional log files under certain conditions, such as if the system is a domain controller or is running a DHCP server application.

Event logs refer generically to all log files used to track events on a system. Event logs are crucial for finding intrusions and diagnosing current system problems. In a Windows environment, for example, three primary event logs are used: security, application, and system.

> **Note**
>
> Be sure that you know the types of information included in the types of log files.

## Security Logs

A system's security log contains events related to security incidents, such as successful and unsuccessful logon attempts and failed resource access. Security logs can be customized, meaning that administrators can fine-tune exactly what they want to monitor. Some administrators choose to track nearly every security event on the system. Although this might be prudent, it can often create huge log files that take up too much space. Figure 8.6 shows a security log from a Windows system.

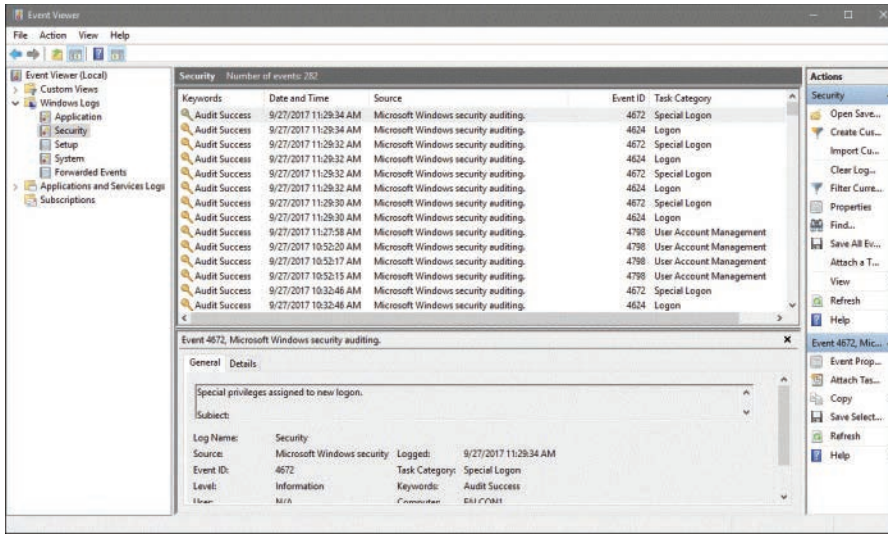



FIGURE 8.6 **A Windows security log from Windows 10**

Figure 8.6 shows that some successful logons and account changes have occurred. A potential security breach would show some audit failures for logon or logoff attempts. To save space and prevent the log files from growing too big, administrators might choose to audit only failed logon attempts and not successful ones.

Each event in a security log contains additional information to make it easy to get the details on the event:

- **Date:** The exact date the security event occurred.
- **Time:** The time the event occurred.
- **User:** The name of the user account that was tracked during the event.
- **Computer:** The name of the computer used when the event occurred.
- **Event ID:** The event ID telling you what event has occurred. You can use this ID to obtain additional information about the particular event. For example, you can take the ID number, enter it at the Microsoft support website, and gather information about the event. Without the ID, it would be difficult to find this information.

To be effective, security logs should be regularly reviewed.

# Application Log

An application log contains information logged by applications that run on a particular system rather than the operating system itself. Vendors of third-party applications can use the application log as a destination for error messages generated by their applications.

The application log works in much the same way as the security log. It tracks both successful events and failed events within applications. Figure 8.7 shows the details provided in an application log.

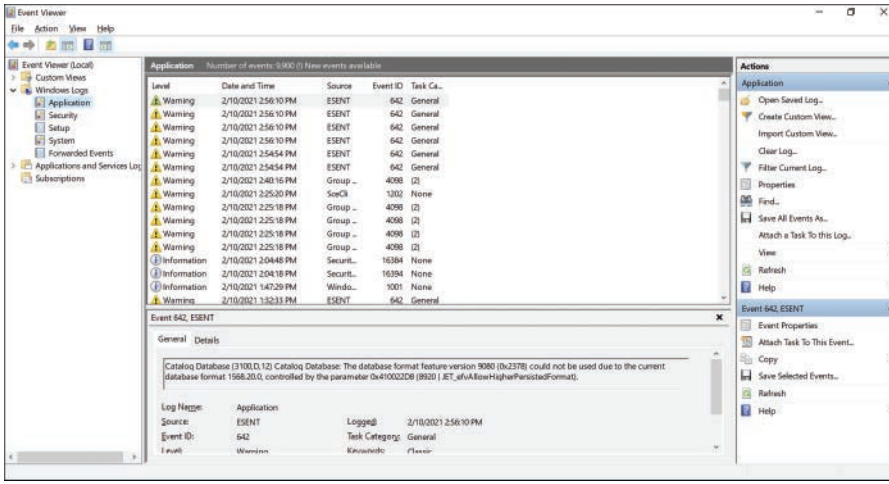



FIGURE 8.7 **An application log in Windows 10**

Figure 8.7 shows that two types of events occurred: general application information events and warning event events. Vigilant administrators would likely want to check the event ID of both the event and warning failures to isolate the cause.

# System Logs

System logs record information about components or drivers in the system, as shown in Figure 8.8. This is the place to look when you are troubleshooting a problem with a hardware device on your system or a problem with network connectivity. For example, messages related to the client element of *Dynamic Host Configuration Protocol (DHCP)* appear in this log. The system log is also the place to look for hardware device errors, time synchronization issues, or service startup problems.

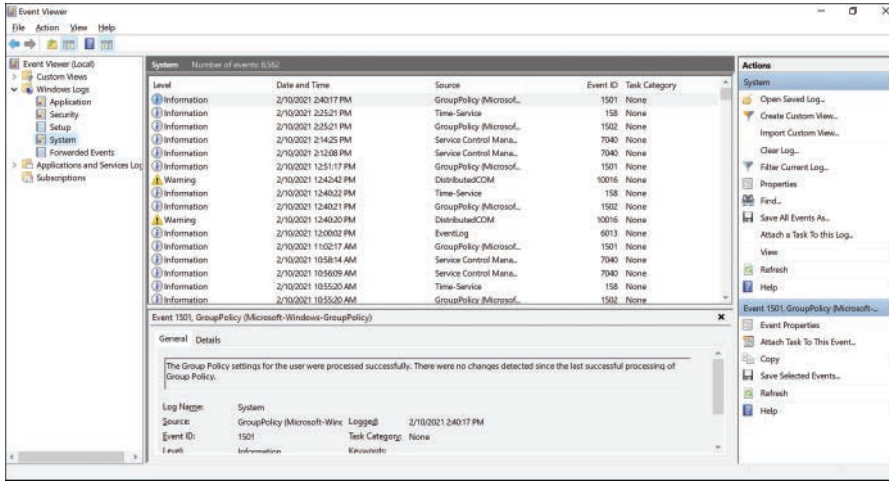



FIGURE 8.8 **A system log in Windows 10**

## History Logs

History logs are most often associated with the tracking of Internet surfing habits. They maintain a record of all sites that a user visits. Network administrators might review these for potential security or policy breaches, but generally these are not commonly reviewed.

Another form of history log is a compilation of events from other log files. For instance, one history log might contain all significant events over the past year from the security log on a server. History logs are critical because they provide a detailed account of alarm events that can be used to track trends and locate problem areas in the network. This information can help you revise maintenance schedules, determine equipment replacement plans, and anticipate and prevent future problems.

> **Note**
>
> Application logs and system logs can often be viewed by any user. Security logs can be viewed only by users who use accounts with administrative privileges.

## Log Management

In a discussion of these logs, it becomes clear that monitoring them can be a huge issue. That is where *log management (LM)* comes in. LM describes the process of managing large volumes of system-generated computer log files.

LM includes the collection, retention, and disposal of all system logs. Although LM can be a huge task, it is essential to ensure the proper functioning of the network and its applications. It also helps you keep an eye on network and system security.

Configuring systems to log all sorts of events is the easy part. Trying to find the time to review the logs is an entirely different matter. To assist with this process, third-party software packages are available to help with the organization and reviewing of log files. To find this type of software, you can enter **log management** into a web browser, and you will have many options to choose from. Some have trial versions of their software that may give you a better idea of how LM works.

*Syslog* is a message logging standard that has been around for many years. The tool used for creating log entries in UNIX/Linux-based systems is conveniently named syslog, but other tools can also be used. Syslog allows separation between three entities: the software that generates the message, the system that stores it, and the software used to analyze or report it. Every message is labeled with identifiers such as a code indicating the software type generating the message and a severity level. A severity level of 0 is an emergency, 1 is an alert, 2 is critical, 3 is error, 4 is warning, 5 is a notice, 6 is information only, and 7 is for debugging.

## Patch Management

All applications, including productivity software, virus checkers, and especially the operating system, release patches and updates often designed to address potential security weaknesses. Administrators must keep an eye out for these patches and install them when they are released.

> **Note**
>
> The various types of updates discussed in this section apply to all systems and devices, including mobile devices and laptops, as well as servers and routers. Special server systems (and services) are typically used to deploy mass updates to clients in a large enterprise network.

Discussion items related to this topic include the following:

- **OS updates:** Most operating system updates relate to either functionality or security issues. For this reason, it is important to keep your systems up to date. Most current operating systems include the capability to automatically find updates and install them. By default, the automatic updates feature is usually turned on; you can change the settings if you do not want this enabled.

**Note**

Always test updates on a lab machine before rolling out on production machines.

- **Firmware updates:** Firmware updates keep the hardware interfaces working properly. Router manufacturers, for example, often issue patches when problems are discovered. Those patches need to be applied to the router to remove any security gaps that may exist. Figure 8.9 shows an example of checking a router's firmware.

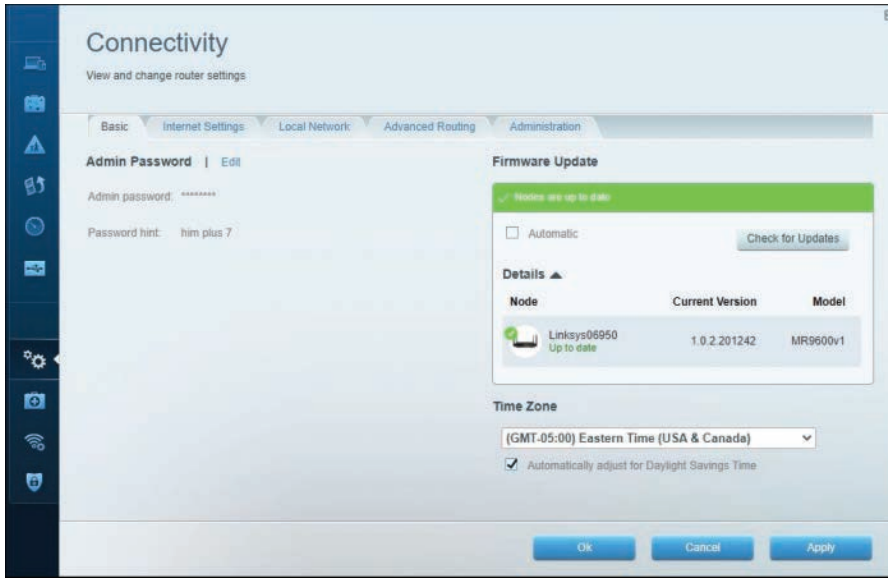



FIGURE 8.9 **Checking a router's firmware**

**ExamAlert**

Just as security holes can exist with operating systems and applications (and get closed through patches), they can also exist in firmware and be closed through updates.

- **Driver updates:** The main reason for updating drivers is that you have a piece of hardware that is not operating correctly. The failure to operate can be caused by the hardware interacting with software it was not intended to prior to shipping (such as OS updates). Because the problem can be from the vendor or the OS provider, updates can be automatically included (such as with Windows Update) or found on the vendor's site.

- **Feature changes/updates:** Not considered as critical as security or functionality updates, feature updates and changes can extend what you could previously do and extend your time using the hardware/software combination you have.
- **Major versus minor updates:** Most updates are classified as major (*must* be done) or minor (*can* be done). Depending on the vendor, the difference in the two may be telegraphed in the numbering: an update of 4.0.0 would be a major update, whereas one of 4.10.357 would be considered a minor one.

**ExamAlert**

As a general rule, the smaller the number of the update, the less significant it is.

- **Vulnerability patches:** Vulnerabilities are weaknesses, and patches related to them should be installed correctly with all expediency. After a vulnerability in an OS, a driver, or a piece of hardware has been identified, the fact that it can be exploited is often spread quickly: a *zero-day exploit* is any attack that begins the very day the vulnerability is discovered.

**Note**

If attackers learn of the weakness the same day as the developer, they have the ability to exploit it until a patch is released. Often, the only thing that you as a security administrator can do between the discovery of the exploit and the release of the patch is to turn off the system. Although this approach can be a costly undertaking in terms of productivity, it can be the only way to keep the network safe.

- **Upgrading versus downgrading:** Not all changes need to be upgraded. If, for example, a newly applied patch changes the functionality of a hardware component to the point that it will no longer operate as you need it to, you can consider reverting back to a previous state. This approach is known as *downgrading* and is often necessary when dealing with legacy systems and implementations.

**ExamAlert**

For the exam, know that removing patches and updates is considered downgrading.

Before you install or remove patches, it is important to do a *configuration backup*. Many vendors offer products that perform configuration backups across the network on a regular basis and allow you to roll back changes if needed. Free tools are often limited in the number of devices they can work with, and some of the more expensive ones include the capability to automatically analyze and identify the changes that could be causing any problems.

## Environmental Factors

Environmental concerns include considerations about temperature, humidity, electrical, and water/flood risks. Computer rooms should have fire and moisture detectors. Most office buildings have water pipes and other moisture-carrying systems in the ceiling. If a water pipe bursts (which is common in minor earthquakes), the computer room could become flooded. Water and electricity don't mix. Moisture monitors would automatically kill power in a computer room if moisture were detected, so the security professional should know where the water cut-offs are located.

Many computer systems require temperature and humidity control for reliable service. Large servers, communications equipment, and drive arrays generate considerable amounts of heat. An environmental system for this type of equipment is a significant expense beyond the actual computer system costs.

Humidity control prevents the buildup of static electricity in the environment. If the humidity drops too low, electronic components are extremely vulnerable to damage from electrostatic shock. Most environmental systems also regulate humidity; however, a malfunctioning system can cause the humidity to be almost entirely extracted from a room. Make sure that environmental systems are regularly serviced.

## Cram Quiz

1. Which of the following involves pushing the network beyond its limits, often taking down the network to test its limits and recovery procedures?

   - ❍ **A.** Crash and burn
   - ❍ **B.** Stress test
   - ❍ **C.** Recovery test
   - ❍ **D.** Load test

**2.** You suspect that an intruder has gained access to your network. You want to see how many failed logon attempts were made in one day to help determine how the person got in. Which of the following might you do?

- ❍ **A.** Review the history logs.
- ❍ **B.** Review the security logs.
- ❍ **C.** Review the logon logs.
- ❍ **D.** Review the performance logs.

**3.** Which utility can be used to write syslog entries on a Linux-based operating system?

- ❍ **A.** memo
- ❍ **B.** record
- ❍ **C.** logger
- ❍ **D.** trace

**4.** Which of the following is not a standard component of an entry in a Windows-based security log?

- ❍ **A.** Event ID
- ❍ **B.** Date
- ❍ **C.** Computer
- ❍ **D.** Domain
- ❍ **E.** User

**5.** You have just used a port scanner for the first time. On one port, it reports that there is not a process listening, and access to this port will likely be denied. Which state is the port most likely to be considered to be in?

- ❍ **A.** Listening
- ❍ **B.** Closed
- ❍ **C.** Filtered
- ❍ **D.** Blocked

**6.** You are required to monitor discards, packet drops, resets, and problems with speed/duplex. Which of the following monitoring tools would assist you?

- ❍ **A.** Interface
- ❍ **B.** Power
- ❍ **C.** Environmental
- ❍ **D.** Application

7. By default, the automatic update feature on most modern operating systems is
   - ❍ **A.** Disabled
   - ❍ **B.** Turned on
   - ❍ **C.** Set to manual
   - ❍ **D.** Ineffective

8. What should you do if a weakness is discovered that affects network security, and no patch has yet been released?
   - ❍ **A.** Post information about the weakness on the vendor's site.
   - ❍ **B.** Call the press to put pressure on the vendor.
   - ❍ **C.** Ignore the problem and wait for the patch.
   - ❍ **D.** Take the at-risk system offline.

# Cram Quiz Answers

1. **B.** Whereas load tests do not try to break the system under intense pressure, stress tests sometimes do. Stress testing has two goals. The first is to see exactly what the network can handle. It is useful to know the network's breaking point in case the network ever needs to be expanded. Second, stress testing allows you to test your backup and recovery procedures.
2. **B.** The security logs can be configured to show failed or successful logon attempts as well as object access attempts. In this case, you can review the security logs and failed logon attempts to get the desired information. The failed logons will show the date and time when the failed attempts occurred.
3. **C.** The syslog feature exists in most UNIX/Linux-based distributions, and entries can be written using logger. The other options are not possibilities for writing syslog entries.
4. **D.** The standard components of an entry in a Windows-based security log include the date, time, user, computer, and event ID. The domain is not a standard component of a log entry.
5. **B.** When a port is closed, no process is listening on that port, and access to this port will likely be denied. When the port is open/listening, the host sends a reply indicating that a service is listening on the port. When the port is filtered or blocked, there is no reply from the host, meaning that the port is not listening or the port is secured and filtered.
6. **A.** An interface monitoring tool is invaluable for troubleshooting problems and errors that include utilization problems, discards, packet drops, resets, and problems with speed/duplex.
7. **B.** By default, the automatic update feature is usually turned on.
8. **D.** Often, the only thing that you, as a security administrator, can do between the discovery of the exploit and the release of the patch is to turn off the service. Although this approach can be a costly undertaking in terms of productivity, it can be the only way to keep the network safe.

# What's Next?

The primary goals of today's network administrators are to design, implement, and maintain secure networks. These tasks are not always easy, so they are the topic of Chapter 9, "Network Security." No network can ever be labeled "secure." Security is an ongoing process involving a myriad of protocols, procedures, and practices.

CHAPTER 9

# Network Security

**This chapter covers the following official Network+ objectives:**

- Explain common security concepts.
- Compare and contrast common types of attacks.
- Given a scenario, apply network hardening techniques.
- Compare and contrast remote-access methods and security implications.
- Explain the importance of physical security.

This chapter covers CompTIA Network+ objectives 4.1, 4.2, 4.3, 4.4, and 4.5. For more information on the official Network+ exam topics, see the "About the Network+ Exam" section in the Introduction.

Network security is one of the toughest areas of IT to be responsible for. It seems as if a new threat surfaces on a regular basis and that you are constantly needing to learn new things just a half a step ahead of potential problems. This chapter focuses on some of the elements administrators and technicians use to keep their networks as secure as possible.

# Common Security Concepts

▶ **Explain common security concepts.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. True or false: Filtering network traffic using a system's MAC address typically is done using an ACL.
2. True or false: LDAP is a protocol that provides a mechanism to access and query directory services systems.
3. Which access control model uses an access control list (ACL) to determine access?
4. True or false: A honeypot is a trap that allows the intruder in but does not allow access to sensitive data.
5. Which IEEE standard defines port-based security for wireless network access control?
6. What enables a user to log in to a system and access multiple systems or resources without the need to repeatedly reenter the username and password?

### Answers

1. True. Filtering network traffic using a system's MAC address typically is done using an access control list (ACL).
2. True. LDAP (Lightweight Directory Access Protocol) is a protocol that provides a mechanism to access and query directory services systems.
3. Discretionary access control (DAC) uses an access control list (ACL) to determine access. The ACL is a table that informs the operating system of the rights each user has to a particular system object, such as a file, a folder, or a printer.
4. True. A honeypot is a trap that allows the intruder in but does not allow access to sensitive data.
5. The IEEE 802.1X standard defines port-based security for wireless network access control.
6. Single sign-on (SSO) enables a user to log in to a system and access multiple systems or resources without the need to repeatedly reenter the username and password.

There are three concepts you will see throughout this chapter and probably implied in every security-related book you will ever read: *confidentiality*, *integrity*, *and availability*, often referred to as the *CIA* triad of security. All security measures should affect one or more of these areas. Confidentiality means preventing unauthorized users from accessing data: passwords, encryption, and access control all support confidentiality. Integrity means ensuring that data has not been altered: hashing and message authentication codes are the most common methods of accomplishing this task (as well as ensuring nonrepudiation with digital signatures). Simply making sure that the data and systems are available for authorized users is what availability is all about: data backups, redundant systems, and disaster recovery plans all support fault tolerance and increased availability.

Threats can come from anywhere. They can include *external* entities such as bored individuals wanting to inflict harm to any system they can find access to and yours just happened to let them in, or *internal* entities such as disgruntled employees unhappy they were passed over for a promotion and feeling as if they have a right to cause harm. Often, the internal threats are the hardest to prevent since these users are already granted access to some resources and have an advantage over those outside the organization.

*Vulnerabilities* are discovered on a regular basis and, as an administrator, you must stay current on information related to discovered problems and be aware of *common vulnerabilities and exposures (CVEs)*: a list of publicly available security flaws that you should be familiar with as an administrator (see https://cve.mitre.org/). When a hole is found in a web browser or other software, and miscreants begin exploiting it the very day it is discovered by the developer (bypassing the one- to two-day response time many software providers need to put out a patch after the hole has been found), it is known as an *exploit attack* or *zero-day attack*. Zero-day attacks are incredibly difficult to respond to. If attackers learn of the weakness the same day as the developer, they have the ability to exploit it until a patch is released. Often, the only thing you, as a security administrator, can do between the discovery of the exploit and the release of the patch is to turn off the service. Although this approach can be a costly undertaking in terms of productivity, it is the only way to keep the network safe.

**ExamAlert**

Be ready to identify types of attacks and common vulnerabilities and exposures (CVEs) such as the one just described. You can expect questions about these types of attacks on the Network+ exam.

# Access Control

*Access control* describes the mechanisms used to filter network traffic to determine who is and who is not allowed to access the network and network resources. Firewalls, proxy servers, routers, and individual computers all can maintain access control to some degree by protecting the *edges* of the network. Because the security strategy limits who can and cannot access the network and its resources, it is easy to understand why access control plays a critical role. Several types of access control strategies exist, as discussed in the following sections.

**ExamAlert**

Be sure that you can identify the purpose and types of access control.

# Mandatory Access Control

Mandatory access control (MAC) is the most secure form of access control. In systems configured to use mandatory access control, administrators dictate who can access and modify data, systems, and resources. MAC systems are commonly used in military installations, financial institutions, and, because of new privacy laws, medical institutions.

MAC secures information and resources by assigning sensitivity labels or attributes to objects and users. When users request access to an object, their sensitivity level is compared to the object's. A label is a feature applied to files, directories, and other resources in the system. It is similar to a confidentiality stamp. When a label is placed on a file, it describes the level of security for that specific file. It permits access by files, users, programs, and so on that have a similar or higher security setting.

# Discretionary Access Control

Unlike mandatory access control, discretionary access control (DAC) is not enforced from the administrator or operating system. Instead, access is controlled by an object's owner. For example, if a secretary creates a folder, he decides who will have access to that folder. This access is configured using permissions and an access control list (ACL).

DAC uses an ACL to determine access. The ACL is a table that informs the operating system of the rights each user has to a particular system object, such

as a file, a folder, or a printer. Each object has a security attribute that identifies its ACL. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a folder), to write to the file or files, and to execute the file (if it is an executable file or program).

Microsoft Windows servers/clients, Linux, UNIX, and macOS are among the operating systems that use ACLs. The list is implemented differently by each operating system.

In Windows Server products, an ACL is associated with each system object. Each ACL has one or more *access control entries (ACEs)* consisting of the name of a user or group of users. The user can also be a role name, such as "secretary" or "research." For each of these users, groups, or roles, the access privileges are stated in a string of bits called an access mask. Generally, the system administrator or the object owner creates the ACL for an object.

> **Note**
>
> A server on a network that has the responsibility of being a repository for accounts (user/computer) is often referred to as a *network controller*. A good example is a domain controller on a Microsoft Active Directory–based network.

# Rule-Based Access Control

Rule-based access control (RBAC) controls access to objects according to established rules. The configuration and security settings established on a router or firewall are a good example.

When a firewall is configured, rules are set up to control access to the network. Requests are reviewed to see if the requestor meets the criteria to be allowed access through the firewall. For instance, if a firewall is configured to reject all addresses in the 192.166.x.x IP address range, and the requestor's IP is in that range, the request would be denied.

In a practical application, RBAC is a variation on MAC. Administrators typically configure the firewall or other device to allow or deny access. The owner or another user does not specify the conditions of acceptance, and safeguards ensure that an average user cannot change settings on the devices.

# Role-Based Access Control

**Note**

Both *rule-based* and *role-based* access control use the acronym *RBAC*.

In role-based access control (RBAC), access decisions are determined by the roles that individual users have within the organization. Role-based access requires the administrator to have a thorough understanding of how a particular organization operates, the number of users, and each user's exact function in that organization.

**ExamAlert**

Because the CompTIA objectives specifically call out role-based access control, be sure you know that with RBAC access decisions are determined by the roles that individual users have within the organization.

Because access rights are grouped by role name, the use of resources is restricted to individuals who are authorized to assume the associated role. For example, within a school system, the role of teacher can include access to certain data, including test banks, research material, and memos. School administrators might have access to employee records, financial data, planning projects, and more.

The use of roles to control access can be an effective means of developing and enforcing enterprise-specific security policies and for streamlining the security management process.

Roles should receive only the privilege level necessary to do the job associated with that role. This general security principle is known as the *least privilege concept*. When people are hired in an organization, their roles are clearly defined. A network administrator creates a user account for a new employee and places that user account in a group with people who have the same role in the organization.

Least privilege is often too restrictive to be practical in business. For instance, using teachers as an example, some more experienced teachers might have more responsibility than others and might require increased access to a particular network object. Customizing access to each individual is a time-consuming process.

ExamAlert

Once just a Security+ objective and concept, this topic has now been added to the Network+ objectives as well. Because you might be asked about the concept of least privilege, know that it refers to assigning network users the privilege level necessary to do the job associated with their role—nothing more and nothing less.

Closely related to least privilege is the concept of a *zero trust* network. As the name implies, it simply means that you don't automatically trust anyone and instead always authenticate and authorize. Everything must be verified explicitly, data protection is held to utmost ideal, and all sessions are encrypted end to end.

# Defense in Depth

*Defense in depth* is based on the premise that implementing security at different levels or layers to form a complete security strategy provides better protection and greater resiliency than implementing an individual security defense. This level of defense can be accomplished in a number of different ways; some of the most popular are through the use of network segmentation, screened subnet, separation of duties, network access control, and honeypots. Each variant of defense in depth is discussed in the sections that follow.

## Network Segmentation

Dividing one network into smaller subnetworks enables you to optimize it in a number of ways. The segmentation is accomplished with switches and VLANs, and the separation can be done to isolate such things as heavy load systems or certain protocols. If you move them to their own subnetwork, the result should be performance increases for other parts of the network.

Note

One popular approach is using *virtual machines (VMs)* to segment or separate systems (software) from the main OS (host versus guest) and the rest of the network through virtual switches.

## Screened Subnet

An important firewall-related concept is that of the *screened subnet*. This concept was formerly known as a *demilitarized zone (DMZ)* and sometimes called a *perimeter network*. A screened subnet is part of a network where you place

servers that must be accessible by sources both outside and inside your network. However, the screened subnet is not connected directly to either network, and it must always be accessed through the firewall. The military term *DMZ* was used previously because it describes an area that has little or no enforcement or policing.

Using screened subnets gives your firewall configuration an extra level of flexibility, protection, and complexity. Figure 9.1 shows a screened subnet (DMZ) configuration.

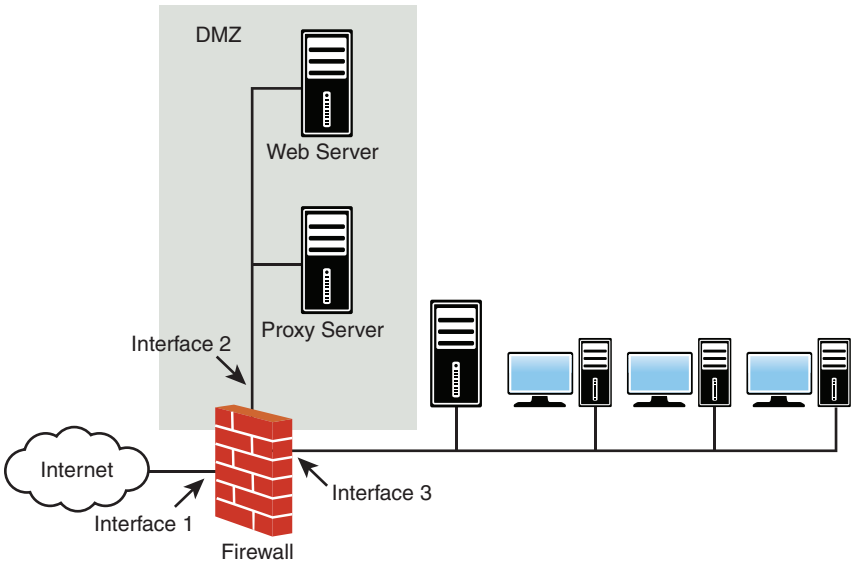



FIGURE 9.1 **A screened subnet (DMZ) configuration**

By using a screened subnet, you can create an additional step that makes it more difficult for an intruder to gain access to the internal network. In Figure 9.1, for example, an intruder who tried to come in through Interface 1 would have to spoof a request from either the web server or proxy server into Interface 2 before it could be forwarded to the internal network. Although it is not impossible for an intruder to gain access to the internal network through a screened subnet, it is difficult.

**ExamAlert**

Be prepared to identify the purpose of a screened subnet and that this concept was previously known as a DMZ.

# Separation of Duties

*Separation of duties* policies are designed to reduce the risk of fraud and to prevent other losses in an organization. A good policy will require more than one person to accomplish key processes. This may mean that the person who processes an order from a customer isn't the same person who generates the invoice or deals with the billing.

Separation of duties helps prevent various problems, such as an individual embezzling money from a company. To embezzle funds successfully, an individual would need to recruit others to commit an act of collusion—that is, an agreement between two or more parties established for the purpose of committing deception or fraud. Collusion, when part of a crime, is also a criminal act in and of itself.

In addition, separation of duties policies can help prevent accidents from occurring in an organization. Suppose that you're managing a software development project. You want someone to perform a quality assurance test on a new piece of code before it's put into production. Establishing a clear separation of duties prevents development code from entering production status until quality testing is accomplished.

Many banks and financial institutions require multiple steps and approvals to transfer money. These policies help reduce errors and minimize the likelihood of fraud.

# Honeypots

When we talk about network security, honeypots and honeynets are often mentioned. Honeypots are a rather clever approach to network security but perhaps a bit expensive. A *honeypot* is a system set up as a decoy to attract and deflect attacks from hackers. The server decoy appears to have everything a regular server does—OS, applications, and network services. The attacker thinks she is accessing a real network server, but she is in a network trap.

The honeypot has two key purposes. It can give administrators valuable information on the types of attacks being carried out. In turn, the honeypot can secure the real production servers according to what it learns. Also, the honeypot deflects attention from working servers, allowing them to function without being attacked.

A honeypot can do the following:

- Deflect the attention of attackers from production servers
- Deter attackers if they suspect their actions may be monitored with a honeypot

- Allow administrators to learn from the attacks to protect the real servers
- Identify the source of attacks, whether from inside the network or outside

**ExamAlert**

Think of a honeypot as a trap that allows the intruder in but does not allow access to sensitive data.

One step up from the honeypot is the honeynet. The *honeynet* is an entire network set up to monitor attacks from outsiders. All traffic into and out of the network is carefully tracked and documented. This information is shared with network professionals to help isolate the types of attacks launched against networks and to proactively manage those security risks. Honeynets function as a production network, using network services, applications, and more. Attackers don't know that they are actually accessing a monitored network.

# RADIUS and TACACS+

Among the potential issues network administrators face when implementing remote access are utilization and the load on the remote-access server. As a network's remote-access implementation grows, reliance on a single remote-access server might be impossible, and additional servers might be required. *Remote Authentication Dial-In User Service (RADIUS)* can help in this scenario.

**ExamAlert**

RADIUS is a protocol that enables a single server to become responsible for all remote-access authentication, authorization, and auditing (or accounting) services.

RADIUS functions as a client/server system. The remote user dials in to the remote-access server, which acts as a RADIUS client, or *network access server (NAS)*, and connects to a RADIUS server. The RADIUS server performs authentication, authorization, and auditing (or accounting) functions and returns the information to the RADIUS client (which is a remote-access server running RADIUS client software); the connection is either established or rejected based on the information received.

*Terminal Access Controller Access Control System (TACACS)* is a security protocol designed to provide centralized validation of users who are attempting to gain access to a router or NAS. Like RADIUS, TACACS is a set of security

protocols designed to provide AAA of remote users. *Terminal Access Controller Access Control System Plus (TACACS+)* is a proprietary version of TACACS from Cisco and is the implementation commonly in use in networks today. TACACS+ uses TCP port 49 by default.

Although both RADIUS and TACACS+ offer AAA services for remote users, some noticeable differences exist:

- TACACS+ relies on TCP for connection-oriented delivery. RADIUS uses connectionless UDP for data delivery.
- RADIUS combines authentication and authorization, whereas TACACS+ can separate their functions.

**ExamAlert**

Both RADIUS and TACACS+ provide authentication, authorization, and accounting services. One notable difference between TACACS+ and RADIUS is that TACACS+ relies on the connection-oriented TCP, whereas RADIUS uses the connectionless UDP.

# Kerberos Authentication

Kerberos is an *Internet Engineering Task Force (IETF)* standard for providing authentication. It is an integral part of network security. Networks, including the Internet, can connect people from all over the world. When data travels from one point to another across a network, it can be lost, stolen, corrupted, or misused. Much of the data sent over networks is sensitive, whether it is medical, financial, or otherwise. A key consideration for those responsible for the network is maintaining the confidentiality of the data. In the networking world, Kerberos plays a significant role in data confidentiality.

In a traditional authentication strategy, a username and password are used to access network resources. In a secure environment, it might be necessary to provide a username and password combination to access each network service or resource. For example, a user might be prompted to type in her username and password when accessing a database, and again for the printer, and again for Internet access. This is a time-consuming process, and it can also present a security risk. Each time the password is entered, there is a chance that someone will see it being entered. If the password is sent over the network without encryption, it might be viewed by malicious eavesdroppers.

Kerberos was designed to fix such problems by using a method requiring only a *single sign-on (SSO)*. This single sign-on enables a user to log in to a

system and access multiple systems or resources without the need to repeatedly reenter the username and password. Additionally, Kerberos is designed to have entities authenticate themselves by demonstrating possession of secret information.

Kerberos is one part of a strategic security solution that provides secure authentication services to users, applications, and network devices by eliminating the insecurities caused by passwords stored or transmitted across the network. Kerberos is used primarily to eliminate the possibility of a network "eavesdropper" tapping into data over the network—particularly usernames and passwords. Kerberos ensures data integrity and blocks tampering on the network. It employs message privacy (encryption) to ensure that messages are not visible to eavesdroppers on the network.

For the network user, Kerberos eliminates the need to repeatedly demonstrate possession of private or secret information.

**ExamAlert**

Kerberos is a nonproprietary protocol and is used for cross-platform authentication. It's the main authentication protocol used with Windows servers.

Kerberos is designed to provide strong authentication for client/server applications by using secret key cryptography. Cryptography is used to ensure that a client can prove its identity to a server (and vice versa) across an unsecure network connection. After a client and server have used Kerberos to prove their identity, they can also encrypt all their communications to ensure privacy and data integrity.

**ExamAlert**

Kerberos enables secure authentication over an unsecure network such as the Internet.

The key to understanding Kerberos is to understand its secret key cryptography. Kerberos uses *symmetric key cryptography*, in which both client and server use the same encryption key to cipher and decipher data.

In secret key cryptography, a plain-text message can be converted into cipher text (encrypted data) and then converted back into plain text using one key. Thus, two devices share a secret key to encrypt and decrypt their communications. Figure 9.2 shows the symmetric key process.

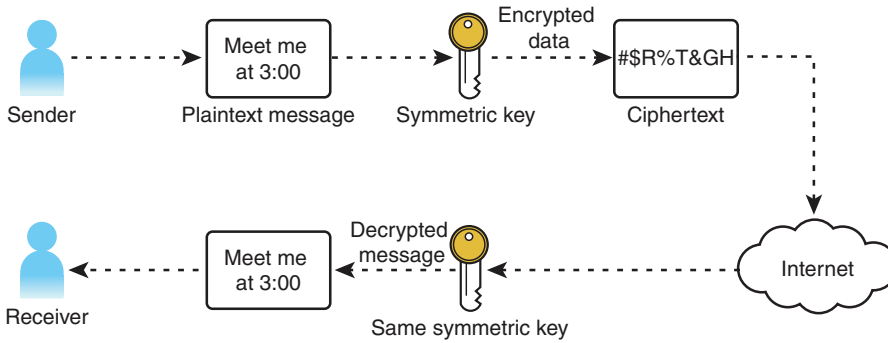



FIGURE 9.2 **The symmetric key process**

**ExamAlert**

Another cryptography method in use is asymmetric key cryptography, or public key cryptography. In this method, a device has both a public and a private key. The private key is never shared. The public key is used to encrypt the communication, and the private key is used for decrypting.

Kerberos authentication works by assigning a unique key, called a *ticket*, to each client that successfully authenticates to a server. The ticket is encrypted and contains the user's password, which is used to verify the user's identity when a particular network service is requested. Each ticket is time stamped. It expires after a period of time, and a new one is issued. Kerberos works in the same way that you go to a movie. First, you go to the ticket counter, tell the person what movie you want to see, and get your ticket. After that, you go to a turnstile and hand the ticket to someone else, and then you're "in." In simplistic terms, that's Kerberos.

**ExamAlert**

You should know that the security tokens used in Kerberos are known as tickets.

# Local Authentication

Most of the time, the goal is to authenticate the user using a centralized authentication server or service of some type. When that cannot be done—such as when there is no Internet connectivity available—authentication is done locally by the operating system using values stored within it. In Windows, for example, the Local Authentication Subsystem (LASS) performs this function and allows users access to the system after their stored username and password variables match.

# Lightweight Directory Access Protocol

*Lightweight Directory Access Protocol (LDAP)* provides a mechanism to access and query directory services systems. In the context of the Network+ exam, these directory services systems are most likely to be UNIX based or Microsoft Active Directory based. Although LDAP supports command-line queries executed directly against the directory database, most LDAP interactions are via utilities such as an authentication program (network logon) or locating a resource in the directory through a search utility.

**ExamAlert**

Know that LDAP, by default, uses port 389.

# Using Certificates

A *public key infrastructure (PKI)* is a collection of software, standards, and policies combined to enable users from the Internet or other unsecured public networks to securely exchange data. PKI uses a public and private cryptographic key pair obtained and shared through a trusted authority. Services and components work together to develop the PKI. Some of the key components of a PKI include the following:

- **Certificates:** Certificates are electronic credentials that validate users, computers, or devices on the network. They are digitally signed statements that associate the credentials of a public key to the identity of the person, device, or service that holds the corresponding private key.
- **Certificate authorities (CAs):** CAs issue and manage certificates. They validate the identity of a network device or user requesting data. CAs can be either independent third parties, known as public CAs, or they can be organizations running their own certificate-issuing server software, known as private CAs.
- **Certificate templates:** These templates are used to customize certificates issued by a certificate server. This customization includes a set of rules and settings created on the CA and used for incoming certificate requests.
- **Certificate revocation list (CRL):** This list identifies certificates that were revoked before they reached the certificate expiration date. Certificates are often revoked because of security concerns, such as a compromised certificate.

# Auditing and Logging

Auditing is the process of monitoring occurrences and keeping a log of what has occurred on a system. A system administrator determines which events should be audited. Tracking events and attempts to access the system helps prevent unauthorized access and provides a record that administrators can analyze to make security changes as necessary. This record, or log, also provides administrators with solid evidence if they need to look into improper user conduct.

**Caution**

Be sure that you can identify the purpose of authentication, authorization, and accounting.

The first step in auditing is to identify what system events to monitor. After the system events are identified, in a Windows environment, the administrator can choose to monitor the success or failure of a system event. For instance, if "logon" is the event being audited, the administrator might choose to log all unsuccessful logon attempts, which might indicate that someone is attempting to gain unauthorized access. Conversely, the administrator can choose to audit all successful attempts to monitor when a particular user or user group is logging on. Some administrators prefer to log both events. However, overly ambitious audit policies can reduce overall system performance.

# Multifactor Authentication Factors

*Multifactor authentication* is defined as having two or more access methods included as part of the authentication process; for example, using both smartcards and passwords. An ATM card and PIN are another common example representing multifactor authentication (in this case, two-factor authentication), as opposed to just one (which constitutes single-factor authentication). The ATM card is something you have, and the PIN is something you know.

The factors used in authentication systems or methods are based on one or more of these five factors:

- **Something you know**, such as a password or PIN
- **Something you have**, such as a smartcard, token, or identification device
- **Something you are**, such as your fingerprints or retinal pattern (often called biometrics)

- **Somewhere you are** (based on geolocation)
- **Something you do**, such as an action you must take to complete authentication

ExamAlert

Be able to identify the five types of factors used in multifactor authentication.

# Additional Access Control Methods

Today, there are many ways to establish access into networks. You could fill an entire tome with a discussion of the possibilities. What follows are some of the more important ones to know for this exam (others appear on other CompTIA exams, such as Security+).

## 802.1X

The IEEE standard 802.1X defines port-based security for wireless network access control. As such, it offers a means of authentication and defines the Extensible Authentication Protocol (EAP) over IEEE 802, which is often known as EAP over LAN (EAPOL). The biggest benefit of using 802.1X is that the access points and the switches do not need to do the authentication but instead rely on the authentication server to do the work.

ExamAlert

Remember that IEEE 802.1X authentication allows only authorized devices to connect to the network. The most secure form of IEEE 802.1X authentication is certificate-based authentication.

## Extensible Authentication Protocol (EAP)

Choosing the correct authentication protocol for remote clients is an important part of designing a secure remote-access strategy. After they are authenticated, users have access to the network and servers. *Extensible Authentication Protocol (EAP)* provides a framework for authentication that is often used with wireless networks. Among the EAP types adopted by the WPA/WPA2 standard are PEAP, EAP-FAST, and EAP-TLS. EAP was developed in response to an increasing demand for authentication methods that use other types of security devices, such as token cards, smartcards, and digital certificates.

To simplify network setup, a number of small office/home office (SOHO) routers use a series of EAP messages to allow new hosts to join the network and use WPA/WPA2. Known as Wi-Fi Protected Setup (WPS), this setup often requires the user to do something to complete the enrollment process: press a button on the router within a short time period, enter a PIN, or bring the new device close by (so that near-field communication can take place).

> **Note**
>
> WPA3 uses the Simultaneous Authentication of Equals (SAE) to replace WPA2's preshared key (PSK) exchange protocol.

Cisco, RSA, and Microsoft worked together to create Protected Extensible Authentication Protocol (PEAP). There is now native support for it in Windows (which previously favored EAP-TLS). Although many consider PEAP and EAP-TLS to be similar, PEAP is more secure because it establishes an encrypted channel between the server and the client.

EAP-FAST (Flexible Authentication via Secure Tunneling) was designed by Cisco to allow for the use of certificates to establish a TLS tunnel in which client credentials are verified.

To put EAP implementations in a chronological order, think EAP-TLS, EAP-FAST, and then PEAP. In between came EAP-TTLS, a form of EAP-TLS that adds tunneling (Extensible Authentication Protocol—Tunneled Transport Layer Security). Of all the choices, PEAP is the one with more vendors than just Cisco and thus is currently favored for use today.

## Network Access Control (NAC)

*Network access control (NAC)* is a method to restrict access to the network based on identity or posture (discussed later in this chapter). This method was created by Cisco to enforce privileges and make decisions on a client device based on information gathered from it (such as the vendor and version of the antivirus software running). If the wanted information is not found (such as that the antivirus definitions are a year old), the client can be placed in a *quarantine network* area to keep it from infecting the rest of the network. It can also be placed in a *guest network* and/or allowed to run *nonpersistent* (versus persistent) *agents*.

A *posture assessment* is any evaluation of a system's security based on settings and applications found. In addition to looking at such values as settings in the Registry or dates of files, NACs can also check *802.1X* values—the group of

networking protocols associated with authentication of devices attempting to connect to the network. 802.1X works with EAP.

**ExamAlert**

As you prepare for the exam, be sure that you can identify posture assessment as any evaluation of a system's security based on settings and applications found.

## MAC Filtering

Another name for a network card or network adapter is a *network controller*. Every controller has a unique MAC address associated with it. Filtering network traffic using a system's MAC address typically is done using an ACL. This list keeps track of all MAC addresses and is configured to allow or deny access to certain systems based on the list. As an example, look at the MAC ACL from a router. Figure 9.3 shows the MAC ACL screen. Specific MAC addresses can be either denied or accepted, depending on the configuration. It would be possible, for example, to configure it so that only the system with the MAC address of 02-00-54-55-4E-01 can authenticate to the router.

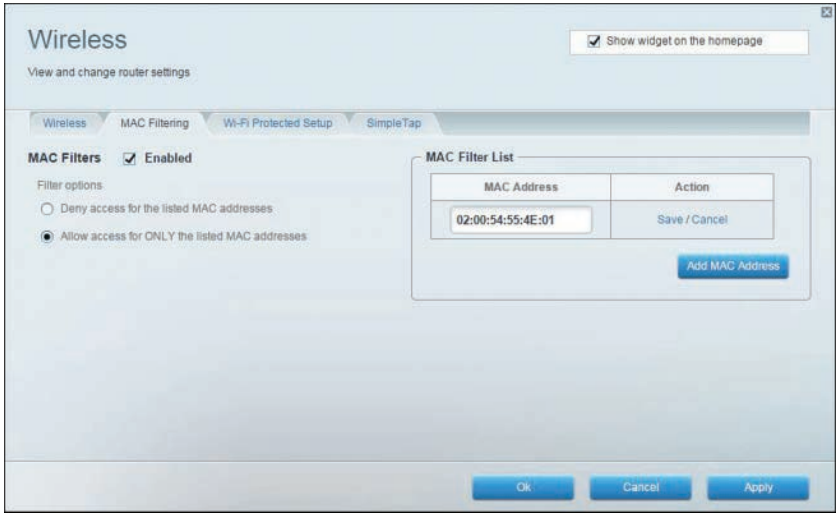



FIGURE 9.3 **A MAC ACL**

**Note**

When administrators are configuring security for wireless networks, filtering by MAC address is a common practice. Typically, in MAC filtering security, MAC addresses can be added to an "allow" ACL or "deny" ACL.

# Risk Management

*Risk management* involves recognizing and acknowledging that risks exist and then determining what to do about them. Sometimes, the best solution is to do nothing. If, for example, there is a risk that some data could be lost in the event of a fire but the value placed on that data is below the cost of protecting it from that harm, the economically feasible solution could be to accept the risk and do nothing further. In most cases, acceptance alone is not enough and two likely approaches are mitigation (trying to minimize the risk) and/or transference (shifting a part of the risk to another party such as an insurance provider).

To determine how to manage risk, assessments are usually employed. An assessment can be done on threats, vulnerabilities, or business operations (process assessment and vendor assessment).

# Penetration Testing

It is becoming more common for companies to hire penetration testers to test their system's defenses. Essentially, a penetration tester will use the same techniques that a hacker would use to find any flaws in a system's security. These flaws may be discovered by means other than directly accessing the system, such as collecting information from public databases, talking to employees/partners, dumpster diving, and social engineering. This approach is known as *passive reconnaissance*. In contrast, *active reconnaissance* directly focuses on the system (port scans, traceroute information, network mapping, and so forth) to identify weaknesses that could be used to launch an attack.

When you're doing penetration testing, it is important to have a scope document outlining the extent of the testing that is to be done. It is equally important to have permission from an administrator who can authorize such testing—in writing—enabling the testing to be conducted.

One weakness a good penetration test looks for is escalation of privilege; that is, a hole created when code is executed with higher privileges than those of the user running it. By breaking out of the executing code, the users are left with higher privileges than they should have.

Three types of penetration testing are black box/unknown environment (the tester has absolutely no knowledge of the system and is functioning in the same manner as an outside attacker), white box/known environment (the tester has significant knowledge of the system, which simulates an attack from an insider—a rogue employee), and gray box/partially known environment (a middle ground between the first two types of testing. In gray box testing, the tester has some limited knowledge of the target system). While the "box" analogy is

used to describe the environment, "hats" have often been used to describe the person doing the testing, but that terminology is now being replaced by level of authorization. Therefore, a white hat tester is equivalent to an authorized tester, a black hat tester to an unauthorized tester, and a gray hat tester to a semi-authorized tester.

**Note**

With so many security-related topics now appearing on the Network+ exam, you have a good head start on Security+ certification study after you successfully finish taking this exam.

## Security Information and Event Management

*Security information and event management (SIEM)* products provide notifications and real-time analysis of security alerts and can help you head off problems quickly. Chapter 8, "Network Operations," discussed event management and looking at log files, including the security log.

SIEM tools collect, correlate, and display data feeds that support response activities. A SIEM can take individual benign events and tie them together to reveal more details about what occurred and why it's of concern.

Dashboards are an important element in SIEM solutions, presenting data (and analysis) in actionable format. Most SIEM packages allow organizations to customize their dashboard(s) based on their needs and requirements. One need of any SIEM is to be able to interpret (and visualize) data coming from different sources and, thus, different formats. Normalizing logs involves extracting and processing entries to put them into a readable and structured format that can be displayed and acted upon.

## Cram Quiz

1. Which of the following ports is used by TACACS+ by default?

   - ❍ **A.** 49
   - ❍ **B.** 51
   - ❍ **C.** 53
   - ❍ **D.** 59

2. Which of the following is the main authentication protocol used with Windows servers?
   - ❍ **A.** LDAP
   - ❍ **B.** Kerberos
   - ❍ **C.** L2TP
   - ❍ **D.** TFTP

3. What are the security tokens used with Kerberos known as?
   - ❍ **A.** Coins
   - ❍ **B.** Vouchers
   - ❍ **C.** Tickets
   - ❍ **D.** Gestures

4. Which of the following is NOT one of the factors associated with multifactor authentication?
   - ❍ **A.** Something you like
   - ❍ **B.** Something you are
   - ❍ **C.** Something you do
   - ❍ **D.** Something you have

5. Which of the following is one step up from the honeypot?
   - ❍ **A.** Geofence
   - ❍ **B.** VLAN
   - ❍ **C.** DMZ
   - ❍ **D.** Honeynet

6. Which of the following is based on the premise that implementing security at different levels or layers to form a complete security strategy provides better protection and greater resiliency than implementing an individual security defense?
   - ❍ **A.** Screened subnet
   - ❍ **B.** Separation of duties
   - ❍ **C.** EAP
   - ❍ **D.** Defense in depth

7. What is a list of publicly available security flaws that you should be familiar with for security otherwise known as?
   - ❍ **A.** CVEs
   - ❍ **B.** MAC filter
   - ❍ **C.** SIEM
   - ❍ **D.** CRL

8. What type of control is present if access decisions are determined by the roles that individual users have within the organization?
   - ❍ **A.** Passive reconnaissance
   - ❍ **B.** RBAC
   - ❍ **C.** Active reconnaissance
   - ❍ **D.** SSO

## Cram Quiz Answers

1. **A.** TACACS+ uses TCP port 49 by default.
2. **B.** Kerberos is the main authentication protocol used with Windows servers.
3. **C.** The tokens used for security in Kerberos are known as tickets.
4. **A.** Something you like is not one of the five factors used in multifactor authentication. The five legitimate possibilities are the following: something you know, something you have, something you are, somewhere you are, and something you do.
5. **D.** One step up from the honeypot is the honeynet.
6. **D.** Defense in depth is based on the premise that implementing security at different levels or layers to form a complete security strategy provides better protection and greater resiliency than implementing an individual security defense.
7. **A.** Common vulnerabilities and exposures (CVEs) are a list of publicly available security flaws that you should be familiar with for security.
8. **B.** In role-based access control (RBAC), access decisions are determined by the roles that individual users have within the organization. Role-based access requires the administrator to have a thorough understanding of how a particular organization operates, the number of users, and each user's exact function in that organization.

# Common Networking Attacks

▶ **Compare and contrast common types of attacks.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What are software programs or code snippets called that execute when a certain predefined event occurs?
2. What type of malware takes control of a system and demands that a third party be paid before control is returned to the rightful owner?

### Answers

1. Logic bombs are software programs or code snippets that execute when a certain predefined event occurs.
2. Ransomware takes control of a system and demands that a third party be paid before restoring control to the rightful party.

Malicious software, or *malware*, is a serious problem in today's computing environments. It is often assumed that malware is composed of viruses. Although this typically is true, many other forms of malware by definition are not viruses, but are equally undesirable. Although we commonly associate them with coming from the outside, do not overlook the possibility for them to come from *inside threats* as well (particularly malicious employees who feel slighted because they did not get a raise or recognition they feel they deserve and have now become an insider threat).

Malware encompasses many types of malicious software and all were intended by their developer to have an adverse effect on the network. The following sections look at some of the more malevolent types.

## Denial-of-Service and Distributed Denial-of-Service Attacks

*Denial-of-service (DoS)* attacks are designed to tie up network bandwidth and resources and eventually bring the entire network to a halt. This type of attack is done simply by flooding a network with more traffic than it can handle.

When more than one computer is used in the attack, it is technically known as a *distributed DoS (DDoS)* attack. These attacks typically use a *botnet* to launch a *command and control attack* through a traffic spike. Almost every attack of this type today is DDoS, and we will use DoS to mean both.

A DoS attack is not designed to steal data but rather to cripple a network and, in doing so, cost a company huge amounts of money. It is possible, in fact, for the attack to be an unintentional, or *friendly*, DoS attack coming from the inside. Just as with friendly fire in combat, it matters not that the attack was unintentional; it does just as much damage.

The effects of DoS attacks include the following:

- Saturating network resources, which then renders those services unusable
- Flooding the network media, preventing communication between computers on the network
- Causing user downtime because of an inability to access required services
- Causing potentially huge financial losses for an organization because of network and service downtime

## Types of DoS Attacks

Several types of DoS attacks exist, and each seems to target a different area. For instance, they might target bandwidth, network service, memory, CPU, or hard drive space. When a server or other system is overrun by malicious requests, one or more of these core resources breaks down, causing the system to crash or stop responding. A *permanent DoS attack* continues for more than a short period of time and requires you to change your routing, IP addresses, or other configurations to get around it.

### Fraggle

In a *Fraggle attack*, spoofed UDP packets are sent to a network's broadcast address. These packets are directed to specific ports, such as port 7 or port 19, and, after they are connected, can flood the system.

### Smurfing

The *Smurf attack* is similar to a Fraggle attack. However, a ping request is sent to a broadcast network address, with the sending address spoofed so that many ping replies overload the victim and prevent it from processing the replies.

## Ping of Death

In a *ping of death attack*, an oversized *Internet Control Message Protocol (ICMP)* datagram is used to crash IP devices that were manufactured before 1996.

## SYN Flood

In a typical TCP session, communication between two computers is initially established by a three-way handshake, referred to as a SYN, SYN/ACK, ACK. At the start of a session, the client sends a SYN message to the server. The server acknowledges the request by sending a SYN/ACK message back to the client. The connection is established when the client responds with an ACK message.

In a *SYN attack*, the victim is overwhelmed with a flood of SYN packets. Every SYN packet forces the targeted server to produce a SYN/ACK response and then wait for the ACK acknowledgment. However, the attacker doesn't respond with an ACK, or spoofs its destination IP address with a nonexistent address so that no ACK response occurs. The result is that the server begins filling up with half-open connections. When all the server's available resources are tied up on half-open connections, it stops acknowledging new incoming SYN requests, including legitimate ones.

## Buffer Overflow

A *buffer overflow* is a type of DoS attack that occurs when more data is put into a buffer (typically a memory buffer) than it can hold, thereby overflowing it (as the name implies).

## Distributed Reflective DoS

A *distributed reflective DoS (DRDoS)* attack is also called an *amplification attack*, and it targets public UDP servers. Two of the most common protocols/servers that a DRDoS attack usually goes after are Domain Name Service (DNS) and Network Time Protocol (NTP) servers, but Simple Network Management Protocol (SNMP), NetBIOS, and other User Datagram Protocol (UDP) protocols are also susceptible.

**ExamAlert**

As you study for the exam, be sure to focus on the difference between DoS and DDoS and know that a botnet is formed by many bots (infected systems) and controlled by a command and control server to carry out a DDoS attack.

### ICMP Flood

An *ICMP flood*, also known as a ping flood, is a DoS attack in which large numbers of ICMP messages are sent to a computer system to overwhelm it. The result is a failure of the TCP/IP protocol stack, which cannot tend to other TCP/IP requests.

## Other Common Attacks

This section details some of the more common attacks used today.

**ExamAlert**

Know all the common types of attacks detailed throughout this section. The Network+ exam is extremely likely to ensure your knowledge here is what an administrator should know.

## Social Engineering

Social engineering is a common form of cracking. It can be used by both outsiders and people within an organization. *Social engineering* is a hacker term for tricking people into revealing their password or some form of security information. It might include trying to get users to send passwords or other information over email, following someone closely into a secured area (known as *tailgating*), walking in with them (known as *piggybacking*), looking over someone's shoulder at their screen (known as *shoulder surfing*), or any other method that tricks users into divulging information. Social engineering is an attack that attempts to take advantage of human behavior.

## Logic Bomb

Software programs or code snippets that execute when a certain predefined event occurs are known as *logic bombs*. Such a bomb may send a note to an attacker when a user is logged on to the Internet and is accessing a certain application, for example. This message could inform the attacker that the user is ready for an attack and open a backdoor. Similarly, a programmer could create a program that always makes sure her name appears on the payroll roster; if it doesn't, then key files begin to be erased. Any code that is hidden within an application and causes something unexpected to happen constitutes a logic bomb.

## Rogue DHCP

A *rogue DHCP* server added to a network has the potential to issue an address to a client isolating it on an unauthorized network where its data can be captured. Although it sounds like a bad thing, *DHCP snooping* is just the opposite. It is the capability for a switch to look at packets and drop DHCP traffic that it determines to be unacceptable based on the defined rules. The purpose is to prevent rogue DHCP servers from offering IP addresses to DHCP clients.

## Rogue Access Points and Evil Twins

A *rogue access point* is a wireless access point that has been placed on a network without the administrator's knowledge. The result is that it is possible to remotely access the rogue access point because it likely does not adhere to company security policies. So, all security can be compromised by a cheap wireless router placed on the corporate network. An *evil twin attack* is one in which a rogue wireless access point poses as a legitimate wireless service provider to intercept information that users transmit.

## Advertising Wireless Weaknesses

Attacks that advertise wireless weaknesses start with *war driving*—driving around with a mobile device looking for open wireless access points with which to communicate and looking for weak implementations that can be cracked (called *WEP cracking* or *WPA cracking*). They then lead to *war chalking*—those who discover a way in to the network leave signals (often written in chalk) on, or outside, the premise to notify others that the vulnerability is there. The marks can be on the sidewalk, the side of the building, a nearby signpost, and so on.

## Phishing

Often users receive a variety of emails offering products, services, information, or opportunities. Unsolicited email of this type is called *phishing* (pronounced "fishing"). This technique involves a bogus offer sent to hundreds of thousands or even millions of email addresses. The strategy plays the odds. For every 1,000 emails sent, perhaps one person replies. Phishing can be dangerous because users can be tricked into divulging personal information such as credit card numbers or bank account information. Today, phishing is performed in several ways. Phishing websites and phone calls are also designed to steal money or personal information.

## Ransomware

With *ransomware*, software—often delivered through a Trojan horse—takes control of a system and demands that a third party be paid. The "control" can be accomplished by encrypting the hard drive, by changing user password information, or via any of a number of other creative ways. Users are usually assured that by paying the extortion amount (the ransom), they will be given the code needed to revert their systems to normal operations.

## DNS Poisoning

With *DNS poisoning*, the DNS server is given information about a name server that it thinks is legitimate when it isn't. This type of attack can send users to a website other than the one to which they wanted to go, reroute mail, or do any other type of redirection wherein data from a DNS server is used to determine a destination. Another name for this is *DNS spoofing*, and fast flux is one of the most popular techniques. Botnets use it to hide the delivery sites behind a changing network of compromised hosts that act as proxies.

## ARP Cache Poisoning

*Address Resolution Protocol (ARP) poisoning* tries to convince the network that the attacker's MAC address is the one associated with an IP address so that traffic sent to that IP address is wrongly sent to the attacker's machine.

## Spoofing

*Spoofing* is a technique in which the real source of a transmission, file, or email is concealed or replaced with a fake source. This technique enables an attacker, for example, to misrepresent the original source of a file available for download. Then he can trick users into accepting a file from an untrusted source, believing it is coming from a trusted source. *MAC spoofing* is the act of faking the MAC address of a machine—faking its physical identity. While the real MAC address cannot be changed, it is possible for drivers to give values provided to them and fool a system into believing that the NIC it is talking to has the MAC address of a recognized/authorized host. *IP spoofing* does a similar action with the IP address rather than the MAC address.

## Deauthentication

*Deauthentication* is also known as a disassociation attack. With this type of attack, the intruder sends a frame to the AP with a spoofed address to make it

look as if it came from the victim but disconnects the user from the network. Because the victim is unable to keep a connection with the AP, this attack increases the chances of the victim choosing to use another AP—a rogue one or one in a hotel or other venue that he has to pay extra to use. The Federal Trade Commission has filed suits against a number of hotels for launching attacks of this type and generating revenue by requiring their guests to pay for "premium" services rather than being able to use the free Wi-Fi.

## Brute Force

There are a number of ways to ascertain a password, but one of the most common is a *brute-force attack* in which one value after another is guessed until the right value is found. Although that could take forever if done manually, software programs can take lots of values in a remarkably short period of time. Wi-Fi Protected Setup (WPS) attacks, for example, have become much more common since the technology is susceptible to brute-force attacks used to guess the user's PIN. When an attacker gains access, the attacker is then on the Wi-Fi network.

## On-Path Attack

In an *on-path attack* (previously known as a *man-in-the-middle attack*), the intruder places himself between the sending and receiving devices and captures the communication as it passes by. The interception of the data is invisible to those sending and receiving the data. The intruder can capture the network data and manipulate it, change it, examine it, and then send it on. Wireless communications are particularly susceptible to this type of attack. A rogue access point, a wireless AP that has been installed without permission, is an example of an on-path attack. If the attack is done with FTP (using the port command), it is known as an *FTP bounce* attack.

## VLAN Hopping

*VLAN hopping*, as the name implies, is an exploit of resources on a virtual LAN that is made possible because the resources exist on said virtual LAN. There is more than one method by which this occurs, but in all of them, the result is the same: an attacking host on a VLAN gains access to resources on other VLANs that are not supposed to be accessible to them (becoming a compromised system). Again, regardless of the method employed, the solution is to properly configure the switches to keep this from happening.

ExamAlert

A compromised system is any that has been adversely impacted (intentionally or unintentionally) by an untrusted source. The compromise can relate to confidentiality, integrity, or availability (CIA).

## ARP Spoofing

With *ARP spoofing* (also known as *ARP poisoning*), the Media Access Control (MAC) address of the data is faked. When this value is faked, it is possible to make it look as if the data came from a network that it did not. This technique can be used to gain access to the network, to fool the router into sending data here that was intended for another host, or to launch a DoS attack. In all cases, the address being faked is an address of a legitimate user, and that makes it possible to get around such measures as allow/deny lists.

## Vulnerabilities and Prevention

The threat from malicious code is a real concern. You need to take precautions to protect your systems. Although you might not eliminate the threat, you can significantly reduce it.

One of the primary tools used in the fight against malicious software is antivirus/antimalware software. Antimalware software (which includes antivirus software and more) is available from a number of companies, and each offers similar features and capabilities. You can find solutions that are host based, cloud/server based, or network based. Common features and characteristics of antivirus software are as follows:

- **Real-time protection:** An installed antivirus program should continuously monitor the system looking for viruses. If a program is downloaded, an application opened, or a suspicious email received, the real-time virus monitor detects and removes the threat. The virus application sits in the background, largely unnoticed by the user.
- **Virus scanning:** An antivirus program must scan selected drives and disks, either locally or remotely. You can manually run scanning or schedule it to run at a particular time.
- **Scheduling:** It is a best practice to schedule virus scanning to occur automatically at a predetermined time. In a network environment, this time typically is off hours, when the overhead of the scanning process won't impact users.

- **Live updates:** New viruses and malicious software are released with alarming frequency. It is recommended that the antivirus software be configured to regularly receive virus updates.
- **Email vetting:** Emails represent one of the primary sources of virus delivery. It is essential to use antivirus software that provides email scanning for both inbound and outbound email.
- **Centralized management:** If antivirus software or antimalware is used in a network environment, it is a good idea to use software that supports managing the virus program from the server. Virus updates and configurations need to be made only on the server, not on each client station.

Managing the threat from viruses is considered a proactive measure, with antivirus software only part of the solution. A complete security protection strategy requires many aspects to help limit the risk of malware, viruses, and other threats:

- **Develop in-house policies and rules:** In a corporate environment or even a small office, you need to establish what information can be placed on a system. For example, should users download programs from the Internet? Can users bring in their own storage media, such as USB flash drives? Is there a corporate BYOD policy restricting the use of personal smartphones and other mobile devices?
- **Monitor virus threats:** With new viruses coming out all the time, you need to check whether new viruses have been released and what they are designed to do.
- **Educate users:** One of the keys to a complete antivirus solution is to train users in virus prevention and recognition techniques. If users know what to look for, they can prevent a virus from entering the system or network. Back up copies of important documents. Keep in mind that no solution is absolute, so care should be taken to ensure that the data is backed up. In the event of a malicious attack, redundant information is available in a secure location.
- **Automate virus scanning and updates:** You can configure today's antivirus software to automatically scan and update itself. Because such tasks can be forgotten and overlooked, it is recommended that you have these processes scheduled to run at predetermined times.
- **Don't run unnecessary services:** Know every service that is running on your network and the reason for it. If you can avoid running the service, equate it with putting another lock on the door and do so.

- **Keep track of open ports:** Just as you don't want unnecessary services running, you don't want unnecessary ports left open. Every one of them is an unguarded door through which a miscreant can enter.
- **Avoid unencrypted channels and clear-text credentials:** The days when these were acceptable have passed. Continuing to use them is tantamount to inviting an attack.
- **Shun unsecure protocols:** Once upon a time, clear-text passwords were okay to use because risks of anyone getting on your network who should not were minimal. During those days, it was okay to use unsecure protocols as well because the priority was on ease of use as opposed to data protection. These practices went out of acceptance decades ago, so you must—in the interest of security—be careful with the following unsecure protocols: Telnet, HTTP, SLIP, FTP, TFTP, and SNMP (v1 and v2). Secure alternatives—offering the same functionality but adding acceptable levels of security—are available for each. Where possible, opt instead for SSH, SNMPv3, TLS/SSL, SFTP, HTTPS, and IPSec.
- **Install patches and updates:** All applications, including productivity software, virus checkers, and especially the operating system, release patches and updates often, designed to address potential security weaknesses. Administrators must keep an eye out for these patches and install them when they are released. Pay particular attention to unpatched/legacy systems and keep them as secure as possible.

One of the best tools to use when dealing with problems is knowledge. In several locations, CompTIA stresses that user education is important, but even more important is that administrators know what is going on and keep learning from what is going on now and what has gone on in the past. As an example, *TEMPEST* is the name of a project commenced by the U.S. government in the late 1950s that all administrators should be familiar with. TEMPEST was concerned with reducing electronic noise from devices that would divulge intelligence about systems and information. This program has become a standard for computer systems certification. *TEMPEST shielding protection* means that a computer system doesn't emit any significant amounts of electromagnetic interference (EMI) or radio frequency interference (RFI) (*RF* emanation). For a device to be approved as a TEMPEST, it must undergo extensive testing, done to exacting standards that the U.S. government dictates. Today, control zones and white noise are used to accomplish the shielding. TEMPEST-certified equipment often costs twice as much as non-TEMPEST equipment.

ExamAlert

Know some of the ways to prevent networking attacks and mitigate vulnerabilities.

# Cram Quiz

1. Which of the following is an attack in which a rogue wireless access point poses as a legitimate wireless service provider to intercept information that users transmit?

   - ❍ **A.** Zero day
   - ❍ **B.** Phishing
   - ❍ **C.** Evil twin
   - ❍ **D.** Social engineering

2. Which of the following is a type of DoS attack that occurs when more data is put into a buffer than it can hold?

   - ❍ **A.** Dictionary attack
   - ❍ **B.** Buffer overflow
   - ❍ **C.** Worm
   - ❍ **D.** Trojan horse

3. Which of the following is an attack in which something that appears as a helpful or harmless program carries and delivers a malicious payload?

   - ❍ **A.** Worm
   - ❍ **B.** Phish
   - ❍ **C.** Evil twin
   - ❍ **D.** Trojan horse

4. Which of the following is an attack in which users are tricked into revealing their passwords or some form of security information?

   - ❍ **A.** Bluesnarfing
   - ❍ **B.** Phishing
   - ❍ **C.** Evil twin
   - ❍ **D.** Social engineering

# Cram Quiz Answers

1. **C.** An evil twin attack is one in which a rogue wireless access point poses as a legitimate wireless service provider to intercept information users transmit.
2. **B.** A buffer overflow is a type of DoS attack that occurs when more data is put into a buffer than it can hold.
3. **D.** Trojan horses appear as helpful or harmless programs but, when installed, carry and deliver a malicious payload.
4. **D.** Social engineering is a way of tricking people (users) into revealing their passwords or some form of security information.

# Network Hardening and Physical Security

- **Given a scenario, apply network hardening techniques.**
- **Explain the importance of physical security.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. True or false: All unnecessary services on a server should be disabled.
2. A system that uses any two items, such as smartcards and passwords, for authentication is referred to as a _____ system.
3. True or false: Common passwords should be used on similar system devices within the same geographic confines.

### Answers

1. True. Unnecessary services serve no purpose and take up overhead. They also represent extra possibilities for an attacker to exploit and use to gain access to your system(s).
2. A system that uses any two items, such as smartcards and passwords, for authentication is referred to as a two-factor authentication system.
3. False. Common passwords should be avoided at all cost because they serve to weaken the security of the system.

### ExamAlert

Remember that the first of the two objectives this section covers begins with "Given a scenario." This means that you may receive a drag-and-drop, matching, or "live OS" scenario where you have to click through to complete a specific objective-based task.

Having great network security does little good if everything can be compromised by someone walking in your office, picking up your server, and walking out the front door with it. Physical security of the premises is equally important to an overall security implementation.

Ideally, your systems should have a minimum of three physical barriers:

- The external entrance to the building, referred to as a *perimeter*, which is protected by one or more *detection methods*. Detection methods usually involve a *camera* and *motion detection*. The protection of the perimeter can be accomplished with burglar alarms, external walls, fencing, surveillance, and so on. This type of protection should be used with an access list, which should exist to specifically identify who can enter a facility and can be verified by a security guard or someone in authority. An *access control vestibule* (previously known as a mantrap) can be used to limit access to only one or two people going into the facility at a time. A properly developed vestibule includes bulletproof glass, high-strength doors, and locks. In high-security and military environments, an armed guard, as well as video surveillance (IP cameras and CCTVs), should be used at the access control vestibule. After a person is inside the facility, additional security and authentication may be required for further entrance.
- A locked door with door access controls protecting the computer center and network closets. You should also rely on such *access control hardware* as badge readers (also known as ID badge readers, proximity readers), key fobs, or keys to gain access. *Biometrics*, such as fingerprint or retinal scans, can be used for authentication.
- The entrance to the computer room itself. This entrance should be another locked door that is carefully monitored and protected by keypads and cipher locks. Although you try to keep as many intruders out with the other two barriers, many who enter the building could be posing as someone they are not—heating and air-conditioning technicians, representatives of the landlord, and so on. Although these pretenses can get them past the first two barriers, they should still be stopped by the locked computer room door. If they do manage to gain entry, *locking racks*, *locking cabinets*, and even *smart lockers* (secure storage and distribution systems with computer and sensors built in) should be used to protect hardware and keep it from being absconded.
- Assets should have *asset tags* (also known as tracking tags) or *tamper tags* attached to them that have unique identifiers for each client device in your environment (usually just incrementing numbers corresponding to values in a database) to help you identify and manage your IT assets. Additionally, tamper detection devices should be installed to protect against unauthorized chassis cover and component removal.

The objective of any physical barrier is to prevent access to computers and network systems. The most effective physical barrier implementations require that

more than one physical barrier be crossed to gain access. This type of approach is called a multiple barrier system.

**ExamAlert**

Physical security is a recent addition to the Network+ exam. Be sure that you are familiar with the topics discussed here.

One step to never overlook in the security equation is that of *employee training*. All employees should be trained to look out for social engineering techniques that could be tried on them, the importance of the assets (data and hardware), and that security—also associated with job security—is everyone's responsibility.

# Disposing of Assets

Almost every asset reaches the end of its life at some point in time. Whether that asset is a workstation, a hard drive, a piece of backup media, or something else altogether, care needs to be taken when disposing of it to reduce the risk of sensitive data falling into the wrong hands. As an example, consider that the capacity of a flash drive (also known as a thumb drive, USB drive, jump drive, etc.) is now greater than that of many hard drives only a few years ago and many users now store all of their files on a small drive that they transport with them.

A policy should be created, and implemented, governing the disposal of all assets that hold data. Options of what can be done include performing factory resets (for laptops, tablets, and similar devices), wiping the data, and sanitizing the device before disposal. Sanitizing is simply removing the data and the traces of it; this is usually done with storage devices, such as hard drives, and is often referred to as purging. Wiping goes further than purging and is also known as overwriting (or shredding). With wiping, the data that was there is first replaced with something else and then removed. That way, if the data is somehow recovered, what comes back is the overwritten data rather than the original data. The simplest overwrite technique writes a pattern of zeros over the original data.

# Implementing Physical Security

Physical security is a combination of good sense and procedure. The purpose of physical security is to restrict access to network equipment only to people who need it.

The extent to which physical security measures can be implemented to protect network devices and data depends largely on their location. For instance, if a server is installed in a cabinet located in a general office area, the only practical physical protection is to make sure that the cabinet door is locked and that access to keys for the cabinet is controlled. Using other antitheft devices might be practical, but that depends on the location of the cabinet.

However, if your server equipment is located in a cupboard or dedicated room, access restrictions for the room are easier to implement and can be more effective. Again, access should be limited only to those who need it. Depending on the size of the room, this factor might introduce a number of other factors.

Servers and other key networking components are those to which you need to apply the greatest level of physical security. Nowadays, most organizations choose to locate servers in a cupboard or a specific room.

Access to the server room should be tightly controlled, and all access doors must be secured by some method, whether it is a lock and key or a retinal scanning system. Each method of server room access control has certain characteristics. Whatever the method of server room access, it should follow one common principle: control. Some access control methods provide more control than others.

## Lock and Key

If access is controlled by lock and key, the number of people with a key should be restricted to only those people who need access. Spare keys should be stored in a safe location, and access to them should be controlled.

Following are some of the features of lock-and-key security:

- **Inexpensive:** Even a good lock system costs only a few hundred dollars.
- **Easy to maintain:** With no back-end systems and no configuration, using a lock and key is the easiest access control method.
- **Less control than other methods:** Keys can be lost, copied, and loaned to other people. There is no record of access to the server room and no way to prove that the key holder is entitled to enter.

> **Tip**
>
> If you use a lock and key for security, make sure that all copies of the original key are stamped DO NOT COPY. That way, it is more difficult for someone to get a copy because reputable key cutters will not make copies of such keys.

## Swipe Card and PIN Access

If budgets and policies permit, swipe card and PIN entry systems are good choices for managing physical access to a server room. Swipe card systems use a credit card–sized plastic card read by a reader on the outside of the door. To enter the server room, you must swipe the card (run it through the reader), at which point it is read by the reader, which validates it. Usually, the swipe card's use to enter the room is logged by the card system, making it possible for the logs to be checked. In higher-security installations, it is common to have a swipe card reader on the inside of the room as well so that a person's exit can be recorded.

Although swipe card systems have relatively few disadvantages, they do need specialized equipment so that they can be coded with users' information. They also have the same drawbacks as keys in that they can be lost or loaned to other people. However, the advantage that swipe cards have over key systems is that swipe cards are hard to copy.

PIN pads can be used alone or with a swipe card system. PIN pads have the advantage of not needing any kind of card or key that can be lost. For the budget conscious, PIN pad systems that do not have any logging or monitoring capability can be purchased for a reasonable price. Following are some of the characteristics of swipe card and PIN pad systems:

- **Moderately expensive:** Some systems, particularly those with management capabilities, are quite expensive.
- **Enhanced controls and logging:** Each time people enter the server room, they must key in a number or use a swipe card. This process enables systems to log who enters and when.
- **Some additional knowledge required:** Swipe card systems need special software and hardware that can configure the cards. Someone has to learn how to configure them.

## Biometrics

Although they might still seem like the realm of James Bond, biometric security systems are becoming far more common. Biometric systems work by using some unique characteristic of a person's identity—such as a fingerprint, a palm print, or a retina scan—to validate that person's identity.

Although the price of biometric systems has been falling over recent years, they are not widely deployed in small to midsized networks. Not only are the systems themselves expensive, but also their installation, configuration, and

maintenance must be considered. Following are some of the characteristics of biometric access control systems:

- **Very effective:** Because each person entering the room must supply proof-of-person evidence, verification of the person entering the server area is as close to 100 percent reliable as you can get.
- **Nothing to lose:** Because there are no cards or keys, nothing can be lost.
- **Expensive:** Biometric security systems and their attendant scanners and software are still relatively expensive and can be afforded only by organizations that have a larger budget; however, prices are sure to drop as more people turn to this method of access control.

# Two-Factor and Multifactor Authentication

When two or more access methods are included as part of the authentication process, you're implementing a *multifactor system*. A system that uses any two items—such as smartcards and passwords—is referred to as a *two-factor authentication* system. A multifactor system can consist of a two-factor system, a three-factor system, and so on. As long as more than one factor is involved in the authentication process, it is considered a multifactor system.

For obvious reasons, the two or more factors employed should not be from the same category. Although you do increase difficulty in gaining system access by requiring the user to enter two sets of username/password combinations, it is preferred to pair a single username/password combination with a biometric identifier or other check.

> **Note**
>
> Be sure that you understand that two-factor authentication is a subset of multifactor authentication.

# Secured Versus Unsecured Protocols

As you know, any network needs a number of protocols to function. This includes both LAN and WAN protocols. Not all protocols are created the same, however. Some are designed for secure transfer, whereas others are not. Table 9.1 lists several protocols and describes their use.

TABLE 9.1 **Protocol Summary**

| Protocol | Name | Description |
|---|---|---|
| FTP | File Transfer Protocol | A protocol for uploading and downloading files to and from a remote host. It also accommodates basic file management tasks. FTP uses ports 20 and 21. |
| SFTP | Secure File Transfer Protocol | A protocol for securely uploading and downloading files to and from a remote host. It is based on SSH security. SFTP uses port 22. |
| HTTP | Hypertext Transfer Protocol | A protocol for retrieving files from a web server. Data is sent in clear text. HTTP uses port 80. |
| HTTPS | Hypertext Transfer Protocol Secure | A secure protocol for retrieving files from a web server. HTTPS uses SSL to encrypt data between the client and host. HTTPS uses port 443. |
| Telnet | Telnet | A protocol that enables sessions to be opened on a remote host. Telnet is not considered secure. Telnet uses port 23. |
| SSH | Secure Shell | A secure alternative to Telnet that enables secure sessions to be opened on a remote host. SSH uses port 22. |
| TLS | Transport Layer Security | A cryptographic protocol whose purpose is to verify that secure communications between a server and a client remain secure. TLS is an enhancement/replacement for SSL. |
| ISAKMP | Internet Security Association and Key Management Protocol | A protocol that provides an independent framework for authentication and key exchange. The actual implementation is usually done by IPSec but could be handled by any implementation capable of negotiating, modifying, and deleting security associations. |
| RSH | A UNIX utility used to run commands on a remote machine | A utility that has been replaced by SSH because RSH sends all data in clear text. |
| SCP | Secure Copy Protocol | A protocol that enables files to be securely copied between two systems. It uses SSH technology to provide encryption services. |
| RCP | Remote Copy Protocol | A protocol that copies files between systems, but transport is not secured. |
| SNMPv1/2 | Simple Network Management Protocol versions 1 and 2 | A network monitoring system used to monitor the network's condition. Both SNMPv1 and v2 are not secured. |

| Protocol | Name | Description |
|---|---|---|
| SNMPv3 | Simple Network Management Protocol version 3 | An enhanced SNMP service offering both encryption and authentication services. |
| IPSec | IP security | IP security that encrypts data during communication between two computers. |
| SLIP | Serial Line Interface Protocol | A protocol that provides basic encapsulation of the IP protocol over serial and modem connections. |

ExamAlert

You will most certainly be asked questions on secure protocols and when they might be used. Review Table 9.1 before taking the Network+ exam.

# Hardening Best Practices

In addition to physically securing network devices and opting to run secure protocols in favor of unsecured ones, an administrator should take the following best practices steps to further network hardening:

- **Utilize Secure SNMP:** The Simple Network Management Protocol (SNMP) collects a lot of data that could be of value to someone looking to compromise a network. Secure SNMP, utilizing SNMPv3, protects the data more by moving from ports 161 and 162 to 10161 and 10162 and enables secure authentication and communication between the SNMP manager and agent.
- **Configure Router Advertisement guard:** With IPv6, routers will send out multicast messages (router advertisements) to announce their availability and associated information. This information is used by Neighbor Discovery Protocol (NDP) to detect what is available and configure accordingly. A problem is that the messages are unsecured, making them susceptible to spoofing. To increase security, you can configure IPv6 *Router Advertisement (RA) guard* to protect the network against RA messages generated by unauthorized routers (rogues) trying to join the network.
- **Employ Port Security and Dynamic ARP:** *Port security* works at Layer 2 of the OSI model and allows an administrator to configure switch ports so that only certain MAC addresses can use the port. This is a common feature on both Cisco's Catalyst as well as Juniper's EX Series switches and essentially differentiates so-called dumb switches from managed

(or intelligent) switches. Similarly, *Dynamic ARP Inspection (DAI)* works with these and other smart switches to protect ports from ARP spoofing.

- **Implement Control Plane Policing:** Many routers and switches include a Control Plane Policing feature that enables you to configure a quality of service (QoS) filter to protect against DoS attacks. When enabled, the control plane (CP) can continue to forward packets despite an attack or abnormally heavy traffic load on the router/switch.
- **Use private VLANs:** Also known as port isolation, creating a *private VLAN* is a method of restricting switch ports (now called private ports) so that they can communicate only with a particular uplink. The private VLAN usually has numerous private ports and only one uplink, which is usually connected to a router, or firewall.
- **Disable unneeded ports:** Disabling unnecessary services (mentioned next) increases security by removing doors that someone could use to enter the server. Similarly, IP ports that are not needed for devices also represent doors that could be used to sneak in. It is highly recommended that unused ports be disabled to increase security along with device ports (both physical and virtual ports).
- **Disable unneeded services:** Every unnecessary service that is running on a server is akin to another door on a warehouse that someone unauthorized may choose to sneak in. Just as an effective way to secure a warehouse is to reduce the number of doors to only those needed, so too is it recommended that a server be secured by removing (disabling) services not in use.
- **Change default passwords:** The easiest way for any unauthorized individual to access a device is to use the default credentials. Many routers, for example, come configured with an "admin" account and a simple value for the password ("admin," "password," and so on). Anyone owning one of those routers knows those values and could use them to access any other of the same make if the values have not been changed. To make it more difficult for unauthorized users to access your devices, change those default usernames and passwords as soon as you start using them.
- **Avoid common passwords and increase complexity:** It is a good thing to preach password security to users, but often administrators are guilty of using too-simplistic passwords on network devices such as routers, switches, and the like. Given the large number of devices in question, sometimes the same passwords are also used on multiple devices. Common sense tells every administrator that this approach is wrong, but often it is done anyway with the hope that no miscreant will try to gain unauthorized access. Don't be that administrator: use complex passwords, with notable

length, and use a different password for each device, increasing the overall security of your network.

- **Enable DHCP snooping:** As was mentioned when discussing rogue DHCP servers earlier in this chapter, DHCP snooping is a good thing. It provides a way for a switch to look at packets and drop DHCP traffic that it determines to be unacceptable based on a set of defined rules to prevent rogue DHCP servers from offering IP addresses to clients.
- **Change the default VLAN:** On switches, the native VLAN is the only VLAN that is not tagged in a trunk. This means that native VLAN frames are transmitted unchanged. By default, the native VLAN is port 1, and that default represents a weakness in that it is something known about your network that an attacker could use. To strengthen security, albeit a small amount, you can change the native VLAN to another port. The command or commands used to do so are dependent on the vendor and model of your switch but can be easily found online.
- **Utilize patch and firmware management:** There is a reason why each firmware update is written. Sometimes, it is to optimize the device or make it more compatible with other devices. Other times, it is to fix security issues and/or head off identified problems. Keep firmware on your production machines current after first testing the upgrades on lab machines and verifying that you're not introducing any unwanted problems by installing. Just as firmware upgrades are intended to strengthen or solve problems, patches and updates do the same with software (including operating systems). Test each release on a lab machine(s) to make sure you are not adding to network woes, and then keep your software current to harden it.
- **Put an access control list in place:** Discussed at length in this chapter, access control is necessary to limit who can access resources to only those who should have access and thus protect those resources. *Access control lists (ACLs)* enable devices in your network to ignore requests from specified users or systems or to grant them access to certain network capabilities. You may find that a certain IP address is constantly scanning your network, and you can block this IP address at the router and the IP address will automatically be rejected any time it attempts to utilize your network.
- **Apply role-based access:** It is recommended that role-based access be applied where possible. The difference between this approach and others was discussed earlier in this chapter.
- **Enforce firewall rules:** Firewall rules are used to dictate what traffic can pass between the firewall and the internal network. Three possible

actions can be taken based on the rule's criteria: block the connection (*explicit deny*), accept the connection, or allow the connection if conditions are met (such as it being secured). It is this last condition that is the most difficult to configure, and conditions usually end with an implicit deny clause. An *implicit deny* clause means that if the proviso in question has not been explicitly granted, access is denied.

> **Note**
>
> Where it exists, an explicit deny takes precedence over all other settings

- **Verify file hashes:** File hashing is used to verify that the contents of files are unaltered. A hash is often created on a file before it is downloaded and then hashed after the download so the two values can be compared to make sure the contents are the same. When downloading files—particularly upgrades, patches, and updates—check hash values and use this one test to keep from installing those entities that have had Trojan horses attached to them.
- **Generate new keys:** Keys are used as a part of the encryption process, particularly with public key infrastructure (PKI), to encrypt and decrypt messages. The longer you use the same key, the longer the opportunity becomes for someone to crack that key. To increase security, generate new keys on a regular basis: The commands to do so will differ based on the utility that you are creating the keys for.

> **ExamAlert**
>
> Most of the items appearing in the preceding list are the topics beneath objective 4.3; make sure you know them for the exam.

# Wireless Security

Wireless systems transmit data through the air and can be much more difficult to secure than those dependent on wires that can be physically protected. The growth of wireless systems in every workplace and home creates many opportunities for attackers looking for signals that can be easily intercepted. This section discusses various types of wireless systems that you'll likely encounter and some of the security issues associated with this technology.

## MAC Filtering

To increase wireless security, some APs enable you to configure MAC address filtering and guest access. MAC address filtering enables you to limit access to only those specified hosts. Guest access uses a different password and network name and enables visitors to use the Internet without having access to the rest of the network (thus avoiding your data and computers).

**ExamAlert**

Make sure that you understand the purpose of MAC address filtering and that this works the same whether the network is wired or wireless.

## Antenna Placement and Power Levels

Antenna placement can be crucial in allowing clients to reach the access point. There isn't a universal solution to this issue, and it depends on the environment in which the access point is placed. As a general rule, the greater the distance the signal must travel, the more it will attenuate, but you can lose a signal quickly over a short distance as well if the building materials reflect or absorb the signal. You should try to avoid placing access points near metal (which includes appliances) or near the ground. Placing them in the center of the area to be served and high enough to get around most obstacles is recommended. On the chance that the signal is actually traveling too far, some access points include *power level* controls, which allow you to reduce the amount of output provided. Both a heat map and a site survey can be used to optimize wireless antenna placement.

## Isolation

As the name implies, *isolation* is the process of keeping something from communicating with others. This can be done on a wireless network with a single client (*wireless client isolation*) or a guest network (*guest network isolation*). With the latter, the guest user cannot see any other connected devices even though they are logged in to the network. Most wireless routers allow for creating a private network in each frequency and thus enabling temporary users (guests) to access the Internet and their own files without jeopardizing the rest of the network's resources.

## Preshared Keys

During the authentication process, keyed security measures are applied before communication can take place. On many APs, authentication can be set to

either *shared* key authentication or *open* authentication. The default setting for older APs typically is open authentication. Open authentication enables access with only the SSID and/or the correct WEP key for the AP. The problem with open authentication is that if you do not have other protection or authentication mechanisms in place, your wireless network is totally open to intruders. When set to shared key mode, the client must meet security requirements before communication with the AP can occur.

Shared key mode requires that a WEP key be configured on both the client system and the AP. This makes authentication with WEP-Shared mandatory, so it is more secure for wireless transmission. WPA-PSK, the acronym for *Wi-Fi Protected Access with Preshared Key*, is a stronger form of encryption in which keys are automatically changed and authenticated between devices after a specified period of time or after a specified number of packets have been transmitted.

> **Note**
>
> One implementation of WPA is known as WPA2 Personal. This implementation uses a preshared key (PSK), whereas WPA2 Enterprise needs an authentication server. WPA3 is a newer standard in use today, and it uses Simultaneous Authentication of Equals (SAE) instead of PSK, enabling users to choose easier-to-remember passwords. An additional benefit is that by using forward secrecy, WPA3 does not compromise traffic already transmitted even if the password itself becomes compromised.

## Geofencing

Any wireless technology, but usually GPS and sometimes RFID, can be used to create a virtual geographic boundary. This boundary is called a *geofence*. After that boundary is defined, software can be used to trigger a response when a device enters or leaves that area. A section of a supermarket, for example, can be configured to text a coupon code to iPhones for a percentage off milk purchases to any phone coming within 10 feet of the dairy section.

Similar technology can be used to take attendance in a classroom, at a meeting location, and so on. Because events can be triggered for not only entering a zone but also leaving it, this technology could be used to send a message to parents if a child leaves the virtually defined neighborhood, and so on. Still in its infancy, geofencing technology is expected to grow in acceptance and application over the next few years.

ExamAlert

Remember that the goal of geofencing is to have a defined boundary and then be able to respond to what either enters or leaves that area.

## Captive Portal

As you might recall from Chapter 6, "Wireless Solutions and Issues," most public networks, including Wi-Fi hotspots, use a *captive portal*, which requires users to agree to some condition before they use the network or Internet. The condition could be to agree to the acceptable use policy, payment charges for the time they are using the network, and so forth.

One of the most popular implementations of captive portals is a Cisco application in its Identity Services Engine. However, there have been vulnerabilities identified with it, which enable attackers to intercept clear-text values.

# IoT Access Considerations

With so many sensors being added to networks today, the Internet of Things (IoT) opens up a can of networking opportunities, but each comes with its own set of security issues. From the standpoint of a network administrator, it is critical that you treat these devices the same as any other resource connected to the network, constantly keep abreast of discovered security vulnerabilities, and patch when/where needed.

# Cram Quiz

1. Which of the following is used to verify that the contents of files are unaltered?
   - ❍ **A.** Key generation
   - ❍ **B.** File hashing
   - ❍ **C.** Biometrics
   - ❍ **D.** Asset tracking

2. Which of the following is a secure alternative to Telnet that enables secure sessions to be opened on a remote host?
   - ❍ **A.** SSH
   - ❍ **B.** RSH
   - ❍ **C.** IPSec
   - ❍ **D.** RDP

3. Which of the following can be used to limit access to only one or two people going into the facility at a time?
   - ❍ **A.** Access control vestibule
   - ❍ **B.** Min cage
   - ❍ **C.** Tholian web
   - ❍ **D.** Cloud minder

4. Which of the following systems use a credit card–sized plastic card that is read by a reader on the outside of the door?
   - ❍ **A.** Contiguity reader
   - ❍ **B.** Key fob
   - ❍ **C.** Swipe card
   - ❍ **D.** Cipher lock

5. Which of the following are considered hardening best practices? (Choose three.)
   - ❍ **A.** Utilize SNMPv2.
   - ❍ **B.** Disable unneeded ports.
   - ❍ **C.** Disable unneeded services.
   - ❍ **D.** Change default passwords.

# Cram Quiz Answers

1. **B.** File hashing is used to verify that the contents of files are unaltered.
2. **A.** SSH is a secure alternative to Telnet that enables secure sessions to be opened on a remote host. SSH uses port 22.
3. **A.** An access control vestibule can be used to limit access to only one or two people going into the facility at a time.
4. **C.** Swipe card systems use a credit card–sized plastic card read by a reader on the outside of the door. To enter the server room, you must swipe the card (run it through the reader), at which point it is read by the reader, which validates it.
5. **B, C, and D.** It is highly recommended that unused ports be disabled to increase security along with device ports (both physical and virtual ports). It is also recommended that a server be secured by removing (disabling) services not in use. To make it more difficult for unauthorized users to access your devices, change default usernames and passwords as soon as you start using them. SNMPv2 is not secure. SNMPv3 should be used in its place.

# Remote-Access Methods

▶ **Compare and contrast remote-access methods and security implications.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. True or false: VPNs require a secure protocol to safely transfer data over the Internet.
2. What port does SSH use for connections?
3. Which tunneling mode encrypts all requests through the VPN regardless of where the service is hosted ?
4. What port does Telnet use for connections?

### Answers

1. True. VPNs require a secure protocol, such as IPSec or TLS, to safely transfer data over the Internet.
2. SSH uses port 22 and TCP for connections.
3. Full tunnel mode encrypts all requests through the VPN regardless of where the service is hosted.
4. Telnet uses port 23 for connections.

Several protocols are associated with remote-control access that you should be aware of: Remote Desktop Protocol (RDP), Secure Shell (SSH), Virtual Network Computing (VNC), and Telnet. RDP is used in a Windows environment and is now called *Remote Desktop Services (RDS)*. It provides a way for a client system to connect to a server, such as Windows Server, and, by using RDP, operate on the server as if they were local client applications. Such a configuration is known as *thin client computing*, whereby client systems use the resources of the server instead of their local processing power.

Windows products (server as well as client) have built-in support for Remote Desktop Connections. The underlying protocol used to manage the connection is RDP. RDP is a low-bandwidth protocol used to send mouse movements, keystrokes, and bitmap images of the screen on the server to the client computer. RDP does not actually send data over the connection—only screenshots and client keystrokes. RDP uses TCP and UDP port 3389.

Building on RDP, a *Remote Desktop Gateway* offers an RDP-type of HTTPS VPN service over TCP 443 and UDP 3391. This allows users from outside the corporate firewall to connect to internal network resources (such as a work computer) from a remote device (Windows PC, Mac, tablet, smartphone, etc.) using Microsoft's Remote Desktop connection. The benefit of a remote desktop gateway is that it increases security by encapsulating the session with TLS and does not require a VPN.

SSH is a tunneling protocol originally created for UNIX/Linux systems. It uses encryption to establish a secure connection between two systems and provides alternative, security-equivalent applications for such utilities as Telnet, File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), and other communications-oriented applications. Although it is available with Windows and other operating systems, it is the preferred method of security for Telnet and other clear-text-oriented programs in the UNIX/Linux environment. SSH uses port 22 and TCP for connections.

*Virtual Network Computing (VNC)* enables remote login, in which clients can access their own desktops while being physically away from their computers. By default, it uses port 5900, and it is not considered overly secure.

Telnet enables sessions to be opened on a remote host and is one of the oldest TCP/IP protocols still in use today. On most systems, Telnet is blocked because of problems with security (it truly does not have any), and SSH is considered a secure alternative to Telnet that enables secure sessions to be opened on the remote host.

**ExamAlert**

Be sure that you know the ports associated with RDP (3389), Telnet (23), FTP (20, 21), VNC (5900), and SSH (22).

**ExamAlert**

The protocols described in this chapter enable access to remote systems and enable users to run applications on the system, using that system's resources. Only the user interface, keystrokes, and mouse movements transfer between the client system and the remote computer.

# Remote File Access

*File Transfer Protocol (FTP)* is an application that allows connections to FTP servers for file uploads and downloads. FTP is a common application that uses ports 20 and 21 by default. It is used to transfer files between hosts on the Internet but is inherently insecure. A number of options have been released to try to create a more secure protocol, including *FTP over SSL (FTPS)*, which adds support for SSL cryptography, and *SSH File Transfer Protocol (SFTP)*, which is also known as Secure FTP.

An alternative utility for copying files is Secure Copy (SCP), which uses port 22 by default and combines an old remote copy program (RCP) from the first days of TCP/IP with SSH.

On the opposite end of the spectrum from a security standpoint is the *Trivial File Transfer Protocol (TFTP)*, which can be configured to transfer files between hosts without any user interaction (unattended mode). It should be avoided anywhere there are more secure alternatives.

# VPNs

A *virtual private network (VPN)* encapsulates encrypted data inside another datagram that contains routing information. The connection between two computers establishes a switched connection dedicated to the two computers. The encrypted data is encapsulated inside *Point-to-Point Protocol (PPP)*, and that connection is used to deliver the data.

A VPN enables users with an Internet connection to use the infrastructure of the public network to connect to the main network and access resources as if they were logged on to the network locally. It also enables two networks to be connected to each other securely.

To put it more simply, a VPN extends a LAN by establishing a remote connection using a public network such as the Internet. A VPN provides a point-to-point dedicated link between two points over a public IP network. For many companies, the VPN link provides the perfect method to expand their networking capabilities and reduce their costs. By using the public network (Internet), a company does not need to rely on expensive private leased lines to provide corporate network access to its remote users. Using the Internet to facilitate the remote connection, the VPN enables network connectivity over a possibly long physical distance. In this respect, a VPN is a form of wide-area network (WAN).

**Note**

Many companies use a VPN to provide a cost-effective method to establish a connection between remote clients and a private network. There are other times a VPN link is handy. You can also use a VPN to connect one private LAN to another, known as LAN-to-LAN internetworking. For security reasons, you can use a VPN to provide controlled access within an intranet. As an exercise, try drawing what the VPN would look like in these two scenarios.

## Components of the VPN Connection

A VPN enables anyone with an Internet connection to use the infrastructure of the public network to dial in to the main network and access resources as if the user were locally logged on to the network. It also enables two networks to securely connect to each other.

Many elements are involved in establishing a VPN connection, including the following:

- **VPN client:** This computer initiates the connection to the VPN server.
- **VPN server:** This server authenticates connections from VPN clients.
- **Access method:** As mentioned, a VPN is most often established over a public network such as the Internet; however, some VPN implementations use a private intranet. The network used must be IP based.
- **VPN protocols:** These protocols are required to establish, manage, and secure data over the VPN connection. Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) are commonly associated with VPN connections. These protocols enable authentication and encryption in VPNs. Authentication enables VPN clients and servers to correctly establish the identity of people on the network. Encryption enables potentially sensitive data to be guarded from the general public.

VPNs have become popular because they enable the public Internet to be safely used as a WAN connectivity solution.

**ExamAlert**

VPNs support analog modems, Integrated Services Digital Network (ISDN) wireless connections, and dedicated broadband connections, such as cable and digital subscriber line (DSL). Remember these details for the exam.

## VPN Connection Types

Two types of client-to-site VPN connections are possible: full tunnel and split tunnel. When full tunnel is used, all requests through the VPN are encrypted regardless of where the service is hosted, and it is not possible to access local network resources. With split tunnel, all incoming requests are encrypted over the VPN, but traffic going to sites outside the client network (including Zoom, Office 365, Google) does not go through the VPN server. Full tunnel is more secure and generally recommended.

When a choice between the two exists, it is recommended that you use full tunnel if you are connecting from an untrusted network such as in a coffee shop or hotel. While split tunnel may be necessary if there is a need to access both local resources and the organization's resources, you should always recognize that it is less secure, so a better option is to disconnect from the VPN first before accessing those other sites.

## VPN Pros and Cons

As with any technology, VPN has both pros and cons. Fortunately with VPN technology, these are clear cut, and even the cons typically do not prevent an organization from using VPNs in its networks. Using a VPN offers two primary benefits:

- **Cost:** If you use the infrastructure of the Internet, you do not need to spend money on dedicated private connections to link remote clients to the private network. Furthermore, when you use the public network, you do not need to hire support personnel to support those private links.
- **Easy scalability:** VPNs make it easy to expand the network. Employees who have a laptop with wireless capability can simply log on to the Internet and establish the connection to the private network.

Table 9.2 outlines some of the advantages and potential disadvantages of using a VPN.

TABLE 9.2 **Pros and Cons of Using a VPN**

| Advantage | Description |
|---|---|
| Reduced cost | When you use the Internet, you do not need to rent dedicated lines between remote clients and a private network. In addition, a VPN can replace remote-access servers and long-distance dial-up network connections that were commonly used in the past by business travelers who needed access to their company intranet. This way, you eliminate long-distance phone charges. |

| Advantage | Description |
|---|---|
| Network scalability | The cost to an organization to build a dedicated private network may be reasonable at first, but it increases exponentially as the organization grows. The Internet enables an organization to grow its remote client base without having to increase or modify an internal network infrastructure. |
| Reduced support | Using the Internet, organizations do not need to employ support personnel to manage a VPN infrastructure. |
| Simplicity | With a VPN, a network administrator can easily add remote clients. All authentication work is managed from the VPN authentication server, and client systems can be easily configured for automatic VPN access. |
| **Disadvantage** | **Description** |
| Security | Using a VPN, data is sent over a public network, so data security is a concern. VPNs use security protocols to address this shortcoming, but VPN administrators must understand data security over public networks to ensure that data is not tampered with or stolen. |
| Reliability | The reliability of the VPN communication depends on the public network and is not under an organization's direct control. Instead, the solution relies on an Internet service provider (ISP) and its quality of service (QoS). |

## IPSec

The *IP Security (IPSec)* protocol is designed to provide secure communications between systems. This includes system-to-system communication in the same network, as well as communication to systems on external networks. IPSec is an IP layer security protocol that can both encrypt and authenticate network transmissions. In a nutshell, IPSec is composed of two separate protocols: *Authentication Header (AH)* and *Encapsulating Security Payload (ESP)*. AH provides the authentication and integrity checking for data packets, and ESP provides encryption services.

**ExamAlert**

IPSec relies on two underlying protocols: AH and ESP. AH provides authentication services, and ESP provides encryption services.

Using both AH and ESP, data traveling between systems can be secured, ensuring that transmissions cannot be viewed, accessed, or modified by those who should not have access to them. It might seem that protection on an internal network is less necessary than on an external network; however, much of the

data you send across networks has little or no protection, allowing unwanted eyes to see it.

> **Note**
>
> The Internet Engineering Task Force (IETF) created IPSec, which you can use on both IPv4 and IPv6 networks.

IPSec provides three key security services:

- **Data verification:** Verifies that the data received is from the intended source
- **Protection from data tampering:** Ensures that the data has not been tampered with or changed between the sending and receiving devices
- **Private transactions:** Ensures that the data sent between the sending and receiving devices is unreadable by any other devices

IPSec operates at the network layer of the Open Systems Interconnection (OSI) reference model and provides security for protocols that operate at the higher layers. Thus, by using IPSec, you can secure practically all TCP/IP-related communications.

## SSL/TLS/DTLS

Security is often provided by working with the Transport Layer Security (TLS) protocol (which has replaced Secure Sockets Layer in most implementations). SSL VPN, also marketed as WebVPN and OpenVPN, can be used to connect locations that would run into trouble with firewalls and NAT when used with IPSec. It is known as an SSL VPN whether the encryption is done with TLS or truly with the older SSL.

> **Note**
>
> SSL was first created for use with the Netscape web browser and is used with a limited number of TCP/IP protocols (such as HTTP and FTP). TLS is not only an enhancement to SSL but also a replacement for it, working with almost every TCP/IP protocol. Because of this, TLS is popular with VPNs and VoIP applications. Just as the term *Kleenex* is often used to represent any paper tissue, whether or not it is made by Kimberly-Clark, *SSL* is often the term used to signify the confidentiality function, whether it is actually SSL in use or TLS (the latest version of which is 1.2).

The Datagram Transport Layer Security (DTLS) protocol is a derivation of SSL/TLS by the OpenSSL project; it provides the same security services but strives to increase reliability.

The National Institute of Standards and Technology (NIST) publishes the *Guide to SSL VPNs*, which you can access at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf.

## Site-to-Site and Client-to-Site

The scope of a VPN tunnel can vary, with the two most common variations being *site-to-site* and *client-to-site* (also known as *host-to-site*). A third variation is *host-to-host*, but it is really a special implementation of site-to-site. In a site-to-site implementation, as the name implies, whole networks are connected together. An example would be divisions of a large company. Because the networks are supporting the VPN, each gateway does the work, and the individual clients do not need to have any VPN.

In a client-to-site scenario, individual clients (such as telecommuters or travelers) connect to the network remotely. Because the individual client makes a direct connection to the network, each client doing so must have VPN client software installed.

**ExamAlert**

Be sure that you understand that site-to-site and client-to-site are the two most common types of VPNs.

## Virtual Desktops

What is called a *virtual desktop* can differ from vendor to vendor, but generally it is a preconfigured image of an operating system and applications wherein the desktop environment is separated from the physical device used to access it. The virtual desktop can be accessed remotely (thin clients were mentioned earlier in this section), and any endpoint device (laptop, tablet, smartphone, etc.) can be used.

Upon connecting, the virtual desktop provider installs the necessary client software on the endpoint device, and the user then interacts with that software on the device with it looking like a physical workstation. Depending on the type of implementation and configuration, users may or may not be able to save changes or permanently install applications, but they experience their desktop

the same way every time they log in, no matter which device they are logging in from.

Virtual desktops differ from virtual machines in that the operating system for the virtual desktop lives in the data center, and not the endpoint. Typically, the virtual desktop is running within a virtual machine housed at the cloud host data center.

# HTTPS/Management URL

HTTP Secure (HTTPS) is the protocol used for "secure" web pages that users should see when they must enter personal information such as credit card numbers, passwords, and other identifiers. It combines HTTP with SSL/TLS to provide encrypted communication. The default port is 443, and the URL begins with https:// instead of http://.

HTTPS is the common protocol used for management URLs to perform tasks such as checking server status, changing router settings, and so on.

# Authentication and Authorization Considerations

When implementing remote access, administrators must recognize that they are increasing risk. The safest network to secure is one without users. The next safest is one in which all users must physically be present within a confined area. Once you open the network up to users from anywhere, you increase the risks of harm to data and security violations. In all cases, administrators should attempt to mitigate these risks as much as possible, and this is particularly true when it comes to authentication and authorization.

Throughout much of this chapter, the discussion has been on security and how to increase it, and thus, there is little new to add here other than to reiterate the importance of authenticating users (using multifactor authentication) and focusing on the CIA security triad—confidentiality, integrity, and availability. You should take every reasonable measure to prevent unauthorized users from accessing data, and, similarly, you should take every reasonable step to make sure that the data and systems are available for authorized users all the time.

# Out-of-Band Management

When a dedicated channel is established for managing network devices, it is known as *out-of-band management*. A connection can be established via a console

router, or modem, and this can be used to ensure management connectivity independent of the status of *in-band* network connectivity (which would include serial port connections, VNC, and SSH). Out-of-band management lets administrators monitor, access, and manage network infrastructure devices remotely and securely, even when everything else is down.

## Cram Quiz

1. Which of the following protocols is used in thin-client computing?
   - ❍ **A.** RDP
   - ❍ **B.** PPP
   - ❍ **C.** PPTP
   - ❍ **D.** RAS

2. Your company wants to create a secure tunnel between two networks over the Internet. Which of the following protocols would you use to do this?
   - ❍ **A.** SSH
   - ❍ **B.** RDP
   - ❍ **C.** PPTP
   - ❍ **D.** SLAP

3. Because of a recent security breach, you have been asked to design a security strategy that will allow data to travel encrypted through both the Internet and intranet. Which of the following protocols would you use?
   - ❍ **A.** IPSec
   - ❍ **B.** SST
   - ❍ **C.** CHAP
   - ❍ **D.** FTP

4. By default, which TCP port is used by the remote desktop gateway service?
   - ❍ **A.** 110
   - ❍ **B.** 443
   - ❍ **C.** 3389
   - ❍ **D.** 3391

5. By default, which port is used by Virtual Network Computing (VNC)?
   - ❍ **A.** 143
   - ❍ **B.** 583
   - ❍ **C.** 8911
   - ❍ **D.** 5900

## Cram Quiz Answers

1. **A.** RDP is used in thin-client networking, where only screen, keyboard, and mouse input is sent across the line. PPP is a dialup protocol used over serial links. PPTP is a technology used in VPNs. RAS is a remote-access service.
2. **C.** To establish the VPN connection between the two networks, you can use PPTP. SSH and RDP are not used to create a point-to-point tunnel. SLAP is not a valid secure protocol.
3. **A.** IPSec is a nonproprietary security standard used to secure transmissions both on the internal network and when data is sent outside the local LAN. IPSec provides encryption and authentication services for data communications. SST is not a valid protocol. Challenge Handshake Authentication Protocol (CHAP) is a remote-access authentication protocol. FTP is incorrect because it is a protocol used for large data transfers, typically from the Internet.
4. **B.** By default, remote desktop gateway uses TCP port 443 (and UDP port 3391) to handle communication between the gateway server and the client.
5. **D.** By default, virtual network computing uses port 5900 to enable remote login.

# What's Next?

The final chapter of this book, "Network Troubleshooting," focuses on all areas of network troubleshooting, including troubleshooting best practices and some of the tools and utilities you use to assist in the troubleshooting process.

No matter how well a network is designed and how many preventive maintenance schedules are in place, troubleshooting is always necessary. Consequently, network administrators must develop those troubleshooting skills.

CHAPTER 10

# Network Troubleshooting

**This chapter covers the following official Network+ objectives:**

- Explain the network troubleshooting methodology.
- Given a scenario, use the appropriate network software tools and commands.
- Given a scenario, troubleshoot general networking issues.

This chapter covers CompTIA Network+ objectives 5.1, 5.3, and 5.5. For more information on the official Network+ exam topics, see the "About the Network+ Exam" section in the Introduction.

Many duties and responsibilities fall under the umbrella of network administration. Of these, one of the most practiced is that of troubleshooting. No matter how well a network is designed and how many preventive maintenance schedules are in place, troubleshooting is always necessary. Therefore, network administrators and technicians must develop those troubleshooting skills.

This chapter focuses on all areas of troubleshooting, including troubleshooting best practices and some of the tools and utilities you can use to assist in the troubleshooting process.

# Troubleshooting Steps and Procedures

- **Explain the network troubleshooting methodology.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What are the key sources from which you can gain information about a computer problem?
2. What is the final step in the network troubleshooting methodology CompTIA expects test takers to follow?

### Answers

1. It is important to get as much information as possible about the problem. You can glean information from three key sources: the computer (in the form of logs and error messages), the computer user experiencing the problem, and your own observation.
2. Document the findings, actions, outcomes, and lessons learned.

Regardless of the problem, effective network troubleshooting follows some specific steps. These steps provide a framework in which to perform the troubleshooting process. When you follow them, they can reduce the time it takes to isolate and fix a problem. The following sections discuss the common troubleshooting steps and procedures as identified by the CompTIA Network+ objectives:

1. Identify the problem.
   - Gather information.
   - Question users.
   - Identify symptoms.
   - Determine if anything has changed.
   - Duplicate the problem, if possible.
   - Approach multiple problems individually.

2. Establish a theory of probable cause.
   - Question the obvious.
   - Consider multiple approaches:
     - Top-to-bottom/bottom-to-top OSI model.
     - Divide and conquer.
3. Test the theory to determine the cause:
   - If the theory is confirmed, determine the next steps to resolve the problem.
   - If the theory is not confirmed, reestablish a new theory or escalate.
4. Establish a plan of action to resolve the problem and identify potential effects.
5. Implement the solution or escalate as necessary.
6. Verify full system functionality and, if applicable, implement preventive measures.
7. Document findings, actions, outcomes, and lessons learned.

**ExamAlert**

You should expect questions asking you to identify the troubleshooting methodology steps in exact order.

# Identify the Problem

The first step in the troubleshooting process is to establish exactly what the problem is. This stage of the troubleshooting process is all about gathering information, identifying symptoms, questioning users, and determining if anything has changed. To get this information, you need knowledge of the operating system used, good communication skills, and a little patience. You need to get as much information as possible about the problem. You can glean information from three key sources: the computer (in the form of logs and error messages), the computer user experiencing the problem, and your own observation.

After you have listed the symptoms, you can begin to identify some of the potential causes of those symptoms.

**ExamAlert**

You do not need to know where error messages are stored on an operating system. You need to know only that the troubleshooting process requires you to read system-generated log errors.

## Identify Symptoms

Some computer problems are isolated to a single user in a single location; others affect several thousand users spanning multiple locations. Establishing the affected area is an important part of the troubleshooting process, and it often dictates the strategies you use to resolve the problem.

**ExamAlert**

You might be provided with either a description of a scenario or a description augmented by a network diagram. In either case, you should carefully read the description of the problem, step by step. In most cases, the correct answer is fairly logical, and the wrong answers can be easily identified.

Problems that affect many users are often connectivity issues that disable access for many users. Such problems often can be isolated to wiring closets, network devices, and server rooms. The troubleshooting process for problems that are isolated to a single user often begins and ends at that user's workstation. The trail might indeed lead you to the wiring closet or server, but that is probably not where the troubleshooting process began. Understanding who is affected by a problem can give you the first clues about where the problem exists. For example, a change in Dynamic Host Configuration Protocol (DHCP) scope (or an exhausted scope) by a new administrator might affect several users, whereas a user playing with the TCP/IP settings of a single computer can affect only that person.

## Determine Whether Anything Has Changed

Whether there is a problem with a workstation's access to a database or an entire network, they were working at some point. Although many people claim that their computer "just stopped working," that is unlikely. Far more likely is that changes to the system or network have caused the problem. Look for newly installed applications, applied patches or updates, new hardware, a physical move of the computer, or a new username and password. Establishing any recent changes to a system can often lead you in the right direction to isolate and troubleshoot a problem.

## Duplicate the Problem if Possible

Every problem has a cause and determining the cause of a problem is key to preventing it from happening again with either this machine or another. One was to know that you have identified the cause is to be able to duplicate the problem. The sole reason for duplicating the problem should be to verify that you have, indeed, found the cause so that you can then take steps to make certain that cause never becomes an issue again. As an example, if the cause of the problem turns out to be a new patch for an application not working properly with a particular operating system, you will want to make sure that that patch/OS combination is not implemented again (steps to consider would include updating the OS, installing only some of the patch, and so on).

## Approach Multiple Problems Individually

One of the toughest situations to tackle is having to deal with more than one problem (a particular workstation won't load Application A, can't print from Application B, and so on). When this is the case, the only way to be able to solve the problems is to address each one individually. Problems should be ranked in order of importance (based on criteria such as business necessity) and solved in that order.

# Establish a Theory of Probable Cause

**ExamAlert**

When approaching a problem, start by questioning the obvious. If that fails, consider ways to tackle the issue from multiple approaches. Consider using a top-to-bottom or bottom-to-top model approach (such as working through the OSI model stack) and assigning any coworkers you have to divide and conquer the problem.

A single problem on a network can have many causes, but with appropriate information gathering, you can eliminate many of them. When you look for a probable cause, it is often best to look at the easiest solution first and then work from there. Even in the most complex of network designs, the easiest solution is often the right one. For instance, if a single user cannot log on to a network, it is best to confirm network settings before replacing the network interface card (NIC). Remember, though, that at this point you need to determine only the most probable cause, and your first guess might be incorrect. Determining the correct cause of the problem might take a few tries.

**ExamAlert**

Avoid discounting a possible answer because it seems too easy. Many of the troubleshooting questions are based on possible real-world scenarios, some of which do have easy or obvious solutions.

# Test the Theory to Determine the Cause

After questioning the obvious, you need to establish a theory. After you formulate a theory, you should attempt to confirm it. An example might be a theory that users can no longer print because they downloaded new software that changed the print drivers, or that they can no longer run the legacy application they used to run after the latest service pack was installed.

If the theory can be confirmed, you must plot a course of action—a list of the next steps to take to resolve the problem. If the theory cannot be confirmed (in the example given, no new software was downloaded and no service pack was applied), you must establish a new theory or consider escalating the problem.

# Establish a Plan of Action

After identifying a cause but before implementing a solution, you should establish a plan for the solution. This is particularly a concern for server systems in which taking the server offline is a difficult and undesirable prospect. After you identify the cause of a problem on the server, it is absolutely necessary to plan for the solution. The plan must include the details of when the server or network should be taken offline and for how long, what support services are in place, and who will be involved in correcting the problem.

Planning is an important part of the whole troubleshooting process and can involve formal or informal written procedures. Those who do not have experience troubleshooting servers might wonder about all the formality, but this attention to detail ensures the least amount of network or server downtime and the maximum data availability.

**Tip**

If part of an action plan includes shutting down a server or another similar event that can impact many users, it is a best practice to let users know when they will be shut out of the network. Having this information allows them to properly shut off any affected applications and not be frustrated by not being able to access the network or other services.

With the plan in place, you should be ready to implement a solution—that is, apply the patch, replace the hardware, plug in a cable, or implement some other solution. In an ideal world, your first solution would fix the problem; however, unfortunately, this is not always the case. If your first solution does not fix the problem, you need to retrace your steps and start again.

You must attempt only one solution at a time. Trying several solutions at once can make it unclear which one corrected the problem.

# Implement the Solution or Escalate

After the corrective change has been made to the server, network, or workstation, you must test the results—never assume. This is when you find out if you were right and the remedy you applied worked. Don't forget that first impressions can deceive, and a fix that seems to work on first inspection might not have corrected the problem.

The testing process is not always as easy as it sounds. If you are testing a connectivity problem, it is not difficult to ascertain whether your solution was successful. However, changes made to an application or to databases you are unfamiliar with are much more difficult to test. It might be necessary to have people who are familiar with the database or application run the tests with you in attendance.

## Determine Whether Escalation Is Necessary

Sometimes the problems you encounter fall outside the scope of your knowledge. Few organizations expect their administrators to know everything, but organizations do expect administrators to fix any problem. To do this, you often need additional help.

> **Note**
>
> System administration is often as much about knowing whom and what to refer to in order to get information about a problem as it is about actually fixing the problem.

Technical escalation procedures do not follow a specific set of rules; rather, the procedures to follow vary from organization to organization and situation to situation. Your organization might have an informal arrangement or a formal one requiring documented steps and procedures to be carried out. Whatever the approach, general practices should be followed for appropriate escalation.

Unless otherwise specified by the organization, the general rule is to start with the closest help and work out from there. If you work in an organization that has an IT team, talk with others on your team; every IT professional has had different experiences, and someone else may know about the issue at hand. If you are still struggling with the problem, it is common practice to notify a supervisor or head administrator, especially if the problem is a threat to the server's data or can bring down the server.

Suppose that, as a server administrator, you notice a problem with a hard disk in a RAID 1 array on a Linux server. You know how to replace drives in a failed RAID 1 configuration, but you have no experience working with software RAID on a Linux server. This situation would most certainly require an escalation of the problem. The job of server administrator in this situation is to notice the failed RAID 1 drive and to recruit the appropriate help to repair the RAID failure within Linux.

**Note**

When you are confronted with a problem, it is yours until it has been solved or passed to someone else. Of course, the passing on of an issue requires that both parties know that it has been passed on.

# Verify Full System Functionality

At times, you might apply a fix that corrects one problem but creates another. Many such circumstances are hard to predict—but not always. For instance, you might add a new network application, but the application requires more bandwidth than your current network infrastructure can support. The result would be that overall network performance would be compromised.

Everything done to a network can have a ripple effect and negatively affect another area of the network. Actions such as adding clients, replacing hubs or switches, and adding applications can all have unforeseen results. It is difficult to always know how the changes you make to a network might affect the network's functioning. The safest thing to do is assume that the changes you make will affect the network in some way and realize that you have to figure out how. At times like this, you might need to think outside the box and try to predict possible outcomes.

It is imperative that you verify full system functionality before you are satisfied with the solution. After you obtain that level of satisfaction, you should look at the problem and ascertain if any preventive measures should be implemented to keep the same problem from occurring again.

# Document Findings, Actions, Outcomes, and Lessons

Although it is often neglected in the troubleshooting process, documentation is as important as any of the other troubleshooting procedures. Documenting a solution involves keeping a record of all the steps taken during the fix—not necessarily just the solution. The lessons learned can be just as important as the solution.

For the documentation to be of use to other network administrators in the future, it must include several key pieces of information. When documenting a procedure, you should include the following information:

- **When:** When was the solution implemented? You must know the date, because if problems occur after your changes, knowing the date of your fix makes it easier to determine whether your changes caused the problems.
- **Why:** Although it is obvious when a problem is being fixed why it is being done, a few weeks later, it might become less clear why that solution was needed. Documenting why the fix was made is important because if the same problem appears on another system, you can use this information to reduce the time needed to find the solution.
- **What:** The successful fix should be detailed, along with information about any changes to the configuration of the system or network that were made to achieve the fix. Additional information should include version numbers for software patches or firmware, as appropriate.
- **Results:** Many administrators choose to include information on both successes and failures. The documentation of failures might prevent you from going down the same road twice, and the documentation of successful solutions can reduce the time it takes to get a system or network up and running.
- **Who:** It might be that information is left out of the documentation or someone simply wants to ask a few questions about a solution. In both cases, if the name of the person who made a fix is in the documentation, that person can easily be tracked down. Of course, documenting who is more of a concern in environments that have a large IT staff or if system repairs are performed by contractors instead of company employees.

# Cram Quiz

1. A user reports that she can no longer access a legacy database. What should be one of the first questions you ask?
   - ❍ **A.** What has changed since the last time you accessed that database?
   - ❍ **B.** How many help calls have you placed in the past few months?
   - ❍ **C.** Who originally installed or created that database?
   - ❍ **D.** How long have you worked here?

2. You've spent two hours trying to fix a problem and then realize that it falls outside of your area of expertise and ability to fix. What should you do in most organizations?
   - ❍ **A.** Let the user immediately know that she needs to call someone else; then exit the scene so another person can help.
   - ❍ **B.** Formulate a workaround; then document the problem and bring it up at the next meeting.
   - ❍ **C.** Escalate the issue with a supervisor or manager.
   - ❍ **D.** Continue working on the problem, trying as many solutions as you can find, until you solve the problem.

3. You get numerous calls from users who cannot access an application. Upon investigation, you find that the application crashed. You restart the application, and it appears to run okay. What is the next step in the troubleshooting process?
   - ❍ **A.** Email the users to let them know that they can use the application again.
   - ❍ **B.** Test the application to ensure that it operates correctly.
   - ❍ **C.** Document the problem and the solution.
   - ❍ **D.** Reload the application executables from the CD and restart it.

4. A user tells you that he is having a problem accessing his email. What is the first step in the troubleshooting process?
   - ❍ **A.** Document the problem.
   - ❍ **B.** Make sure that the user's email address is valid.
   - ❍ **C.** Discuss the problem with the user.
   - ❍ **D.** Visit the user's desk to reload the email client software.

5. You have successfully fixed a problem with a server and have tested the application and let the users back on to the system. What is the next step in the troubleshooting process?
   - ❍ **A.** Document the problem.
   - ❍ **B.** Restart the server.
   - ❍ **C.** Document the problem and the solution.
   - ❍ **D.** Clear the error logs of any reference to the problem.

# Cram Quiz Answers

1. **A.** Establishing any recent changes to a system can often lead you in the right direction to isolate and troubleshoot a problem.
2. **C.** When a problem is outside of your ability to fix, you must escalate the issue. Unless otherwise specified by the organization, the general rule is to start with the closest help and work out from there. None of the other options are acceptable choices.
3. **B.** After you fix a problem, you should test it fully to ensure that the network operates correctly before you allow users to log back on. Emailing the users and documenting the problem are valid but only after the application has been tested. Reloading the application is incorrect because you would reload the executable only as part of a systematic troubleshooting process. Because the application loads, it is unlikely that the executable has become corrupted.
4. **C.** Not enough information is provided for you to come up with a solution. In this case, the next troubleshooting step would be to talk to the user and gather more information about exactly what the problem is. All the other answers are valid troubleshooting steps but only after the information gathering has been completed.
5. **C.** After you have fixed a problem, tested the fix, and let users back on to the system, you should create detailed documentation that describes the problem and the solution. Documenting the problem is incorrect because you must document both the problem and the solution. You do not need to restart the server, so that answer is incorrect. You would clear the logs only after the system's documentation has been created.

# Software Troubleshooting Tools

▶ **Given a scenario, use the appropriate network software tools and commands.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What cross-platform tool is used for network performance measurement/tuning and can produce standardized performance measurements for any network?
2. What TCP/IP command can be used to troubleshoot DNS problems?
3. What is the Linux, macOS, and UNIX equivalent of the **ipconfig** command?
4. What utility is part of the TCP/IP suite and has the function of resolving IP addresses to MAC addresses?

### Answers

1. The iperf tool is used for network performance measurement/tuning and can produce standardized performance measurements for any network.
2. The **nslookup** command is a TCP/IP diagnostic tool used to troubleshoot DNS problems. On Linux, UNIX, and macOS systems, you can also use the **dig** command for the same purpose.
3. The **ifconfig** command is the Linux, macOS, and UNIX equivalent of the **ipconfig** command.
4. The function of **arp** is to resolve IP addresses to MAC addresses.

### ExamAlert

Remember that this objective begins with "Given a scenario." This means that you may receive a drag-and-drop, matching, or "live OS" scenario where you have to click through to complete a specific objective-based task.

A large part of network administration involves having the right tools for the job and knowing when and how to use them. Selecting the correct tool for a networking job sounds like an easy task, but network administrators can choose from a mind-boggling number of tools and utilities.

Given the diverse range of tools and utilities available, it is unlikely that you will encounter all the tools available—or even all those discussed in this

chapter. For the Network+ exam, you are required to have general knowledge of the software tools available and what they are designed to do.

# Wi-Fi Analyzer

As the name implies, a Wi-Fi analyzer is used to identify Wi-Fi problems. It can be helpful in finding the ideal place for locating an access point or the ideal channel to use. Many software-based Wi-Fi analyzers are available, and some use the word *scanner* in place of *analyzer*. One good feature of most wireless survey tools is that they can be used to create heat maps showing the quantity and quality of wireless network coverage in areas. They can also allow you to see access points (including rogues) and security settings. They can be used to help you design and deploy an efficient network, and they can also be used (by you or others) to find weaknesses in your existing network.

# Protocol Analyzer

*Protocol analyzers* are used to do just that—analyze network protocols such as TCP, UDP, HTTP, and FTP. Protocol analyzers can be hardware or software based. In use, protocol analyzers help diagnose computer networking problems, alert you to unused protocols, identify unwanted or malicious network traffic, and help isolate network traffic-related problems.

Like packet sniffers, protocol analyzers capture the communication stream between systems. But unlike the sniffer, the protocol analyzer captures more than network traffic; it reads and decodes the traffic. Decoding enables the administrator to view the network communication in English. From this communication, administrators can get a better idea of the traffic that is flowing on the network. As soon as unwanted or damaged traffic is spotted, analyzers make it easy to isolate and repair. For example, if there is a problem with specific TCP/IP communication, such as a broadcast storm, the analyzer can find the source of the TCP/IP problem and isolate the system causing the storm. Protocol analyzers also provide many real-time trend statistics that help you justify to management the purchase of new hardware.

You can use protocol analyzers for two key reasons:

- **Identify protocol patterns:** By creating a historical baseline of analysis, administrators can spot trends in protocol errors. That way, when a protocol error occurs, it can be researched in the documentation to see if that error has occurred before and what was done to fix it.

- **Decode information:** By capturing and decoding network traffic, administrators can see what exactly is going on with the network at a protocol level. This process helps find protocol errors as well as potential intruders.

**Caution**

Protocol analyzers enable administrators to examine the bandwidth that a particular protocol is using.

# Bandwidth Speed Tester

Two types of websites that can be invaluable when it comes to networking are *speed test sites* and *looking-glass sites*. Speed test sites, as the name implies, are *bandwidth speed testers* that report the speed of the connection that you have to them and can be helpful in determining if you are getting the rate your ISP has promised.

Looking-glass sites are servers running *looking-glass (LG)* software that allows you to see routing information. The servers act as a read-only portal giving information about the backbone connection. Most of these servers will show **ping** information, trace (**tracert/traceroute**) information, and Border Gateway Protocol (BGP) information.

**ExamAlert**

Think of a looking-glass site as a graphical interface to routing-related information.

# Port Scanner

*Port scanners* are software-based security utilities designed to search a network host for open ports on a TCP/IP-based network. As a refresher, in a TCP/IP-based network, a system can be accessed through one of 65,535 available port numbers. Each network service is associated with a particular port.

**Note**

Chapter 3, "Addressing, Routing, and Switching," includes a list of some of the most common TCP/IP suite protocols and their port assignments.

Many of the thousands of ports are closed by default; however, many others, depending on the OS, are open by default. These are the ports that can cause trouble. Like packet sniffers, port scanners can be used by both administrators and hackers. Hackers use port scanners to try to find an open port that they can use to access a system. Port scanners are easily obtained on the Internet either for free or for a modest cost. After it is installed, the scanner probes a computer system running TCP/IP, looking for a UDP or TCP port that is open and listening.

When a port scanner is used, several port states may be reported:

- **Open/listening:** The host sent a reply indicating that a service is listening on the port. There was a response from the port.
- **Closed or denied or not listening:** No process is listening on that port. Access to this port will likely be denied.
- **Filtered or blocked:** There was no reply from the host, meaning that the port is not listening or the port is secured and filtered.

> **Note**
>
> Sometimes, an Internet service provider (ISP) takes the initiative and blocks specific traffic entering its network before the traffic reaches the ISP's customers, or after the traffic leaves the customers and before it exits the network. This is done to protect customers from well-known attacks.

Because others can potentially review the status of ports, it is critical that administrators know which ports are open and potentially vulnerable. As mentioned, many tools and utilities are available for this purpose. The quickest way to get an overview of the ports used by the system and their status is to issue the **netstat -a** command from the command line. The following is a sample of the output from the **netstat -a** command and active connections for a computer system:

```
Proto   Local Address          Foreign Address     State
 TCP    0.0.0.0:135            mike-PC:0           LISTENING
 TCP    0.0.0.0:10114          mike-PC:0           LISTENING
 TCP    0.0.0.0:10115          mike-PC:0           LISTENING
 TCP    0.0.0.0:20523          mike-PC:0           LISTENING
 TCP    0.0.0.0:20943          mike-PC:0           LISTENING
 TCP    0.0.0.0:49152          mike-PC:0           LISTENING
 TCP    0.0.0.0:49153          mike-PC:0           LISTENING
 TCP    0.0.0.0:49154          mike-PC:0           LISTENING
```

```
TCP    0.0.0.0:49155          mike-PC:0              LISTENING
TCP    0.0.0.0:49156          mike-PC:0              LISTENING
TCP    0.0.0.0:49157          mike-PC:0              LISTENING
TCP    127.0.0.1:5354         mike-PC:0              LISTENING
TCP    127.0.0.1:27015        mike-PC:0              LISTENING
TCP    127.0.0.1:27015        mike-PC:49187          ESTABLISHED
TCP    127.0.0.1:49187        mike-PC:27015          ESTABLISHED
TCP    192.168.0.100:49190    206.18.166.15:http     CLOSED
TCP    192.168.1.66:139       mike-PC:0              LISTENING
TCP    [::]:135               mike-PC:0              LISTENING
TCP    [::]:445               mike-PC:0              LISTENING
TCP    [::]:2869              mike-PC:0              LISTENING
TCP    [::]:5357              mike-PC:0              LISTENING
TCP    [::]:10115             mike-PC:0              LISTENING
TCP    [::]:20523             mike-PC:0              LISTENING
TCP    [::]:49152             mike-PC:0              LISTENING
TCP    [::]:49153             mike-PC:0              LISTENING
TCP    [::]:49154             mike-PC:0              LISTENING
TCP    [::]:49155             mike-PC:0              LISTENING
TCP    [::]:49156             mike-PC:0              LISTENING
TCP    [::]:49157             mike-PC:0              LISTENING
UDP    0.0.0.0:123            *:*
UDP    0.0.0.0:500            *:*
UDP    0.0.0.0:3702           *:*
UDP    0.0.0.0:3702           *:*
```

As you can see from the output, the system has many listening ports. Not all these suggest that a risk exists, but the output does let you know that there are many listening ports and that they might be vulnerable. To test for actual vulnerability, you use a port scanner. For example, you can use a free online scanner to probe the system. Many free online scanning services are available. Although a network administrator might use these free online tools out of curiosity, for better security testing, you should use a quality scanner.

**Caution**

Administrators use the detailed information revealed from a port scan to ensure network security. Port scans identify closed, open, and listening ports. However, port scanners also can be used by people who want to compromise security by finding open and unguarded ports.

# iperf

The *iperf* tool is used for active measurements of the maximum achievable bandwidth and used for network tuning. It is open-source and cross-platform compatible and has become widely accepted thanks to its ability to produce

standardized performance measurements for any network, enabling the comparison of similar numbers across all platforms.

## NetFlow Analyzer

NetFlow is a proprietary Cisco protocol used for network flow analysis. A *NetFlow analyzer* is used to collect IP network traffic as it enters or exits an interface and can identify such values as the source and destination of traffic, class of service, and the causes of congestion. RFC 3954 (the NetFlow standard) does not specify a specific listening port and the most common port used by NetFlow is port 2055 (UDP), but other ports can also be used (such as 9555, 9995, 9025, and 9026).

## TFTP Server

A Trivial File Transfer Protocol (TFTP) can be used to send files between servers and is finding new use today in applications uploading HTML pages on the HTTP server. The TFTP server uses port 69 by default.

## Terminal Emulator

A *terminal emulator* is any software program that emulates a computer terminal. Most often, the terminal being emulated is that of a command-line window, though it need not be (if it is graphical, it is usually called a terminal window instead of a terminal emulator), allowing the running of command-line utilities. Those utilities can be running on the local machine or remotely through the use of Telnet (using port 23 and considered very insecure) or a similar utility.

## IP Scanner

An *IP scanner* is any tool that can scan for IP addresses and related information. An administrator can use it to scan available ports, discover devices, and get detailed hardware and software information on workstations and servers to manage inventory.

**ExamAlert**

Remember all of the software tools mentioned in the preceding sections. You will likely be given a scenario where you need to use the appropriate tool.

# Command-Line Tools

For anyone working with TCP/IP networks, troubleshooting connectivity is something that must be done. This section describes the tools used in the troubleshooting process and identifies scenarios in which they can be used.

You can use many utilities when troubleshooting TCP/IP. Although the utilities available vary from platform to platform, the functionality between platforms is quite similar. Table 10.1 lists the TCP/IP troubleshooting tools covered on the Network+ exam, along with their purpose.

TABLE 10.1 **Common TCP/IP Troubleshooting Tools and Their Purposes**

| Tool | Description |
|---|---|
| **tracert/ traceroute** | Tracks the path a packet takes as it travels across a network. **tracert** is used on Windows systems; **traceroute** is used on UNIX, Linux, and macOS systems. |
| **tracert -6**<br>**traceroute6**<br>**traceroute -6** | Performs the same function as **tracert/traceroute**, but using the IPv6 protocol in place of IPv4. |
| **ping** | Tests connectivity between two devices on a network with IPv4. |
| **ping6/ping -6** | Tests connectivity between two devices on a network using the IPv6 protocol in place of IPv4. |
| **hostname** | Displays the name assigned to the host. |
| **arp** | Enables you to view and work with the IP address to MAC address resolution cache. |
| **arp ping** | Uses ARP to test connectivity between systems rather than the Internet Control Message Protocol (ICMP), as done with a regular ping. |
| **netstat** | Enables you to view the current TCP/IP connections on a system. |
| **telnet** | Allows remote access to a host. Because it is not secure, its usage is usually discouraged in favor of newer, more secure options such as SSH. |
| **ipconfig** | Enables you to view and renew a TCP/IP configuration on a Windows system. |
| **ifconfig** | Enables you to view a TCP/IP configuration on a UNIX, Linux, or macOS system. |
| **nslookup/dig** | Performs manual DNS lookups. **nslookup** can be used on Windows, UNIX, macOS, and Linux systems. **dig** can be used on UNIX, Linux, and macOS systems. |
| **tcpdump** | Acts as a Linux-based packet analyzer. |
| **route** | Enables you to view and configure the routes in the routing table. |
| **nmap** | Acts as a popular vulnerability scanner. |

The following sections look in more detail at these utilities and the output they produce.

**Note**

Many of the utilities discussed in this chapter have a help facility that you can access by typing the command followed by **/?** or **-?**. On a Windows system, for example, you can get help on the **netstat** utility by typing **netstat /?**. Sometimes, using a utility with an invalid switch also brings up the help screen.

**ExamAlert**

Be prepared to identify what software tool to use in a given scenario. Remember, you might be able to use more than one tool. You will be expected to pick the best one for the situation described.

You will be asked to identify the output from a command, and you should be able to interpret the information provided by the command. In a performance-based question, you may be asked to enter the appropriate command for a given scenario.

# The Trace Route Utility (tracert/traceroute)

The trace route utility does exactly what its name implies—it traces the route between two hosts. It does this by using ICMP echo packets to report information at every step in the journey. Each of the common network operating systems provides a trace route utility, but the name of the command and the output vary slightly on each. However, for the purposes of the Network+ exam, you should not concern yourself with the minor differences in the output format. Table 10.2 shows the **traceroute** command syntax used in various operating systems.

**Note**

The phrase *trace route utility* is used in this section to refer generically to the various route-tracing applications available on common operating systems. In a live environment, you should become familiar with the version of the tool used on the operating systems you are working with.

TABLE 10.2 **Trace Route Utility Commands**

| Operating System | Trace Route Command Syntax |
|---|---|
| Windows systems | **tracert *IP address*** |
| | **tracert -6 *IP address*** |
| Linux/UNIX/macOS | **traceroute *IP address*** |
| | **traceroute6 *IP address*** |
| | **traceroute -6 *IP address*** |

ExamAlert

Be prepared to identify the IP tracing command syntax used with various operating systems for the exam. Review Table 10.2 for this information.

The **traceroute** command provides a lot of useful information, including the IP address of every router connection it passes through and, in many cases, the name of the router (although this depends on the router's configuration). **traceroute** also reports the length, in milliseconds, of the round trip the packet made from the source location to the router and back. This information can help identify where network bottlenecks or breakdowns might be. The following is an example of a successful **tracert** command on a Windows system:

```
C:\> tracert 24.7.70.37

Tracing route to c1-p4.sttlwa1.home.net [24.7.70.37]
 over a maximum of 30 hops:
 1 30 ms 20 ms 20 ms 24.67.184.1
 2 20 ms 20 ms 30 ms rd1ht-ge3-0.ok.shawcable.net
 [24.67.224.7]
 3 50 ms 30 ms 30 ms rc1wh-atm0-2-1.vc.shawcable.net
 [204.209.214.193]
 4 50 ms 30 ms 30 ms rc2wh-pos15-0.vc.shawcable.net
 [204.209.214.90]
 5 30 ms 40 ms 30 ms rc2wt-pos2-0.wa.shawcable.net
 [66.163.76.37]
 6 30 ms 40 ms 30 ms c1-pos6-3.sttlwa1.home.net [24.7.70.37]
Trace complete.
```

Similar to the other common operating systems covered on the Network+ exam, the **tracert** display on a Windows-based system includes several columns of information. The first column represents the hop number. You may recall that *hop* is the term used to describe a step in the path a packet takes as it crosses the network. The next three columns indicate the roundtrip time, in

milliseconds, that a packet takes in its attempts to reach the destination. The last column is the hostname and the IP address of the responding device.

However, not all trace route attempts are successful. The following is the output from a **tracert** command on a Windows system that does not manage to get to the remote host:

```
C:\> tracert comptia.org

Tracing route to comptia.org [216.119.103.72]
over a maximum of 30 hops:
 1 27 ms 28 ms 14 ms 24.67.179.1
 2 55 ms 13 ms 14 ms rd1ht-ge3-0.ok.shawcable.net
 [24.67.224.7]
 3 27 ms 27 ms 28 ms rc1wh-atm0-2-1.shawcable.net
 [204.209.214.19]
 4 28 ms 41 ms 27 ms rc1wt-pos2-0.wa.shawcable.net
 [66.163.76.65]
 5 28 ms 41 ms 27 ms rc2wt-pos1-0.wa.shawcable.net
 [66.163.68.2]
 6 41 ms 55 ms 41 ms c1-pos6-3.sttlwa1.home.net
 [24.7.70.37]
 7 54 ms 42 ms 27 ms home-gw.st6wa.ip.att.net
 [192.205.32.249]
 8 * * * Request timed out.
 9 * * * Request timed out.
 10 * * * Request timed out.
 11 * * * Request timed out.
 12 * * * Request timed out.
 13 * * * Request timed out.
 14 * * * Request timed out.
 15 * * * Request timed out.
```

In this example, the trace route request gets to only the seventh hop, at which point it fails. This failure indicates that the problem lies on the far side of the device in step 7 or on the near side of the device in step 8. In other words, the device at step 7 is functioning but might not make the next hop. The cause of the problem could be a range of things, such as an error in the routing table or a faulty connection. Alternatively, the seventh device might be operating at 100 percent, but device 8 might not be functioning at all. In any case, you can isolate the problem to just one or two devices.

**Note**

In some cases, the owner of a router might configure it to not return ICMP traffic like that generated by **ping** or **traceroute**. If this is the case, the **ping** or **traceroute** will fail just as if the router did not exist or was not operating.

**ExamAlert**

Although we have used the Windows **tracert** command to provide sample output in these sections, the output from **traceroute** on a UNIX, Linux, or macOS system is extremely similar.

The trace route utility can also help you isolate a heavily congested network. In the following example, the trace route packets fail in the midst of the **tracert** from a Windows system, but subsequently they continue. This behavior can be an indicator of network congestion:

```
C:\> tracert comptia.org

Tracing route to comptia.org [216.119.103.72]over a maximum of 30
hops:
 1 96 ms 96 ms 55 ms 24.67.179.1
 2 14 ms 13 ms 28 ms rd1ht-ge3-0.ok.shawcable.net
 [24.67.224.7]
 3 28 ms 27 ms 41 ms rc1wh-atm0-2-1.shawcable.net
 [204.209.214.19]
 4 28 ms 41 ms 27 ms rc1wt-pos2-0.wa.shawcable.net
 [66.163.76.65]
 5 41 ms 27 ms 27 ms rc2wt-pos1-0.wa.shawcable.net
 [66.163.68.2]
 6 55 ms 41 ms 27 ms c1-pos6-3.sttlwa1.home.net [24.7.70.37]
 7 54 ms 42 ms 27 ms home-gw.st6wa.ip.att.net
 [192.205.32.249]
 8 55 ms 41 ms 28 ms gbr3-p40.st6wa.ip.att.net
 [12.123.44.130]
 9 * * * Request timed out.
 10 * * * Request timed out.
 11 * * * Request timed out.
 12 * * * Request timed out.
 13 69 ms 68 ms 69 ms gbr2-p20.sd2ca.ip.att.net
 [12.122.11.254]
 14 55 ms 68 ms 69 ms gbr1-p60.sd2ca.ip.att.net
 [12.122.1.109]
 15 82 ms 69 ms 82 ms gbr1-p30.phmaz.ip.att.net
 [12.122.2.142]
 16 68 ms 69 ms 82 ms gar2-p360.phmaz.ip.att.net
 [12.123.142.45]
 17 110 ms 96 ms 96 ms 12.125.99.70
 18 124 ms 96 ms 96 ms light.crystaltech.com [216.119.107.1]
 19 82 ms 96 ms 96 ms 216.119.103.72
Trace complete.
```

Generally speaking, trace route utilities enable you to identify the location of a problem in the connectivity between two devices. After you determine this

location, you might need to use a utility such as **ping** to continue troubleshooting. In many cases, as in the examples provided in this chapter, the routers might be on a network such as the Internet and therefore not within your control. In that case, you can do little except inform your ISP of the problem.

When you're dealing with IPv6, the same tools exist but are followed with -6; so **tracert** becomes **tracert -6** and **traceroute** becomes **traceroute -6**.

# ping

Most network administrators are familiar with the **ping** utility and are likely to use it on an almost daily basis. The basic function of the **ping** command is to test the connectivity between the two devices on a network. All the command is designed to do is determine whether the two computers can see each other and to notify you of how long the round trip takes to complete.

Although **ping** is most often used on its own, a number of switches can be used to assist in the troubleshooting process. Table 10.3 shows some of the commonly used switches with **ping** on a Windows system.

TABLE 10.3 **ping Command Switches**

| Option | Description |
|---|---|
| **ping -t** | Pings a device on the network until stopped |
| **ping -a** | Resolves addresses to hostnames |
| **ping -n count** | Specifies the number of echo requests to send |
| **ping -r count** | Records the route for count hops |
| **ping -s count** | Sets the time stamp for *count* hops |
| **ping -w timeout** | Sets the timeout in milliseconds to wait for each reply |
| **ping -6** or **ping6** | Pings a device on the network using IPv6 instead of IPv4 |

ExamAlert

You will likely be asked about **ping**, its switches, and how it can be used in a troubleshooting scenario.

The **ping** command works by sending ICMP echo request messages to another device on the network. If the other device on the network hears the ping request, it automatically responds with an ICMP echo reply. By default, the **ping** command on a Windows-based system sends four data packets; however, if the **-t** switch is used, a continuous stream of ping requests can be sent.

**ping** is perhaps the most widely used of all network tools; it is primarily used to verify connectivity between two network devices. On a good day, the results from the **ping** command are successful, and the sending device receives a reply from the remote device. Not all ping results are that successful. To use **ping** effectively, you must interpret the results of a failed **ping** command.

## The Destination Host Unreachable Message

The "Destination Host Unreachable" error message means that a route to the destination computer system cannot be found. To remedy this problem, you might need to examine the routing information on the local host to confirm that the local host is correctly configured, or you might need to make sure that the default gateway information is correct. The following is an example of a ping failure that gives the "Destination Host Unreachable" message:

```
Pinging 24.67.54.233 with 32 bytes of data:
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Ping statistics for 24.67.54.233:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

## The Request Timed Out Message

The "Request Timed Out" error message is common when you use the **ping** command. Essentially, this error message indicates that your host did not receive the ping message back from the destination device within the designated time period. Assuming that the network connectivity is okay on your system, this message typically indicates that the destination device is not connected to the network, is powered off, or is not correctly configured. It could also mean that some intermediate device is not operating correctly. In some rare cases, it can also indicate that the network has so much congestion that timely delivery of the ping message could not be completed. It might also mean that the ping is being sent to an invalid IP address or that the system is not on the same network as the remote host, and an intermediary device is not correctly configured. In any of these cases, the failed ping should initiate a troubleshooting process that might involve other tools, manual inspection, and possibly reconfiguration. The following example shows the output from a ping to an invalid IP address:

```
C:\> ping 169.76.54.3
```

```
Pinging 169.76.54.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 169.76.54.3:
 Packets: Sent = 4, Received = 0, Lost = 4 (100%
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

During the ping request, you might receive some replies from the remote host that are intermixed with "Request Timed Out" errors. This is often the result of a congested network. An example follows; notice that this example, which was run on a Windows system, uses the **-t** switch to generate continuous pings:

```
C:\> ping -t 24.67.184.65

Pinging 24.67.184.65 with 32 bytes of data:

Reply from 24.67.184.65: bytes=32 time=55ms TTL=127
Reply from 24.67.184.65: bytes=32 time=54ms TTL=127
Reply from 24.67.184.65: bytes=32 time=27ms TTL=127
Request timed out.
Request timed out.
Request timed out.
Reply from 24.67.184.65: bytes=32 time=69ms TTL=127
Reply from 24.67.184.65: bytes=32 time=28ms TTL=127
Reply from 24.67.184.65: bytes=32 time=28ms TTL=127
Reply from 24.67.184.65: bytes=32 time=68ms TTL=127
Reply from 24.67.184.65: bytes=32 time=41ms TTL=127

Ping statistics for 24.67.184.65:
 Packets: Sent = 11, Received = 8, Lost = 3 (27% loss),
Approximate round trip times in milli-seconds:
 Minimum = 27ms, Maximum = 69ms, Average = 33ms
```

In this example, three packets were lost. If this command continued on your network, you would need to troubleshoot to find out why packets were dropped.

## The Unknown Host Message

The "Unknown Host" error message is generated when the hostname of the destination computer cannot be resolved. This error usually occurs when you ping an incorrect hostname, as shown in the following example, or try to use **ping** with a hostname when hostname resolution (via DNS or a HOSTS text file) is not configured:

```
C:\> ping www.comptia.ca
```

```
Unknown host www.comptia.ca
```

If the ping fails, you need to verify that the ping is sent to the correct remote host. If it is, and if name resolution is configured, you have to dig a little more to find the problem. This error might indicate a problem with the name resolution process, and you might need to verify that the DNS or WINS server is available. Other commands, such as **nslookup** or **dig**, can help in this process.

## The Expired TTL Message

The time to live (TTL) is a key consideration in understanding the **ping** command. The function of the TTL is to prevent circular routing, which occurs when a ping request keeps looping through a series of hosts. The TTL counts each hop along the way toward its destination device. Each time it counts one hop, the hop is subtracted from the TTL. If the TTL reaches 0, it has expired, and you get a message like the following:

```
Reply from 24.67.180.1: TTL expired in transit
```

If the TTL is exceeded with **ping**, you might have a routing problem on the network. You can modify the TTL for **ping** on a Windows system by using the **ping -i** command.

## Troubleshooting with ping

Although **ping** does not completely isolate problems, you can use it to help identify where a problem lies. When troubleshooting with **ping**, follow these steps:

1. Ping the IP address of your local loopback using the command **ping 127.0.0.1**. If this command is successful, you know that the TCP/IP protocol suite is installed correctly on your system and is functioning. If you cannot ping the local loopback adapter, TCP/IP might need to be reloaded or reconfigured on the machine you are using.

**ExamAlert**

The loopback is a special function within the TCP/IP protocol stack that is supplied for troubleshooting purposes. The Class A IP address 127.*x.x.x* is reserved for the IPv4 loopback. Although convention dictates that you use 127.0.0.1, you can use any address in the 127.*x.x.x* range, except for the network number itself (127.0.0.0) and the broadcast address (127.255.255.255). You can also ping by using the default hostname for the local system, which is called localhost (for example, **ping localhost**). The same function can be performed in IPv6 by using the address ::1.

2. Ping the assigned IP address of your local network interface card (NIC). If the ping is successful, you know that your NIC is functioning on the network and has TCP/IP correctly installed. If you cannot ping the local NIC, TCP/IP might not be correctly bound to the NIC, or the NIC drivers might be improperly installed.
3. Ping the IP address of another known good system on your local network. By doing so, you can determine whether the computer you are using can see other computers on the network. If you can ping other devices on your local network, you have network connectivity.

   If you cannot ping other devices on your local network, but you could ping the IP address of your system, you might not be connected to the network correctly.
4. After you confirm that you have network connectivity for the local network, you can verify connectivity to a remote network by sending a ping to the IP address of the default gateway.
5. If you can ping the default gateway, you can verify remote connectivity by sending a ping to the IP address of a system on a remote network.

**ExamAlert**

You might be asked to relate the correct procedure for using **ping** for a connectivity problem. A performance-based question may ask you to implement the **ping** command to test for connectivity.

Using just the **ping** command in these steps, you can confirm network connectivity on not only the local network, but also on a remote network. The whole process requires as much time as it takes to enter the command, and you can do it all from a single location.

If you are an optimistic person, you can perform step 5 first. If that works, all the other steps will also work, saving you the need to test them. If your step 5 trial fails, you can go to step 1 and start the troubleshooting process from the beginning.

**Note**

All but one of the **ping** examples used in this section show the **ping** command using the IP address of the remote host. It is also possible to ping the Domain Name Service (DNS) name of the remote host (for example, **ping www.comptia.org**, **ping server1**). However, you can do this only if your network uses a DNS server. On a Windows-based network, you can also **ping** by using the Network Basic Input/Output System (NetBIOS) computer name.

When dealing with IPv6, the same tools exist, but are followed with **6** or **-6**; so **ping** becomes **ping6** or **ping -6**.

## hostname

Sometimes all you really want to know is the hostname assigned to a particular host. When that is the case, you can use the **hostname** command to provide that information. It reports back the character string that refers to the name of the host the command was entered on. The following example illustrates the command in action:

```
C:\> hostname

EADULANEY7040
```

## ARP

*Address Resolution Protocol (ARP)* is used to resolve IP addresses to MAC addresses. This is significant because on a network, devices find each other using the IP address, but communication between devices requires the MAC address.

> **ExamAlert**
>
> Remember that the function of ARP is to resolve IP addresses to Layer 2 or MAC addresses.

When a computer wants to send data to another computer on the network, it must know the MAC address (physical address) of the destination system. To discover this information, ARP sends out a discovery packet to obtain the MAC address. When the destination computer is found, it sends its MAC address to the sending computer. The ARP-resolved MAC addresses are stored temporarily on a computer system in the ARP cache. Inside this ARP cache is a list of matching MAC and IP addresses. This ARP cache is checked before a discovery packet is sent to the network to determine whether there is an existing entry.

Entries in the ARP cache are periodically flushed so that the cache does not fill up with unused entries. The following code shows an example of the **arp** command with the output from a Windows system:

```
C:\> arp -a

Interface: 24.67.179.22 on Interface 0x3
 Internet Address Physical Address Type
 24.67.179.1 00-00-77-93-d8-3d dynamic
```

As you might notice, the type is listed as dynamic. Entries in the ARP cache can be added statically or dynamically. Static entries are added manually and do not expire. The dynamic entries are added automatically when the system accesses another on the network.

As with other command-line utilities, several switches are available for the **arp** command. Table 10.4 shows the available switches for Windows-based systems.

TABLE 10.4 **arp Switches**

| Switch | Description |
|---|---|
| **-a** or **-g** | Displays both the IP and MAC addresses and whether they are dynamic or static entries |
| **inet_addr** | Specifies a specific Internet address |
| **-N if_addr** | Displays the ARP entries for a specified network interface |
| **eth_addr** | Specifies a MAC address |
| **if_addr** | Specifies an Internet address |
| **-d** | Deletes an entry from the ARP cache |
| **-s** | Adds a static permanent address to the ARP cache |

## arp ping

Earlier in this chapter we talked about the **ping** command and how it is used to test connectivity between devices on a network. Using the **ping** command is often an administrator's first step to test connectivity between network devices. If the ping fails, it is assumed that the device you are pinging is offline. But this may not always be the case.

Most companies now use firewalls or other security measures that may block Internet Control Message Protocol (ICMP) requests. This means that a ping request will not work. Blocking ICMP is a security measure; if a would-be hacker cannot hit the target, he may not attack the host.

ExamAlert

One type of attack is called an *ICMP flood attack* (also known as a *ping attack*). The attacker sends continuous ping packets to a server or network system, eventually tying up that system's resources, making it unable to respond to requests from other systems.

If ICMP is blocked, you have still another option to test connectivity with a device on the network: the **arp ping**. As mentioned, the ARP utility is used to resolve IP addresses to MAC addresses. The **arp ping** utility does not use

the ICMP protocol to test connectivity like **ping** does; rather, it uses the ARP protocol. However, ARP is not routable, and the **arp ping** cannot be routed to work over separate networks. The **arp ping** works only on the local subnet.

Just like with a regular **ping**, an **arp ping** specifies an IP address; however, instead of returning regular **ping** results, the **arp ping** responds with the MAC address and name of the computer system. So, when a regular **ping** using ICMP fails to locate a system, the **arp ping** uses a different method to find the system. With **arp ping**, you can directly ping a MAC address. From this, you can determine whether duplicate IP addresses are used and, as mentioned, determine whether a system is responding.

**arp ping** is not built in to Windows, but you can download a number of programs that allow you to ping using ARP. Linux, however, has an **arp ping** utility ready to use.

ExamAlert

**arp ping** is not routable and can be used only on the local network.

# The netstat Command

The **netstat** command displays the protocol statistics and current TCP/IP connections on the local system. Used without any switches, the **netstat** command shows the active connections for all outbound TCP/IP connections. In addition, several switches are available that change the type of information **netstat** displays. Table 10.5 shows the various switches available for the **netstat** utility.

TABLE 10.5 **netstat Switches**

| Switch | Description |
|---|---|
| **-a** | Displays the current connections and listening ports |
| **-e** | Displays Ethernet statistics |
| **-n** | Lists addresses and port numbers in numeric form |
| **-p** | Shows connections for the specified protocol |
| **-r** | Shows the routing table |
| **-s** | Lists per-protocol statistics |
| **interval** | Specifies how long to wait before redisplaying statistics |

**ExamAlert**

You can use the **netstat** and **route print** commands to show the routing table on a local or remote system.

The **netstat** utility is used to show the port activity for both TCP and UDP connections, showing the inbound and outbound connections. When used without switches, the **netstat** utility has four information headings.

- **Proto:** Lists the protocol being used, either UDP or TCP
- **Local address:** Specifies the local address and port being used
- **Foreign address:** Identifies the destination address and port being used
- **State:** Specifies whether the connection is established

In its default use, the **netstat** command shows outbound connections that have been established by TCP. The following shows sample output from a **netstat** command without using any switches:

```
C:\> netstat

Active Connections
 Proto Local Address Foreign Address State
 TCP laptop:2848 MEDIASERVICES1:1755 ESTABLISHED
 TCP laptop:1833 www.dollarhost.com:80 ESTABLISHED
 TCP laptop:2858 194.70.58.241:80 ESTABLISHED
 TCP laptop:2860 194.70.58.241:80 ESTABLISHED
 TCP laptop:2354 www.dollarhost.com:80 ESTABLISHED
 TCP laptop:2361 www.dollarhost.com:80 ESTABLISHED
 TCP laptop:1114 www.dollarhost.com:80 ESTABLISHED
 TCP laptop:1959 www.dollarhost.com:80 ESTABLISHED
 TCP laptop:1960 www.dollarhost.com:80 ESTABLISHED
 TCP laptop:1963 www.dollarhost.com:80 ESTABLISHED
 TCP laptop:2870 localhost:8431 TIME_WAIT
 TCP laptop:8431 localhost:2862 TIME_WAIT
 TCP laptop:8431 localhost:2863 TIME_WAIT
 TCP laptop:8431 localhost:2867 TIME_WAIT
 TCP laptop:8431 localhost:2872 TIME_WAIT
```

As with any other command-line utility, the **netstat** utility has a number of switches. The following sections briefly explain the switches and give sample output from each.

## netstat -e

The **netstat -e** command shows the activity for the NIC and displays the number of packets that have been both sent and received. Here's an example:

```
C:\WINDOWS\Desktop> netstat -e

Interface Statistics

 Received Sent

Bytes 17412385 40237510
Unicast packets 79129 85055
Non-unicast packets 693 254
Discards 0 0
Errors 0 0
Unknown protocols 306
```

As you can see, the **netstat -e** command shows more than just the packets that have been sent and received:

- **Bytes:** The number of bytes that the NIC has sent or received since the computer was turned on.
- **Unicast packets:** Packets sent and received directly by this interface.
- **Nonunicast packets:** Broadcast or multicast packets that the NIC picked up.
- **Discards:** The number of packets rejected by the NIC, perhaps because they were damaged.
- **Errors:** The errors that occurred during either the sending or receiving process. As you would expect, this column should be a low number. If it is not, this could indicate a problem with the NIC.
- **Unknown protocols:** The number of packets that the system could not recognize.

## netstat -a

The **netstat -a** command displays statistics for both Transport Control Protocol (TCP) and User Datagram Protocol (UDP). Here is an example of the **netstat -a** command:

```
C:\WINDOWS\Desktop> netstat -a

Active Connections

 Proto Local Address Foreign Address State
 TCP laptop:1027 LAPTOP:0 LISTENING
```

```
TCP laptop:1030 LAPTOP:0 LISTENING
TCP laptop:1035 LAPTOP:0 LISTENING
TCP laptop:50000 LAPTOP:0 LISTENING
TCP laptop:5000 LAPTOP:0 LISTENING
TCP laptop:1035 msgr-ns41.msgr.hotmail.com:1863 ESTABLISHED
TCP laptop:nbsession LAPTOP:0 LISTENING
TCP laptop:1027 localhost:50000 ESTABLISHED
TCP laptop:50000 localhost:1027 ESTABLISHED
UDP laptop:1900 *:*
UDP laptop:nbname *:*
UDP laptop:nbdatagram *:*
UDP laptop:1547 *:*
UDP laptop:1038 *:*
UDP laptop:1828 *:*
UDP laptop:3366 *:*
```

As you can see, the output includes four columns, which show the protocol, the local address, the foreign address, and the port's state. The TCP connections show the local and foreign destination addresses and the connection's current state. UDP, however, is a little different. It does not list a state status because, as mentioned throughout this book, UDP is a connectionless protocol and does not establish connections. The following list further explains the information provided by the **netstat -a** command:

- **Proto:** The protocol used by the connection.
- **Local address:** The IP address of the local computer system and the port number it is using. If the entry in the local address field is an asterisk (*), the port has not yet been established.
- **Foreign address:** The IP address of a remote computer system and the associated port. When a port has not been established, as with the UDP connections, *:* appears in the column.
- **State:** The current state of the TCP connection. Possible states include established, listening, closed, and waiting.

## netstat -r

The **netstat -r** command is often used to view a system's routing table. A system uses a routing table to determine routing information for TCP/IP traffic. The following is an example of the **netstat -r** command from a Windows system:

```
C:\WINDOWS\Desktop> netstat -r

Route table
```

```
===========================================================================
===========================================================================
Active Routes:
Network Destination Netmask Gateway Interface Metric
 0.0.0.0 0.0.0.0 24.67.179.1 24.67.179.22 1
 24.67.179.0 255.255.255.0 24.67.179.22 24.67.179.22 1
 24.67.179.22 255.255.255.255 127.0.0.1 127.0.0.1 1
 24.255.255.255 255.255.255.255 24.67.179.22 24.67.179.22 1
 127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
 224.0.0.0 224.0.0.0 24.67.179.22 24.67.179.22 1
255.255.255.255 255.255.255.255 24.67.179.22 2 1
Default Gateway: 24.67.179.1
===========================================================================
Persistent Routes:
 None
```

**Caution**

The **netstat -r** command output shows the same information as the output from the **route print** command.

## netstat -s

The **netstat -s** command displays a number of statistics related to the TCP/IP protocol suite. Understanding the purpose of every field in the output is beyond the scope of the Network+ exam, but for your reference, sample output from the **netstat -s** command is shown here:

```
C:\> netstat -s

IP Statistics

 Packets Received = 389938
 Received Header Errors = 0
 Received Address Errors = 1876
 Datagrams Forwarded = 498
 Unknown Protocols Received = 0
 Received Packets Discarded = 0
 Received Packets Delivered = 387566
 Output Requests = 397334
 Routing Discards = 0
 Discarded Output Packets = 0
 Output Packet No Route = 916
 Reassembly Required = 0
 Reassembly Successful = 0
 Reassembly Failures = 0
 Datagrams Successfully Fragmented = 0
 Datagrams Failing Fragmentation = 0
 Fragments Created = 0
```

```
ICMP Statistics

 Received Sent
 Messages 40641 41111
 Errors 0 0
 Destination Unreachable 223 680
 Time Exceeded 24 0
 Parameter Problems 0 0
 Source Quenches 0 0
 Redirects 0 38
 Echos 20245 20148
 Echo Replies 20149 20245
 Timestamps 0 0
 Timestamp Replies 0 0
 Address Masks 0 0
 Address Mask Replies 0 0

TCP Statistics

 Active Opens = 13538
 Passive Opens = 23132
 Failed Connection Attempts = 9259
 Reset Connections = 254
 Current Connections = 15
 Segments Received = 330242
 Segments Sent = 326935
 Segments Retransmitted = 18851

UDP Statistics

 Datagrams Received = 20402
 No Ports = 20594
 Receive Errors = 0
 Datagrams Sent = 10217
```

## telnet

The **telnet** utility is used for remote access to a host via the Telnet service. This utility was mentioned in previous chapters, and the same caveat that accompanies it there must be given here: because it is an older utility that lacks security features, it is highly recommended that it not be used and other utilities—such as SSH—which provide the same functionality be used in its place.

# ipconfig

The **ipconfig** command is a technician's best friend when it comes to viewing the TCP/IP configuration of a Windows system. Used on its own, the **ipconfig**

command shows basic information, such as the name of the local network interface, the IP address, the subnet mask, and the default gateway. Combined with the **/all** switch, it shows a detailed set of information, as shown in the following example:

```
C:\> ipconfig /all

Windows IP Configuration
 Host Name . . . . . . . . . . . . : server
 Primary Dns Suffix . . . . . . . :
 Node Type . . . . . . . . . . . . : Hybrid
 IP Routing Enabled. . . . . . . . : No
 WINS Proxy Enabled. . . . . . . . : No
 DNS Suffix Search List. . . . . . : tampabay.rr.com
Ethernet adapter Local Area Connection:
 Connection-specific DNS Suffix . : tampabay.rr.com
 Description . . . . . . . . . . . : Broadcom NetLink (TM) Gigabit
Ethernet
 Physical Address. . . . . . . . . : 00-25-64-8C-9E-BF
 DHCP Enabled. . . . . . . . . . . : Yes
 Autoconfiguration Enabled . . . . : Yes
 Link-local IPv6 Address . . . . . : fe80::51b9:996e:9fac:7715%10
(Preferred)
 IPv4 Address. . . . . . . . . . . : 192.168.1.119(Preferred)
 Subnet Mask . . . . . . . . . . . : 255.255.255.0
 Lease Obtained. . . . . . . . . . : Thursday, January 28, 2021
6:00:54 AM
 Lease Expires . . . . . . . . . . : Friday, January 29, 2021 6:00:54 AM
 Default Gateway . . . . . . . . . : 192.168.1.1
 DHCP Server . . . . . . . . . . . : 192.168.1.1
 DHCPv6 IAID . . . . . . . . . . . : 234890596
 DHCPv6 Client DUID. . . . . . . . :
00-01-00-01-13-2A-5B-37-00-25-64-8C-9E-BF
 DNS Servers . . . . . . . . . . . : 192.168.1.1
 NetBIOS over Tcpip. . . . . . . . : Enabled
 Connection-specific DNS Suffix Search List :
 tampabay.rr.com
```

As you can imagine, you can use the output from the **ipconfig /all** command in a massive range of troubleshooting scenarios. Table 10.6 lists some of the most common troubleshooting symptoms, along with where to look for clues about solving them in the **ipconfig /all** output.

> **Note**
>
> When looking at **ipconfig** information, you should be sure that all information is present and correct. For example, a missing or incorrect default gateway parameter limits communication to the local segment.

TABLE 10.6 **Common Troubleshooting Symptoms that ipconfig Can Help Solve**

| Symptom | Field to Check in the Output |
|---|---|
| The user cannot connect to any other system. | Ensure that the TCP/IP address and subnet mask are correct. If the network uses DHCP, ensure that DHCP is enabled. |
| The user can connect to another on the same subnet but cannot connect to a remote system. | Ensure the default gateway is configured correctly. |
| The user is unable to browse the Internet. | Ensure the DNS server parameters are correctly configured. |
| The user cannot browse across remote subnets. | Ensure the WINS or DNS server parameters are correctly configured, if applicable. |

ExamAlert

You should be prepared to identify the output from an **ipconfig** command in relationship to a troubleshooting scenario.

Using the **/all** switch might be the most popular, but there are a few others. They include the switches listed in Table 10.7.

ExamAlert

**ipconfig** and its associated switches are widely used by network administrators and therefore should be expected to make an appearance on the exam.

TABLE 10.7 **ipconfig Switches**

| Switch | Description |
|---|---|
| **?** | Displays the **ipconfig** help screen |
| **/all** | Displays additional IP configuration information |
| **/release** | Releases the IPv4 address of the specified adapter |
| **/release6** | Releases the IPv6 address of the specified adapter |
| **/renew** | Renews the IPv4 address of a specified adapter |
| **/renew6** | Renews the IPv6 address of a specified adapter |
| **/flushdns** | Purges the DNS cache |
| **/registerdns** | Refreshes the DHCP lease and reregisters the DNS names |
| **/displaydns** | Displays the information in the DNS cache |

**Tip**

The **ipconfig /release** and **ipconfig /renew** commands work only when your system is using DHCP.

**ExamAlert**

The **ipconfig** command on the Windows client and Windows Server operating systems provides additional switches and functionality geared toward Active Directory and Dynamic DNS. You do not need to be concerned with these switches for the exam, but you can view information on them by using the **ipconfig /?** command.

# ifconfig

**ifconfig** performs the same function as **ipconfig**, but on a Linux, UNIX, or macOS system. Because Linux relies more heavily on command-line utilities than Windows, the Linux and UNIX version of **ifconfig** provides much more functionality than **ipconfig**. On a Linux or UNIX system, you can get information about the usage of the **ifconfig** command by using **ifconfig -help**. The following output provides an example of the basic **ifconfig** command run on a Linux system:

```
eth0 Link encap:Ethernet HWaddr 00:60:08:17:63:A0
 inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
 UP BROADCAST RUNNING MTU:1500 Metric:1
 RX packets:911 errors:0 dropped:0 overruns:0 frame:0
 TX packets:804 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:100
 Interrupt:5 Base address:0xe400

lo Link encap:Local Loopback
 inet addr:127.0.0.1 Mask:255.0.0.0
 UP LOOPBACK RUNNING MTU:3924 Metric:1
 RX packets:18 errors:0 dropped:0 overruns:0 frame:0
 TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
```

Although the **ifconfig** command displays the IP address, subnet mask, and default gateway information for both the installed network adapter and the local loopback adapter, it does not report DHCP lease information. Instead, you can use the **pump -s** command to view detailed information on the DHCP lease, including the assigned IP address, the address of the DHCP server, and the time remaining on the lease. You can also use the **pump** command to release and renew IP addresses assigned via DHCP and to view DNS server information.

# nslookup

The **nslookup** utility is used to troubleshoot DNS-related problems. Using **nslookup**, you can, for example, run manual name resolution queries against DNS servers, get information about your system's DNS configuration, or specify what kind of DNS record should be resolved.

When **nslookup** is started, it displays the current hostname and the IP address of the locally configured DNS server. You then see a command prompt that enables you to specify further queries. This is known as *interactive* mode. Table 10.8 lists the commands you can enter in interactive mode.

TABLE 10.8 **nslookup Switches**

| Switch | Description |
|---|---|
| **all** | Prints options, as well as current server and host information |
| **[no]debug** | Prints debugging information |
| **[no]d2** | Prints exhaustive debugging information |
| **[no]defname** | Appends the domain name to each query |
| **[no]recurse** | Asks for a recursive answer to the query |
| **[no]search** | Uses the domain search list |
| **[no]vc** | Always uses a virtual circuit |
| **domain=NAME** | Sets the default domain name to **NAME** |
| **srchlist=N1 [/N2/.../N6]** | Sets the domain to **N1** and the search list to **N1**, **N2**, and so on |
| **root=NAME** | Sets the root server to **NAME** |
| **retry=***X* | Sets the number of retries to *X* |
| **timeout=***X* | Sets the initial timeout interval to *X* seconds |
| **type=***X* | Sets the query type (for example, **A**, **ANY**, **CNAME**, **MX**, **NS**, **PTR**, **SOA**, or **SRV**) |
| **querytype=***X* | Same as **type** |
| **class=***X* | Sets the query class (for example, **IN** [Internet], **ANY**) |
| **[no]msxfr** | Uses Microsoft fast zone transfer |
| **ixfrver=***X* | Sets the current version to use in an IXFR transfer request |
| **server NAME** | Sets the default server to **NAME**, using the current default server |
| **exit** | Exits the program |

Instead of using interactive mode, you can execute **nslookup** requests directly at the command prompt. The following sample shows the output from the **nslookup** command when a domain name is specified to be resolved:

```
C:\> nslookup comptia.org

Server: nsc1.ht.ok.shawcable.net
Address: 64.59.168.13

Non-authoritative answer:
Name: comptia.org
Address: 208.252.144.4
```

As you can see from the output, **nslookup** shows the hostname and IP address of the DNS server against which the resolution was performed, along with the hostname and IP address of the resolved host.

# dig

The **dig** command is used on a Linux, UNIX, or macOS system to perform manual DNS lookups. **dig** performs the same basic task as **nslookup**, but with one major distinction: the **dig** command does not have an interactive mode and instead uses only command-line switches to customize results.

**dig** generally is considered a more powerful tool than **nslookup**, but in the course of a typical network administrator's day, the minor limitations of **nslookup** are unlikely to be too much of a factor. Instead, **dig** is often the tool of choice for DNS information and troubleshooting on UNIX, Linux, or macOS systems. Like **nslookup**, **dig** can be used to perform simple name resolution requests. The output from this process is shown in the following listing:

```
; <<>> DiG 8.2 <<>> examcram.com
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUERY SECTION:
;; examcram.com, type = A, class = IN

;; ANSWER SECTION:
examcram.com. 7h33m IN A 63.240.93.157

;; AUTHORITY SECTION:
examcram.com. 7h33m IN NS usrxdns1.pearsontc.com.
examcram.com. 7h33m IN NS oldtxdns2.pearsontc.com.
```

```
;; Total query time: 78 msec
;; FROM: localhost.localdomain to SERVER: default - 209.53.4.130
;; WHEN: Sat Oct 16 20:21:24 2018
;; MSG SIZE sent: 30 rcvd: 103
```

As you can see, **dig** provides a number of pieces of information in the basic output—more so than **nslookup**. Network administrators can gain information from three key areas of the output: **ANSWER SECTION**, **AUTHORITY SECTION**, and the last four lines of the output.

The **ANSWER SECTION** of the output provides the name of the domain or host being resolved, along with its IP address. The *A* in the results line indicates the record type that is being resolved.

The **AUTHORITY SECTION** provides information on the authoritative DNS servers for the domain against which the resolution request was performed. This information can be useful in determining whether the correct DNS servers are considered authoritative for a domain.

The last four lines of the output show how long the name resolution request took to process and the IP address of the DNS server that performed the resolution. It also shows the date and time of the request, as well as the size of the packets sent and received.

## The tcpdump Command

The **tcpdump** command is used on Linux/UNIX systems to print the contents of network packets. It can read packets from a network interface card or from a previously created saved packet file and write packets to either standard output or a file.

## The route Utility

The **route** utility is an often-used and very handy tool. With the **route** command, you display and modify the routing table on your Windows and Linux systems. Figure 10.1 shows the output from a **route print** command on a Windows system.

```
C:\>route print
===========================================================================
Interface List
 10...00 25 64 8c 9e bf ......Broadcom NetLink (TM) Gigabit Ethernet
  1...........................Software Loopback Interface 1
 14...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 15...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.1    192.168.1.119     10
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.1.0    255.255.255.0         On-link    192.168.1.119    266
    192.168.1.119  255.255.255.255         On-link    192.168.1.119    266
    192.168.1.255  255.255.255.255         On-link    192.168.1.119    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.1.119    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.1.119    266
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 14     58 ::/0                     On-link
  1    306 ::1/128                  On-link
 14     58 2001::/32                On-link
 14    306 2001:0:9d38:6ab8:2001:1013:3f57:fe88/128
                                    On-link
 10    266 fe80::/64                On-link
 14    306 fe80::/64                On-link
 14    306 fe80::2001:1013:3f57:fe88/128
                                    On-link
 10    266 fe80::51b9:996e:9fac:7715/128
                                    On-link
  1    306 ff00::/8                 On-link
 14    306 ff00::/8                 On-link
 10    266 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

FIGURE 10.1 **The output from a route print command on a Windows system**

> **Note**
>
> The discussion here focuses on the Windows **route** command, but other operating systems have equivalent commands. On a Linux system, for example, the command is also **route**, but the usage and switches are different.

In addition to displaying the routing table, the Windows version of the **route** command has a number of other switches, as detailed in Table 10.9. For complete information about all the switches available with the **route** command on a Windows system, type **route** at the command line. To see a list of the **route** command switches on a Linux system, use the command **route -help**.

TABLE 10.9 **Switches for the route Command in Windows**

| Switch | Description |
|---|---|
| **add** | Enables you to add a static route to the routing table. |
| **delete** | Enables you to remove a route from the routing table. |
| **change** | Enables you to modify an existing route. |
| **-p** | When used with the **add** command, makes the route permanent. If the **-p** switch is not used when a route is added, the route is lost upon reboot. |
| **print** | Enables you to view the system's routing table. |
| **-f** | Removes all gateway entries from the routing table. |

## nmap

The **nmap** utility is a free download for Windows or Linux used to scan ports on machines. Those scans can show what services are running as well as information about the target machine's operating system. The utility can be used to scan a range of IP addresses or just a single IP address.

# Basic Network Platform Commands

When you're working with routers, one of the most useful troubleshooting command-line tools is **show**. This Cisco-based utility takes a plethora of options after it and can be used to view almost any variable or value. Three of the most popular options are shown in Table 10.10.

TABLE 10.10 **Three Popular Options for the show Command**

| Option | Description |
|---|---|
| **interfaces** | Displays statistics for all interfaces configured on the router or access server |
| **config** | Displays the current system configuration |
| **ip route** | Displays the routing table |

ExamAlert

Know the three options for the command shown in Table 10.10 for the Network+ exam.

# Cram Quiz

1. What command can you issue from the command line to view the status of the system's ports?

   - ❍ **A. netstat -p**
   - ❍ **B. netstat -o**
   - ❍ **C. netstat -a**
   - ❍ **D. netstat -y**

2. Which of the following tools can you use to perform manual DNS lookups on a Linux system? (Choose two.)

   - ❍ **A. dig**
   - ❍ **B. nslookup**
   - ❍ **C. tracert**
   - ❍ **D. dnslookup**

3. Which of the following commands generates a "Request Timed Out" error message?

   - ❍ **A. ping**
   - ❍ **B. netstat**
   - ❍ **C. ipconfig**
   - ❍ **D. nbtstat**

4. Which of the following commands would you use to add a static entry to the ARP table of a Windows system?

   - ❍ **A. arp -a *IP Address MAC Address***
   - ❍ **B. arp -s *MAC Address IP Address***
   - ❍ **C. arp -s *IP Address MAC Address***
   - ❍ **D. arp -i *IP Address MAC Address***

5. Which command created the following output?

```
Server: nen.bx.ttfc.net
Address: 209.55.4.155
Name: examcram.com
Address: 63.240.93.157
```

   - ❍ **A. nbtstat**
   - ❍ **B. ipconfig**
   - ❍ **C. tracert**
   - ❍ **D. nslookup**

6. Which command displays statistics for all interfaces configured on the router or access server?
   - ❍ **A. show ip route**
   - ❍ **B. show config**
   - ❍ **C. show interfaces**
   - ❍ **D. show me state**

# Cram Quiz Answers

1. **C.** You can quickly determine the status of common ports by issuing the **netstat -a** command from the command line. This command output lists the ports used by the system and whether they are open and listening.
2. **A and B.** Both the **dig** and **nslookup** commands can be used to perform manual DNS lookups on a Linux system. You cannot perform a manual lookup with the **tracert** command. There is no such command as **dnslookup**.
3. **A.** The **ping** command generates a "Request Timed Out" error when it cannot receive a reply from the destination system. None of the other commands listed produce this output.
4. **C.** The **arp -s *IP Address MAC Address*** command would correctly add a static entry to the ARP table. None of the other answers are valid ARP switches.
5. **D.** The output was produced by the **nslookup** command. The other commands listed produce different output.
6. **C.** The **show interfaces** command displays statistics for all interfaces configured on the router or access server. **show ip route** displays the routing table. **show config** displays the current system configuration. "Show Me State" is Missouri's unofficial nickname, which appears on its license plates.

# Troubleshooting General Networking Issues

▶ **Given a scenario, troubleshoot general networking issues.**

## CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What one, hard-coded address must be unique on a network for networking to function properly?
2. What can you try to do to handle DHCP exhaustion if you cannot increase the scope?
3. A client has an incorrect gateway configured. What is the most likely manifestation of this error?

### Answers

1. The MAC address must be unique for each network interface card, and there can be no duplicates.
2. You can shorten the lease period for each client and, hopefully, recover addresses sooner for issue to other clients.
3. With an incorrect gateway, the client will not be able to access networking services beyond the local network.

### ExamAlert

Remember that this objective begins with "Given a scenario." This means that you may receive a drag-and-drop, matching, or "live OS" scenario where you have to click through to complete a specific objective-based task.

You will no doubt find yourself troubleshooting networking problems much more often than you would like to. When you troubleshoot these problems, a methodical approach is likely to pay off.

ExamAlert

Wiring problems are related to the cable used in a network. For the purposes of the exam, infrastructure problems are classified as those related to network devices, such as hubs, switches, and routers.

# Common Considerations

There are a number of things to take into consideration when trying to troubleshoot a problem—mainly, whether you can isolate what you are trying to find and the extent of the issue. Five broad considerations are outlined in Table 10.11.

TABLE 10.11 **Common Considerations**

| Option | Description |
|---|---|
| Device configuration review | Look at the device configuration and make certain that you are not creating, or experiencing, a bottleneck due to a configuration error. |
| Routing tables | Check routing tables to make certain that the routes within are the most cost effective in terms of hops and routes taken. |
| Interface status | Focus on optimization, redundancy, and performance as much as possible. |
| VLAN assignment | A virtual local area network (VLAN) allows you to create groups of users and systems and segment them on the network. This segmentation lets you hide segments of the network from other segments and thereby control access. You can also set up VLANs to control the paths that data takes to get from one point to another. A VLAN is a good way to contain network traffic to a certain area in a network but be sure that the resources you are using can support what you create. |
| Network performance baselines | Creating baselines is only a part of the equation; you also have to analyze them. However, too many administrators collect information that they never do anything with. Be sure to look at the baseline information regularly and track current conditions to see what needs to be improved upon. |

# Common Problems to Be Aware Of

In the eyes of CompTIA and the Network+ exam, you should be aware of some problems more than others. Although other sections have looked at problems in particular areas, pay special attention to those that fall within this section as you study for the exam.

## Collisions

Generally, as more systems are added to a network, the possibility for more collisions to occur increase, and the network becomes slower. The type of collision detection used (discussed in Chapter 3) can impact performance.

## Broadcast Storm

When an abnormally high number of broadcast packets are sent across the network within a short period of time, this is known as a *broadcast storm*, and it can degrade network performance as switches become overwhelmed with trying to keep up with the flood of packets.

## Multicast Flooding

Similar to broadcast storms, *multicast flooding* tends to be more prevalent on VLANs and occurs when a switch receives a multicast packet that has an IP address for a group it has not learned. Since the switch does not know what to do with it, the switch floods that packet out of all ports on the VLAN. Many switches have an option to disallow this behavior, and you configure them to only forward unregistered packets to ports on a VLAN that are connected to specific ports.

## Asymmetrical Routing

When a packet travels from a source to a destination in one path and takes a different path when it returns to the source, it is known as *asymmetrical routing*. The biggest weakness to this is the risk that packets might not arrive in the right order.

> **Note**
>
> The opposite of asymmetrical routing is symmetrical routing: the network uses a single route for incoming and outgoing packets.

## Switching Loops

A *switching loop* can occur any time there are multiple paths between two endpoints: more than one connection between two switches, for example. When there is a loop, it creates broadcast storms as broadcasts and multicasts are forwarded by switches out every port (the switch[es] will repeatedly rebroadcast

the messages, thus flooding the network). Layer 2 headers do not support a time to live (TTL) value, so a frame sent into a looped topology can loop forever.

## Routing Loops

Similar to switching loops, a *routing loop* can go on forever. This typically is a problem when the routing tables contain cyclical entries. For example, suppose router A needs to send data to router C and believes the best way to get there is to forward it first to router B. Router B gets the data, sees it is for C, and has in its own table that the best way to get there is to go through router A. In this scenario, a loop is created that can go on forever, preventing the data from reaching its destination.

## Missing Route

A missing route can also prevent data from reaching its destination. Often the cause can be broken topology, reliance on static routes, or misconfiguration of the routing protocol.

## Low Optical Link Budget

While it may sound like a problem with the company's comptroller, in reality, *low optical link budget* refers to the optical power budget in a fiber-optic communication link. This is the allocation of available optical power considering such factors as attenuation, splice losses, and connector losses.

## Incorrect VLAN

While VLANs offer a plethora of positives, problems can occur when a user moves or gets connected to the wrong one. On a regular basis, an administrator should ensure that the user system is plugged into the correct VLAN port and that there are no problems with users connecting to an interface which is not assigned to them.

## DNS Issues

When the wrong Domain Name Service (DNS) values (typically primary and secondary) are entered during router configuration, users cannot take advantage of the DNS service. Depending on where the wrong values are given, name resolution may not occur (if all values are incorrect), or resolution could

take a long time (if only the primary value is incorrect), thus giving the appearance that the web is taking a long time to load.

Make sure the correct values appear for DNS entries in the router configuration to avoid name resolution problems.

## Incorrect Gateway

The default gateway configured on the router is the place where the data goes after it leaves the local network. Although many routes can be built dynamically, it is often necessary to add the first routes when installing/replacing a router. You can use the **ip route** command on most Cisco routers to do this from the command line, or most routers include a graphical interface for simplifying the process.

When you have the gateways configured, use the **ping** and **tracert/traceroute** utilities to verify connectivity and proper configuration.

**ExamAlert**

Know the tools to use to test connectivity.

## Incorrect Subnet Mask

When the subnet mask is incorrect, the router thinks the network is divided into segments other than how it is actually configured. Because the purpose of the router is to route traffic, a wrong value here can cause it to try to route traffic to subnets that do not exist. The value of the subnet mask on the router must match the true configuration of the network.

## Duplicate or Incorrect IP Address

Every IP address on a network must be unique. This is true not only for every host, but for the router as well, and every network card in general. The scope of the network depends on the size of the network that the card is connected to; if it is connected to the LAN, the IP address must be unique on that LAN, whereas if it is connected to the Internet, that address must be unique on it.

If there is a duplicate address, in the best scenario you will receive messages indicating duplicate IP addresses, and in the worst scenario, network traffic will become unreliable. In all cases, you must correct the problem and make certain duplicate addresses exist nowhere on your network, including the routers.

## Duplicate MAC Addresses

The MAC address is hard-coded into the NIC and cannot be changed. It consists of two components: one identifies the vendor, and the other identifies a serial number so that it will be unique. Of all things on the network, this is the one value that must stay constant for ARP, RARP, and other protocols to be able to translate IP addresses to machines and have communication across the network.

Given that, the only way for a MAC address to not be unique is for someone to be trying to add a rogue device impersonating another (typically a server). If this is the case, there will be serious problems on the network, and you must find—and disable—the unauthorized device immediately.

## Expired IP Address

DHCP leases IP addresses to clients and—when functioning properly—continues to renew those leases as long at the client needs them. An expired address can mean that the DHCP server is down or unavailable, and the client will typically lose its address, rendering it unable to continue communicating on the network.

Each system must be assigned a unique IP address so that it can communicate on the network. Clients on a LAN have a private IP address and matching subnet mask. Table 10.12 shows the private IP ranges. If a system has the wrong IP or subnet mask, it cannot communicate on the network. If the client system has *misconfigured DHCP settings*, such as an IP address in the 169.254.0.0 APIPA range, the system is not connected to a DHCP server and is not able to communicate beyond the network.

TABLE 10.12 **Private Address Ranges**

| Class | Address Range | Default Subnet Mask |
|---|---|---|
| A | 10.0.0.0 to 10.255.255.255 | 255.0.0.0 |
| B | 172.16.0.0 to 172.31.255.255 | 255.255.0.0 |
| C | 192.168.0.0 to 192.168.255.255 | 255.255.255.0 |

ExamAlert

You need to know the private address ranges in Table 10.12.

## Rogue DHCP Server

A *rogue DHCP server* is any DHCP server on the network that was added by an unauthorized party and is not under the administrative control of the network administrators. It can be used to give false values or to set up clients for network attacks, such as on-path/man-in-the-middle attack.

## Certificate Issues

An *untrusted SSL certificate* is usually one that is not signed or that has expired. Sometimes, this issue can be caused by a client using an older browser or one that is not widely supported. As a general rule, though, users should be instructed to stop attempting to visit a site if they see this error.

## NTP Issues/Incorrect Time

*Incorrect time* on a network can be more than just an annoyance because timestamps are important if you're trying to document an attack. Most network devices use Network Time Protocol (NTP) to keep the system time as defined by a designated server. You should make sure that server has the correct time on it and is updated, patched, and secured just as you would any other network critical server.

## DHCP Scope Exhaustion

The DHCP scope is the pool of possible IP addresses a DHCP server can issue. If that pool becomes exhausted and not enough addresses are available for the devices needing to connect, devices will not be given the values they need (many will then resort to using APIPA addresses in the 169.254 range, as discussed earlier).

The only solution is to increase the scope and/or decrease the lease time. If you reduce the lease time from days to hours, more addresses should become available as hosts leave the network at the end of their shifts, and those values become available for use by others.

## Blocked Ports, Services, or Addresses

As a security rule, only needed ports should be enabled and allowed on a network. Unfortunately, you don't always have a perfect idea of which ports you need, and it is possible to inadvertently have some blocked TCP/UDP ports that you need to use.

If you find your firewall is blocking a needed port, you should open that port (make an exception) and allow it to be used.

## Incorrect Firewall Settings

*Incorrect firewall settings* typically fall under the category of blocking ports that you need open (previously addressed) or allowing ports that you don't need. From a security perspective, the latter situation is worse because every open port represents a door that an intruder could use to access the system or at least a vulnerability. Be sure to know which ports are open, and close any that are not needed.

## Incorrect ACL Settings

The purpose of an access control list (ACL) is to define who or what can access your system. Incorrect ACL settings could keep too many off, but typically the error is allowing too many on. Used properly, an ACL can enable devices in your network to ignore requests from specified users or systems or to grant them certain network privileges. You may find that a certain IP address is constantly scanning your network, and you can block this IP address. If you block it at the router, the IP address will automatically be rejected anytime it attempts to use your network.

## Unresponsive Service

When a service does not respond, the reason could be that it is overloaded, is down, or has bad configuration. The first order of business is to ascertain which of these three the situation is and then decide what you need to do to fix it. If the server/service is overloaded, you can look for a way to increase the capacity or balance the load. If the server/service is down, you can investigate why and what needs to be done to bring it back up again. If the server/service is misconfigured, you can make the necessary changes to configure it properly.

## BYOD Challenges

Bring-your-own-device (BYOD) challenges occur when employees are allowed to bring personally owned mobile devices (laptops, tablets, and smartphones) to their workplace and use them on the network. Good onboarding and offboarding procedures (discussed in Chapter 8, "Network Operations") as well as MDM policies should be used to help protect network resources and still allow these devices to be used in the workplace.

## Licensed Feature Issues

Many devices, such as switches, have features that are available with them only if licensed. Many times, you can enable the feature and use it on a trial basis before purchasing (a grace period, if you will), but you must purchase and install the number of licenses required for that feature before the grace period ends or the feature will disable itself. To keep legal, you should always be cognizant of licensing issues and careful to not run afoul of them.

# Hardware Failure

If you are looking for a challenge, troubleshooting hardware infrastructure problems is for you. It is often not an easy task and usually involves many processes, including baselining and performance monitoring. One of the keys to identifying the hardware failure is to know what devices are used on a particular network and what each device is designed to do. Table 10.13 lists some of the common hardware components used in a network infrastructure, as well as some common problem symptoms and troubleshooting methods.

TABLE 10.13 **Common Network Hardware Components, Their Functions, and Troubleshooting Strategies**

| Networking Device | Function | Troubleshooting and Failure Signs |
|---|---|---|
| Hub | Hubs are used with a star network topology and UTP cable to connect multiple nodes. | Because hubs connect multiple network devices, if many devices are unable to access the network, the hub may have failed. When a hub fails, all devices connected to it cannot access the network. In addition, hubs use broadcasts and forward data to all the connected ports, increasing network traffic. When network traffic is high, and the network is operating slowly, it may be necessary to replace slow hubs with switches. |
| Switch | Like hubs, switches are used with a star topology to create a central connectivity device. | The inability of several network devices to access the network may indicate a failed switch. If the switch fails, all devices connected to the switch cannot access the network. Switches forward data only to the intended recipient, allowing them to manage data better than hubs. |
| Router | Routers are used to separate broadcast domains and to connect different networks. | If a router fails, network clients are unable to access remote networks connected by the router. For example, if clients access a remote office through a network router, and the router fails, the remote office is unavailable. You can test router connectivity using utilities such as **ping** and **tracert**. |

| Networking Device | Function | Troubleshooting and Failure Signs |
|---|---|---|
| Wireless access point | Wireless access points provide the bridge between the wired and wireless network. | If wireless clients cannot access the wired network, the AP may have failed. However, you should check many configuration settings first. |

ExamAlert

Be familiar with the devices listed in Table 10.13 and their failure signs.

For more information on network hardware devices and their functions, refer to Chapter 4, "Network Implementations."

# Network Performance Issues

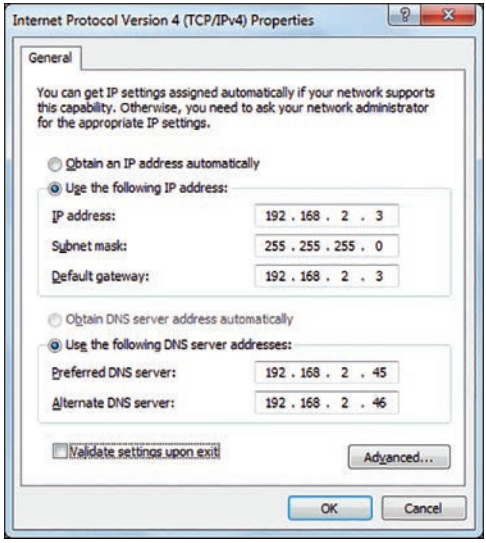
Chapter 8 looked at many performance issues, and most of the issues discussed in this section already have been addressed as they relate to networking. Be aware of those issues and that it is always a balancing act trying to get optimum performance from a network when working with so many disparate devices.

# Cram Quiz

1. Although many routes can be built dynamically, it is often necessary to add the first routes when installing or replacing a router. Which of the following commands can you use on most Cisco routers to do this from the command line?
   - ❍ **A. ip route**
   - ❍ **B. add route**
   - ❍ **C. first route**
   - ❍ **D. route change**

2. Which of the following best describes the function of the default gateway?
   - ❍ **A.** It converts hostnames to IP addresses.
   - ❍ **B.** It converts IP addresses to hostnames.
   - ❍ **C.** It enables systems to communicate with systems on a remote network.
   - ❍ **D.** It enables systems to communicate with routers.

**3.** Consider the following figure. Which of the following statements is true?




- ❍ **A.** The system cannot access the local network.
- ❍ **B.** The system cannot access remote networks.
- ❍ **C.** The system cannot have hostname resolution.
- ❍ **D.** The system has the wrong subnet mask.

**4.** Which of the following bits of IP information are mandatory to join the network? (Choose two.)

- ❍ **A.** Subnet mask
- ❍ **B.** IP address
- ❍ **C.** DNS address
- ❍ **D.** Default gateway

**5.** All of a sudden, some devices on your local network are not receiving their normal IP addresses, and some of them are now using APIPA addresses in the 169.254 range. What has most likely occurred?

- ❍ **A.** Low optical link budget
- ❍ **B.** NTP time issue
- ❍ **C.** Broadcast storm
- ❍ **D.** DHCP scope exhaustion

## Cram Quiz Answers

1. **A.** Although many routes can be built dynamically, it is often necessary to add the first routes when installing or replacing a router. You can use the **ip route** command on most Cisco routers to do this from the command line.
2. **C.** The default gateway enables the system to communicate with systems on a remote network, without the need for explicit routes to be defined. The default gateway can be assigned automatically using a DHCP server or can be input manually.
3. **B.** The IP addresses of the client system and the default gateway are the same. This error probably occurred when the IP address information was input. In this configuration, the client system would likely access the local network and resources but not remote networks because the gateway address to remote networks is wrong. The DNS, IP, and subnet mask settings are correct.
4. **A and B.** Configuring a client requires at least the IP address and a subnet mask. The default gateway, DNS server, and WINS server are all optional, but network functionality is limited without them.
5. **D.** The DHCP scope is the pool of possible IP addresses a DHCP server can issue. If that pool becomes exhausted and not enough addresses are available for the devices needing to connect, devices will not be given the values they need (many will then resort to using APIPA addresses in the 169.254 range).

# What's Next?

Congratulations! You finished the reading and are now familiar with all the objectives on the Network+ exam. You are now ready for the practice exams that are posted online to accompany this book. There are two multiple-choice question exams to help you determine how prepared you are for the actual exam and which topics you need to review further.

*This page intentionally left blank*

# Glossary

## Numbers and Symbols

**10BASE-T** The 802.3i specification for running Ethernet at 10 Mbps over twisted-pair cabling. The maximum length of a 10BASE-T (also written as *10Base-T*) segment is 100 meters (328 feet).

**10GBASE-T** A 2006 standard to provide 10 Gbps connections over unshielded or shielded twisted-pair cables, over distances up to 100 meters using category 6a (category 6 can reach 55 meters).

**100BASE-T** The IEEE 802.3 specification for running Ethernet at 100 Mbps over twisted-pair cabling. The maximum length of a 100BASE-T segment is 100 meters (328 feet).

**1000BASE-LX** A standard for Gigabit Ethernet intended for use with long-wavelength (LX) transmissions over long cable runs of fiber-optic cabling.

**1000BASE-SX** A fiber-optic Gigabit Ethernet standard for operation over multimode fiber.

**1000BASE-T** An IEEE 802.3ab standard that specifies Gigabit Ethernet over Category 5 or better

UTP cable. The standard allows for full-duplex transmission using four pairs of twisted cable up to 100 meters.

**568A/568B standards** Telecommunications standards from the Telecommunications Industry Association (TIA) and the Electronics Industry Association (EIA). These 568 standards specify the pin arrangements for the RJ-45 connectors on UTP or STP cables. The number 568 refers to the order in which the wires within the UTP cable are terminated and attached to the connector.

# A

**A** An address record. This refers to one of three machines typically: the host sending data, the host receiving data, or an intermediary between the two (the next hop).

**AAA** Authentication, authorization, and accounting. Authentication is the process to determine whether someone is authorized to use the network—if the person can log on to the network. Authorization refers to identifying the resources a user can access after the user is authenticated. Accounting refers to the tracking methods used to identify who uses the network and what they do on the network.

**AAAA** Authentication, authorization, accounting, and auditing. Authentication is the process to determine whether someone is authorized to use the network—if the person can log on to the network. Authorization refers to identifying the resources a user can access after the user is authenticated. Accounting refers to the tracking methods used to identify who uses the network and what they do on the network. Auditing refers to the ability to associate actions with the machine/user in question.

**AAAA record** The DNS record that maps a hostname to a 128-bit IPv6 address. This is also known as the IPv6 address record.

**access control vestibule** A physical security access control system that requires one set of doors to close before the second set opens. Previously known as a mantrap.

**access point (AP)** A transmitter and receiver (transceiver) device commonly used to facilitate communication between a wireless client and a wired network. Wireless APs (or WAPs) are used with the wireless infrastructure network topology to provide a connection point between WLANs and a wired Ethernet LAN.

**ACK** The acknowledgment message sent between two hosts during a TCP session.

**ACL (access control list)** The list of trustees assigned to a file or directory. A trustee can be any object available to the security subsystem. The term *ACL* is also used with routers and firewall systems to refer to the list of permitted computers or users.

**Active Directory** A directory services system used in Windows network environments that enables

network objects to be stored in a database. This database can then be divided and distributed among different servers on the network.

**active hub** A hub that has power supplied to it for the purposes of regenerating the signals that pass through it.

**ad hoc topology** A wireless network layout whereby devices communicate directly among themselves without using an access point. Sometimes called an unmanaged or peer-to-peer wireless topology.

**address** A set of numbers used to identify and locate a resource or device on a network. An example is an IP address such as 192.168.2.1.

**administrator** A person responsible for the control and security of the user accounts, resources, and data on a network.

**Administrator account** On a Windows system, the default account that has rights to access everything and to assign rights to other users on the network. Unlike other user accounts, the Administrator account cannot be deleted.

**ADSL (asymmetric digital subscriber line)** A service that transmits digital voice and data over existing (analog) phone lines.

**AES (Advanced Encryption Standard)** An encryption algorithm for securing sensitive networks used by U.S. government agencies. It has become the encryption standard for corporate networks.

**AH (Authentication Header)** One of the two separate protocols IPSec consists of (the other being ESP). AH provides the authentication and integrity checking for data packets.

**antivirus software** A software application that detects and removes viruses.

**AP (access point)** A network device that offers connectivity between wireless clients and (usually) a wired portion of the network.

**APC (angle physical contact)** A connector commonly used with fiber cables—usually single mode—to keep the signal from bouncing back down the line.

**APIPA (Automatic Private IP Addressing)** A technology implemented on certain Windows platforms through which a system assigns itself an IP address in the absence of a DHCP server. Addresses are assigned from the 169.254.*x*.*x* address range.

**application layer** Layer 7 of the OSI model, which provides support for end users and for application programs using network resources.

**application-level firewall** A firewall that operates at the application layer of the OSI model. An application layer firewall can inspect data packets traveling to or from an application.

**application log** A log file on a Windows system that provides information on events that occur within an application.

**APT (Advanced Persistent Threat)** An unauthorized person or program in a network, undetected, for an exceedingly long period of time.

**archive bit** A flag that is set on a file after it has been created or altered. Some backup methods reset the flag to indicate that it has been backed up.

**ARIN (American Registry for Internet Numbers)** The regional Internet registry responsible for managing both IPv4 and IPv6 IP number distribution.

**ARP (Address Resolution Protocol)** A protocol in the TCP/IP suite used to resolve IP addresses to MAC addresses. Specifically, the ARP command returns a Layer 2 address for a Layer 3 address.

**ARP ping** The ARP utility that resolves IP addresses to MAC addresses. The ARP ping utility tests connectivity by pinging a MAC address directly.

**ARP table** A table of entries used by ARP to store resolved ARP requests. Entries can also be manually stored.

**array** A group of devices arranged in a fault-tolerant configuration. *See also* RAID.

**AS (autonomous system)** A collection of connected IP routing prefixes under the control of a network administrator or entity that offers a common and defined routing policy to the Internet.

**ASIC (application-specific integrated circuit)** An integrated circuit designed for a particular use instead of for general-purpose uses.

**ASP (application service provider)** A vendor who provides computer-based services over the network.

**ATM (Asynchronous Transfer Mode)** A packet-switching technology that provides transfer speeds ranging from 1.544 Mbps to 622 Mbps.

**attenuation** The loss of signal experienced as data transmits over distance and across the network medium.

**AUP (acceptable use policy)** A policy created by an organization defining what is acceptable on their resources (network, computers, and so on).

**authentication** The process by which a user's identity is validated on a network. The most common authentication method is a username and password combination.

# B

**B (bearer) channel** In ISDN, a 64 Kbps channel that carries data. *See also* D (delta) channel.

**backbone** A network segment that acts as a trunk between other network segments. Backbones typically are high-bandwidth implementations, such as fiber-optic cable.

**backup schedule** A document or plan that defines what type of backups are made, when, and what data is backed up.

**bandwidth** The width of the range of electrical frequencies, or how many channels the medium can support. Bandwidth correlates to the amount of data that can traverse the medium at one time, but other factors determine the maximum speed supported by a cable.

**baseband** A term applied to any medium that can carry only a single data signal at a time. Compare with broadband.

**baseline** A measurement of performance of a device or system for the purposes of future comparison. Baselining is a common server administration task.

**baud rate** The speed or rate of signal transfer. Baud rate bandwidth is measured in cycles per second, or hertz (Hz). The word *baud* is derived from the name of French telegraphy expert J. M. Baudot.

**BCP (business continuity plan)** The strategy for addressing potential threats to a company and creation of systems to aid in the prevention of threats and recovery from problems.

**beaconing** In a wireless network, the continuous transmission of small packets (beacons) that advertise the presence of a base station (access point).

**BERT (bit-error rate test)** A test to see the number of received bits of a data stream that has changed due to noise, interference, or other distortion.

**BGP (Border Gateway Protocol)** A protocol used between gateway hosts on the Internet. BGP examines the routing table, which contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. BGP communicates between the routers using TCP.

**binary** A base 2 numbering system used in digital signaling. It uses only the numbers 1 and 0.

**binding** The process of associating a protocol with a NIC.

**biometrics** The science and technology of measuring and analyzing biological data. Biometrics are used for security purposes to analyze and compare characteristics such as voice patterns, retina patterns, and hand measurements.

**BIOS (Basic Input/Output System)** A basic set of instructions that a device needs to operate. Compare with UEFI.

**bit** An electronic digit used in the binary numbering system. Bit is a contraction of the terms *binary* and *digit*.

**blackout** A total loss of electrical power.

**BLE (Bluetooth Low Energy)** A form of Bluetooth networking technology that uses very little energy.

**Bluetooth** A low-cost, short-range RF technology designed to replace many of the cords used to connect devices. Bluetooth uses 2.4 GHz RF and provides transmission speeds up to 2 Mbps.

**BNC (British Naval Connector/ Bayonet Neill-Concelman) connector** A family of connectors typically associated with thin coaxial cabling and 10BASE2 networks. BNC connectors use a twist-and-lock mechanism to connect devices to the network.

**BOOTP (Bootstrap Protocol)** A TCP/IP protocol used by a network device to obtain an IP address and other network information, such as

server address and default gateway from a configuration server.

**bound medium** Any medium that has physical constraints, such as coaxial, fiber-optic, and twisted pair. Compare with unbound medium.

**boundless medium** *See* unbound medium.

**BPDU (bridge protocol data unit)** A simple data message exchanged between switches. It contains information on ports and provides the status of ports and bridges to other switches.

**BRI (Basic Rate Interface)** An ISDN digital communications line that consists of three independent channels: two B channels each at 64 Kbps and one D channel at 16 Kbps. ISDN BRI is often referred to as 2B+D. *See also* ISDN and PRI.

**bridge** A device that connects and passes packets between two network segments that use the same communications protocol. Bridges operate at the data link layer of the OSI model. A bridge filters, forwards, or floods an incoming frame based on the packet's MAC address.

**bridging address table** A list of MAC addresses that a bridge keeps and uses when it receives packets. The bridge uses the bridging address table to determine which segment the destination address is on before it sends the packet to the next interface or drops the packet (if it is on the same segment as the sending node).

**broadband** A communications strategy that uses analog or digital signaling over multiple communications channels.

**broadcast** A packet-delivery system in which a copy of a packet is transmitted to all hosts attached to the network.

**broadcast storm** An undesirable condition in which broadcasts become so numerous that they bog down the flow of data across the network.

**brownout** A short-term decrease in the voltage level, usually caused by the startup demands of other electrical devices.

**BSSID (basic service set identifier)** The MAC address of the wireless access point (AP).

**buffer** An area of memory in a device used to temporarily store data before it is forwarded to another device or location.

**bus topology** A linear LAN architecture in which all devices connect to a common cable, called a bus or backbone.

**butt set** A type of handset typically associated with telephony systems. It is used to test and access the phone line using clip wires that attach to the phone cable.

**BYOD (bring your own device)** A policy governing employees bringing personally owned devices (laptops, smartphones, and the like) to the workplace and the use of those devices to access company data.

**byte** A set of bits (usually 8) that operate as a unit to signify a character.

# C

**CaaS (Communication as a Service)** A cloud computing model for providing ubiquitous access to shared pools of configurable resources.

**cable modem** A device that provides Internet access over cable television lines.

**cable stripper** A tool used to strip the sheathing from copper cabling.

**cable tester** A device used to check for electrical continuity along a length of cable. *Cable tester* is a generic term that can be applied to devices such as volt/ohm meters and TDRs.

**caching-only server** A type of DNS server that operates the same way as secondary servers except that a zone transfer does not take place when the caching-only server is started.

**CAM (content addressable memory)** A type of computer memory used in high-speed searching applications.

**CAN (campus-area network)** A wide-area network (WAN) created to service a campus area.

**CARP (Common Address Redundancy Protocol)** A protocol that enables multiple hosts on the same network to share a set of IP addresses and thus provides failover redundancy. It is commonly used with routers and firewalls and can provide load balancing.

**carrier** A signal that carries data. The carrier signal is modulated to create peaks and troughs, which represent binary bits.

**CASB (cloud access security broker)** Software that sits between cloud service users and cloud applications to monitor all activity and enforce security policies.

**CAT (Computer and Telephone)** A designation of resources, usually wiring, used to provide service to computers or telephones.

**Cat 5** Data-grade cable that typically was used with Fast Ethernet operating at 100 Mbps with a transmission range of 100 meters.

**Cat 5e** Data-grade cable used on networks that run at 10/100 Mbps and even up to 1000 Mbps. Category 5e cabling can be used up to 100 meters, depending on the implementation and standard used. Category 5e cable provides a minimum of 100 MHz of bandwidth.

**Cat 6** High-performance UTP cable that can transmit data up to 10 Gbps.

**Cat 6a** Cable that offers improvements over Category 6 by offering a minimum of 500 MHz of bandwidth. It specifies transmission distances up to 100 meters with 10 Gbps networking speeds. Also called augmented 6.

**Cat 7** Cable that offers improvements over Category 6a by offering 600 MHz of bandwidth and improved crosstalk suppression. It specifies transmission distances up to 100 meters with 10 Gbps networking speeds.

**Cat 8** Twisted-pair cabling that offers improvement in speed over Cat 7, but it is intended only for short distances (such as between switches and servers in a datacenter). It offers 2000 MHz of bandwidth and specifies distances up to 30 meters with 40 Gbps networking speeds.

**CCTV (closed-circuit TV)** An acronym for video cameras used to watch a particular place and send (transmit) to a particular location.

**CDMA (code-division multiple access)** A multiple-access channel method used to provide bandwidth sharing.

**change control** A process in which a detailed record of every change made to the network is documented.

**channel** A communications path used for data transmission.

**CHAP (Challenge Handshake Authentication Protocol)** A protocol that challenges a system to verify identity. CHAP is an improvement over Password Authentication Protocol (PAP) in which one-way hashing is incorporated into a three-way handshake. RFC 1334 applies to both PAP and CHAP.

**checksum** A basic method of error checking that involves calculating the sum of bytes in a section of data and then embedding the result in the packet. When the packet reaches the destination, the calculation is performed again to make sure that the value is still the same.

**CIA (confidentiality, integrity, and availability)** A triad model of computing security in which attention is paid to the three elements named.

**CIDR (classless interdomain routing)** An IP addressing scheme that enables a single IP address to designate many unique IP addresses. CIDR addressing uses an IP address followed by a / and the IP network prefix. An example of a CIDR address is 192.168.100.0/16. CIDR is sometimes called supernetting.

**circuit-level firewall** A type of network security system whereby network traffic is filtered based on specified session rules and may be restricted to recognized computers only.

**circuit switching** A method of sending data between two parties in which a dedicated circuit is created at the beginning of the conversation and is broken at the end. All data transported during the session travels over the same path, or circuit.

**Class A network** A TCP/IP network that uses addresses from 1 to 126 and supports up to 126 subnets with 16,777,214 unique hosts each.

**Class B network** A TCP/IP network that uses addresses from 128 to 191 and supports up to 16,384 subnets with 65,534 unique hosts each.

**Class C network** A TCP/IP network that uses addresses from 192 to 223 and supports up to 2,097,152 subnets with 254 unique hosts each.

**Class D network** A TCP/IP network that uses addresses from 224.0.0.0 to 239.255.255.255 for

multicasting data to multicast-capable hosts on a network.

**Class E network** A TCP/IP network that uses addresses from 240.0.0.0 to 255.255.255.255 for future development and research.

**CLI (command-line interface)** A nongraphical interface, such as a text window, used for running commands and interacting with the system.

**client** A node that uses the services from another node on a network.

**client/server networking** A networking architecture in which front-end, or client, nodes request and process data stored by the back-end, or server, node.

**cloud computing** The hosting, storage, and delivery of computing as a service rather than a product. The end user accesses remotely stored programs and other resources through the Internet without the need for expensive local networking devices, services, and support. Various industry cloud computing concepts include public, private, hybrid, and community cloud.

**clustering** A technology that enables two or more computers to act as a single system to provide improved fault tolerance, load balancing, and failover capability.

**CNAME (canonical name)** An alias or nickname for a canonical hostname record in a Domain Name System (DNS) database. CNAME records are used to give a single computer multiple names (aliases).

**coaxial cable** A data cable, commonly referred to as coax, that is made of a solid copper core insulated and surrounded by braided metal and covered with a thick plastic or rubber covering. Coax is the standard cable used in cable television and in older bus topology networks.

**cold site** A disaster recovery site that provides office space, but the customer provides and installs all the equipment needed to continue operations.

**cold spare** A redundant piece of hardware stored in case a component should fail. It is typically used for server systems.

**collision** The result of two frames simultaneously transmitting on an Ethernet network and colliding, thereby destroying both frames.

**collision domain** A segment of an Ethernet network between managing nodes, where only one packet can be transmitted at a time. Switches, bridges, and routers can be used to segment a network into separate collision domains.

**communication** The transfer of information between nodes on a network.

**concentrator** A device that combines several communications channels into one. It is often used to combine multiple terminals into one line.

**connectionless communication** Packet transfer in which delivery is not guaranteed.

**connection-oriented communication** Packet transfer in which delivery is guaranteed.

**connectivity** The linking of nodes on a network for communication to take place.

**convergence** The capability of a router to detect and accommodate to change when a change in network routing is made.

**copy backup** Normally, a backup of an entire hard drive. A copy backup is similar to a full backup, except that the copy backup does not alter the state of the archive bits on files.

**CoS (class of service)** A parameter used in data and voice to differentiate the types of payloads being transmitted.

**cost** A value used to encourage or discourage the use of a certain route through a network. Routes that are to be discouraged are assigned a higher cost, and those that are to be encouraged are assigned a lower cost. *See also* metric.

**CPU (central processing unit)** The main processor in a computing device.

**cracker** A person who attempts to break software code or gain access to a system to which he or she is not authorized. *See also* hacker.

**cracking** The process of attempting to break software code, normally to defeat copyright protection or alter the software's functioning. Also the process of attempting to gain unauthorized access to a computer system. *See also* hacker.

**CRAM-MD5** A challenge-response authentication mechanism.

**CRC (cyclic redundancy check)** A method used to check for errors in packets that have been transferred across a network. A computation bit is added to the packet and recalculated at the destination to determine whether the entire content of the packet has been correctly transferred.

**crimper** A tool used to join connectors to the ends of network cables.

**crossover cable** A cable that can be used to directly connect two devices—such as two computer systems—or as a means to expand networks that use devices such as hubs or switches. A traditional crossover cable is a UTP cable in which the wires are crossed for the purposes of placing the transmit line of one device on the receive line of the other. A T1 crossover is used to connect two T1 CSU/DSU devices in a back-to-back configuration.

**crosstalk** Electronic interference caused when two wires are too close to each other, and the adjacent cable creates interference.

**CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)** A contention media access method that uses collision-avoidance techniques.

**CSMA/CD (Carrier Sense Multiple Access with Collision Detection)** A contention media access method that uses collision-detection and retransmission techniques.

**CSU/DSU (channel service unit/data service unit)** A device that acts as a translator between the LAN data format and the WAN data format. Such a conversion is necessary

because the technologies used on WAN links are different from those used on LANs.

**cut-through packet switching** A method of switching that does not copy the entire packet into the switch buffers. Instead, the destination address is captured into the switch, the route to the destination node is determined, and the packet is quickly sent out the corresponding port. Cut-through packet switching maintains a low latency.

**CVE (common vulnerabilities and exposures)** A list of publicly known vulnerabilities containing ID numbers, descriptions, and references.

**CVW (collaborative virtual workspace)** An environment used for collaboration and interaction of participants that may be spread over large distances.

**CWDM (coarse wavelength-division multiplexing)** A method of multiplexing in which different signals operate at different speeds. The best example of this is cable modems, allowing for different speeds of uploading and downloading.

# D

**DaaS (Desktop as a Service)** Software that separates the desktop environment and associated application software from the physical client device that is used to access it.

**data field** In a frame, the field or section that contains the data.

**data link layer** Layer 2 of the OSI model, which is above the physical layer. Data comes off the cable, goes through the physical layer, and goes into the data link layer. The data link layer has two distinct sublayers: MAC and LLC.

**datagram** An information grouping transmitted as a unit at the network layer. *See also* packet.

**dB** Decibels. A sound measurement.

**DB-9** A nine-pin connector used for serial port or parallel port connection between PCs and peripheral devices.

**DB-25** A 25-pin connector used for serial port or parallel port connection between PCs and peripheral devices.

**D (delta) channel** The channel used on ISDN to communicate signaling and other related information. Use of the D channel leaves the B channels free for data communication. *See also* B (bearer) channel.

**DCS (distributed computer system)** A system in which the whole is divided into many parts. The best example of this is using multiple computers to work together and appear to the user as a single entity.

**DDNS (Dynamic Domain Name Service)** A form of DNS that enables systems to be registered and deregistered with DNS dynamically. DDNS is facilitated by DHCP, which passes IP address assignments to the DNS server for entry into the DNS server records. This is in contrast with the conventional DNS

system, in which entries must be manually made.

**DDoS (distributed denial-of-service) attack** A DoS attack that utilizes more than one computer in the attack. *See* DoS (denial-of-service) attack.

**dedicated line** A dedicated circuit used in WANs to provide a constant connection between two points.

**default gateway** Normally, a router or a multihomed computer to which packets are sent when they are destined for a host on a different network.

**demarcation point** The point at which communication lines enter a customer's premises. Sometimes shortened to simply *demarc*.

**destination address** The network address to which data is sent.

**DHCP (Dynamic Host Configuration Protocol)** A protocol that provides dynamic IP addressing to DHCP-enabled workstations on the network.

**dial-up networking** The connection of a remote node to a network using POTS.

**differential backup** A backup of only the data that has been created or changed since the previous full backup. In a differential backup, the state of the archive bits is not altered.

**dig** A command used on a Linux, UNIX, or macOS system to perform manual DNS lookups.

**directory services** A system that enables network resources to be viewed as objects stored in a database. This database can then be divided and distributed among different servers on the network. An example of directory services includes LDAP or Microsoft Active Directory (AD).

**disaster recovery plan** A plan for implementing duplicate computer services if a natural disaster, a human-made disaster, or another catastrophe occurs. A disaster recovery plan includes offsite backups and procedures to activate information systems in alternative locations.

**distance-vector routing** A type of routing in which a router uses broadcasts to inform neighboring routers on the network of the routes it knows about. Compare with link-state routing.

**DLC (data link control)** The service provided by the data link layer of the OSI model.

**DLP (data loss prevention)** A system designed to detect and respond to potential breaches.

**DLR (device-level ring)** A protocol that provides a means of detecting, managing, and recovering from faults in a ring-based topology network.

**DNAT (Destination Network Address Translation)** A technique for transparently changing the destination of an end route and performing the inverse function for any replies.

**DNS (Domain Name Service)** A service/system/server used to translate domain names, such as www.quepublishing.com, into IP addresses, such as 165.193.123.44.

DNS uses a hierarchical namespace that enables the database of host-name-to-IP address mappings to be distributed across multiple servers.

**DOCSIS (Data-Over-Cable Service Interface Specification)** A telecommunications standard for transmitting high-speed data over existing cable TV systems.

**domain** A logical boundary of an Active Directory structure on Windows servers. Also, a section of the DNS namespace.

**domain name server** A server that runs application software that enables the server to perform a role associated with the DNS service.

**DoS (denial-of-service) attack** A type of hacking attack in which the target system is overwhelmed with requests for service, which keeps it from servicing any requests—legitimate or otherwise.

**downtime** A period of time during which a computer system or network is unavailable. This may be due to scheduled maintenance or hardware or software failure.

**DR (designated router)** An OSPF router intended to reduce network traffic by maintaining the complete routing database and then sending updates to the other routers on the shared network segment.

**DSCP (differentiated services code point)** An architecture that specifies a simple and coarse-grained mechanism for classifying and managing network traffic and providing QoS on modern networks.

**DSL (digital subscriber line)** A public network technology that delivers high bandwidth over conventional copper wiring over limited distances.

**DSSS (direct sequence spread spectrum)** A modulation technique in which the transmitted signal takes up more than the information signal that modulates the carrier or broadcast frequency.

**DSU (data service unit)** A network communications device that formats and controls data for transmission over digital lines. A DSU is used with a CSU.

**DTE (data terminal equipment)** A device used at the user end of a user network interface that serves as a data source, a destination, or both. DTE devices include computers, protocol translators, and multiplexers.

**DWDM (dense wavelength-division multiplexing)** A form of multiplexing optical signals that replaces SONET/SDH regenerators with erbium-doped fiber amplifiers (EDFAs) and can also amplify the signal and allow it to travel a greater distance. The main components of a DWDM system include a terminal multiplexer, line repeaters, and a terminal demultiplexer.

**dynamic routing** A routing system that enables routing information to be communicated between devices automatically and that can recognize changes in the network topology and update routing tables accordingly. Compare with static routing.

**dynamic window** A flow control mechanism that prevents the sender of data from overwhelming the receiver. The amount of data that can be buffered in a dynamic window varies in size, hence its name.

# E

**E1 (E-Carrier Level 1)** A link that operates over two separate sets of wires, typically twisted-pair cable, and carries data at a rate of 2.048 million bits per second. E1 is the European equivalent of T1 used in the United States.

**E3 (E-Carrier Level 3)** A link that carries 16 E1 signals with a data rate of 34.368 million bits per second. E3 is the European equivalent of T3 used in the United States.

**EAP (Extensible Authentication Protocol)** An extension of PPP that supports authentication methods more secure than a standard username and password combination. EAP is commonly used as an authentication protocol for token cards, smartcards, and digital certificates.

**EDNS (Extension Mechanisms for DNS)** An Internet Engineering Task Force specification (RFC 2671) that increases the size of the flags fields, return codes, and label types available in basic DNS.

**EGP (Exterior Gateway Protocol)** A protocol that defines distance-vector protocols commonly used between hosts on the Internet to exchange routing table information. BGP is an example of an EGP. *See* BGP.

**EIA/TIA** The Electronic Industries Alliance/Telecommunications Industry Association is a trade organization responsible for a number of communications standards.

**EIGRP (Enhanced Interior Gateway Routing Protocol)** A protocol that enables routers to exchange information more efficiently than earlier network protocols. Routers configured to use EIGRP keep copies of their neighbors' routing information and query these tables to help find the best possible route for transmissions to follow.

**EIRP (Effective Isotropic Radiated Power)** A measure of the radiated power of an antenna in a specific direction.

**EMI (electromagnetic interference)** External interference of electromagnetic signals that causes a reduction in data integrity and increased error rates in a transmission medium.

**encapsulation** A technique used by protocols in which header and trailer information is added to the protocol data unit as it is passed down through the protocol stack on a sending system. The reverse process, decapsulation, is performed at the receiving system as the packet travels up through the protocol suite.

**encryption** A technique used to modify data for security purposes prior to transmission so that the data cannot be read without the decryption method.

**ESD (electrostatic discharge)** A condition created when two objects of dissimilar electrical charge come

into contact with each other. The result is that a charge from the object with the higher electrical charge discharges itself into the object with the lower-level charge. This discharge can be harmful to computer components and circuit boards.

**ESP (Encapsulating Security Payload)** One of the two separate protocols IPSec consists of (the other being AH). ESP provides encryption services.

**ESS (extended service set)** Two or more basic service sets (BSS) that are connected, therefore using multiple APs. An ESS is used to create WLANs or larger wireless networks and is a collection of APs and clients.

**ESSID (extended service set identifier)** The network name used with an ESS wireless network design. The terms *ESSID* and *SSID* are used interchangeably, but they are different. The SSID is the name used with basic service set (BSS) networks. With an ESS, not all APs necessarily use the same name.

**Ethernet** The most common LAN technology. Ethernet can be implemented using coaxial, twisted-pair, or fiber-optic cable. Ethernet typically uses the CSMA/CD media access method and has various implementation standards.

**EUI (extended unique identifier)** A naming convention for MAC addresses.

**Event Viewer** A utility available on Windows server systems and client systems. It is commonly used to gather systems information and also is used in the troubleshooting process.

# F

**failover** The automatic switching from one device or system to another. Servers can be configured in a failover configuration so that if the primary server fails, the secondary server automatically takes over.

**Fast Ethernet** The IEEE 802.3u specification for data transfers of up to 100 Mbps over twisted-pair cable. *See also* 100BASE-FX, 100BASE-T, and 100BASE-TX.

**fault tolerance** The capability of a component, system, or network to endure a failure.

**FC (Fibre Channel)** *See* Fibre Channel.

**FCoE (Fibre Channel over Ethernet)** A technology that encapsulates Fibre Channel frames over Ethernet networks allowing FC to use 10 Gigabit Ethernet networks (or higher) while preserving the Fibre Channel protocol.

**FCS (frame check sequence)** A method of error detection added to a frame in a communications protocol.

**FDDI (Fiber Distributed Data Interface)** A high-speed data transfer technology designed to extend the capabilities of existing LANs by using a dual-ring topology and a token-passing access method.

**FDM (frequency-division multiplexing)** A technology that

divides the output channel into multiple smaller-bandwidth channels, each of which uses a different frequency range.

**FHRP (First Hop Redundancy Protocol)** A redundancy protocol designed to protect a subnet's default gateway by allowing one or more additional routers to provide backup for that address.

**FHSS (frequency-hopping spread spectrum)** A multiple access method of transferring radio signals in the frequency-hopping code division multiple access (FH-CDMA) scheme.

**fiber-optic cable** A physical medium that can conduct modulated light transmissions. Compared with other transmission media, fiber-optic cable is more expensive, but it is not susceptible to EMI or crosstalk, and it is capable of high data rates and increased distances. Also known as fiber optics or optical fiber.

**Fibre Channel** A technology that defines full gigabit-per-second (commonly runs at 2-, 4-, 8-, and 16-gigabit per second data rates) data transfer over fiber-optic cable. Commonly used with storage-area network (SAN) implementations.

**firewall** A program, system, device, or group of devices acting as a barrier between one network and another. Firewalls are configured to enable certain types of traffic to pass while blocking others.

**flow control** A method of controlling the amount of data transmitted within a given period of time. Different types of flow control exist. *See also* dynamic window and static window.

**FM (frequency modulation)** A form of radio modulation. This communication technique transmits information over a radio wave.

**FQDN (fully qualified domain name)** The entire domain name. It specifies the name of the computer, the domain in which it resides, and the top-level DNS domain (for example, www.marketing.quepublishing.com).

**fragment-free switching** A switching method that uses the first 64 bytes of a frame to determine whether the frame is corrupted. If this first part is intact, the frame is forwarded.

**frame** A grouping of information transmitted as a unit across the network at the data link layer of the OSI model.

**Frame Length field** In a data frame, the field that specifies the length of a frame.

**Frame Type field** In a data frame, the field that names the protocol being sent in the frame.

**frequency** The number of cycles of an alternating current signal over a unit of time. Frequency is expressed in hertz (Hz).

**FTP (File Transfer Protocol)** A protocol that provides for the transfer of files between two systems. FTP users authenticate using clear-text sign-in procedures, making FTP an unsecure protocol. FTP is part of

the TCP/IP suite and operates at Layer 7 of the OSI model.

**FTPS (File Transfer Protocol Security)** A file transfer protocol that uses SSL/TLS to add security.

**F-type connecter** A screw-type connector used with coaxial cable. In computing environments, it is most commonly used to connect cable modems to ISP equipment or incoming cable feeds.

**full backup** A backup in which files, regardless of whether they have been changed, are copied to the backup medium. In a full backup, the files' archive bits are reset.

**full duplex** A system in which data simultaneously transmits in two directions. Compare with half duplex.

# G

**gateway** A hardware or software solution that enables communications between two dissimilar networking systems or protocols. A gateway can operate at any layer of the OSI model but is commonly associated with the application layer.

**Gb (gigabit)** 1 billion bits, or 1000 Mb.

**GBIC (gigabit interface converter)** A Gigabit Ethernet and Fibre Channel transceiver standard.

**Gbps (gigabits per second)** The throughput of a given network medium in terms of 1 billion bps.

**Giant frame** A packet too large for an Ethernet network. It exceeds 1518 bytes (excluding the preamble, frame delimiter, and inter-frame gap).

**Gigabit Ethernet** An IEEE 802.3 specification that defines standards for data transmissions of 1 Gbps. *See also* 1000BASE-T.

**GLBP (Gateway Load-Balancing Protocol)** A proprietary Cisco protocol that adds basic load-balancing functionality in an attempt to overcome the limitations of existing redundant router protocols.

**GPG (GNU Privacy Guard)** An IETF RFC 4880-compliant alternative to the PGP suite of cryptographic software.

**GRE (Generic Routing Encapsulation)** A routing encapsulation method that comes in a plain wrapper.

**GSM (Global System for Mobile Communications)** A standard created by the European Telecommunications Standards Institute (ETSI) used to describe communication protocols for second-generation (2G) cellular networks and devices. It has now become the default global standard for mobile communications in more than 219 countries and territories.

**guaranteed flow control** A method of flow control in which the sending and receiving hosts agree on a rate of data transmission. After the rate is determined, the communication takes place at the guaranteed rate until the sender is finished. No buffering takes place at the receiver.

# H

**HA (high availability)** A system goal/attribute aimed at ensuring operational uptime higher than normal.

**hacker** A person who carries out attacks on a computer software program. *See also* cracker.

**half duplex** A connection in which data is transmitted in both directions but not simultaneously. Compare with full duplex.

**handshake** The initial communication between two data communication devices, during which they agree on protocol and transfer rules for the session.

**hardware address** The hardware-encoded MAC address burned into every NIC.

**hardware loopback** A device plugged into an interface for the purposes of simulating a network connection. This enables the interface to be tested as if it is operating while connected.

**HDLC (High-Level Data Link Control)** An ISO developed bit-oriented synchronous data link layer protocol used for point-to-point or point-to-multipoint connections.

**HDMI (High-Definition Multimedia Interface)** An audio/video interface for transferring data and compressed or uncompressed data to a monitor, projector, television, or digital audio device.

**HIDS (host intrusion detection system)** A intrusion detection system (IDS) that is based at the host (rather than the network). It monitors and analyzes data coming to and from the host.

**HIPS (host intrusion prevention system)** A intrusion prevention system (IPS) that is based at the host (rather than the network). It responds and reacts to threats coming to and from the host.

**hop** The means by which routing protocols determine the shortest way to reach a given destination. Each router constitutes one hop. If a router is four hops away from another router, for example, three routers, or hops, exist between the first router and the destination. In some cases, the final step is also counted as a hop.

**horizontal cross-connect** The distribution point for a horizontal cable. It ties the telecommunication room to the end user. Specifically, the horizontal cabling extends from the telecommunications outlet, or network outlet with RJ-45 connectors, at the client end. It includes all cable from that outlet to the telecommunication room to the horizontal cross-connect.

**host** Typically, any device on the network that has been assigned an IP address.

**host firewall** A firewall system installed and configured on and used for an individual host. Contrast to a network firewall that provides firewall services for all network nodes.

**host ID** An identifier used to uniquely identify a client or resource on a network.

**hostname** A name assigned to a system for the purposes of

identifying it on the network in a more user-friendly manner than by the network address.

**HOSTS file** A text file that contains hostname-to-IP address mappings. All commonly used platforms accommodate static name resolution using the HOSTS file.

**hot site** A disaster recovery site, or alternative site, that can be immediately functional in the event of a disaster at the primary site.

**hot spare** In a RAID configuration, a drive that sits idle until another drive in the RAID array fails, at which point the hot spare takes over the role of the failed drive.

**hot swap** The removal and replacement of a component in a system while the power is still on and the system is functioning.

**hotspot** An area in which an access point provides public wireless broadband network services to mobile visitors through a WLAN. Hotspots are often located in heavily populated places such as airports, hotels, and coffee shops.

**HSPA (High-Speed Packet Access)** A telephony protocol designed to increase speeds over previous protocols by combining features from others.

**HSRP (Hot Standby Router Protocol)** A Cisco proprietary protocol used for establishing redundant gateways.

**HT (High Throughput)** A feature of 802.11n for increased throughput on the network. The newer Very High Throughput (VHT) 802.11ac standard further increases network throughput.

**HTTP (Hypertext Transfer Protocol)** A protocol used by web browsers over port 80 to transfer pages, links, and graphics from the remote node to the user's computer.

**HTTPS (Hypertext Transfer Protocol Secure)** A protocol that performs the same function as HTTP but does so over an encrypted link over port 443, ensuring the confidentiality of any data that is uploaded or downloaded. Also referred to as S-HTTP.

**hub** A largely obsolete hardware device that acts as a connection point on a network that uses twisted-pair cable. It operates at the physical layer of the OSI model and forwards signals to all ports. Also known as a concentrator or a multiport repeater.

**HVAC (heating, ventilation, and air conditioning)** A self-defining acronym.

**Hz (hertz)** The unit of frequency defined as the number of cycles per second of a periodic phenomenon.

# I

**IaaS (Infrastructure as a Service)** The most basic method of cloud service computing; the users install everything from the operating system up.

**IANA (Internet Assigned Numbers Authority)** An organization responsible for IP addresses, domain

names, and protocol parameters. Some functions of IANA, such as domain name assignment, have been devolved into other organizations.

**ICA (Independent Computing Architecture)** A Cisco proprietary protocol for application servers.

**ICANN (Internet Corporation for Assigned Names and Numbers)** The nonprofit organization responsible for coordinating domain names and addresses.

**ICMP (Internet Control Message Protocol)** A network layer Internet protocol documented in RFC 792 that reports errors and provides other information relevant to IP packet processing. Utilities such as **ping** and **tracert** use functionality provided by ICMP.

**ICS (industrial control system)** A general term used to describe industrial control systems such as supervisory control and data acquisition (SCADA) systems.

**ICS (Internet connection sharing)** The use of one device with access to the Internet as an access point for other devices to connect.

**IDF (intermediate distribution frame)** A secondary wiring closet in a network using multiple wiring closets. A wiring closet known as the main distribution frame (MDF) connects to secondary wiring closets. *See also* MDF.

**IDS (intrusion detection system)** A software application or hardware device that monitors a network or system for malicious or non-policy-related activity and reports to a centralized management system.

**IEEE (Institute of Electrical and Electronics Engineers)** A professional organization that, among other things, develops standards for networking and communications.

**IEEE 1394** A standard that defines a system for connecting up to 63 devices on an external bus. IEEE 1394 is used with consumer electronic devices such as video cameras and MP3 players. IEEE 1394 is based on a technology developed by Apple called FireWire. FireWire was subsequently replaced by Thunderbolt.

**IEEE 802.1** A standard that defines the OSI model's physical and data link layers. This standard allows two IEEE LAN stations to communicate over a LAN or WAN and is often called the internetworking standard.

**IEEE 802.1X** An IEEE security standard designed for authenticating wireless devices. This standard uses Extensible Authentication Protocol (EAP) to provide a central authentication server to authenticate each user on the network.

**IEEE 802.3** A standard that specifies physical layer attributes, such as signaling types, data rates, and topologies, as well as the media access method used. It also defines specifications for the implementation of the physical layer and the MAC sublayer of the data link layer, using CSMA/CD. This standard also includes the original specifications for Fast Ethernet.

**IEEE 802.11** The original IEEE wireless standard, which defines standards for wireless LAN communication.

**IEEE 802.11a** A wireless networking standard operating in the 5 GHz band. 802.11a supports a maximum theoretical data rate of 54 Mbps. Depending on interference, 802.11a could have a range of 150 feet at the lowest speed setting. Higher-speed transmissions would see a lower range. 802.11a uses the CSMA/CA media access method and is incompatible with 802.11b and 802.11g.

**IEEE 802.11ac** A wireless standard that provides even higher throughput for WLANs on the 5 GHz frequency range. The specification's goal is at least 1 gigabit per second throughput for multistation WLANs and a single station link throughput of at least 500 Mbps. It supports MIMO spatial streams as well as the newer MU-MIMO technology. 802.11ac is backward compatible with 802.11b, g, and n.

**IEEE 802.11ax** A wireless standard (Wi-Fi 6) that succeeds the previous standards. It works over both the 2.4 GHz and 5 GHz bands and also works with the 6 GHz band. It provides a number of performance benefits, including the capability to avoid interference with other nearby networks.

**IEEE 802.11b** A commonly deployed IEEE wireless standard that uses the 2.4 GHz RF range and offers speeds up to 11 Mbps. Under ideal conditions, the transmission range can be as far as 75 meters.

**IEEE 802.11g** An IEEE wireless standard that is backward compatible with 802.11b. 802.11g offers a data rate of 54 Mbps. Like 802.11b, 802.11g uses the 2.4 GHz RF range.

**IEEE 802.11n** A wireless standard that significantly increased throughput in both the 2.4 GHz and 5 GHz frequency range. The baseline goal of the standard reaches speeds of 100 Mbps, but given the right conditions, 802.11n speeds can reach 600 Mbps. 802.11n is backward compatible with 802.11b and g.

**IETF (Internet Engineering Task Force)** A group of research volunteers responsible for specifying the protocols used on the Internet and the architecture of the Internet.

**ifconfig** A command used on Linux- and UNIX-based systems to obtain configuration for and configure network interfaces.

**IGMP (Internet Group Management Protocol)** A protocol used for communication between devices within the same multicast group. IGMP provides a mechanism for systems to detect and make themselves aware of other systems in the same group.

**IGP** The interior gateway protocol that identifies the protocols used to exchange routing information between routers within a LAN or interconnected LANs. *See* EGP.

**IGRP (Interior Gateway Routing Protocol)** A distance vector interior gateway protocol (IGP) developed by Cisco.

**IKE (Internet Key Exchange)** An IPSec protocol that uses X.509 certificates for authentication.

**IMAP4 (Internet Message Access Protocol version 4)** A protocol that enables email to be retrieved from a remote server. It is part of the TCP/IP suite, and it is similar in operation to POP3 but offers more functionality.

**incremental backup** A backup of only files that have been created or changed since the last backup. In an incremental backup, the archive bit is cleared to indicate that a file has been backed up.

**infrared** A wireless data communication method that uses light pulses in the infrared range as a carrier signal.

**infrastructure topology** A wireless topology that defines a wireless network composed of an access point connected to a wired LAN. Wireless devices communicate with the wired LAN through the access point (AP).

**inherited rights** The file system or directory access rights valid at a given point as a result of those rights being assigned at a higher level in the directory structure.

**intelligent hub/switch** A hub or switch that contains some management or monitoring capability.

**intelligent UPS** An uninterruptible power supply that has associated software for monitoring and managing the power provided to the system. For information to be passed between the UPS and the system, the UPS and system must be connected, which normally is achieved through a serial or USB connection.

**interface** A device, such as a card or plug, that connects pieces of hardware with a computer so that information can be moved from place to place (for example, between computers and printers, hard drives, and other devices, or between two or more nodes on a network). Also, the part of an application or operating system that the user sees.

**interference** Anything that can compromise a signal's quality. On bound media, crosstalk and EMI are examples of interference. In wireless environments, atmospheric conditions that degrade a signal's quality would be considered interference.

**internal loopback address** Functionality built in to the TCP/IP stack that enables you to verify the correct functioning of the stack. You can ping any IPv4 address in the 127.*x*.*x*.*x* range, except the network address (127.0.0.0) or the broadcast address (127.255.255.255). The address 127.0.0.1 is most commonly used. In IPv6, the localhost (loopback) address is 0:0:0:0:0:0:0:1 or can also be expressed as ::1.

**Internet domain name** The name of an area of the DNS namespace. The Internet domain name normally is expressed along with the top-level domain to which it belongs (for example, comptia.org).

**Internet layer** In the TCP/IP architectural model, the layer responsible for addressing, packaging, and routing functions.

Protocols that operate at this layer are responsible for encapsulating packets into Internet datagrams. All necessary routing algorithms are run here.

**internetwork** A group of networks connected by routers or other connectivity devices so that the networks function as one network.

**InterNIC (Internet Network Information Center)** The organization that was primarily responsible for domain name allocation. Now known just as NIC (Network Information Center).

**intrusion detection** The process or procedures that warn you about successful or failed unauthorized access to a system.

**IoT (Internet of Things)** A network of physical devices embedded with software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

**IP (Internet Protocol)** A network layer protocol, documented in RFC 791, that offers a connectionless internetwork service. IP provides features for addressing, packet fragmentation and reassembly, type-of-service specification, and security.

**IP address** The unique address used to identify the network number and node address of a device connected to a TCP/IP network. IPv4 addresses typically are expressed in dotted-decimal format, such as 192.168.1.1. A typical IPv6 address looks like 2001:0:4137:9e76:18d1:2094:b980:a30.

**IPS (intrusion prevention system)** A network device that continually scans the network, looking for inappropriate activity.

**ipconfig** A Windows command that provides information about the configuration of the TCP/IP parameters, including the IP address.

**IPSec (IP Security)** A protocol used to provide strong security standards for encryption and authentication on virtual private networks.

**IPv4 (Internet Protocol version 4)** A suite of protocols used for communication on a local-area network and for accessing the Internet.

**IPv6 (Internet Protocol version 6)** The newer version of IP, which has a larger range of usable addresses than IPv4, and enhanced security.

**IrDA** A wireless networking technology that uses infrared beams to send data transmissions between devices.

**ISAKMP (Internet Security Association and Key Management Protocol)** Defined by RFC 2408, a protocol typically used by IKE for key exchange.

**iSCSI (Internet Small Computer Systems Interface)** An IP-based networking storage standard for linking and managing data storage facilities. iSCSI allows SCSI commands to be sent over IP networks, including LANs, WANs, and the Internet.

**ISDN (Integrated Services Digital Network)** An internationally

adopted standard for providing end-to-end digital communications between two points. ISDN is a dialup technology allowing data, voice, and other source traffic to be transmitted over a dedicated link.

**ISDN terminal adapter** A device that enables communication over an ISDN link.

**IS-IS (Intermediate System-to-Intermediate System)** A link-state protocol that discovers the shortest path for data to travel using the shortest path first (SPF) algorithm. IS-IS routers distribute topology information to other routers, allowing them to make the best path decisions.

**ISO (International Organization for Standardization)** A voluntary organization founded in 1946 that is responsible for creating international standards in many areas, including communications and computers. This also includes the development of the OSI model.

**ISP (Internet service provider)** A company or organization that provides facilities for clients to access the Internet.

**IT (information technology)** A fascinating field of study and career choice.

**ITS (intelligent transportation system)** A traffic management system intended for use in creating smart transportation networks.

**IV (initialization vector)** A fixed-size input used in cryptography. The larger the initialization vector, the more it increases the difficulty in cracking and minimizes the risk of replay.

# J–K

**jumbo frame** An Ethernet frame with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes.

**Kb (kilobit)** 1000 bits.

**Kbps (kilobits per second)** A measurement of the number of kilobits transmitted, or capable of being transmitted, in a second.

**KB (kilobyte)** 1000 bytes.

**Kerberos** A network authentication protocol designed to ensure that the data sent across networks is encrypted and safe from attack. Its primary purpose is to provide authentication for client/server applications.

**KVM (keyboard video mouse)** A device that allows one keyboard, one mouse, and one monitor to be used with multiple devices.

# L

**L2TP (Layer 2 Tunneling Protocol)** A VPN protocol that defines its own tunneling protocol and works with the advanced security methods of IPSec. L2TP enables PPP sessions to be tunneled across an arbitrary medium to a home gateway at an ISP or corporation.

**LACP (Link Aggregation Control Protocol)** An IEEE specification that provides a control method of bundling several physical ports into one single channel.

**LAN (local-area network)** A group of connected computers located in a single geographic area—usually a building or office—that shares data and services.

**latency** The delay induced by a piece of equipment or device used to transfer data.

**LC (local connector)** A media connector used with fiber-optic cabling.

**LDAP (Lightweight Directory Access Protocol)** A protocol used to access and query compliant directory services systems, such as Microsoft Active Directory.

**LDAPS (Lightweight Directory Access Protocol over SSL)** A protocol that uses SSL, and port 636, to add additional security to LDAP.

**learning bridge** A bridge that builds its own bridging address table instead of requiring someone to manually enter information. Most modern bridges are learning bridges. Also called a smart bridge.

**LEC (local exchange carrier)** A regulatory term used in telephony to represent the local telephone provider.

**LED (light-emitting diode)** A type of semiconductor that emits light and is commonly used in displays.

**legacy** An older computer system or technology.

**line conditioner** A device used to stabilize the flow of power to the connected component. Also known as a power conditioner or voltage regulator.

**link light** An LED on a networking device, such as a hub, switch, or NIC. The illumination of the link light indicates that, at a hardware level, the connection is complete and functioning.

**link-state routing** A dynamic routing method in which routers tell neighboring routers of their existence through packets called link-state advertisements (LSAs). By interpreting the information in these packets, routers can create maps of the entire network. Compare with distance-vector routing.

**Linux** A UNIX-like operating system kernel created by Linus Torvalds. Linux is distributed under an open-source license agreement, as are many of the applications and services that run on it.

**LLC (logical link control) layer** A sublayer of the data link layer of the OSI model. The LLC layer provides an interface for network layer protocols and the MAC sublayer.

**LLDP (Link Layer Discovery Protocol)** A protocol used by network devices for advertising on an IEEE 802 local-area network.

**logical addressing scheme** The addressing method used in providing manually assigned node addressing.

**logical topology** The appearance of the network to the devices that use it, even if in physical terms the layout of the network is different. *See also* physical topology.

**loop** A continuous circle that a packet takes through a series of nodes in a network until it eventually times out.

**loopback plug** A device used for loopback testing.

**loopback testing** A troubleshooting method in which the output and input wires are crossed or shorted in a manner that enables all outgoing data to be routed back into the card.

**LSA (link state advertisements)** A method of OSPF communication in which the router sends the local routing topology to all other local routers in the same OSPF area.

**LTE (Long-Term Evolution)** A wireless communication standard more commonly referred to as 4G LTE.

**LWAPP (Lightweight Access Point Protocol)** A protocol that simplifies communication with multiple access points at the same time. More commonly known as Lightweight.

# M

**MaaS (Mobility as a Service)** Mobility solutions that are consumed as a service as opposed to personal vehicles. Also known as Transportation as a Service.

**MAC (Media Access Control) address** A six-octet number, described in hexadecimal, that uniquely identifies a host on a network. It is a unique number burned into the network interface.

**MAC layer** In the OSI model, the lower of the two sublayers of the data link layer. It is defined by the IEEE as being responsible for interaction with the physical layer.

**MAN (metropolitan-area network)** A network that spans a defined geographic location, such as a city or suburb.

**master name server** The supplying name server that has authority in a DNS zone.

**Mb (megabit)** 1 million bits. Used to rate transmission transfer speeds.

**Mbps (megabits per second)** A measurement of the number of megabits sent, or capable of being sent, in a second.

**MB (megabyte)** 1 million bytes. Usually refers to file size.

**MBps (megabytes per second)** A measurement of the number of megabytes sent in a second.

**MDF (main distribution frame)** A type of wiring closet known as the main distribution frame. The primary wiring closet for a network typically holds the majority of the network gear, including routers, switches, wiring, servers, and more. This is also typically the wiring closet where outside lines run into the network. One of the key components in the MDF is a primary patch panel. The network connector jacks attached to this patch panel lead out of the building for network connections. *See also* IDF.

**MDI (medium-dependent interface)** A type of port found on Ethernet networking devices, such as hubs and switches, in which the wiring is straight through.

MDI ports are sometimes called uplink ports. They are intended for use as connectivity points to other hubs and switches.

**MDIX (media-dependent interface crossover)** A type of port found on Ethernet networking devices in which the wiring is crossed so that the transmit line of one device becomes the receive line of the other. MDI-X is used to connect hubs and switches to client computers.

**media converter** A device used to interconnect different types of cables within an existing network. For example, the media converter can be used to connect newer Gigabit Ethernet technologies with older 100BASE-T networks.

**media tester** A range of software or hardware tools designed to test a particular media type.

**mesh** A type of network topology in which each node connects to every other node. The mesh network provides a high level of redundancy because it provides alternative routes for data to travel should a single route become unavailable.

**metric** A value that can be assigned to a route to encourage or discourage the use of the route. *See also* cost.

**MGCP (Media Gateway Control Protocol)** A protocol for controlling IP-based media gateways through the public switched telephone networks (PSTNs).

**mGRE (Multipoint Generic Routing Encapsulation)** A tunneling protocol that can encapsulate other network layer protocols inside multipoint links to increase security over an IP network.

**MIB (Management Information Base)** A data set that defines the criteria that can be retrieved and set on a device using SNMP.

**microsegmentation** The process of using switches to divide a network into smaller segments.

**microwaves** A wireless technology sometimes used to transmit data between buildings and across vast distances.

**MIMO (multiple input, multiple output)** The use of multiple antennas—often at both the transmitter and receiver—to improve communications in IEEE 802.11n and 802.11ac Wi-Fi networks.

**MLA (master license agreement)** The main contract defining services to be offered by a provider.

**MMF (multimode fiber)** A type of fiber in which many beams of light travel through the cable, bouncing off the cable walls. This strategy actually weakens the signal, reducing the length and speed at which the data signal can travel. *See also* SMF.

**modem (modulator-demodulator)** A device used to modulate and demodulate the signals that pass through it. It converts the direct current pulses of the serial digital code from the controller into the analog signals compatible with the telephone network.

**MOA (memorandum of agreement)** An agreement expressing a

convergence of will between the parties and indicating an intended common line of action.

**MOU (memorandum of understanding)** An agreement (bilateral or multilateral) between parties defining terms and conditions of an agreement.

**MPLS (multiprotocol label switching)** A technology designed to speed up network traffic flow by moving away from the use of traditional routing tables. Instead of routing tables, MPLS uses short labels to direct packets and forward them through the network.

**MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)** An implementation of CHAP specific to Microsoft operating systems and commonly offered in both server and desktop operating systems. The two versions of MS-CHAP are MS-CHAPv1 (defined in RFC 2433) and MS-CHAPv2 (defined in RFC 2759).

**MSA (master service agreement)** A contract between parties, in which the parties agree to most of the terms that will govern future transactions or future agreements.

**MSDS (material safety data sheet)** A document defining the hazards of working with a chemical or compound, safety precautions, and guidelines for dealing with spills or accidents.

**MT-RJ connector** A media connector used with fiber-optic cabling.

**MTBF (mean time between failure)** The predicted time between inherent failures of a system.

**MTTR (mean time to repair)** The average time that a device will take to recover from a failure.

**MTU (maximum transmission unit)** The largest data size that a protocol/layer can transmit.

**multicast** A single-packet transmission from one sender to a specific group of destination nodes.

**multihomed** A term used to refer to a device that has more than one network interface.

**multimeter** A tool used to measure voltage, current, and resistance.

**multiplatform** A term used to refer to a programming language, technology, or protocol that runs on different types of CPUs or operating systems.

**multiplexing** A technique of combining multiple channels over a transmission path and then recovering or demultiplexing the separate channels at the receiving end. Examples include FDM, TDM, CDM, and WDM.

**MU-MIMO (multiuser multiple input, multiple output)** A set of advanced MIMO technologies included with IEEE 802.11ac and 802.11ax that dramatically enhances wireless throughput.

**MX (Mail Exchange)** A DNS record entry used to identify the mail server.

# N

**NAC (network access control)** A computer networking security

solution that uses a set of network protocols with the goal to unify endpoint security solutions such as antivirus, vulnerability assessment, and authentication. Also known as network admission control.

**name server** A server that contains a database of name resolution information used to resolve network names to network addresses.

**NAS (network-attached storage)** An array of disks providing network storage capacity to the users on the network. It is a specialized file-level computer storage device connected to a network.

**NAT (Network Address Translation)** A standard that enables the translation of IP addresses used on one network to a different IP address that is acceptable for use on another network. This translation enables multiple systems to access an external network, such as the Internet, through a single IP address.

**NCP (Network Control Protocol)** A protocol used to define control between network protocols or layers.

**NDA (nondisclosure agreement)** A document agreeing that information shared will not be shared further with other parties.

**NDR (nondelivery receipt)** A message informing the sender that a previous message has not been delivered because a delivery problem occurred.

**NetBEUI (NetBIOS Extended User Interface)** A nonroutable, Microsoft proprietary networking protocol designed for use in small networks.

**NetBIOS (Network Basic Input/Output System)** A software application that enables different applications to communicate between computers on a LAN.

**netstat** A Windows operating system command-line utility that displays protocol statistics and current TCP/IP network connections.

**network card** *See* NIC.

**network ID** The part of a TCP/IP address that specifies the network portion of the IP address. The network ID is determined by the class of the address, which in turn is determined by the subnet mask used.

**network interface layer** The bottom layer of the TCP/IP architectural model, which is responsible for sending and receiving frames.

**network layer** Layer 3 of the OSI model, which is where routing based on node addresses (IP addresses) occurs.

**network operating system** An operating system that runs on the servers on a network. NOSs include Windows Server, UNIX, and Linux.

**NFC (near-field communication)** Any protocol that enables two electronic devices to establish communication by bringing them within 1.6 inches of each other. It is gaining in popularity for use with a smartphone and electronic payment systems.

**NFS (Network File System)** A file sharing and access protocol most commonly associated with UNIX and Linux systems.

**NFV (Network Function Virtualization)** A network architecture in which virtualization technologies are used to connect/create communication services.

**NGFW (next-generation firewall)** A traditional firewall combined with any other network device (such as an intrusion prevention system) to get additional functionalities.

**NIC (network interface card)** A hardware component that serves as the interface, or connecting component, between a network and the node. It has a transceiver, a MAC address, and a physical connector for the network cable. Also called a network adapter or network card.

**NIDS (network intrusion detection system)** An intrusion detection system that analyzes and monitors at the network level rather than the host level.

**NIPS (network intrusion prevention system)** A network security system that monitors, blocks, and reports malicious network activity.

**NIU (network interface unit)** A generic term for a network interface device (NID) or point of demarcation.

**nm (nanometer)** A measurement equal to one billionth of a meter.

**NMS (network management system)** An application that acts as a central management point for network management. Most NMS systems use SNMP to communicate with network devices. *See also* SNMP.

**NNTP (Network News Transfer Protocol)** An Internet protocol that controls how news articles are to be queried, distributed, and posted. NNTP uses port 119.

**noise** Another name for EMI. *See also* EMI.

**NS (name server)** A type of DNS record used to identify the name servers responsible for the DNS zone. A DNS name server stores DNS address records such as A and AAAA and also stores mail exchange (MX) records for a domain.

**nslookup** Windows and Linux/UNIX command-line utility used to query Domain Name System (DNS) servers and clients to obtain DNS information.

**NTP (Network Time Protocol)** A protocol used to communicate time synchronization information between devices on the network. NTP is part of the TCP/IP suite. NTP uses port 123.

# O

**OCSP (Online Certificate Status Protocol)** A protocol used for obtaining the revocation status of an X.509 digital certificate.

**OCx (Optical Carrier)** A set of standards used for digital signals with SONET fiber networks.

**OID (object identifier)** An ITU identifier employed for naming any

object with a globally unambiguous persistent name.

**on-path attack** An attack in which a party between the sender and receiver intercepts data between the two and then uses it for malicious intent. Previously known as a man-in-the-middle attack.

**OS (operating system)** The main computer program that manages and integrates all the applications running on a computer. The OS handles all interactions with the processor.

**OSI (Open Systems Interconnection) reference model** A seven-layer model created by the ISO to standardize and explain the interactions of networking protocols.

**OSPF (Open Shortest Path First)** A link-state routing protocol used on TCP/IP networks. Compare with distance-vector routing.

**OTDR (optical time-domain reflectometer)** A tool used to locate problems with optical media, such as cable breaks.

**OUI (organizationally unique identifier)** A 24-bit number that uniquely identifies a vendor, a manufacturer, or other organization globally or worldwide.

# P

**PaaS (Platform as a Service)** A cloud computing service model in which the provider supplies the operating system and the user is responsible for the stack above it.

**packet** A unit of data that travels in communication networks.

**packet filtering** A firewall method in which each packet that attempts to pass through the firewall is examined to determine its contents. The packet is then allowed to pass, or it is blocked, as appropriate.

**packet sniffer** A device or application that enables data to be copied from the network and analyzed. In legitimate applications, it is a useful network troubleshooting tool.

**PAN (personal-area network)** A network layout whereby devices work together in close proximity to share information and services, commonly using technologies such as Bluetooth or infrared.

**PAP (Password Authentication Protocol)** A simple authentication protocol in which the username and password are sent to the remote-access server in clear text, making it possible for anyone listening to network traffic to steal both. PAP typically is used only when connecting to older UNIX-based remote-access servers that do not support any additional authentication protocols.

**passive hub** A hub that has no power and therefore does not regenerate the signals it receives. Compare with active hub.

**password** A set of characters used with a username to authenticate a user on a network and to provide the user with rights and permissions to files and resources.

**PAT (Port Address Translation)** A variation on NAT (Network Address

Translation). With PAT, all systems on the LAN are translated into the same IP address, but with a different port number assignment. *See also* NAT.

**patch** A fix for a bug in a software application. Patches can be downloaded from the Internet to correct errors or security problems in software applications.

**patch cable** A cable, normally twisted pair, used to connect two devices. Strictly speaking, a patch cable is the cable that connects a port on a hub or switch to the patch panel, but today people commonly use the term to refer to any cable connection.

**patch panel** A device in which the cables used in coaxial or twisted-pair networks converge and are connected. The patch panel is usually in a central location.

**PC (personal computer)** A general-purpose computer intended for use by individual users.

**PCM (phase change memory)** A type of nonvolatile random-access memory (RAM).

**PDoS (permanent denial of service)** A denial-of-service type attack that damages a system so badly that it requires replacement or reinstallation of hardware.

**PDU (power distribution unit)** A device fitted with multiple outputs designed to distribute electric power, especially to racks of computers and networking equipment.

**peer-to-peer networking** A network environment that does not have dedicated servers, where communication occurs between similarly capable network nodes that act as both clients and servers.

**permissions** Authorization provided to users that allows them to access objects on a network. Network administrators generally assign permissions. Permissions are slightly different from but are often used with rights.

**PGP (Pretty Good Privacy)** A popular encryption/decryption program used for cryptography.

**physical address** The MAC address on every NIC. The physical address is applied to a NIC by the manufacturer. Except for rare occurrences, it is never changed.

**physical layer** Layer 1 of the OSI model, where all physical connectivity is defined.

**physical network diagram** A diagram that displays the physical layout of a network, including placement of systems and all network cabling.

**physical topology** The actual physical layout of the network. Common physical topologies include star, bus, mesh, and ring. Compare with logical topology.

**ping** A TCP/IP stack utility that works with ICMP and that uses echo requests and replies to test connectivity to other systems.

**PKI (public key infrastructure)** A collection of software, standards, and policies combined to enable users from the Internet or other unsecured public networks to

securely exchange data. PKI uses a public and private cryptographic key pair obtained and shared through a trusted authority.

**plenum** The space between the structural ceiling and a drop-down ceiling. It is commonly used for heating, ventilation, and air-conditioning systems and to run network cables.

**plug and play** An architecture designed to enable the operating system to detect hardware devices and for the driver to be automatically loaded and configured.

**PoE (Power over Ethernet)** A technology that enables electrical power to be transmitted over twisted-pair Ethernet cable. The power is transferred, along with data, to provide power to remote devices.

**PoE+ (Power over Ethernet plus)** A technology that provides more power than PoE (increasing from 12.95W to 25.5W) and raising the maximum current (from 350mA to 600mA).

**policies and procedures** Policies refer to an organization's documented rules regarding what is to be done, or not done, and why. Network procedures differ from policies in that they identify the way in which tasks are to be performed.

**polling** The media access method for transmitting data in which a controlling device is used to contact each node to determine whether it has data to send.

**POP3 (Post Office Protocol version 3)** A protocol that is part of the TCP/IP suite used to retrieve mail stored on a remote server. The most commonly used version of POP is POP3. POP3 is an application layer protocol that runs unsecured over port 110 by default. POP3S uses secure port 995.

**port** In physical networking terms, a pathway on a networking device that enables other devices to be connected. In software terms, it is the entry point into an application, a system, or a protocol stack.

**port mirroring** A process by which two ports on a device, such as a switch, are configured to receive the same information. Port mirroring is useful in troubleshooting scenarios.

**POTS (plain old telephone system)** The current analog public telephone system. *See also* PSTN.

**PPP (Point-to-Point Protocol)** A common dial-up networking protocol that includes provisions for security and protocol negotiation. It provides host-to-network and switch-to-switch connections for one or more user sessions.

**PPPoE (Point-to-Point Protocol over Ethernet)** An Internet connection authentication protocol that uses two separate technologies, Ethernet and PPP, to provide a method for multiple users to share a common digital subscriber line (DSL), cable modem, or wireless connection to the Internet.

**PPTP (Point-to-Point Tunneling Protocol)** A protocol that encapsulates private network data in IP packets. These packets are transmitted over synchronous and

asynchronous circuits to hide the Internet's underlying routing and switching infrastructure from both senders and receivers.

**presentation layer** Layer 6 of the OSI model, which prepares information to be used by the application layer.

**PRI (Primary Rate Interface)** A high-level network interface standard for use with ISDN. PRI is defined as having a rate of 1.544 Mbps, and it consists of a single 64 Kbps D channel plus 23 T1 B channels for voice or data. *See also* BRI and ISDN.

**primary name server** The DNS server that offers zone data from files stored locally on the machine.

**private network** A network to which access is limited, restricted, or controlled. Most corporate networks are private networks. Compare with public network.

**proprietary** A standard or specification created by a single manufacturer, vendor, or other private enterprise.

**protocol** A set of rules or standards that control data transmission and other interactions between networks, computers, peripheral devices, and operating systems.

**protocol analyzer** Hardware- or software-based tools, with their primary function being to analyze network protocols such as TCP, UDP, HTTP, FTP, and more.

**proxy** A device, application, or service that acts as an intermediary between two hosts on a network, eliminating the capability for direct communication.

**proxy server** A server that acts as a go-between for a workstation and the Internet. A proxy server typically provides an increased level of security, caching, NAT, and administrative control.

**PSK (preshared key)** A value (key) shared with another party so that they can encrypt messages to then be securely sent.

**PSTN (public switched telephone network)** A term that refers to all the telephone networks and services in the world. The same as POTS, PSTN refers to the world's collection of interconnected public telephone networks that are both commercial and government owned. All the PSTN is digital, except the connection between local exchanges and customers (which is called the local loop or last mile), which remains analog.

**PTP (Point-to-Point)** A protocol that is used to establish a direct connection between two nodes. More commonly referenced as PPP.

**PTR (pointer)** A DNS record used to map an IP address to a hostname.

**PUA (privileged user agreement)** Established, and agreed upon, rules of behavior that define what privileged users can and cannot do with their elevated permissions.

**public network** A network, such as the Internet, to which anyone can connect with the most minimal of restrictions. Compare with private network.

**punchdown block** A device used to connect network cables from equipment closets or rooms to other parts of a building. Connections to networking equipment such as hubs or switches are established from the punchdown block. Also used in telecommunications wiring to distribute phone cables to their respective locations throughout the building.

**punchdown tool** A hand tool that enables the connection of twisted-pair wires to wiring equipment such as a patch panel.

**PVC (permanent virtual circuit)** A permanent dedicated virtual link shared in a Frame Relay network, replacing a hardwired dedicated end-to-end line.

# Q–R

**QoS (quality of service)** The strategies used to manage and increase the flow of network traffic. QoS features enable administrators to predict bandwidth use, monitor that use, and control it to ensure that bandwidth is available to the applications that need it.

**QSFP (Quad Small Form-factor Pluggable)** A compact, hot-pluggable transceiver used for data communications.

**RA (router advertisement)** An ICMPv6 packet type used by routers to advertise their presence periodically (or in response to a solicitation message).

**RADIUS (Remote Authentication Dial-In User Service)** A security standard that employs a client/server model to authenticate remote network users. Remote users are authenticated using a challenge-and-response mechanism between the remote-access server and the RADIUS server.

**RAID (Redundant Array of Inexpensive/Independent Disks)** Any of many methods of storing data on multiple drives and enabling the overlapping of I/O operations. The various RAID levels offer either fault-tolerance or performance advantages.

**RARP (Reverse Address Resolution Protocol)** A protocol, part of the TCP/IP suite, that resolves MAC addresses to IP addresses. Its relative ARP resolves IP addresses to MAC addresses. RARP resides on the network layer of the OSI model.

**RAS (Remote Access Service)** A Windows service that enables access to the network through remote connections.

**RDP (Remote Desktop Protocol)** A presentation layer protocol that supports a Remote Desktop Connection between an RDP client (formerly known as Windows Terminal Client) and a server.

**regulations** Actual legal restrictions with legal consequences.

**remote control** In networking, the physical control of a remote computer through software.

**remote node** A node or computer connected to a network through a remote connection. Dialing in to the Internet from home is an example of the remote node concept.

**repeater** A device that regenerates and retransmits signals on a network. Repeaters usually are used to strengthen signals going long distances.

**resolver** A system that requests the resolution of a name to an IP address. This term can be applied to both DNS and WINS clients.

**restore** To transfer data from backup media to a server. The opposite of back up.

**RF (radio frequency)** A rate of oscillation used by radio waves and radio signals.

**RFC (Request For Comments)** The process by which standards relating to the Internet, the TCP/IP suite, and associated technologies are created, commented on, and approved.

**RFI (radio frequency interference)** Interference that affects radio frequency communication.

**RFP (Request For Proposal)** A document that solicits proposals, often through a bidding process.

**RG (Radio Guide)** A specification commonly used with connection types. More frequently used as *Radio Grade*.

**RG-6/59** Designations for the coaxial cable used in thin coaxial networks that operate on the Ethernet standard.

**rights** Authorization provided to users that allows them to perform certain tasks. The network administrator generally assigns rights. Slightly different from but often used with the term *permissions*.

**RIP (Routing Information Protocol)** A protocol that uses hop count as a routing metric to control the direction and flow of packets between routers on an internetwork.

**RJ (Registered Jack)** A specification for a family of cable connectors.

**RJ-11 connector** A connector used with telephone systems. It can have up to six conductors.

**RJ-45 connector** A connector used with twisted-pair cable. It can support eight conductors for four pairs of wires.

**route** The entire path between two nodes on a network.

**router** A device that works at the network layer of the OSI model to control the flow of data between two or more network segments.

**RPO (recovery point objective)** The maximum acceptable period in which data might be lost from a major incident.

**RSA** An algorithm for public-key cryptography. It can be used for encryption purposes. RSA is used as a secure solution for e-commerce.

**RSH (Remote Shell)** A protocol, and corresponding application, used to remotely run a shell across an IP-based network.

**RSSI (Received Signal Strength Indication)** A measurement of the power present in a received radio signal.

**RSTP (Rapid Spanning Tree Protocol)** The default protocol for preventing loops on Ethernet networks.

**RTO (recovery time objective)** The acceptable duration of time within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity.

**RTP (Real-Time Transport Protocol)** The Internet standard protocol for the transport of real-time data, including audio and video.

**RTSP (Real-Time Streaming Protocol)** A protocol used for establishing and maintaining communications with a media server.

**RTT (round-trip time or real transfer time)** A measurement of the length of time it takes for data to be sent and returned.

**runt** A packet too small for an Ethernet network.

# S

**SA (security association)** The establishment of shared security attributes between two entities on a network to support secure communications between them.

**SAE (Simultaneous Authentication of Equals)** A password-based authentication method used with WPA3 that results in a more secure initial key exchange in personal mode than was possible with WPA2 and PSK.

**SaaS (Software as a Service)** A cloud computing service model in which a user runs everything supplied by the provider.

**sag** A momentary drop in the voltage provided by a power source.

**SAN (storage-area network)** A network that provides access to consolidated, block-level data storage. It is usually found on high-speed networks and shared by all servers on a network.

**SC (standard connector)** A type of connector used with fiber cabling.

**SCADA (supervisory control and data acquisition)** A system operating with coded signals to remotely control a device or equipment.

**SCP (Secure Copy Protocol)** A basic file-copying protocol that uses Secure Shell (SSH) technology to provide security to the transfer.

**screened subnet** An area for placing web and other servers that serve the general public outside the firewall, thereby isolating them from internal network access. Previously known as a demilitarized zone, or DMZ.

**SDLC (Software Development Life Cycle)** The life cycle of software development.

**SDN (software-defined network)** An approach to networking that allows network administrators to programmatically manage network behavior dynamically via open interfaces and provide abstraction of lower-level functionality.

**SDP (Session Description Protocol)** A format of streaming media initialization parameters.

**SDSL (symmetrical digital subscriber line)** A DSL implementation that offers the same speeds

for uploads and downloads. It is not widely implemented in the home/small business environment and cannot share a phone line.

**SDWAN (software-defined WAN)** A wide-area network in which the networking hardware has been decoupled from the control mechanism.

**secondary name server** A type of DNS server that gets its zone data from another DNS name server that has authority in that zone.

**security log** A log located in the Windows Event Viewer that provides information on audit events that the administrator has determined to be security-related. These events include logons, attempts to log on, attempts to access areas that are denied, and attempts to log on outside normal hours.

**segment** A physical section of a network.

**server** A network node that fulfills service requests for clients. Usually referred to by the type of service it performs, such as file server, communications server, or print server.

**server-based application** An application run from a network share rather than from a copy installed on a local computer.

**server-based networking** A network operating system dedicated to providing services to workstations, or clients. *See also* client/server networking.

**service pack** A software update that fixes multiple known problems and, in some cases, provides additional functionality to an application or operating system.

**session** The length of time a dialog remains open between two nodes.

**session layer** Layer 5 of the OSI model, which establishes, manages, and terminates sessions between applications on different nodes.

**SFP (small form-factor pluggable)** A line of small optical transceivers that have recently become available.

**SFTP (Secure File Transfer Protocol)** An implementation of File Transfer Protocol (FTP) that uses Secure Shell (SSH) technology to provide additional authentication and encryption services for file transfers.

**SGCP (Simple Gateway Control Protocol)** A communication protocol used with VoIP.

**SHA (Secure Hash Algorithm)** A cryptographic hash algorithm used in security and defined by the United States National Security Agency.

**shared system** The infrastructure component routed directly into an internetwork's backbone for optimal systems access. It provides connectivity to servers and other shared systems.

**SIEM (security information and event management)** Any of a family of products that combine security information management and event management to achieve a more holistic approach to security.

**SIP (Session Initiation Protocol)** An application layer protocol designed to establish and maintain multimedia sessions such as Internet telephony calls.

**SLA (service-level agreement)** An agreement between a customer and provider detailing the level of service to be provided on a regular basis and in the event of problems.

**SLAAC (Stateless Address Auto Configuration)** A feature of IPv6 networks that allows devices to connect to the Internet without requiring any intermediate IP support from a DHCP server.

**SLIP (Serial Line Internet Protocol)** An antiquated IP-based protocol for modem connections and serial ports.

**SMB (Server Message Block)** An application-layer network protocol used primarily for providing shared access to files, printers, and ports as well as miscellaneous communications between nodes.

**SMF (single-mode fiber)** A type of fiber that uses a single direct beam of light, thus allowing for greater distances and increased transfer speeds. *See also* MMF.

**SMS (Short Message Service)** A text-based communication service for phones, web, and other devices.

**SMTP (Simple Mail Transfer Protocol)** An Internet protocol used for the transfer of email messages and attachments.

**SNAT (Static NAT)** A simple form of NAT. SNAT maps a private IP address directly to a static unchanging public IP address. *See also* NAT.

**SNMP (Simple Network Management Protocol)** A protocol that provides network devices with a method to monitor and control network devices; manage configurations, statistics collection, performance, and security; and report network management information to a management console. SNMP runs over port 161 and is part of the TCP/IP suite.

**SNMP agent** A software component that enables a device to communicate with, and be contacted by, an SNMP management system.

**SNMP trap** An SNMP utility that sends an alarm to notify the administrator that something within the network activity differs from the established threshold, as defined by the administrator.

**SNTP (Simple Network Time Protocol)** An IP-based protocol used to coordinate time among devices across the network.

**SOA (Start of Authority)** A record of information containing data on DNS zones and other DNS records. A DNS zone is the part of a domain for which an individual DNS server is responsible. Each zone contains a single SOA record.

**SOHO (small office/home office)** A small network typically serving 1 to 10 users.

**SONET (Synchronous Optical Network)** A U.S. standard for data transmission that operates at speeds

up to 2.4 Gbps over optical networks referred to as OC-*x*, where *x* is the level. The international equivalent of SONET is Synchronous Digital Hierarchy (SDH).

**SOP (standard operating procedure)** The normal, accepted way that business is conducted.

**source address** The address of the host that sent the frame. The source address is contained in the frame so that the destination node knows who sent the data.

**source-route bridge** A bridge used in source-route bridging to send a packet to the destination node through the route specified by the sending node.

**SOW (statement of work)** A formal document that defines work activities to be performed for a client.

**SPB (Shortest Path Bridging)** Defined in IEEE 802.1aq, a standard defining a routing (Layer 2) protocol.

**SPI (stateful packet inspection)** A type of firewall that works at the network layer and keeps track of the state of active connections.

**spike** An instantaneous, dramatic increase in the voltage input to a device. Spikes are responsible for much of the damage done to network hardware components.

**SPS (standby power supply)** A type of power supply in which the SPS monitors the power line and switches to battery power as soon as it detects a problem. During the time it takes to switch to battery power, the computer does not receive any power and may power down. This is in contrast to an online UPS, which constantly provides battery power.

**SQL (Structured Query Language)** The language designed for working with, and managing, data in a relational database management system.

**SRV (service record)** Within DNS, a record used to identify computers that host specific services.

**SSD (solid-state drive)** An alternative to physical drives, such as traditional hard drives, a solid-state storage drive/device uses integrated circuits to store data persistently (usually with flash memory).

**SSH (Secure Shell)** An application, such as Telnet, that enables a session to be opened on a remote host. SSH differs from Telnet in that it provides additional authentication methods and encryption for data as it traverses the network. SSH uses TCP/IP port 22.

**SSID (service set identifier)** A unique client identifier sent over the WLAN that acts as a simple password used for authentication between a wireless client and an access point. The SSID is used to differentiate between networks. Therefore, the client system and the AP must use the same SSID.

**SSL (Secure Sockets Layer)** A method of securely transmitting information to and receiving information from a remote website. SSL is implemented through HTTPS. SSL operates at the presentation

layer of the OSI model and uses TCP/IP port 443. SSL has been succeeded by TLS.

**SSO (single sign-on)** A method of access in which users are given access to all the applications and systems they need when they initially log on.

**ST (straight tip or snap twist)** A type of connector used with cabling.

**STA (Spanning Tree Algorithm)** A standard defined by IEEE 802.1 as part of STP to eliminate loops in an internetwork with multiple paths.

**star** A type of physical network design in which all nodes connect to a centralized device—in most cases a network switch.

**static IP address** An IP address manually assigned to a network device, as opposed to dynamically via DHCP.

**static routing** A routing method in which all routes must be entered into a device manually and in which no route information is exchanged between routing devices on the network. Compare with dynamic routing.

**static window** A mechanism used in flow control that prevents the sender of data from overwhelming the receiver. The amount of data that can be buffered in a static window is configured dynamically by the protocol.

**ST connector** A type of fiber connector.

**store-and-forward** A fast-packet-switching method that produces higher latency than other switching methods because the entire contents of the packet are copied into the switch's onboard buffers. CRC calculations are performed before the packet can be passed on to the destination address.

**STP (shielded twisted-pair)** Twisted-pair network cable that has shielding to insulate the cable from EMI.

**STP (Spanning Tree Protocol)** A protocol developed to eliminate the loops caused by the multiple paths in an internetwork. STP is defined in IEEE 802.1.

**subdomain** A privately controlled segment of the DNS namespace that exists under other segments of the namespace as a division of the main domain. Sometimes also called a child domain.

**subnet** A logical division of a network, based on the address to which all the devices on the network are assigned.

**subnet mask** A 32-bit address used to mask, or screen, a portion of an IP address to differentiate the part of the address that designates the network and the part that designates the host.

**subnetting** The process of using parts of the node portion of an assigned IP address to create more network IDs. Although subnetting increases the number of network IDs, it decreases the number of node addresses available for each network ID.

**supernetting** The process of aggregating IP network addresses

and using them as a single network address range.

**surge** A voltage increase that is less dramatic than that of a spike but can last much longer. Sometimes called a swell. The opposite of a brownout.

**surge protector** An inexpensive and simple device placed between a power outlet and a network component to protect the component from spikes and surges. Also known as a surge suppressor.

**SVC (switched virtual circuit)** A virtual circuit dynamically established on demand to form a dedicated link. It is broken when transmission is complete.

**switch** A Layer 2 networking device that forwards frames based on destination addresses.

**SYN** A message sent to initiate a TCP session between two devices. The full term is synchronization packet.

**synchronous transmission** A digital signal transmission method that uses a precise clocking method and a predefined number of bits sent at a constant rate.

**syslog (system logging protocol)** A standard used to send log messages (system or event) to a syslog server. These events include driver failures, device conflicts, read/write errors, timeouts, and bad block errors.

# T

**T1/E1** A form of T-Carrier line that offers transmission speeds of 1.544 Mbps. E1 refers to the European equivalent of T1. *See also* T-carrier.

**T1 crossover** *See* crossover cable.

**T3/E3** A carrier line that offers transmission speeds of up to 44.736 Mbps, using 672 64-Kbps B channels. E3 refers to the European equivalent of T3. *See also* T-carrier.

**TA (terminal adapter)** A device that connects a node to an ISDN network.

**TACACS (Terminal Access Controller Access Control System)** A family of related protocols handling remote authentication and related services for networked access control through a centralized server.

**TACACS+ (Terminal Access Controller Access Control System Plus)** A Cisco security protocol designed to provide centralized validation of users who are attempting to gain access to a router or network access server (NAS). TACACS+ is a set of security protocols designed to provide authentication, authorization, and accounting (AAA) of remote users. TACACS+ uses TCP port 49 by default.

**T-carrier (terrestrial carrier)** High-speed dedicated digital lines that can be leased from telephone companies. T-carrier lines can support both voice and data transmissions and are often used to create point-to-point private networks.

**TCP (Transmission Control Protocol)** A connection-oriented, reliable data transmission communication service that operates at the

transport layer of the OSI model. TCP is part of the TCP/IP suite.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** A suite of protocols that includes TCP and IP. TCP/IP was originally designed for use on large internetworks but has now become the de facto protocol for networks of all sizes.

**TCP/IP socket** A socket, or connection to an endpoint, used in TCP/IP communication transmissions.

**TDM (time-division multiplexing)** A method of dividing a single communication channel into multiple channels, enabling data signals to be transferred simultaneously as subchannels in one communication channel. Despite being only a single channel, data signals take turns sending data.

**TDR (time-domain reflectometer)** A device used to test copper cables to determine whether and where a break is on the cable. For optical cables, an optical TDR is used.

**telco (telephone company)** A slang term for the telephone provider in question.

**Telnet** A standard terminal emulation protocol in the TCP/IP stack. Telnet is used to perform terminal emulation over TCP/IP via remote terminal connections, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet has been replaced in most instances by the more secure SSH.

**temperature monitor** A device used to monitor temperature typically in a server room or wiring closet.

**Terminal Services** A service on Windows Server platforms that enables clients to connect to the server as if it were a multiuser operating system. All the processing for the client session is performed on the server. Only screen updates and user input are transmitted across the network connection. Remote Desktop Services (RDS) has replaced Terminal Services in recent versions of Windows.

**TFTP (Trivial File Transfer Protocol)** A simplified version of FTP that enables file transfers but does not offer any security or file management capabilities. TFTP uses TCP/IP port 69.

**throughput tester** A device used to test the actual data throughput of a network cable.

**TIA (Telecommunications Industry Association)** An organization that, along with the Electronic Industries Alliance (EIA), develops standards for telecommunications technologies.

**TKIP (Temporal Key Integrity Protocol)** A encryption protocol designed to address the shortcomings of the WEP security protocol. It is defined in IEEE 802.11i.

**T-line** A digital communication line used in WANs. Commonly used T designations are T1 (Trunk Level 1) and T3 (Trunk Level 3). It is also possible to use only part of a T1 line, which is known as fractional T1. T1 lines support a data transmission rate of up to 1.544 Mbps.

**TLS (Transport Layer Security)** A security protocol designed to ensure privacy between communicating client/server applications. When a server and client communicate, TLS ensures that no one can eavesdrop and intercept or otherwise tamper with the data message. TLS is the successor to SSL.

**TMS (transportation management system)** A software module that sits between warehouse management and an ERP system.

**token** A frame that provides controlling information. In a token ring network, the node that possesses the token is the one that is allowed to transmit next.

**tone generator** A device used with a tone locator to locate and diagnose problems with twisted-pair cabling. Commonly referred to as fox and hound.

**toner probe** A network tool used to locate the ends of a run of network cable.

**topology** The shape or layout of a physical network and the flow of data through the network. *See also* logical topology *and* physical topology.

**ToS (type of service)** A field in an IPv4 header that defines such things as the priority of the packet.

**trace route** A function of the TCP/IP suite, implemented in utilities such as traceroute and tracert, which enables the entire path of a packet to be tracked between source and destination hosts. It is used as a troubleshooting tool.

**tracert** A Windows command-line utility used to track the route a data packet takes to get to its destination.

**transmit** To send data using light, electronic, or electric signals. In networking, this is usually done in the form of digital signals composed of bits.

**transparent bridging** A situation in which the bridges on a network tell each other which ports on the bridge should be opened and closed, which ports should be forwarding packets, and which ports should be blocking packets—all without the assistance of any other device.

**transport layer** Layer 4 of the OSI model. Protocols at this layer perform functions such as segmenting data so that it can be sent over the network and then reassembling the segmented data on the receiving end. The transport layer also deals with some of the errors that can occur in a stream of data, such as dropped and duplicated packets.

**transport protocol** A communications protocol responsible for establishing a connection and ensuring that all data has arrived safely. It is defined in Layer 4 of the OSI model.

**Trojan** A type of program that appears legitimate but performs some illicit activity when it is run.

**TTL (time to live)** A value assigned to a packet of data to prevent it from moving around the network indefinitely. The TTL value is decremented each time the packet crosses a router, until it reaches 0, at

which point it is removed from the network.

**TTLS (Tunneled Transport Layer Security)** An extension of TLS that adds tunneling and is often combined with EAP.

**twisted pair** A type of cable that uses multiple twisted pairs of copper wire.

**TX/RX (transmit and receive)** The commonly used abbreviations for transmit and receive. These can refer to wiring, physical switches, buffers, or any other element.

# U

**UC (unified communications)** A combination of real-time (instant messaging, VoIP, and so on) with non-real-time (email, SMS, and so on) communications on the same platform.

**UDP (User Datagram Protocol)** A communications protocol that provides connectionless, unreliable communication services and operates at the transport layer of the OSI model. It requires a network layer protocol such as IP to guide it to the destination host.

**unbound medium (or boundless medium)** Any medium that does not have physical constraints. Examples of unbound media are infrared, wireless, and microwave. Compare with bound medium.

**UNC (Universal Naming Convention)** An industry-naming standard for computers and resources that provides a common syntax that should work in most systems, including Windows and UNIX. An example of a UNC name is \\servername\sharename.

**unicast** Communication that takes place over a network between a single sender and a single receiver.

**UPC (ultra-polished connector)** A type of connector used with fiber networks.

**UPS (uninterruptible power supply)** A system that provides protection against power surges and power outages. During blackouts, a UPS gives you time to shut down systems or devices on the network before the temporary power interruption becomes permanent. A UPS is also called battery backup.

**uptime** The length of time a device has been on and operating.

**URL (Uniform Resource Locator)** A name used to identify a website and a page on the Internet. An example of a URL is www.quepublishing.com/products.

**USB (universal serial bus)** A type of interface between a computer system and peripheral devices. The USB interface enables you to add or remove devices without shutting down the computer. USB supports up to 127 devices. USB also supports autodetection and plug and play.

**UTM (unified threat management)** An approach to threat management that combines multiple security-related products (antivirus/antimalware software, IPS, and so on) into a single management console.

**UTP (unshielded twisted-pair)** A type of cable that uses multiple twisted pairs of copper wire in a casing that does not provide much protection from EMI. The most common network cable in Ethernet networks, UTP is rated in categories including Category 1 through Category 8, as well as Category 5e, Category 6a, and Category 7a.

# V

**VDSL (variable digital subscriber line)** An asymmetric version of DSL that supports high-bandwidth applications such as VoIP and HDTV. It is the fastest available form of DSL and uses fiber-optic cabling.

**vertical cross-connect** The main location where outside cables enter the building for distribution. This may include Internet and phone cabling.

**VIP (virtual IP)** An IP address that does not correspond, one-to-one, to an actual physical network interface.

**virus** A software program designed specifically to adversely affect a system or network. A virus is usually designed to be passed on to other systems with which it comes in contact.

**VLAN (virtual LAN)** A group of devices located on one or more LAN segments, whose configuration is based on logical instead of physical connections. This enables the devices to operate as if they were connected to the same physical switch, regardless of whether they are connected to the same switch.

**VM (virtual machine)** Any emulation of a computer system.

**VNC (virtual network computing)** A process that involves enabling a remote login, in which clients can access their own desktops while physically away from their computers. Also known as virtual network connection.

**vNIC (virtual network interface card)** Any abstract emulation of a network interface card (NIC). The vNIC may, or may not, correspond directly to a physical network interface controller.

**VoIP (Voice over IP)** Any of a number of technologies that enable voice communication across the Internet Protocol.

**volume set** Multiple disks or partitions of disks that have been configured to read as one drive.

**VPN (virtual private network)** A network that uses a public network such as the Internet as a backbone to connect two or more private networks. A VPN provides users with the equivalent of a private network in terms of security. VPNs can also be used as a means of establishing secure remote connectivity between a remote system and another network.

**VRF (virtual routing and forwarding)** A technology that allows multiple instances of a routing table to coexist within the same router at the same time.

**VRRP (Virtual Router Redundancy Protocol)** An IP-based routing protocol that automatically assigns available routers to participating hosts.

**VTC (video teleconference)** Any combination of audio and video real-time technologies.

**VTP (VLAN Trunking Protocol)** A Cisco proprietary protocol that manages the addition, deletion, and renaming of VLANs for the entire network. Information about changes to a VLAN or the addition of a new VLAN to a network is distributed to all switches on the network simultaneously and does not need to be done one at a time.

# W

**WAF (web application firewall)** A firewall that filters, monitors, and blocks HTTP traffic to and from a web application; this differs from a regular firewall in that the WAF is able to filter the content of specific web applications.

**WAN (wide-area network)** A data communications network that serves users across a broad geographic area. WANs often use transmission devices such as modems or CSUs/DSUs to carry signals over leased lines or common carrier lines.

**WAP (Wireless Application Protocol/wireless access point)** A protocol for wireless mobile access (now outdated) and the devices that make it possible for hosts to connect (widely used).

**warm site** A disaster recovery site offering most equipment and applications. Compare to a cold site that refers to a disaster recovery site with limited hardware and typically only a reserved location. A hot site is one with duplicate hardware and software and can be operational within minutes of a disaster.

**WDM (wavelength division multiplexing)** A fiber transmission method that uses multiple light wavelengths to send data over the same medium.

**web server** A server that runs an application and makes the contents of certain directories on that server, or other servers, available to clients for download, via a protocol such as HTTP.

**WEP (Wired Equivalent Privacy)** A data encryption method used to protect the transmission between 802.11 wireless clients and access points. WEP security has come under scrutiny because it uses an insufficient key length and provides no automated method for distributing the keys.

**Wi-Fi** A voluntary standard that manufacturers can adhere to, which aims to create compatibility between wireless devices. Wi-Fi (also written as WiFi) is an abbreviation for wireless fidelity.

**Wi-Fi 4** A common name used for the 802.11n wireless standard.

**Wi-Fi 5** A common name used for the 802.11ac wireless standard.

**Wi-Fi 6** A common name used for the 802.11ax wireless standard.

**WINS (Windows Internet Name Service)** A NetBIOS name-to-IP address resolution service that runs on Windows Server platforms.

**WINS database** A dynamically built database of NetBIOS names and IP addresses used by WINS.

**wire crimper** A tool used to create networking cables. The type of wire crimping tool used depends on the cable being made.

**wireless channel** The band of frequency used for wireless communications. Each IEEE wireless standard specifies the channels that can be used.

**wireless networking** Networking that uses any unbound media, such as infrared, microwave, or radio waves.

**wiring schematics** Network documentation designed to show the physical wiring of a network. The wiring schematic can often be used in the troubleshooting process.

**WLAN (wireless LAN)** A local-area network created using wireless transmission methods, such as radio or infrared, rather than traditional wired solutions.

**workstation** A client computer on a network that does not offer any services of its own but uses the services of the servers on the network.

**worm** A self-replicating program that can perform destructive acts to a single computer or across a network, both wired and wireless.

**WPA (Wi-Fi Protected Access)** A data encryption method used on 802.11 wireless LANs. WPA is an industry-supported standard designed to address WEP's security shortcomings.

**WPA2 (Wi-Fi Protected Access v2)** A secure wireless data encryption method based on 802.11i that replaces WPA.

**WPA3 (Wi-Fi Protected Access v3)** A secure wireless data encryption method based on 802.11i that replaces WPAv2. The WPA3 standard replaces the preshared key (PSK) exchange with Simultaneous Authentication of Equals (SAE).

**WPS (Wi-Fi Protected Setup)** A security standard created by the Wi-Fi Alliance to increase security features of networks. The most visible manifestation of this is the button on some home routers that must be pressed to allow a new device to connect to the network within a short time period. Currently, WPS is not considered secure because flaws in the WPS PIN feature have been identified.

**WWN (World Wide Name)** A unique identifier assigned to a manufacturer by the Institute of Electrical and Electronic Engineers (IEEE). It is hard-coded into a Fibre Channel (FC) device.

**WWW (World Wide Web)** A service running on the Internet that has become so successful that it is often mistaken for the Internet itself.

# X–Z

**XDSL (extended digital subscriber line)** All the variations of DSL available lumped together under one label.

**zero-day vulnerability** A newly discovered vulnerability for which a patch or fix has not yet been issued.

**zone transfer** The passing of DNS information from one name server to a secondary name server.

*This page intentionally left blank*

# Index

## Numerics

**10Base-T, 210–211**
**10GBASE-LR, 214**
**10GBASE-SR, 214**
**10GBASE-T, 212–213**
**40GBASE-T, 213**
**100Base-T, 211–212**
**568A/568B wiring standards, 200–201**
**802.1Q, 134, 135**
**802.1x, EAP (Extensible Authentication Protocol), 417**
**1000BASE-LX, 213**
**1000BASE-SX, 213**
**1000Base-T, 212**

## A

**absorption, 263–264**
**access control, 405. *See also* security**
802.1x, 416
defense in depth, 408
discretionary, 405–406
MAC filtering, 418
mandatory, 405
NAC (network access control), 417
network segmentation, 408
RADIUS (Remote Authentication Dial-In User Service), 411–412
role-based, 406–408
rule-based, 406
screened subnet, 408–409
TACACS (Terminal Access Controller Access Control System), 412
**access/edge layer, 174**
**ACLs (access control lists), 146, 167, 405–406**
**ad hoc topology, 9**

**aggregation, 142**
**AH (Authentication Header), 57**
**antennas, 243–244, 432**
coverage, 244–245
ratings, 244
**antimalware software, 423**
**antivirus software, 423**
**anycast addresses, 106–107**
**APIPA (Automatic Private IP Addressing), 111–112**
**application layer, 47**
**applications, patch management, 336–339**
**APs (access points), 8, 162–163, 247, 259**
authentication, 251–252
rogue, 422
troubleshooting, 264–265
WPA (Wi-Fi Protected Access), 252–254
WPA-PSK (Wi-Fi Protected Access with Pre-Shared Key), 251–252
**architecture, 172**
SDN (software-defined networking), 174
application layer, 174
control layer, 175
infrastructure layer, 175
management plane, 175
spine and leaf, 175–176
three-tiered, 172–173
access/edge layer, 174
core layer, 173
distribution/aggregation layer, 173
**ARP (Address Resolution Protocol), 147–148, 430–431**
**arp ping command, 431–432**
**attacks, 420**
advertising wireless weaknesses, 422
ARP cache poisoning, 422
ARP spoofing, 423
brute force, 422
deauthentication, 422
DNS poisoning, 422
DoS (denial-of-service), 420–421
logic bombs, 422
on-path, 422
phishing, 422
ransomware, 422
rogue APs, 422
rogue DHCP servers, 422
social engineering, 421–422
spoofing, 422
VLAN hopping, 422
**attenuation, 221–222**
**auditing, 415**
**authentication, 137**
Kerberos, 412–414
local, 414
multifactor, 426
**authorization, 137**
**availability, 317–319**
MTBF (mean time between failures), 316
MTTR (mean time to recovery), 316
RTO (recovery time objective), 317
**AWS (Amazon Web Services), 289**

## B

**backups, 309, 311–312**
best practices, 312–313
differential, 310
full, 309–310
incremental, 310–311
**bandwidth, 26, 219**
**baselines, 293–294**
**biometrics, 426**
**BNC connectors, 194–195**
**BOOTP (BOOT Protocol), 111**
**bridges, 161**
**broadband, 22, 25–26**
**broadcast addresses, 102**

**brute force attacks, 422**
**buffer overflow attacks, 420**
**buffering, 45–46**
**bus topology, 2–3**
**BYOD (bring-your-own-device), 254, 455**

## C

**cable broadband, 25–26**
**cable modems, 161**
**cabling, 158–159, 186–187, 217–218, 220–221. *See also* connectors; Ethernet; tools**
568A/568B wiring standards, 200–201
applications, 221
attenuation, 221–222
bandwidth, 219
baseband transmissions, 185
coaxial, 190–191
cross-over, 201–203, 225
dB loss, 221–222
fiber distribution panels, 208
fiber-optic, 192–193, 225
full-duplex mode, 185–186
general media considerations, 184
half-duplex mode, 185–186
horizontal, 205–206
interference, 222
loopback, 204
network cross-connects, 204–205
open/short faults, 223–224
patch panels, 207–208
plenum, 194
PVC-based, 194
RG-6, 197
RG-59, 197
rollover, 203
simplex mode, 185–186
specifications/limitations, 220
splits, 222–223
STP (shielded twisted-pair), 187
straight-through, 201–203
throughput testing, 218–219
transmission rates, 186
twinaxial, 191–192
twisted-pair, 187–190
UTP (unshielded twisted-pair), 187
vertical, 206
**caching, 166–167**
**CANs (campus-area networks), 17**
**captive portals, 261, 432**
**CAs (certificate authorities), 414**
**CASB (Cloud Access Security Broker), 284**
**cellular technology access, 241**
**certificates, 414**
**change management documentation, 302–303**
**CIDR (classess interdomain routing), 100**
**circuit switching, 124–125**
**client/server networks, 14–15**
**client-to-site VPNs, 438**
**cloud computing, 35, 283, 284**
connectivity options, 289
DaaS (Desktop as a Service), 288–289
deployment models
hybrid and community clouds, 289
IaC (Infrastructure as Code), 289
private cloud, 289
public cloud, 289
elasticity, 289
IaaS (Infrastructure as a Service), 284, 287–288
multitenancy, 289
PaaS (Platform as a Service), 284, 286–287
relationship between resources, 290
SaaS (Software as a Service), 284, 285–286

scalability, 289–290
security, 290
VPC (virtual private cloud), 289
**cloud sites, 316**
**clustering, 318**
**coaxial cable, 190–191**
**cold sites, 315**
**commands**
arp ping, 431–432
dig, 442–443
FTP, 60
hostname, 430
ipconfig, 437–440
netstat, 432–437
nslookup, 441–442
ping, 425–426, 428–430. *See also* ping command
show, 445
tcpdump, 443
tracert, 126–127, 421–422
**configuration-related documentation, 303**
**connectionless protocols, 54**
**connection-oriented protocols, 54**
**connectors**
BNC, 194–195
fiber, 197–199
F-type, 197
RJ-11, 195–196
RJ-45, 196
**convergence, 127–128**
**core layer, 173**
**cross-over cable, 201–203, 225**
**cryptography, 412**
**CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), 132–133**
**CSMA/CD (Carrier Sense Multiple Access/Collision Detection), 130–132**
**CSU/DSU (channel service unit/data service unit), 34**
**cut-through switching, 158**
**CWDM (coarse wavelength-division multiplexing), 31**

## D

**DaaS (Desktop as a Service), 288–289**
**DAC (discretionary access control), 405–406**
**data link layer, 44**
**datacenters**
location types, 176–177
traffic flows, 176
**deauthentication, 422**
**decapsulation, 49–50**
**default gateway, 100–102, 120–122**
**default route, 123**
**defense in depth, 408**
**demarcation point, 32–33**
**DHCP (Dynamic Host Configuration Protocol), 62–63, 86–88, 109**
DNS suffixes and, 89
relays and IP helpers, 89
rogue servers, 422
**differential backups, 310**
**dig command, 442–443**
**disaster recovery, 308, 309. *See also* power management**
backups, 309, 311–312
best practices, 312–313
differential, 310
full, 309–310
incremental, 310–311
cloud sites, 316
cold sites, 315
environmental concerns, 339
hot sites, 315–316
MTBF (mean time between failures), 316
MTTR (mean time to recovery), 316
RTO (recovery time objective), 317
snapshots, 312
SPOF (single point of failure), 316
UPSs (uninterruptible power supplies), 313–314
warm sites, 316
**disposal of assets policies, 425**

**distance-vector routing, 126–128**
**distributed switching, 123**
**distribution/aggregation layer, 173**
**DNS (Domain Name System), 62, 78–79, 85–86**
HOSTS file resolution, 79–80
namespace, 81–83
poisoning, 422
records, 83–84
types of entries, 83
**documentation, 285–287**
baselines, 293–294
change management, 302–303
configuration, 303
labeling, 304
network wiring schematics, 287–289, 305–307
troubleshooting and, 289–290
physical and logical network diagrams, 290–293
policies, 295–301
procedures, 301–302
regulations, 303–304
**DoS (denial-of-service) attacks, 420–421**
**DRDoS (distributed reflective DoS) attacks, 420–421**
**DSL (digital subscriber line), 23**
modems, 161
speeds, 24
variations, 23–24
**DTLS (Datagram Transport Layer Security), 438**
**duplexing, 224–225**
**DWDM (dense wavelength-division multiplexing), 30**
**dynamic addressing, 108–110**
**dynamic routing, 45**

## E

**EAP (Extensible Authentication Protocol), 417**
**EIGRP (Enhanced IGRP), 127**
**elasticity, 289**
**EMI (electromagnetic interference), 222**
**encapsulation, 49–50**
**error checking, 45**
**ESP (Encapsulating Security Payload), 57**
**Ethernet**
10Base-T, 210–211
10GBASE-LR, 214
10GBASE-SR, 214
10GBASE-T, 212–213
40GBASE-T, 213
100Base-T, 211–212
1000BASE-LX, 213
1000BASE-SX, 213
1000Base-T, 212

## F

**Fast Ethernet, 211–212**
**fault tolerance, 317**
**FC (Fibre Channel), 178–179**
**FCoE (Fibre Channel over Ethernet), 178–179**
**FHRP (First Hop Redundancy Protocol), 319**
**fiber connectors, 197–199**
**fiber distribution panels, 208**
**fiber-optic cable, 192–193, 225**
**firewalls, 153–154**
screened subnet, 408–409
**firmware updates, 337**
**flow control, 45–46**
**fractional T, 27**
**Fraggle attacks, 420**
**fragment-free switching, 158**
**FTP (File Transfer Protocol), 58–60, 435**
**F-type connectors, 197**
**full backups, 309–310**
**full-duplex mode, 185–186**
**fusion splicer, 231**

## G

**geofencing, 432**
**Gigabit Ethernet, 212**
**Global System for Mobile Communications (GSM), 241**
**GPS (Global Positioning System), 90**
**GRE (Generic Routing Encapsulation), 58**

## H

**half-duplex mode, 185–186**
**headends, 168**
**high availability, 318–319**
**honeypots, 410–411**
**horizontal cables, 205–206**
**hostname command, 430**
**HOSTS file resolution, 79–81**
**hot sites, 315–316**
**HTTP (Hypertext Transfer Protocol), 64**
**HTTPS (Hypertext Transfer Protocol Secure), 70, 439**
**hub-and-spoke topology, 5–6. *See also* star topology**
**hubs, 160**
**hybrid routing protocols, 130**
**hybrid topology, 7**
**hypervisor, 34–35**

## I

**IaaS (Infrastructure as a Service), 287–288**
**IANA (Internet Assigned Numbers Authority), 98**
**ICMP (Internet Control Message Protocol), 57**
**ICMP flood attacks, 421**
**IDS (intrusion detection system), 154–155**
**IMAP4 (Internet Message Access Protocol version 4), 65**
over SSL, 71
**incremental backups, 310–311**
**infrastructure topology, 8**
**Internet access**
cable broadband, 25–26
DSL (digital subscriber line), 23–25
speeds, 24
variations, 23–24
leased lines, 27–29
metro-optical networks, 29
CWDM (coarse wavelength-division multiplexing), 31
DWDM (dense wavelength-division multiplexing), 30
PON (passive optical network), 30
SDH (Synchronous Digital Hierarchy), 30
SONET (Synchronous Optical Network), 29
PSTN (public switched telephone network), 26
satellite, 31–32
**IoT (Internet of Things), 432**
**IP (Internet Protocol), 54–55**
**IP addressing, 94**
APIPA (Automatic Private IP Addressing), 111–112
BOOTP (BOOT Protocol), 111
DNAT (Destination Network Address Translation), 116
dynamic addressing, 108–110
IPv4, 95, 98–99
address types, 102–103
CIDR (classless interdomain routing), 100
classes, 95–96
default gateways, 100–102
private address ranges, 99–100
subnet mask assigment, 97
subnetting, 97–98
VIP (virtual IP address), 102
IPv6, 103
address types, 105–107
distinguishing from IPv4, 103–105

IPv4 and, 107–108
neighbor discovery, 107
MAC addresses, 112–114, 144
NAT (Network Address Translation), 114–115
nodes, 94
PAT (Port Address Translation), 115–116
SNAT (Static Network Address Translation), 116
static addressing, 108
subnet mask, 95
**ipconfig command, 437–440**
**iperf, 418–419**
**IPS (intrusion prevention system), 154–155**
**IPSec (IP Security), 57–58, 437–438**
**IPv4, 95, 98–99**
address types, 102–103
CIDR (classess interdomain routing), 100
classes, 95–96
default gateways, 100–102
distinguishing from IPv6, 103–105
IPv6 and, 107–108
private address ranges, 99–100
subnet mask assigment, 97
subnetting, 97–98
VIP (virtual IP address), 102
**IPv6, 103**
address types, 105–107
distinguishing from IPv4, 103–105
IPv4 and, 107–108
neighbor discovery, 107
**iSCSI, 178**
**IS-IS (Intermediate System-to-Intermediate System), 129**
**ISO (International Organization for Standardization), 41**

## J-K

**jumbo frames, 141**
**Kerberos, 412–414**

## L

**LACP (Link Aggregation Control Protocol), 135**
**LANs (local-area networks), 15**
**LDAP (Lightweight Directory Access Protocol), 69–70, 414**
**LDAPS (Lightweight Directory Access Protocol over SSL), 71**
**leased lines, 27–28**
**link-local addresses, 106**
**link-state routing, 129**
**load balancers, 165–166, 317**
**load tests, 330–331**
**local authentication, 414**
**logic bombs, 422**
**logical link control (LLC) layer, 44**
**logical network diagrams, 290–293**
**logs, 415**
application, 334
history, 335
management, 335–336
security, 332–333
system, 334–335
**loopback adapter, 228**
**loopback cable, 204**

## M

**MAC (mandatory access control), 405**
**MAC (media access control) layer, 44**
**MAC addresses, 112–114, 144**
**MANs (metropolitan-area networks), 16–17**
**MDI-X (medium-dependent interface crossed) port, 25, 142**
**media converter, 163–164**
**media couplers/converters, 200**
**mesh topology, 6, 10–12**
**metro-optical networks, 29**
CWDM (coarse wavelength-division multiplexing), 31
DWDM (dense wavelength-division multiplexing), 30

OCx (optical carrier) levels, 29–30
PON (passive optical network), 30
SDH (Synchronous Digital Hierarchy), 30
SONET (Synchronous Optical Network), 29

**mGRE (Multipoint Generic Routing Encapsulation), 19**

**MIBs (management information bases), 68**

**modems, 161–162**

**monitoring network performance, 323, 324**
network device logs, 332
application logs, 334
history logs, 335
management, 335–336
security logs, 332–333
system logs, 334–335
performance metrics, 324–328
SNMP monitors, 328–329
MIBs (management information bases), 329

**MPLS (Multiprotocol Label Switching), 18–19**

**MSAU (multistation access unit), 4**

**MTBF (mean time between failures), 316**

**MTTR (mean time to recovery), 316**

**MTU (maximum transmission unit), 55, 223**

**multicast addresses, 106**

**multicasting, 102–103**

**multifactor authentication, 426**

**multilayer switches, 159–160**

**multipathing, 317**

**multiplexing, 21214, 224–225**

**multitenancy, 289**

## N

**NAS (network-attached storage), 179**

**NAT (Network Address Translation), 114–115**

**NetFlow, 419**

**netstat command, 432–437**

**network layer, 44–45**

**networked devices, 168–169**

**networking devices**
bridges, 161
firewalls, 153–154
headends, 168
hubs, 160
IDS (intrusion detection system), 154–155
IPS (intrusion prevention system), 154–155
LED status indicators, 224
load balancer, 165–166
media converter, 163–164
media couplers/converters, 200
modems, 161–162
proxy server, 166–168
repeaters, 165
routers, 155–156
switches, 157–159
cabling, 158–159
multilayer, 159–160
transceivers, 199
voice gateway, 164–165
VPN concentrators, 168
wireless LAN controller, 165

**networks, 14. *See also* architecture; documentation; Internet access; monitoring networkperformance; performance; topology(ies); VLANs (virtual local-area networks); wireless networks**
APs (access points), 162–163
CANs (campus-area networks), 17
client/server, 14–15
CSU/DSU (channel service unit/data service unit), 34
diagrams, 290–293
documentation, 285–287
hardening, 431–432
LANs (local-area networks), 15

MANs (metropolitan-area networks), 16–17
PANs (personal-area networks), 17
peer-to-peer, 14–15
performance metrics, 324–328
performance monitoring, 324
SANs (storage-area networks), 17, 177–178
SDWANs (software-defined wide area networks), 18
segmentation, 408
termination points, 32
demarc, 32–33
smart jacks, 33
verifying, 34
troubleshooting
common issues, 449–456
performance, 457
virtual, 34
cloud computing, 35
hypervisor, 34–35
NFV (network function virtualization), 35
virtual router, 36
virtual local-area, 133
WANs (wide-area networks), 16
WLANs (wireless LANs), 15

**NFV (network function virtualization), 35**

**NIC teaming, 318**

**nmap utility, 445**

**nslookup command, 441–442**

**NTP (Network Time Protocol), 64, 89–90**

## O

**OCx (optical carrier) levels, 29–30**

**OSI (Open Systems Interconnection) model, 41, 42–43,47–48**
application layer, 47
data link layer, 44
encapsulation/decapsulation, 49–50
network layer, 44–45
physical layer, 43–44
presentation layer, 46
session layer, 46
TCP/IP model and, 48
transport layer, 45–46

**OSPF (Open Shortest Path First) protocol, 45, 129**

**out-of-band management, 400–401**

## P

**PaaS (Platform as a Service), 286–287**

**packet switching, 123–124**

**PANs (personal-area networks), 17**

**partial mesh topology, 7**

**passwords**
policies and, 298–300
strength, 300–301

**PAT (Port Address Translation), 115–116**

**patch management, 336–339**

**patch panels, 207–208**

**on-path attacks, 422**

**PDU (protocol data unit), 50**

**peer-to-peer networks, 14–15**

**penetration testing, 418**

**performance**
load tests, 330–331
metrics, 324–328, 331
monitoring, 324
stress tests, 331
testing, 330
troubleshooting, 457

**phishing attacks, 422**

**physical layer, 43–44**

**physical network diagrams, 290–293**

**physical security, 425**
biometrics, 426
lock and key, 425
multifactor authentication, 426
swipe card and PIN access, 425–426

**PIN access, 425–426**

**ping command, 425–426, 428–430**
results, 426
"Destination Unreachable" message, 426
expired TTL message, 427–428
"Request Timed Out" message, 426–427
"Unknown Host" message, 427–428
**ping of death attacks, 420**
**plenum, 194**
**PoE (Power over Ethernet), 143**
**poison reverse, 128**
**policies, 295–298, 318**
disposal of assets, 425
separation of duties, 409–410
**PON (passive optical network), 30**
**POP3 (Post Office Protocol version 3), 65, 71**
**port aggregation, 318**
**port binding, 135**
**port forwarding, 116**
**port mirroring, 142–143**
**port(s), 73–75, 223**
authentication, 143
mirroring, 142–143
well-known, 75
**power management, 314**
UPSs (uninterruptible power supplies), 313–314
**presentation layer, 46**
**preshared keys, 432**
**private address ranges, 99–100**
**procedures, 301–302**
**propagation time, 32**
**protocol analyzer, 415–416**
**protocols, 53**
BOOTP (BOOT Protocol), 111
connection oriented vs. connectionless, 54
DHCP (Dynamic Host Configuration Protocol), 62–63, 86–88,88, 109
DNS suffixes and, 89
relays and IP helpers, 89
DNS (Domain Name System), 62, 78–79
HOSTS file resolution, 79–81
namespace, 81–83
records, 83–84
types of entries, 83
FTP (File Transfer Protocol), 58–60, 435
GRE (Generic Routing Encapsulation), 58
HTTP (Hypertext Transfer Protocol), 64
HTTPS (Hypertext Transfer Protocol Secure), 70
ICMP (Internet Control Message Protocol), 57
IP (Internet Protocol), 54–55
IPSec (IP Security), 57–58
LDAP (Lightweight Directory Access Protocol), 69–70
LDAPS (Lightweight Directory Access Protocol over SSL), 71
NTP (Network Time Protocol), 64, 89–90
POP3 (Post Office Protocol version 3), 65
ports and, 73–75
RDP (Remote Desktop Protocol), 72
secured vs. unsecured, 427–431
SFTP (Secure File Transfer Protocol), 61
SIP (Session Initiation Protocol), 72–73
SMB (Server Message Block), 70
SMTP (Simple Mail Transfer Protocol), 62
SMTPS (Simple Mail Transfer Protocol Secure), 71
SNMP (Simple Network Management Protocol), 66
agents, 67–68
communities, 69
components, 66–67

management systems, 67
MIBs (management information bases), 68
version 3, 69
SSH (Secure Shell), 60–61
TCP (Transmission Control Protocol), 55–56
Telnet, 61–62
TFTP (Trivial File Transfer Protocol), 63–64
UDP (User Datagram Protocol), 56–57

**proxy servers, 166–168**

**PSTN (public switched telephone network), 26**

**punchdown blocks, 208–209**

**PVC-based cable, 194**

## Q-R

**QoS (Quality of Service), 145**

**RADIUS (Remote Authentication Dial-In User Service), 411–412**

**ransomware, 422**

**RARP (Reverse Address Resolution Protocol), 148**

**RBAC (rule-based access control), 406**

**RDP (Remote Desktop Protocol), 72**

**redundancy, 6, 318–319**

**reflection, 263–264**

**refraction, 263–264**

**regulations, 303–304**

**remote access, 434–435**

**repeaters, 165**

**RFCs (requests for comments), 55**

**RG-6 cable, 197**

**RG-59 cable, 197**

**ring topology, 3–4**

**RIP (Routing Information Protocol), 127**

**risk management, 418**

**RJ-11 connectors, 195–196**

**RJ-45 connectors, 196**

**RO (ring-out) port, 4**

**rogue APs, 422**

**rogue DHCP servers, 422**

**role-based access control, 406–408**

**rollover cable, 203**

**route utility, 443–445**

**routers, 155–156**
default gateway, 120–122
routing table, 122
show command, 445
for wireless networks, 250–254

**routing**
default route, 123
distance-vector, 126–128
dynamic, 126
hybrid protocols, 130
link-state, 129
metrics, 133
poison reverse, 128
split horizon, 128
static, 122–123

**RTO (recovery time objective), 317**

## S

**SaaS (Software as a Service), 285–286**

**SANs (storage-area networks), 17, 177–178**

**satellite Internet access, 31–32**

**schematics, 287–289, 305–307**
troubleshooting and, 289–290

**screened subnet, 408–409**

**SCSI (Small Computer Systems Interface), 178**

**SDH (Synchronous Digital Hierarchy), 30**

**SDN (software-defined networking), 18, 174**
application layer, 174
control layer, 175
infrastructure layer, 175
management plane, 175

**SDWANs (software-defined wide area networks), 18**

**security. *See also* attacks; VPNs (virtual private networks)**
access control, 405
discretionary, 405–406
MAC filtering, 418
mandatory, 405
NAC (network access control), 417
role-based, 406–408
rule-based, 406
auditing, 415
authentication, 137
authorization, 137
certificates, 414
CIA triad, 405
cloud computing and, 290
defense in depth, 408
DTLS (Datagram Transport Layer Security), 438
honeypots, 410–411
IPSec (IP Security), 437–438
Kerberos, 412–414
LDAP (Lightweight Directory Access Protocol), 414
local authentication, 414
multifactor authentication, 415–416
network hardening, 431–432
network segmentation, 408
penetration testing, 418
physical, 425
biometrics, 426
lock and key, 425
multifactor authentication, 426
swipe card and PIN access, 425–426
RADIUS (Remote Authentication Dial-In User Service), 411–412
remote access, 434–435
risk management, 418
screened subnet, 408–409
separation of duty policies, 409–410
TACACS (Terminal Access Controller Access Control System), 412
TLS (Transport Layer Security), 438
vulnerabilities, 405, 423
wireless
antenna placement and power levels, 432
captive portals, 432
geofencing, 432
isolation, 432
MAC filtering, 432
preshared keys, 432

**segmentation, 45**
VLAN, 137–138

**self-healing, 11**

**session layer, 46**

**SFP (small form-factor pluggable) modules, 199**

**SFTP (Secure File Transfer Protocol), 61**

**SIEM (security information and event management), 418**

**simplex mode, 185–186**

**SIP (Session Initiation Protocol), 72–73**

**site surveys, 262**

**site-local addresses, 106**

**smart jacks, 33**

**SMB (Server Message Block), 70**

**SMTP (Simple Mail Transfer Protocol), 62**

**SMTPS (Simple Mail Transfer Protocol Secure), 71**

**Smurf attacks, 420**

**snapshots, 312**

**SNAT (Static Network Address Translation), 116**

**SNMP (Simple Network Management Protocol), 66, 328–329**
agents, 67–68
communities, 69
components, 66–67
management systems, 67

MIBs (management information bases), 68, 329
version 3, 69
**social engineering, 421–422**
**SONET (Synchronous Optical Network), 29**
**spectrum analyzer, 231–232**
**spine and leaf architecture, 175–176**
**split horizon, 128**
**SPOF (single point of failure), 316**
**spoofing attacks, 422**
**SQL (Structured Query Language), 71–72**
**SSH (Secure Shell), 60–61**
**SSID (service set identifier), 247, 248**
**SSL (Secure Sockets Layer), 438**
**star topology, 5–6**
**static addressing, 108**
**static routing, 45, 122–123**
**storage, network-attached, 179**
**store-and-forward switching, 158**
**STP (shielded twisted-pair), 187**
**STP (Spanning Tree Protocol), 138–140**
**straight-through cable, 201–203**
**stratum, 90**
**stress tests, 331**
**subnet mask, 95**
**subnetting, 97–98**
**swipe cards, 425–426**
**switches, 5, 157–159**
cabling, 158–159
interface configuration, 140–141
management, 144
multilayer, 159–160
**switching, 123**
circuit, 124–125
comparing methods, 125
distributed, 123
packet, 123–124
**SYN flood attacks, 420**

## T

**T connectors, 2**
**T3 lines, 28–29**
**TACACS (Terminal Access Controller Access Control System), 412**
**T-carrier lines**
fractional T, 27
T3, 28–29
**TCP (Transmission Control Protocol), 55–56**
**tcpdump command, 443**
**TCP/IP model, 41. *See also* IP addressing**
OSI model and, 48
**TDM (time-division multiplexing), 185**
**TDR (time-domain reflectometer), 229**
**Telnet, 61–62**
**terminal emulator, 419**
**termination points, 32**
demarc, 32–33
smart jacks, 33
verifying, 34
**TFTP (Trivial File Transfer Protocol), 63–64, 419**
**three-tiered architecture, 172–173**
access/edge layer, 174
core layer, 173
distribution/aggregation layer, 173
**throughput testing, 218–219**
**TIA/EIA 568A/568B wiring standards, 200–201**
**TLS (Transport Layer Security), 46, 438**
**tone generator, 228**
**tools**
cable crimpers, 226–227
cable tester, 230–231
fiber light meter, 232
fusion splicer, 231
loopback adapter, 228
multimeter, 230

OTDR (optical time-domain reflectometer), 229
punchdown, 227
spectrum analyzer, 231–232
tap, 231
TDR (time-domain reflectometer), 229
tone generator, 228
wire map, 231
**topology(ies), 2**
bus, 2–3
convergence, 127–128
hybrid, 7
mesh, 6
ring, 3–4
star, 5–6
wireless
ad hoc, 9
infrastructure, 8
mesh, 10–12
**tracert command, 126–127, 421–422**
**traffic flows, 176**
**traffic shaping, 146**
**transceivers, 199, 224**
**transport layer, 45–46**
**troubleshooting**
document findings, actions, outcomes, and lessons, 411
establish a plan of action, 408–409
establish a theory of probably cause, 407–408
hardware failure, 456–457
identifying the problem, 405–406
approach multiple problems individually, 407
determine whether anything has changed, 406
duplicate the problem, 407
symptoms, 406
implement the solution, 409–410
networks
common issues, 449–456
performance, 457
tools, 420
ARP (Address Resolution Protocol), 430–431
arp ping, 431–432
bandwidth speed tester, 416
command-line, 420
dig command, 442–443
hostname command, 430
IP scanner, 419
ipconfig command, 437–440
iperf, 418–419
NetFlow, 419
netstat command, 432–437
nmap utility, 445
nslookup command, 441–442
ping command, 425–426, 428–430. *See also* ping command
port scanner, 416–418
protocol analyzer, 415–416
route utility, 443–445
show command, 445
tcpdump command, 443
terminal emulator, 419
TFTP server, 419
tracert/traceroute command, 421–422
Wi-Fi analyzer, 415
verify full system functionality, 410
wireless networks, 258–261
APs (access points), 264–265
signal loss, 258
**trunking, 135, 142**
**TTL (time to live), 427–428**
**twinaxial cable, 191–192**
**twisted-pair cabling, 187–190**

## U

**UDP (User Datagram Protocol), 56–57**
**unicast addresses, 102**
**unshielded twisted-pair (UTP), 25**
**updates, 337–338**

**URL (uniform resource locator), 167**
**UTP (unshielded twisted-pair), 187**

## V

**vertical cables, 206**
**VIP (virtual IP address), 102**
**virtual desktops, 438**
**virtual networks, 34**
cloud computing, 35
hypervisor, 34–35
NFV (network function virtualization), 35
virtual router, 36
**VLANs (virtual local-area networks), 133, 134**
802.1Q, 134
advantages of, 134
hopping, 422
membership, 135–137
port binding, 135
segmentation, 137–138
**VLSM (Variable Length Subnet Masking), 98**
**voice gateway, 164–165**
**VPNs (virtual private networks), 435, 438**
client-to-site, 438
components, 436
concentrators, 168
connection types, 436
pros and cons, 436–437
**VRRP (Virtual Router Redundancy Protocol), 319**
**VTP (VLAN Trunking Protocol), 135**
**vulnerabilities, 423**

## W-X-Y-Z

**WANs (wide-area networks), 16**
MPLS (Multiprotocol Label Switching), 18–19
**WAPs (wireless access points), 162**
**warm sites, 316**
**WDM (wavelength-division multiplexing), 212–214**
**well-known ports, 75**
**Wi-Fi 6e, 240**
**Wi-Fi analyzer, 415**
**windowing, 46**
**wired mesh topology, 6. *See also* mesh topology**
**wireless networks**
802.11a standard, 236–237
802.11ac, 240
802.11ax, 240
802.11b/g standard, 237, 238
ad hoc topology, 9
antennas, 243–244
coverage, 244–245
ratings, 244
APs (access points), 8, 162–163, 246–248, 259
troubleshooting, 264–265
BYOD (bring-your-own-device), 254
captive portals, 261, 432
cellular technology access, 241
channel bonding, 242–243
collisions, 242
configuring the wireless connection, 248
MAC address filtering, 249–250
routers, 248–249, 250–254
data rate, 241–242
establishing communication between devices, 246–248
IDF, 209–210
infrastructure topology, 8
mesh topology, 10–12
RF (radio frequency) channels, 15, 236–237, 239
802.11a/ac/ax, 239
802.11b/g/n/ax, 239
overlapping, 237–238
security
antenna placement and power levels, 432

geofencing, 432
isolation, 432
MAC filtering, 432
preshared keys, 432
signal loss
absorption and, 263–264
interference and, 262–263
reflection and, 263–264
refraction and, 263–264
troubleshooting, 258
site surveys, 262
speed, 241–242
SSID (service set identifier), 247, 248
throughput, 242
troubleshooting, 258–261
Wi-Fi 6e, 240
wireless LAN controller, 165
WPA (Wi-Fi Protected Access), 252–254
**wiring**
closets. *See also* cabling
fiber distribution panels, 208
MDF, 209–210
patch panels, 207–208
punchdown blocks, 208–209
schematics, 287–289, 305–307
troubleshooting and, 289–290
**WLANs (wireless LANs). *See also* wireless networks**
**WPA (Wi-Fi Protected Access), 252–254**

## REGISTER YOUR PRODUCT at PearsonITcertification.com/register

### Access Additional Benefits and SAVE 35% on Your Next Purchase

- Download available product updates.
- Access bonus material when applicable.
- Receive exclusive offers on new editions and related products. (Just check the box to hear from us when setting up your account.)
- Get a coupon for 35% for your next purchase, valid for 30 days. Your code will be available in your PITC cart. (You will also find it in the Manage Codes section of your account page.)

Registration benefits vary by product. Benefits will be listed on your account page under Registered Products.

---

**PearsonITcertification.com–Learning Solutions for Self-Paced Study, Enterprise, and the Classroom**

Pearson is the official publisher of Cisco Press, IBM Press, VMware Press, Microsoft Press, and is a Platinum CompTIA Publishing Partner–CompTIA's highest partnership accreditation.

At **PearsonITcertification.com** you can

- Shop our books, eBooks, software, and video training.
- Take advantage of our special offers and promotions (pearsonitcertifcation.com/promotions).
- Sign up for special offers and content newsletters (pearsonitcertifcation.com/newsletters).
- Read free articles, exam profiles, and blogs by information technology experts.
- Access thousands of free chapters and video lessons.

**Connect with PITC – Visit PearsonITcertifcation.com/community**

Learn about PITC community events and programs.

PEARSON IT CERTIFICATION

Addison-Wesley • Cisco Press • IBM Press • Microsoft Press • Pearson IT Certification • Prentice Hall • Que • Sams • VMware Press

To receive your 10% off Exam Voucher, register your product at:

www.pearsonitcertification.com/register

and follow the instructions.

Pearson

# Where are the companion content files?

## Register this digital version of CompTIA Network+ N10-008 Exam Cram to access important downloads.

Register this eBook to unlock the companion files. Follow these steps:

1. Go to **pearsonITcertification.com/account** and log in or create a new account.
2. Enter the ISBN: **9780137375769** (NOTE: Please enter the print book ISBN provided to register the eBook you purchased.)
3. Answer the challenge question as proof of purchase.
4. Click on the "Access Bonus Content" link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

This eBook version of the print title does not contain the practice test software that accompanies the print book.

You May Also Like—Premium Edition eBook and Practice Test. To learn about the Premium Edition eBook and Practice Test series, visit **pearsonITcertification.com/practicetest**