

EXAM ✓ CRAM

CompTIA

Network+[®]

N10-006

Fifth Edition

Save 10%
on Exam
Voucher

See Inside



PEARSON IT
CERTIFICATION



EMMETT DULANEY

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

EXAM ✓ **CRAM**

**CompTIA[®]
Network+**

N10-006

Emmett Dulaney

800 East 96th Street
Indianapolis, Indiana 46240 USA

CompTIA® Network+ N10-006 Exam Cram, Fifth Edition

Copyright © 2015 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-5410-3

ISBN-10: 0-7897-5410-X

Library of Congress Control Number: 2015934591

Printed in the United States of America

Second Printing: September 2015

Trademarks

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

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Special Sales

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

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

For questions about sales outside the U.S., please contact international@pearsoned.com.

Editor-in-Chief

Dave Dusthimer

Acquisitions Editor

Betsy Brown

Development Editor

Jeff Riley

Managing Editor

Sandra Schroeder

Senior Project Editor

Tonya Simpson

Copy Editor

Keith Cline

Indexer

Johnna VanHoose
Dinse

Proofreader

Paula Lowell

Technical Editor

Christopher A.
Crayton

Editorial Assistant

Vanessa Evans

Media Producer

Lisa Matthews

Cover Designer

Alan Clements

Compositor

Mary Sudul

Contents at a Glance

	Introduction	1
CHAPTER 1	Introduction to Networking	9
CHAPTER 2	The OSI Model and Networking Protocols	41
CHAPTER 3	Addressing and Routing	93
CHAPTER 4	Components and Devices	135
CHAPTER 5	Cloud Computing Basics	161
CHAPTER 6	Installation and Configuration	173
CHAPTER 7	Cabling and Wiring	219
CHAPTER 8	Wireless	279
CHAPTER 9	Network Management	325
CHAPTER 10	Network Optimization	367
CHAPTER 11	Network Security	383
CHAPTER 12	Network Troubleshooting	471
	Glossary	555
	Index	603

On the CD:

Practice Exam 1
Answers to Practice Exam 1
Practice Exam 2
Answers to Practice Exam 2

Table of Contents

Introduction	1
CHAPTER 1	
Introduction to Networking	9
LANs, WANs, MANs, SCADA/ICS, Medianets, and Network Models	10
LANs	10
WANs	11
MANs	12
SCADA/ICS	12
Medianets	13
Network Models	13
Centralized Versus Distributed Computing	15
Network Topologies	17
Bus Topology	17
Ring Topology	18
Star Topology	20
Wired Mesh Topology	21
Wireless Topologies	22
Point-to-Point, Point-to-Multipoint, and Wireless Mesh Topologies	24
Hybrid Topologies	27
Creating a SOHO Network	32
What's Next?	39
CHAPTER 2	
The OSI Model and Networking Protocols	41
The Networking Models	42
The OSI Seven-Layer Model	42
The TCP/IP Four-Layer Model	48
Identifying the OSI Layers at Which Various Network Components Operate	48
Dynamic Host Configuration Protocol (DHCP)	51
The DHCP Process	53
DHCP and DNS Suffixes	54
DHCP Relays and IP Helpers	54

Domain Name Service (DNS)	56
The DNS Namespace	58
Types of DNS Entries	60
DNS Records	61
DNS in a Practical Implementation	62
Simple Network Management Protocol (SNMP)	65
Components of SNMP	65
SNMP Management Systems	66
SNMP Agents	67
Management Information Bases	67
SNMP Communities	68
SNMPv3	69
Protocols	71
Connection-Oriented Protocols Versus Connectionless Protocols	72
Internet Protocol	73
Transmission Control Protocol	73
User Datagram Protocol	74
File Transfer Protocol	75
Secure File Transfer Protocol	76
Trivial File Transfer Protocol	77
Simple Mail Transfer Protocol	78
Hypertext Transfer Protocol	78
Hypertext Transfer Protocol Secure	79
Post Office Protocol Version 3/Internet Message Access Protocol Version 4	79
Telnet	80
Secure Shell	80
Internet Control Message Protocol	81
Address Resolution Protocol/Reverse Address Resolution Protocol	82
Network Time Protocol	83
Network News Transfer Protocol	84
Secure Copy Protocol	84
Lightweight Directory Access Protocol	85
Internet Group Management Protocol	85
Transport Layer Security	85

Session Initiation Protocol/Real-Time Transport Protocol	86
Remote Desktop Protocol	87
Server Message Block	88
Understanding Port Functions	88
What's Next?	92

CHAPTER 3

Addressing and Routing	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
Classless Interdomain Routing	100
Default Gateways	100
IPv4 Address Types	102
IPv6 Addressing	102
Comparing IPv4 and IPv6 Addressing	107
Assigning IP Addresses	107
Identifying MAC Addresses	111
NAT, PAT, SNAT, and DNAT	113
Managing TCP/IP Routing	119
The Default Gateway	119
Routing Tables	120
Static Routing	121
Dynamic Routing	122
Routing Metrics	126
Configuring Routers and Switches	128
Proxy Servers	128
The Spanning Tree Protocol	130
Trunking	132
Port Mirroring	132
Port Authentication	133
High Availability	133
What's Next?	134

CHAPTER 4

Components and Devices 135

- Common Network Devices 136
 - Access Point 136
 - Analog Modem 137
 - Content Filter 138
 - Firewall. 138
 - IDS and IPS 139
 - Hub 140
 - Load Balancer 141
 - Packet Shaper 142
 - Router 142
 - Switch 143
 - Multilayer Switch. 146
 - VPN Concentrator. 147
 - Network Devices Summary 147
- Switch Configuration 150
 - Virtual Local-Area Networks 150
 - Working with Spanning Tree 155
 - Interface Configuration and Switch Management 156
 - Power over Ethernet 157
 - Switch Management. 157
 - Managed and Unmanaged. 158
- What's Next? 159

CHAPTER 5

Cloud Computing Basics 161

- Cloud Concepts 162
 - Software as a Service 163
 - Platform as a Service. 163
 - Infrastructure as a Service 163
 - Private Cloud 164
 - Public Cloud 164
 - Community Cloud 165
 - Hybrid Cloud 165
- Virtualization and Storage-Area Networks 167
 - Virtualization. 167

Storage-Area Networks	170
What's Next?	172

CHAPTER 6

Installation and Configuration	173
WAN Technologies	174
Switching Methods	174
Integrated Services Digital Network	177
Leased Lines	179
Fiber, SONET, and OCx Levels	181
Frame Relay	183
Asynchronous Transfer Mode	185
Summary of WAN Technologies	186
Other WAN Technologies	187
Internet Access Technologies	191
DSL Internet Access	192
Cable Internet Access	195
Broadband Security Considerations	198
Dialup	198
The Public Switched Telephone Network	201
Satellite Internet Access	201
Wireless Internet Access	203
Cellular	204
Safety Practices	208
Focusing on Safety	208
Electrical Safety and ESD	209
Installation Safety	210
Fire Suppression	210
In Case of an Emergency	212
Installing and Configuring Equipment	214
Distribution Frames	214
Cable Management	215
Power Management	216
Device Placement and Labeling	216
Rack Systems	216
What's Next?	218

CHAPTER 7

Cabling and Wiring 219

- General Media Considerations 220
 - Broadband Versus Baseband Transmissions 221
 - Simplex, Half-Duplex, and Full-Duplex Modes 223
 - Media Interference 223
 - Attenuation 224
 - Data Transmission Rates 224
 - Types of Network Media 225
 - Types of Media Connectors 232
 - Media Couplers/Converters 238
 - 568A and 568B Wiring Standards 240
 - Straight-Through Versus Crossover Cables 240
 - Rollover and Loopback Cables 243
 - Components of Wiring Distribution 244
 - Helpful Tools 252
- Comparing and Contrasting LAN Technologies 258
 - IEEE 802.2 Standard 259
 - 802.3 Ethernet Standards 263
 - Related Network Concepts 269
 - Cram Quiz Answers 272
- Troubleshooting Common Issues 273
 - WAN-Related Issues 273
 - Customer Premise Equipment 275
 - Company Security Policies 276
 - Satellite Issues 277
- What's Next? 278

CHAPTER 8

Wireless 279

- Understanding Wireless Basics 280
 - Wireless Access Points 281
 - Wireless Antennas 284
 - Wireless Radio Channels 289
 - Data Rate Versus Goodput 292
 - Beacon Management Frame 293
 - Spread-Spectrum Technology 294

- Orthogonal Frequency-Division Multiplexing 295
- Infrared Wireless Networking 295
- Establishing Communications Between Wireless Devices 296
- Configuring the Wireless Connection. 299
- 802.11 Wireless Standards 305
 - The Magic Behind 802.11n and 802.11ac 307
 - A Summary of 802.11 Wireless Standards 308
- Securing Wireless Networks 311
 - Wired Equivalent Privacy 311
 - Wi-Fi Protected Access. 312
 - WPA2 313
 - WPA Enterprise 314
 - Other Dangers. 315
- Wireless Troubleshooting Checklist 318
 - Factors Affecting Wireless Signals 322
- What’s Next? 324

CHAPTER 9

- Network Management 325**
 - Documentation Management. 327
 - Wiring Schematics 329
 - Physical and Logical Network Diagrams 332
 - Baselines 335
 - Policies, Procedures, Configurations, and Regulations. 336
 - Monitoring Network Performance 344
 - Common Reasons to Monitor Networks 345
 - Packet Sniffers 348
 - Throughput Testing. 349
 - Port Scanners 351
 - Network Performance, Load, and Stress Testing 353
 - Tracking Event Logs 355
 - Patches and Updates 362
 - What’s Next? 366

CHAPTER 10

Network Optimization 367

- Unified Communication Technologies 368
 - Quality of Service 368
 - Traffic Shaping 369
 - VoIP 370
 - Video 370
 - Real-Time Services 371
 - Unified Communication Devices 372
- Network Segmentation 374
 - SCADA Systems 375
 - Legacy Systems 375
 - Separate Private/Public Networks 375
 - Honeypots and Honeynets 376
 - Testing Lab 377
 - Load Balancing 377
 - Performance Optimization 378
 - Security 380
 - Compliance 380
- What's Next? 382

CHAPTER 11

Network Security 383

- Tunneling, Encryption, and Access Control 384
 - VPNs 385
 - Point-to-Point Tunneling Protocol 387
 - Layer 2 Tunneling Protocol 388
 - IPsec 389
 - Site-to-Site, Host-to-Site, and Host-to-Host 390
 - Overview of Access Control 391
 - Remote-Access Protocols and Services 394
 - Remote-Control Protocols 397
 - MAC Filtering 398
 - TCP/IP Filtering 399
- Disaster Recovery 402
 - Full Backups 403
 - Differential Backups 404

- Incremental Backups 404
- Tape Rotations 405
- Backup Best Practices 406
- Using Uninterruptible Power Supplies 407
- Hot and Cold Spares 408
- Hot, Warm, and Cold Sites 409
- Risk-Related Policies and Procedures 411
- Managing Common Security Threats 416
 - Viruses 417
 - Worms and Trojan Horses 418
 - Denial-of-Service and Distributed
 - Denial-of-Service Attacks 419
 - Other Common Attacks 421
 - Vulnerabilities and Prevention 426
- Authentication, Authorization, and Accounting (AAA) 431
 - Passwords and Password Policies 433
 - Kerberos Authentication 435
 - Public Key Infrastructure 438
 - TACACS/RADIUS 441
 - Remote Authentication Protocols 442
 - Secured Versus Unsecured Protocols 444
 - Adding Physical Security to the Mix 446
 - Two-factor and Multifactor Authentication 448
- Firewalls, Appliances, and Physical Security 451
 - Stateful and Stateless Firewalls 453
 - Packet-Filtering Firewalls 454
 - Circuit-Level Firewalls 456
 - Application Layer Firewalls 456
 - Comparing Firewall Types 457
 - Firewall Wrap-Up 457
 - Demilitarized Zones (Perimeter Network) 458
 - Other Security Devices 459
 - Physical Security Controls 462
- Responding to Incidents 466
 - First Responders 466
 - Securing the Area 467

Document the Scene	467
eDiscovery and Evidence/Data Collection	467
Chain of Custody	468
Final Responsibilities	468
What's Next?	470

CHAPTER 12

Network Troubleshooting	471
Troubleshooting Steps and Procedures	472
Identify the Problem	473
Establish a Theory of Probable Cause	475
Test the Theory to Determine Cause	475
Establish a Plan of Action	476
Implement the Solution or Escalate	476
Verify Full System Functionality	478
Document the Findings, Actions, and Outcomes	478
Troubleshooting the Network	482
Common Problems to Be Aware Of	483
Troubleshooting Wiring	488
Wiring Issues	490
Troubleshooting Infrastructure Hardware	494
Configuring and Troubleshooting Client Connectivity	496
Troubleshooting an Incorrect VLAN	501
Topology Errors	502
Working with Command-Line Utilities	507
The Trace Route Utility (<code>tracert/traceroute</code>)	509
ping	513
pathping	518
ARP	518
The <code>netstat</code> Command	520
nbtstat	526
The <code>ipconfig</code> Command	527
ifconfig	529
nslookup	530
dig	531
The <code>host</code> Command	533

The route Utility	533
Networking Tools	537
Wire Crimpers, Strippers, and Snips	538
Voltage Event Recorder	539
Environmental Monitors	540
Toner Probes	541
Protocol Analyzer	542
Media/Cable Testers	543
TDR and OTDR	543
Multimeter	544
Network Qualification Tester	545
Butt Set	545
Wireless Detection	546
Speed Tests and Looking Glasses	546
Managing Common Security Threats	549
What's Next?	554
Glossary	555
Index	603

On the CD:

- Practice Exam 1
- Answers to Practice Exam 1
- Practice Exam 2
- Answers to Practice Exam 2

About the Authors

Emmett Dulaney (CompTIA Network+, Cloud+, Security+, A+, and others) is the author of numerous books on certifications and operating systems. He is a columnist for *Certification Magazine* and *Campus Technology*. He is also an associate professor at a small university and the author of the *CompTIA A+ Complete Study Guide* and the *CompTIA Security+ Study Guide*.

Mike Harwood (MCSE, A+, Network+, Server+, Linux+) has more than 14 years of experience in information technology and related fields. He has held a number of roles in the IT field, including network administrator, instructor, technical writer, website designer, consultant, and online marketing strategist. Mike has been a regular on-air technology contributor for CBC radio and has coauthored numerous computer books, including the *Network+ Exam Cram* published by Pearson.

About the Technical Editor

Christopher A. Crayton is an author, a technical editor, a technical consultant, a security consultant, a trainer, and a SkillsUSA state-level technology competition judge. Formerly, he worked as a computer and networking instructor at Keiser College (2001 Teacher of the Year); a network administrator for Protocol, a global electronic customer relationship management (eCRM) company; and at Eastman Kodak headquarters as a computer and network specialist. Chris has authored several print and online books, including *The A+ Exams Guide*, Second Edition (Cengage Learning, 2008), *Microsoft Windows Vista 70-620 Exam Guide Short Cut* (O'Reilly, 2007), *CompTIA A+ Essentials 220-601 Exam Guide Short Cut* (O'Reilly, 2007), *The A+ Exams Guide*, *The A+ Certification and PC Repair Handbook* (Charles River Media, 2005), *The Security+ Exam Guide* (Charles River Media, 2003), and *A+ Adaptive Exams* (Charles River Media, 2002). He is also co-author of the *How to Cheat at Securing Your Network* (Syngress, 2007). As an experienced technical editor, Chris has provided many technical edits and reviews for several major publishing companies, including Pearson Education, McGraw-Hill, Cengage Learning, Wiley, O'Reilly, Syngress, and Apress. He holds MCSE, A+, and Network+ certifications.

Dedication



*For Heb, who really knew how to network
and touched so many that his presence will
be felt for decades to come.*

—Emmett Dulaney

Acknowledgments

An enormous amount of credit for this book goes to Christopher A. Crayton, without whom this edition would be only a shadow of what it is. It was an honor to work with him, and I owe him enormous gratitude. Thanks are also due to Mike Harwood, who wrote the first few editions, and to a team of talented individuals at Pearson, three of whom deserve special attention: Betsy Brown, Jeff Riley, and Christopher Cleveland.

—Emmett Dulaney

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: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/ register for convenient access to any updates, downloads, or errata that might be available for this book.

Becoming a CompTIA Certified IT Professional is Easy

It's also the best way to reach greater professional opportunities and rewards.

Why Get CompTIA Certified?

Growing Demand

Labor estimates predict some technology fields will experience growth of over 20% by the year 2020.* CompTIA certification qualifies the skills required to join this workforce.

Higher Salaries




IT professionals with certifications on their resume command better jobs, earn higher salaries and have more doors open to new multi-industry opportunities.

Verified Strengths

91% of hiring managers indicate CompTIA certifications are valuable in validating IT expertise, making certification the best way to demonstrate your competency and knowledge to employers.**

Universal Skills

CompTIA certifications are vendor neutral—which means that certified professionals can proficiently work with an extensive variety of hardware and software found in most organizations.

 Learn	 Certify	 Work
<p>Learn more about what the exam covers by reviewing the following:</p> <ul style="list-style-type: none"> • Exam objectives for key study points. • Sample questions for a general overview of what to expect on the exam and examples of question format. • Visit online forums, like LinkedIn, to see what other IT professionals say about CompTIA exams. 	<p>Purchase a voucher at a Pearson VUE testing center or at CompTIAstore.com.</p> <ul style="list-style-type: none"> • Register for your exam at a Pearson VUE testing center. • Visit pearsonvue.com/CompTIA to find the closest testing center to you. • Schedule the exam online. You will be required to enter your voucher number or provide payment information at registration. • Take your certification exam. 	<p>Congratulations on your CompTIA certification!</p> <ul style="list-style-type: none"> • Make sure to add your certification to your resume. • Check out the CompTIA Certification Roadmap to plan your next career move.

Learn more: Certification.CompTIA.org/networkplus

* Source: CompTIA 9th Annual Information Security Trends study: 500 U.S. IT and Business Executives Responsible for Security

** Source: CompTIA Employer Perceptions of IT Training and Certification

*** Source: 2023 IT Skills and Salary Report by CompTIA Authorized Partner

Introduction

Welcome to the *CompTIA Network+ N10-006 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 N10-006. 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 hot spots 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+ (N10-006 Edition) exam is a revised version of the original exam. The new Network+ objectives are aimed toward those who have at least 9 months of experience in network support and administration. CompTIA believes that new Network+ candidates require more hands-on experience in network administration and troubleshooting, but this should not discourage those who do not. Quite simply, the nature of the questions on the new exam is not dissimilar to the old, and you can get by without actual hands-on experience. Still, a little hands-on experience never hurt anyone and can certainly add to your confidence going into the exam.

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+ N10-006 exam. This table also lists the chapter in which each exam topic is covered. Some objectives and subobjectives are addressed in multiple chapters.

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

Chapter	N10-006 Exam Objective	N10-006 Exam Subobjective
1 (Introduction to Networking)	1.0 Network Architecture	1.6 Differentiate between common network topologies. 1.7 Differentiate between network infrastructure implementations. 1.12 Given a set of requirements, implement a basic network.

Chapter	N10-006 Exam Objective	N10-006 Exam Subobjective
2 (The OSI Model and Networking Protocols)	1.0 Network Architecture 2.0 Network Operations 5.0 Industry standards, practices, and network theory	1.3 Install and configure the following networking services/applications (DHCP and DNS). 2.1 Given a scenario, use appropriate monitoring tools. 5.1 Analyze a scenario and determine the corresponding OSI layer. 5.9 Compare and contrast the following ports and protocols. 5.10 Given a scenario, configure and apply the appropriate ports and protocols.
3 (Addressing and Routing)	1.0 Network Architecture	1.3 Install and configure the following networking services/applications. 1.8 Given a scenario, implement and configure the appropriate addressing schema. 1.9 Explain the basics of routing concepts and protocols.
4 (Components and Devices)	1.0 Network Architecture 2.0 Network Operations	1.1 Explain the functions and applications of various network devices. 2.6 Given a scenario, configure a switch using proper features.
5 (Cloud Computing Basics)	1.0 Network Architecture	1.1 Explain the functions and applications of various network devices.
6 (Installation and Configuration)	1.0 Network Architecture 5.0 Industry standards, practices, and network theory	1.4 Explain the characteristics and benefits of various WAN technologies. 5.6 Summarize safety practices. 5.7 Given a scenario, install and configure equipment in the appropriate location using best practices.

Chapter	N10-006 Exam Objective	N10-006 Exam Subobjective
7 (Cabling and Wiring)	<p>1.0 Network Architecture</p> <p>4.0 Troubleshooting</p> <p>5.0 Industry standards, practices, and network theory</p>	<p>1.5 Install and properly terminate various cable types and connectors using appropriate tools.</p> <p>4.8 Given a scenario, troubleshoot and resolve common WAN issues.</p> <p>5.2 Explain the basics of network theory and concepts.</p> <p>5.4 Given a scenario, deploy the appropriate wired connectivity standard.</p>
8 (Wireless)	<p>2.0 Network Operations</p> <p>3.0 Network Security</p> <p>4.0 Troubleshooting</p> <p>5.0 Industry standards, practices, and network theory</p>	<p>2.7 Install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.</p> <p>3.3 Given a scenario, implement network hardening techniques: Wireless security.</p> <p>4.3 Given a scenario, troubleshoot and resolve common wireless issues.</p> <p>5.3 Given a scenario, deploy the appropriate wireless standard.</p>
9 (Network Management)	<p>2.0 Network Operations</p> <p>5.0 Industry standards, practices, and network theory</p>	<p>2.1 Given a scenario, use appropriate monitoring tools.</p> <p>2.2 Given a scenario, analyze metrics and reports from monitoring and tracking performance tools.</p> <p>2.3 Given a scenario, use appropriate resources to support configuration management.</p> <p>2.5 Given a scenario, install and apply patches and updates.</p> <p>5.8 Explain the basics of change management procedures.</p>
10 (Network Optimization)	<p>1.0 Network Architecture</p> <p>2.0 Network Operations</p>	<p>1.10 Identify the basic elements of unified communication technologies.</p> <p>2.4 Explain the importance of implementing network segmentation.</p>

Chapter	N10-006 Exam Objective	N10-006 Exam Subobjective
11 (Network Security)	1.0 Network Architecture 3.0 Network Security 5.0 Industry standards, practices, and network theory	1.2 Compare and contrast the use of networking services and applications. 3.1 Compare and contrast risk related concepts. 3.2 Compare and contrast common network vulnerabilities and threats. 3.3 Given a scenario, implement network hardening techniques. 3.4 Compare and contrast physical security controls. 3.5 Given a scenario, install and configure a basic firewall. 3.6 Explain the purpose of various network access control models. 3.7 Summarize basic forensic concepts. 5.5 Given a scenario, implement the appropriate policies or procedures.
12 (Network Troubleshooting)	4.0 Troubleshooting	4.1 Given a scenario, implement the following network troubleshooting methodology. 4.2 Given a scenario, analyze and interpret the output of troubleshooting tools. 4.4 Given a scenario, troubleshoot and resolve common copper cable issues. 4.5 Given a scenario, troubleshoot and resolve common fiber cable issues. 4.6 Given a scenario, troubleshoot and resolve common network issues. 4.7 Given a scenario, troubleshoot and resolve common security issues.

Booking and Taking the Network+ Certification Exam

Unfortunately, testing is not free. You're charged \$246 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. Many clients 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 5 weeks of passing your exam, contact CompTIA at fulfillment@comptia.org, or call 1-630-268-1818 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 hot spots. 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!

CHAPTER 6

Installation and Configuration

This chapter covers the following official Network+ objectives:

- ▶ Explain the characteristics and benefits of various WAN technologies.
- ▶ Summarize safety practices.
- ▶ Given a scenario, install and configure equipment in the appropriate location using best practices.

This chapter covers CompTIA Network+ objectives 1.4, 5.6, and 5.7. For more information on the official Network+ exam topics, see the “About the Network+ Exam” section in the Introduction.

If you think of networking as something that can be represented on a plane, there would be two ends of the spectrum. At one end of the spectrum, there would be small networks of only a few nodes and devices connected together. At the other end of the spectrum is the *wide-area network* (WAN): An amalgamation of multiple *local-area networks* (LANs) creating an entity that is only as strong as its weakest link.

This chapter focuses mostly on the WAN end of the spectrum, but also covers such small network practices such as dialup connectivity. It also looks at best practices and safety practices associated with networking today.

WAN Technologies

- ▶ **Explain the characteristics and benefits of various WAN technologies.**
- ▶ **Given a scenario, install and configure equipment in the appropriate location using best practices.**

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 T-lines used for, and what is the maximum speed of T1 and T3?
2. What are the X.25 transmission speed restrictions?
3. What is the difference between circuit switching and packet switching?

Answers

1. T-carrier lines create point-to-point network connections for private networks. T1 lines offer transmission speeds of up to 1.544Mbps, whereas T3 lines offer transmission speeds of 44.736Mbps.
2. X.25 is restricted to transmission rates of 56Kbps or 64Kbps with digital implementations.
3. Circuit switching offers a dedicated transmission channel that is reserved until it is disconnected. Packet switching enables packets to be routed around network congestion.

Many of today's network environments are not restricted to a single location or LAN. Instead, many networks span great distances, becoming *wide-area networks* (WANs). When they do, hardware and software are needed to connect these networks. This section reviews the characteristics of various WAN technologies. Before discussing the specific WAN technologies, let's look at an important element of WAN technologies: switching methods.

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 differences between packet and circuit switching methods.

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 device. 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 6.1 provides an overview of the various switching technologies.

TABLE 6.1 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 device.
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. Uses a dedicated physical link between the sending and receiving devices.	Offers the capability of storing messages temporarily to reduce network congestion.

Integrated Services Digital Network

ISDN has long been an alternative to the slower modem WAN connections but at a higher cost. ISDN enables the transmission of voice and data over the same physical connection.

ISDN connections are considerably faster than regular modem connections. To access ISDN, a special phone line is required. This line usually is paid for through a monthly subscription. You can expect these monthly costs to be significantly higher than those for traditional dialup modem connections.

To establish an ISDN connection, you dial the number associated with the receiving computer, much as you do with a conventional phone call or modem dialup connection. A conversation between the sending and receiving devices is then established. The connection is dropped when one end disconnects or hangs up. The line pickup of ISDN is fast, enabling a connection to be established, or brought up, much more quickly than a conventional phone line.

ISDN has two defined interface standards: *Basic Rate Interface* (BRI) and *Primary Rate Interface* (PRI).

BRI

BRI ISDN uses three separate channels; two bearer (B) channels of 64Kbps each and a delta channel of 16Kbps. B channels can be divided into four D channels, which enable businesses to have eight simultaneous Internet connections. The B channels carry the voice or data, and the D channels are used for signaling.

ExamAlert

BRI ISDN channels can be used separately using 64Kbps transfer or combined to provide 128Kbps transfer rates.

PRI

PRI is a form of ISDN that generally is carried over a T1 line and can provide transmission rates of up to 1.544 Mbps. PRI is composed of 23 B channels, each providing 64Kbps for data/voice capacity, and one 64 Kbps D channel, which is used for signaling.

Comparing BRI and PRI ISDN

Table 6.2 compares BRI to PRI ISDN.

ExamAlert

ISDN is considered a leased line because access to ISDN is leased from a service provider.

TABLE 6.2 **BRI to PRI ISDN Comparison**

Characteristic	BRI	PRI
Speed	128Kbps	1.544Mbps
Channels	2B+D	23B+D
Transmission carrier	ISDN	T1

ExamAlert

Be ready to answer questions about the characteristics of both BRI and PRI; the exam may include the information provided in Table 6.2.

Leased Lines

T-carrier lines are high-speed dedicated digital lines that can be leased from telephone companies. This creates 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 1.544Mbps 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 6.312Mbps. They accomplish this by using 96 64Kbps B channels.
- ▶ **T3:** Offers transmission speeds of up to 44.736Mbps, using 672 64Kbps B channels. Digital signal 3 (DS3) is a more accurate name in North America, but T3 is what most refer to the link as.

ExamAlert

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

- ▶ **T4:** Offers impressive transmission speeds of up to 274.176Mbps by using 4,032 64Kbps 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 64Kbps 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 6.3 describes the T/E/J carriers.

TABLE 6.3 **Comparing T/E/J Carriers**

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

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 44.736Mbps.

T3 lines are dedicated circuits that provide high capacity and generally are used by large companies, *Internet service providers* (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.

Fiber, SONET, and OCx Levels

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 51.84Mbps. 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 51.84Mbps to 2.488Gbps 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 6.4 lists the OCx levels you should be familiar with.

ExamAlert

Before taking the exam, review the information provided in Table 6.4. Be sure that you are familiar with OC-3 and OC-12 specific transmission rates.

TABLE 6.4 **OCx Levels and Transmission Rates**

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

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 different locations and 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 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 7, “Cabling and Wiring,” discusses several other methods of multiplexing.

ExamAlert

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

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

ExamAlert

Make sure that you associate CWDM with television cabling.

Frame Relay

To understand Frame Relay, it is important to understand some ancient history and X.25. X.25 was one of the original packet-switching technologies, but today it has been replaced in most applications by Frame Relay. Various telephone companies, along with network providers, developed X.25 in the mid-1970s to transmit digital data over analog signals on copper lines. Because so many different entities had their hands in the development and implementation of X.25, it works well on many different kinds of networks with different types of traffic. X.25 is one of the oldest standards, and therein lie both its greatest advantage and its greatest disadvantage. On the upside, X.25 is a global standard that can be found all over the world. On the downside, its maximum transfer speed is 56Kbps—which is reasonable when compared to other technologies in the mid-1970s but slow and cumbersome today. However, in the 1980s a digital version of X.25 was released, increasing throughput to a maximum of 64Kbps. This, too, is slow by today's standards.

Because X.25 is a packet-switching technology, it uses different routes to get the best possible connection between the sending and receiving device at a given time. As conditions on the network change, such as increased network traffic, so do the routes that the packets take. Consequently, each packet is likely to take a different route to reach its destination during a single communication session. The device that makes it possible to use the X.25 service is called a *packet assembler/disassembler* (PAD), which is required at each end of the X.25 connection.

At its core, Frame Relay is a WAN protocol that operates at the physical and data link layers of the OSI model. Frame Relay enables data transmission for intermittent traffic between LANs and between endpoints in a WAN.

Frame Relay was designed to provide standards for transmitting data packets in high-speed bursts over digital networks, using a public data network service. Frame Relay is a packet-switching technology that uses variable-length

packets. Essentially, Frame Relay is a streamlined version of X.25. It uses smaller packet sizes and fewer error-checking mechanisms than X.25, and consequently it has less overhead than X.25.

A Frame Relay connection is built by using *permanent virtual circuits* (PVCs) that establish end-to-end communication. This means that Frame Relay is not dependent on the best-route method of X.25. Frame Relay can be implemented on several WAN technologies, including 56Kbps, T1, T3, and ISDN lines.

To better understand how it works, look at some of the components of Frame Relay technology. All devices in the Frame Relay WAN fall into two primary categories:

- ▶ **Data terminal equipment (DTE):** In the Frame Relay world, the term *DTE* refers to terminating equipment located within a company's network. Termination equipment includes such hardware as end-user systems, servers, routers, bridges, and switches.
- ▶ **Data circuit-terminating equipment (DCE):** DCE refers to the equipment owned by the carrier. This equipment provides the switching services for the network and therefore is responsible for actually transmitting the data through the WAN.

As previously mentioned, Frame Relay uses virtual circuits to create a communication channel. These virtual circuits establish a bidirectional communication link from DTE devices. Two types of virtual circuits are used with Frame Relay:

- ▶ **Permanent virtual circuit (PVC):** A permanent dedicated virtual link shared in a Frame Relay network, replacing a hard-wired dedicated end-to-end line
- ▶ **Switched virtual circuit (SVC):** Represents a temporary virtual circuit established and maintained only for the duration of a data transfer session

Figure 6.1 shows the components of a Frame Relay network.

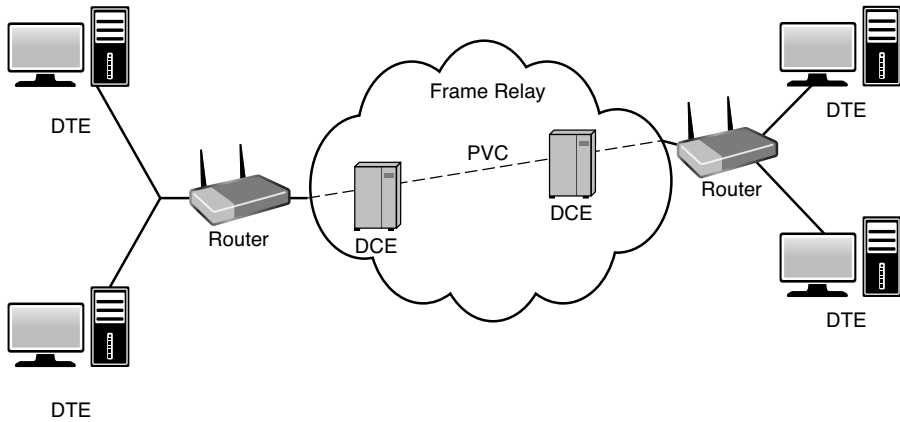


FIGURE 6.1 A Frame Relay network.

Asynchronous Transfer Mode

Introduced in the early 1990s, Asynchronous Transfer Mode (ATM) was heralded as a breakthrough technology for networking because it was an end-to-end solution, ranging in use from a desktop to a remote system. Although it was promoted as both a LAN and WAN solution, ATM did not live up to its hype due to associated implementation costs and a lack of standards. The introduction of Gigabit Ethernet, which offered great transmission speeds and compatibility with existing network infrastructure, further dampened the momentum of the ATM bandwagon. ATM has, however, found a niche with some ISPs and is also commonly used as a network backbone.

ATM is a packet-switching technology that provides transfer speeds ranging from 1.544Mbps to 622Mbps. It is well suited for a variety of data types, such as voice, data, and video. Using fixed-length packets, or *cells*, that are 53 bytes long, ATM can operate more efficiently than variable-length-packet packet-switching technologies such as Frame Relay. Having a fixed-length packet allows ATM to be concerned only with the header information of each packet. It does not need to read every bit of a packet to determine its beginning and end. ATM's fixed cell length also makes it easily adaptable to other technologies as they develop. Each cell has 48 bytes available for data, with 5 bytes reserved for the ATM header.

ATM is a circuit-based network technology because it uses a virtual circuit to connect two networked devices. Like Frame Relay, ATM is a circuit-based network technology that also uses PVCs and SVCs. PVCs and SVCs were discussed in the preceding section.

ATM is compatible with the most widely used and implemented networking media types available today, including single-mode and multimode fiber, coaxial cable, unshielded twisted-pair, and shielded twisted-pair. Although ATM can be used over various media, the limitations of some of the media types make them impractical choices for deployment in an ATM network. ATM can also operate over other media, including FDDI, T1, T3, SONET, OC-3, and Fibre Channel.

Summary of WAN Technologies

Table 6.5 provides an overview of the technologies discussed so far.

TABLE 6.5 **Comparing WAN Technologies**

WAN Technology	Speed	Supported Media	Switching Method Used	Key Characteristics
ISDN	BRI: 64Kbps to 128Kbps PRI: 64Kbps to 1.5Mbps	Copper/ fiber-optic	Can be used for circuit-switching or packet-switching connections	ISDN can be used to transmit all types of traffic, including voice, video, and data. BRI uses 2B+D channels; PRI uses 23B+D channels. B channels are 64Kbps. ISDN uses the public network and requires dial-in access.
T-carrier (T1, T3)	T1: 1.544Mbps T3: 44.736Mbps	Copper/ fiber-optic	Circuit switching	T-carrier is used to create point-to-point network connections for private networks.
ATM	1.544Mbps to 622Mbps	Copper/ fiber-optic	Cell switching	ATM uses fixed cells that are 53 bytes long.
X.25	56Kbps/64Kbps	Copper/ fiber-optic	Packet switching	X.25 is limited to 56Kbps. X.25 provides a packet-switching network over standard phone lines.

WAN Technology	Speed	Supported Media	Switching Method Used	Key Characteristics
Frame Relay	56Kbps to 1.544Mbps	Copper/ fiber-optic	PVCs and SVCs	Frame Relay is a packet-oriented protocol, and it uses variable-length packets.
SONET/OCx	51.8Mbps to 2.4Gbps	Fiber-optic	N/A	SONET defines synchronous data transfer over optical cable.

ExamAlert

For the Network+ exam, be sure that you can identify the characteristics of the various WAN technologies from Table 6.5.

Other WAN Technologies

Table 6.5 lists the most popular WAN technologies used today, but there are several others to be aware of as well:

- ▶ **PPP:** Point-to-Point Protocol 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. PPP does not provide data security, but it does provide authentication using the *Challenge Handshake Authentication Protocol* (CHAP). A PPP connection allows remote users to log on to the network and have access as though they were local users on the network. PPP by itself does not provide for any encryption services for the channel. As you might have guessed, the unsecure nature of PPP makes it largely unsuitable for WAN connections. To counter this issue, other protocols have been created that take advantage of PPP's flexibility and build on it. For example, PPP can be used with the *Encryption Control Protocol* (ECP). You should make sure that all of your PPP connections use secure channels, dedicated connections, or high-speed connections.
- ▶ **Multilink PPP:** Building off of PPP, Multilink PPP allows you to configure multiple links to act as one, thus increasing the speed of the connection. This technology has gained popularity with the cloud, but still suffers from problems inherent with PPP.

- ▶ **MPLS (Multiprotocol Label Switching):** Used in high-performance-based telecom 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.
- ▶ **GSM/CDMA:** The *Global System for Mobile Communications* (GSM) can work with *code division-multiple access* (CDMA) to provide various means of cell phone coverage. The methods that can be used include LTE/4G, HSPA+, 3G, or Edge.
- ▶ **Metro-Ethernet:** This is nothing more than an Ethernet-based MAN (metropolitan-area network; discussed in Chapter 1, “Introduction to Networking”). There are various levels of deployment that can be implemented, but all have limitations based on the underlying technology.

Cram Quiz

1. Your company currently uses a standard PSTN communication link to transfer files between LANs. Until now, the transfer speeds have been sufficient for the amount of data that needs to be transferred. Recently, a new application was purchased that requires a minimum transmission speed of 1.5Mbps. You have been given the task to find the most cost-effective solution to accommodate the new application. Which of the following technologies would you use?
 - A. T3
 - B. X.25
 - C. T1
 - D. BRI ISDN
2. Which of the following best describes the process to create a dedicated circuit between two communication endpoints and direct traffic between those two points?
 - A. Multiplexing
 - B. Directional addressing
 - C. Addressing
 - D. Circuit switching

3. Which of the following statements are true of ISDN? (Choose the two best answers.)
- A. BRI ISDN uses two B+1 D channels.
 - B. BRI ISDN uses 23 B+1 D channels.
 - C. PRI ISDN uses two B+1 D channels.
 - D. PRI ISDN uses 23 B+1 D channels.
4. You have been hired to establish a WAN connection between two offices: one in Vancouver and one in Seattle. The transmission speed can be no less than 2Mbps. Which of the following technologies could you choose?
- A. T1
 - B. PSTN
 - C. T3
 - D. ISDN
5. On an ISDN connection, what is the purpose of the D channel?
- A. It carries the data signals.
 - B. It carries signaling information.
 - C. It enables multiple channels to be combined to provide greater bandwidth.
 - D. It provides a temporary overflow capacity for the other channels.
6. Which of the following circuit-switching strategies does ATM use? (Choose the two best answers.)
- A. SVC
 - B. VCD
 - C. PVC
 - D. PCV
7. Due to recent cutbacks, your boss approaches you, demanding an alternative to the company's costly dedicated T1 line. Only small amounts of data require transfer over the line. Which of the following are you likely to recommend?
- A. ISDN
 - B. FDDI
 - C. The PSTN
 - D. X.25

8. Which of the following technologies requires a logical connection between the sending and receiving devices?
- A. Circuit switching
 - B. Virtual-circuit packet switching
 - C. Message switching
 - D. High-density circuit switching

Cram Quiz Answers

1. **C.** A T1 line has a transmission capability of 1.544Mbps and is considerably cheaper than a T3 line. X.25 and BRI ISDN cannot provide the required transmission speed.
 2. **D.** Circuit switching is the process of creating a dedicated circuit between two communications endpoints and directing traffic between those two points. None of the other answers are valid types of switching.
 3. **A, D.** BRI ISDN uses 2 B+1 D channels, which are two 64Kbps data channels, and PRI ISDN uses 23 B+1 D channels. The D channel is 16Kbps for BRI and 64Kbps for PRI.
 4. **C.** The only possible answer capable of transfer speeds above 2Mbps is a T3 line. None of the other technologies listed can provide the transmission speed required.
 5. **B.** The D channel on an ISDN link carries signaling information, whereas the B, or bearer, channels carry the data.
 6. **A, C.** ATM uses two types of circuit switching: PVC and SVC. VCD and PCV are not the names of switching methods.
 7. **C.** When little traffic will be sent over a line, the PSTN is the most cost-effective solution; although it is limited to 56Kbps. All the other WAN connectivity methods accommodate large amounts of data and are expensive compared to the PSTN.
 8. **B.** When virtual-circuit switching is used, a logical connection is established between the source and the destination device.
-

Internet Access Technologies

- ▶ Explain the characteristics and benefits of various WAN technologies.
- ▶ Given a scenario, install and configure equipment in the appropriate location using best practices.

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?

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.

Internet access has become an integral part of modern business. You have several ways to obtain Internet access. 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 modem 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 is most commonly associated with high-speed Internet access; because it is a relatively inexpensive Internet access, it is often found in homes and small businesses. 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 VHDSL (*very high-rate digital subscriber line*), 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):** 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 10Mbps, 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 opt for an option that enables phone line sharing at the expense of bandwidth. In addition, some of the DSL variants are simply older technologies. Although the name persists, they have been replaced with newer DSL implementations. When you work in a home/small office environment, you should expect to work with an ADSL system.

Table 6.6 summarizes the maximum speeds of the various DSL options. Maximum speeds are rarely obtained.

TABLE 6.6 **DSL Speeds**

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

*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.

DSL Troubleshooting Procedures

Troubleshooting DSL is similar to troubleshooting any other Internet connection. The following are a few things to check when users are experiencing problems with a DSL connection:

- ▶ **Physical connections:** The first place to look when troubleshooting a DSL problem is the network cable connections. From time to time, these cables can come loose or inadvertently be detached, and they are often overlooked as the cause of a problem. DSL modems typically have a minimum of three connections: one for the DSL line, one for the local network, and one for the power. Make sure that they are all plugged in appropriately.
- ▶ **The network interface card (NIC):** While you are checking the cable at the back of the system, take a quick look to see whether the network card LED is lit. If it is not, something could be wrong with the card. It might be necessary to swap out the network card and replace it with one that is known to be working.
- ▶ **Drivers:** Ensure that the network card is installed and has the correct drivers. Many times, simply using the most up-to-date driver can resolve connectivity issues.
- ▶ **Protocol configuration:** The device you are troubleshooting might not have a valid IP address. Confirm the IP address by using the appropriate tool for the operating system (and version of IP whether it be IPv4 or IPv6) being used—for example, `ipconfig` or `ifconfig`. If the system requires the automatic assignment of an IP address, confirm that the system is automatically set to obtain an IP address. It might be necessary to use the `ipconfig /release` and `ipconfig /renew` commands to get a new IP address.

- ▶ **DSL LEDs:** Each DSL box has an LED on it. The light sequences are often used to identify connectivity problems or problems with the box itself. Refer to the manufacturer's website for specific information about error codes and LEDs, but remember the basics. A link light should be on to indicate that the physical connection is complete, and a flashing LED indicates that the connection is active.

ExamAlert

When troubleshooting remote connectivity on a cable or DSL modem, use the LEDs that are always present on these devices to aid in your troubleshooting process.

Ultimately, if none of these steps cures or indicates the cause of the problem, you might have to call the DSL provider for assistance.

Cable Internet Access

Cable 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. 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 ability 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. In day-to-day application, the average nationwide average is approximately 32Mbps down and 9.6Mbps up. Figure 6.2 shows an example of speed test results.

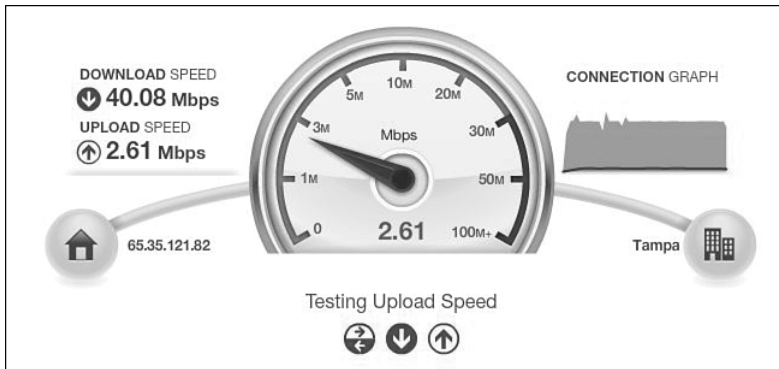


FIGURE 6.2 Sample speed test results.

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 (by DSL providers, at least) 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

Although the debate between cable and DSL goes on, for regular users, it doesn't make that much difference which one you choose. Although cable modem technology delivers *shared bandwidth* within the local neighborhood, its speeds are marginally higher but influenced by this shared bandwidth. DSL delivers *dedicated local bandwidth* but is sensitive to distance that impacts overall performance. With the monthly costs about the same, it is too close to call.

Cable Troubleshooting Procedures

In general, cable Internet access is a low-maintenance system with few problems. When problems do occur, you can try various troubleshooting measures:

- ▶ **Check the user's end:** Before looking at the cable modem, make sure that the system is configured correctly and that all cables are plugged

in. If a hub, switch, or router is used to share the cable Internet access among a group of computers, make sure that the device is on and correctly functioning.

- ▶ **Check the physical connections:** Like DSL modems, cable modems have three connections: one for the cable signal, one for the local network, and one for the power. Make sure that they are all appropriately plugged in.
- ▶ **Ensure that the protocol configuration on the system is valid:** If an IP address is assigned via *Dynamic Host Configuration Protocol* (DHCP), the absence of an address is a sure indicator that connectivity is at fault. Try obtaining a new IP address by using the appropriate command for the operating system platform you use. If the IP addresses are statically configured, make sure that they are correctly set. Trying to use any address other than that specified by the ISP might prevent a user from connecting to the network.
- ▶ **Check the indicator lights on the modem:** Most cable modems have indicator lights that show the modem's status. Under normal conditions, a single light labeled Ready or Online should be lit. Most cable providers give the user a modem manual that details the functions of the lights and what they indicate in certain states. Generally, any red light is bad. Flashing LEDs normally indicate traffic on the connection.
- ▶ **Cycle the power on the modem:** Cycling the power on the modem is a surefire way to reset it.
- ▶ **Call the technical support line:** If you are sure that the connectors are all in place and the configuration of the system is correct, the next step is to call the technical support line of the cable provider. If the provider experiences problems that affect many users, you might get a message while you're on hold, informing you of that. If not, you eventually get to speak to someone who can help you troubleshoot the problem. One of the good things about cable access is that the cable company can remotely monitor and reset the modem. The cable company should tell you whether the modem is correctly functioning.

Unless the modem is faulty, which is not that common, by this point the user should be back on the Internet, or at least you should fully understand why the user cannot connect. If the problem is with the cable provider's networking equipment, you and the user simply have to wait for the system to come back on.

Broadband Security Considerations

Whether you use DSL or cable Internet access, keep a few things in mind. Each of these technologies offers always-on service. This means that even when you are away from your computer, it still connects to the Internet. As you can imagine, this creates a security risk. The longer you are online, the better the chances that someone can remotely access your system.

The operating systems in use today all have some security holes that attackers wait to exploit. These attacks often focus on technologies such as email or open TCP/UDP ports. Combining OS security holes with an always-on Internet technology is certainly a dangerous mix.

Today, DSL and cable Internet connections must be protected by mechanisms such as firewalls. The firewall offers features such as packet filtering and *Network Address Translation* (NAT). The firewall can be a third-party software application installed on the system, or it can be a hardware device.

In addition to a firewall, it is equally important to ensure that the operating system you use is completely up to date in terms of service packs and security updates. Today's client systems typically offer automatic update features that alert you when a new security update is available.

If you diligently follow a few security measures, both DSL and cable Internet can provide safe Internet access.

Dialup

Although it's somewhat slow, one of the most popular means to connect to the Internet or a remote network may still be the good old telephone line and modem. Because the same line used for a household phone is used for dialup access, it is called the POTS (*plain old telephone system*) method of access. Although many parts of the world are served by broadband providers offering services such as those discussed so far in this chapter, some people still must (or choose to) connect with a modem.

Internet access through a phone system requires two things: a modem and a dialup access account through an ISP. Modems are devices that convert the digital signals generated by a computer system into analog signals that can travel across a phone line. A computer can have either an internal or external modem. External modems tend to be less problematic to install and troubleshoot because they don't require reconfiguration of the host system. Internal modems use one of the serial port assignments (that is, a COM port) and therefore must be configured not to conflict with other devices.

The second piece of the puzzle, the dialup ISP account, can easily be obtained by contacting one of the many local, regional, or national ISPs. Most ISPs offer a range of plans normally priced based on the amount of time the user is allowed to spend online. Almost without exception, ISPs offer 56Kbps access, the maximum possible under current standards. Most ISPs also provide email accounts, access to newsgroup servers, and often small amounts of web space.

It is a good idea to carefully research an ISP choice. Free services exist, but they generally restrict users to a certain number of online hours per month or use extensive banner advertising to pay for the services.

Another big consideration for dialup Internet access is how many lines the ISP has. ISPs never have the same number of lines as subscribers; instead, they work on a first-come, first-served basis for dialup clients. This means that sometimes users get busy signals when they try to connect. Before signing up for a dialup Internet access account, ask the company what its ratio of lines to subscribers is, and use that figure as part of your comparison criteria.

With a modem and an ISP account, you are ready to connect. But what happens if things don't go as you plan? Welcome to the interesting and sometimes challenging world of troubleshooting dialup connections.

Dialup Troubleshooting Procedures

Troubleshooting a dialup connection problem can be tricky and time-consuming, because you must consider many variables. Of the remote connectivity mechanisms discussed in this chapter, you are far more likely to have problems with a POTS connection than with any of the others. The following are some places to start your troubleshooting under various conditions.

Note

In some cases, users may not even use an ISP; instead, they may directly dial another system on the corporate network. In that case, all the troubleshooting steps in this section apply. The exception is that you must rely on the technical support capabilities of the person responsible for the remote system rather than the ISP if you have a problem.

If the user cannot dial out, try the following:

- ▶ **Check physical connections:** The most common problem with modem connections is that something has become unplugged; modems rarely fail after they initially work. For an external modem, you also need to

verify that the modem has power and that it is connected to the correct COM port.

- ▶ **Check that the line has a dial tone:** You can do this by plugging a normal phone into the socket to see whether you can dial out. Also, a modem generally has a speaker, and you can set up the modem to use the speaker so that you can hear what is going on.

If the user can dial out but cannot connect to the network, try the following:

- ▶ **Make sure that the user is dialing the correct number:** This suggestion sounds obvious, but sometimes numbers change or are incorrectly entered.
- ▶ **Call the ISP:** You can call the ISP to determine whether it is having problems.
- ▶ **Check the modem speaker:** Find out whether you get busy signals from the ISP by turning on the modem speaker.

If the user can dial out and can get a connection but is then disconnected, try the following:

- ▶ **Make sure that the modem connection is correctly configured:** The most common modem configuration is 8 data bits, 1 stop bit, and no parity (commonly called *eight-one-none*).
- ▶ **Check the username and password:** Make sure that the correct username and password combination is configured for the dialup connection.
- ▶ **Verify that the connection settings are correct:** Pay particular attention to things such as the IP address. Nearly all ISPs assign IP addresses through DHCP, and trying to connect with a statically configured IP address is not permitted.
- ▶ **Make sure that the user has not exceeded a preset connection time limit:** Some ISPs restrict the number of monthly access hours. If the user has such a plan, check to ensure that some time credit is left.
- ▶ **Try specifying a lower speed for the connection:** Modems are designed to negotiate a connection speed with which both devices are comfortable. Sometimes, during the negotiation process, the line can be dropped. Initially setting a lower speed might get you a connection. You can then increase the modem speed to accommodate a better connection.

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

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 56Kbps with a modem and 128Kbps 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.

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.

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 dialup 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 more costly 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.

Home Satellite Troubleshooting Procedures

Your ability to troubleshoot satellite Internet connections might be limited. Home satellite Internet is a line-of-sight wireless technology, and the installation configuration must be precise. Because of this requirement, many satellite companies insist that the satellite be set up and configured by trained staff members. If you install a satellite system in a way that does not match the manufacturer's recommendations, you might void any warranties.

Given this limitation, troubleshooting satellite connections often requires you to concentrate less on connectivity issues and more on physical troubleshooting techniques. Perhaps more than for any other Internet technology, calls to technical support occur early in the troubleshooting process. Satellite Internet has a few aspects that you should be aware of:

- ▶ **Rain fade:** Refers to signal loss due to moisture interference. The general rule is that the smaller the dish, the more susceptible it is to rain fade. Home and small businesses use small dishes.
- ▶ **Latency:** Refers to the time lapse between sending or requesting information and the time it takes to return. As you might expect, satellite communication experiences high latency due to the distance it has to travel.
- ▶ **Line of sight:** Despite the distance, satellite is basically a line-of-sight technology. This means that the path between the satellite dish and the satellite should be as unobstructed as possible.

Wireless Internet Access

Not too long ago, it would have been inconceivable to walk into your local coffee shop with your laptop under your arm and surf the Web while drinking a latte. Putting aside that beverages and laptops don't mix, wireless Internet access has become common.

Wireless Internet access is provided by an ISP providing public wireless Internet access known as *hotspots*. Hotspots offer Internet access for mobile network devices such as laptops, handheld computers, and cell phones in airports, coffee shops, conference rooms, and so on. A hotspot is created using one or many wireless access points near the hotspot location.

Client systems might need to install special application software for billing and security purposes; others require no configuration other than obtaining the network name (*service set identifier* [SSID]). Hotspots do not always require a fee for service because companies use them as a marketing tool to lure Internet users to their businesses.

Hotspots are not everywhere, but finding them is not difficult. Typically, airports, hotels, and coffee shops advertise that they offer Internet access for customers or clients. In addition, ISPs list their hotspot sites online so that they are easily found.

Establishing a connection to a wireless hotspot is a straightforward process. If not equipped with built-in wireless capability, laptops require an external wireless adapter card. With the physical requirements of the wireless card taken care of, connect as follows:

1. When you arrive at the hotspot site, power up your laptop or other mobile device. In some instances, you might need to reboot your system if it was on standby to clear out old configuration settings.

2. The card might automatically detect the network. If this is the case, configuration settings, such as the SSID, are automatically detected, and the wireless Internet is available. If Internet access is free, there is little else to do; if it is a paid-for service, you need to enter a method of payment. One thing to remember is to verify that you use encryption for secure data transfer.
3. If for some reason the wireless settings are not automatically detected, you need to open your wireless NIC's configuration utility and manually set the configurations. These settings can include setting the mode to infrastructure, inputting the correct SSID, and setting the level of encryption used.

In addition to using an ISP, some companies such as hotels and cafes provide wireless Internet access by connecting a wireless router to a DSL or cable Internet connection. The router becomes the wireless access point to which the users connect, and it enables clients to connect to the Internet through the broadband connection. The technology is based on the 802.11 standards, typically 802.11n/ac today, and client systems require only an internal or external wireless adapter.

Note

Want more wireless? Chapter 8, "Wireless," covers wireless technologies in detail.

Cellular

Just as POTS can serve as a means to connect to the Internet, so, too, can the cellular network. When the cellular network is used for this purpose, it is often marketed as a *mobile data service* and uses a wireless NIC to connect the mobile device or desktop to the network.

One technology that enables this is *Long-Term Evolution (LTE)*, which is often referred to as *4G* because it is the fourth generation in a long series of products offering similar services. Another technology is *Worldwide Interoperability for Microwave Access (WiMAX)*, which is based on 802.16. Table 6.7 shows peak upload and download speeds for both LTE and WiMAX. Actual implementations by carriers vary but are always below the theoretical possibilities.

TABLE 6.7 **LTE and WiMax Speeds**

	Peak Upload Speed	Peak Download Speed
LTE	50Mbps	100Mbps
WiMAX	56Mbps	1Gbps

Note

It is important to know that there have been several versions of both LTE and WiMAX. While discussing them in association with 4G here (technically, LTE Advanced and WiMAX Advanced), versions also existed for 3G (LTE and Mobile WiMAX). As of this writing, WiMAX Release 2 is expected to be commercially released in the near future.

Evolved High Speed Packet Access (HSPA+) is known as a *3G transitional* technology that supports legacy architecture. It can offer theoretical upload speeds of 22Mbps and downloads of 84Mbps.

ExamAlert

When you take the exam, associate HSPA+ with 3G cellular networking and LTE/WiMAX with 4G.

Edge, an acronym for *enhanced data rates for GSM evolution*, is a technology that is backward compliant and provides faster data rates (3G) on the GSM standard. Networks built for Edge are used to deliver streaming data at speeds up to 384Kbps (slow by most standards but faster than GSM).

ExamAlert

For the exam, know that Edge is faster than GSM.

Cram Quiz

1. Which of the following technologies require dialup access? (Choose the two best answers.)
 - A. FDDI
 - B. ISDN
 - C. Packet switching
 - D. The PSTN
2. Which of the following is an advantage of ISDN over the PSTN?
 - A. ISDN is more reliable.
 - B. ISDN is cheaper.
 - C. ISDN is faster.
 - D. ISDN uses 53Kbps fixed-length packets.
3. Which of the following technologies is known as a 3G transitional technology that supports legacy architecture?
 - A. HSPA+
 - B. LTE
 - C. WiMAX
 - D. PON
4. What is the theoretical download speed possible with WiMAX?
 - A. 84Mbps
 - B. 100Mbps
 - C. 1Gbps
 - D. 10Gbps
5. 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

6. What is the speed usually offered with dialup service?
- A. 1Gbps
 - B. 256Kbps
 - C. 144Kbps
 - D. 56Kbps

Cram Quiz Answers

1. **B and D.** Both the PSTN and ISDN require dialup connections to establish communication sessions.
 2. **C.** One clear advantage that ISDN has over the PSTN is its speed. ISDN can combine 64Kbps 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. **A.** HSPA+ (*Evolved High Speed Packet Access*) is known as a 3G transitional technology that supports legacy architecture.
 4. **C.** The theoretical download speed possible with WiMAX is 1Gbps. The speed possible with HSPA+ is 84Mbps, whereas that possible with LTE is 100Mbps.
 5. **D.** Latency refers to the time lapse between sending or requesting information and the time it takes to return.
 6. **D.** Almost without exception, ISPs offer 56Kbps access, the maximum possible under current standards.
-

Safety Practices

- **Summarize safety practices.**

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. Cleaning products, and their handling, would be addressed in what type of documentation?
2. True or False: The two types of failure response are to fail open or fail closed.
3. What type of fire extinguisher should be used on electrical fires?

Answers

1. Cleaning products, and their handling, are addressed in MSDS (*material safety data sheet*) documentation.
2. True. The two types of failure response are to fail open or fail closed.
3. A Type C extinguisher should be used on electrical fires.

New to this version of the Network+ exam is objective 5.6: Summarize safety practices. This topic has always existed within the CompTIA A+ objectives, and will be familiar to those who already hold that certification, but it has not previously been tested on the Network+ exam.

Note

The fact that this topic has carried over from A+ to Network+ illustrates its importance. Given that, even if you have recently obtained the A+ certification, you should still look over the topics here and be certain that you can answer questions about them.

Focusing on Safety

When working with anything, it is important to know the potential safety hazards, how to address them, and how to avoid them. It is imperative that you understand such issues as *material safety data sheets* (MSDSs) and know how to reference them when needed. Any type of chemical, equipment,

or supply that has the potential to harm the environment or people has to have an MSDS associated with it. These are traditionally created by the manufacturer, and you can obtain them from the manufacturer or from the U.S. Environmental Protection Agency at www.epa.gov. These sheets are not intended for consumer use, but are aimed at emergency workers and employees who are exposed to the risks of the particular product. Among the information they include are such things as boiling point, melting point, flash point, and potential health risks. They also cover storage and disposal recommendations, and the procedures to follow in the case of a spill or leak.

ExamAlert

For the exam, associate MSDS with the EPA.

HVAC (*heating, ventilating, and air conditioning*) is one of the biggest expenses for a building. Many companies market scheduling and monitoring software that can help reduce HVAC costs and increase efficiency as well as increase safety. *Heat recovery ventilation* (HRV) uses equipment known as heat exchangers to move fresh air into buildings that are adequately insulated without causing all the conditioned air to be lost. When HRVs also condition for humidity, they fall into the category of *energy recovery ventilators* (ERVs).

Electrical Safety and ESD

One of the most dangerous components when working with computers is electricity. *Electrostatic discharge* (ESD) occurs when two objects of dissimilar electrical charge come in contact with each other; the charge can damage electronic components and humans as well. Proper ESD precautions include wearing an antistatic wrist strap and properly grounding yourself.

Grounding equipment also crucial to safety. A dedicated ground (traditionally signified by an orange electrical outlet) prevents a discharge from any other device from damaging this one.

ExamAlert

A dedicated ground, or isolated ground, has only the one outlet connected to it so that a spike sent to ground from one device does not adversely affect another device.

Installation Safety

Common sense is the best tool you have when it comes to installation safety. If lifting heavy boxes or equipment, be sure to bend at the hips when lifting and get enough people to assist to keep from anyone getting hurt. Place equipment in appropriate spaces and follow all installation rules/guidelines (particularly with items such as racks). Understand the purpose for the tools you use and use them for that purpose; don't use a screwdriver as a chisel, for instance. Although it might take longer to do something correctly, it increases safety when you do.

Fire Suppression

Fire suppression is a key consideration in computer-center design. Fire suppression is the act of actually extinguishing a fire versus preventing one. Two primary types of fire-suppression systems are in use: fire extinguishers and fixed systems.

Fire Extinguishers

Fire extinguishers are portable systems. The selection and use of fire extinguishers is critical. Four primary types of fire extinguishers are available, classified by the types of fires they put out: A, B, C, and D. Table 6.8 describes the four types of fires and the capabilities of various extinguishers.

TABLE 6.8 **Fire Extinguisher Ratings**

Type	Use	Retardant Composition
A	Wood and paper	Largely water or chemical
B	Flammable liquids	Fire-retardant chemicals
C	Electrical	Nonconductive chemicals
D	Flammable metals	Varies, type specific

Note

A Type K extinguisher that is marketed for use with cooking oil fires can also be found in stores. In actuality, this is a subset of class B extinguishers.

Several multipurpose types of extinguishers combine extinguisher capabilities in a single bottle. The more common multipurpose extinguishers are A-B, B-C, and ABC.

ExamAlert

For the exam, know that Type C fire extinguishers are used for electrical fires.

The recommended procedure for using a fire extinguisher is called the *PASS method*: pull, aim, squeeze, and sweep. Fire extinguishers usually operate for only a few seconds. So, if you use one, make sure that you don't fixate on a single spot. Most fire extinguishers have a limited effective range of from 3 to 8 feet.

Note

A major concern with electrical fires is that they can reoccur quickly if the voltage isn't removed. Make sure to remove voltage from systems when a fire occurs.

Most fire extinguishers require an annual inspection. This is a favorite area of citation by fire inspectors. You can contract with services to do this on a regular basis: They will inspect or replace your fire extinguishers according to a scheduled agreement.

Fixed Systems

Fixed systems are usually part of the building systems. The most common fixed systems combine fire detectors with fire-suppression systems, where the detectors usually trigger either because of a rapid temperature change or because of excessive smoke. The fire-suppression system uses either water sprinklers or fire-suppressing gas. Water systems work with overhead nozzles, and these systems are the most common method in modern buildings. Water systems are reliable, relatively inexpensive, and require little maintenance.

The one drawback to water-based systems is that they cause extreme damage to energized electrical equipment such as computers. These systems can be tied into relays that terminate power to computer systems before they release water into the building.

Gas-based systems were originally designed to use carbon dioxide and later Halon gas. Halon gas is not used anymore because it damages the ozone layer; environmentally acceptable substitutes are now available, with FM200 being one of the most common. The principle of a gas system is that it displaces the oxygen in the room, thereby removing this necessary component of a fire.

Note

Evacuate the room immediately in the event of a fire. Gas-based systems work by removing oxygen from the fire, and this can suffocate anyone in the room as well.

Special ventilation systems are usually installed in gas systems to limit air circulation when the gas is released. Gas systems are also expensive, and they're usually implemented only in computer rooms or other areas where water would cause damage to technology or other intellectual property.

ExamAlert

The major drawback to gas-based systems is that they require sealed environments to operate.

In Case of an Emergency

Regardless of the planning and precautions in place, sometimes accidents happen. When they do, it is important to have emergency procedures in place for dealing with them. You should have a layout of the building handy that can be referenced in case the building must be evacuated and have a fire escape plan that all employees are aware of. Make sure that they know the safety/emergency exits and you have a working emergency alert system in place.

Make sure that when your systems fail, they do so appropriately. The two methods of responding to failure are to fail open or fail closed. *Failing open* means that things are essentially left as they are when the problem occurs, and *failing closed* means that systems are shut down when the problem is encountered. The correct response depends on the situation and the types of systems you are working with.

Cram Quiz

1. Which government agency can you turn to in order to find MSDS sheets?
 - A. FTC
 - B. FCC
 - C. EPA
 - D. FDA

2. Which of the following type of fire extinguisher is marketed for use with cooking oil fires?
 - A. K
 - B. C
 - C. D
 - D. A

3. Which of the following is a major drawback to gas-based extinguisher systems?
 - A. They must be recharged on a weekly basis.
 - B. They are not available within the United States.
 - C. They rely on operators to activate.
 - D. They require sealed environments in which to operate.

Cram Quiz Answers

1. **C.** MSDS sheets are created by the manufacturer and can be obtained from them or the EPA (*Environmental Protection Agency*).
 2. **A.** Type K fire extinguishers are marketed for use with cooking oil fires. These are a subset of Type B extinguishers.
 3. **D.** The major drawback to gas-based systems is that they require sealed environments to operate.
-

Installing and Configuring Equipment

- **Given a scenario, install and configure equipment in the appropriate location using best practices.**

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 main wiring closet known as: MDF or IDF?
2. A _____ is a freestanding or wall-mounted unit with a number of RJ-45 port connections on the front.
3. What is the name for a server rack system in which servers are attached to the rack at only two locations (one on each side)?

Answers

1. The main wiring closet is the MDF: *main distribution frame*.
2. A *patch panel* is a freestanding or wall-mounted unit with a number of RJ-45 port connections on the front.
3. In a two-post rack, servers are attached to the rack system at two locations (one on each side).

Topics in this chapter have focused on the benefits of various WAN technologies and safety practices. This section expands that to look at the actual installation and configuration of equipment using best practices.

Note

The term *best practices* is a bit of a copout. The important thing to know is what CompTIA expects you to select on their exam whether that is what an administrator would implement in the field.

Distribution Frames

A distribution frame is a concept from telephony of various stations. You have a *main distribution frame* (MDF) and various *intermediate distribution frames* (IDFs). The MDF is a termination point where cables originate from.

Everything lesser than that (switching stations) are IDFs. Where these come into play with most networks is with wiring closets.

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.

ExamAlert

Be prepared to identify the difference between an IDF and an MDF.

Cable Management

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.

Cable trays can be used to carry cabling throughout the building. Trays run overhead and usually either resemble racks/wire shelving (having open bottoms) or have solid bottoms to blend in easier with the aesthetics of the environment. Trays are often used when reconfiguration may be a regular thing or it is too costly to run wiring through pipe, walls, and other building fixtures.

ExamAlert

For the exam, know that cable trays make it easy to reconfigure wiring when needed.

Power Management

As great as the configuration may be, a network just cannot run without power. When you design the network, make sure to include power converters (which step the voltage down), power inverters (which step the power up), redundancy (should a circuit become unstable), and plenty of UPS (*uninterruptible power supply*) devices.

Device Placement and Labeling

Device placement is important for safety reasons, electrical access, and for air flow. Make certain you install each device safely and in accordance with manufacturer's recommendations.

Make certain, as well, that you carefully label and document everything that you do. Imagine what you would need to have if you had to troubleshoot the system and had no prior knowledge of it and then create those necessary elements for someone who may have to step into your shoes. Be sure to label systems, ports, circuits, and patch panels. Be sure to follow standard naming conventions that you use consistently throughout.

ExamAlert

For the exam, know that the labeling and naming structure you use should make intuitive sense, in case a new administrator needs to come in and troubleshoot and resolve issues.

Rack Systems

Most server rooms are now nothing more than rows of racks. When dealing with them, know that security is important, both physical (you cannot have them tumbling over) and accesswise, and you need to carefully monitor them (for access and for environmental conditions).

The four main components of rack systems are as follows:

- ▶ **Server rail racks:** These are the rails that hold the servers within the rack.

- ▶ **Two-post racks:** As the name implies, the servers are attached to the rack system at two locations (one on each side).
- ▶ **Four-post racks:** The servers are attached to the rack system at four locations (two on each side).
- ▶ **Free-standing racks:** These can stand on their own and support the servers within, as opposed to being mounted to a wall.

ExamAlert

The great thing about the racks is that the name of each does a noble job of explaining what you are dealing with.

Cram Quiz

1. Which of the following is a server rack system in which servers are attached to the rack at four locations (two on each side)?
 - A. Anchored rack
 - B. Four-post rack
 - C. Generous rack
 - D. Affixed rack

2. Which of the following are often used when wiring reconfiguration in a building may be a regular thing or it is too costly to run wiring through pipe, walls, and other fixtures?
 - A. KVMs
 - B. Cable ledges
 - C. Cable racks
 - D. Cable trays

3. Which of the following are used to step power up from one voltage to another?
 - A. Switches
 - B. Translators
 - C. Converters
 - D. Inverters

Cram Quiz Answers

1. **B.** A four-post is a server rack system in which servers are attached to the rack at four locations (two on each side).
 2. **D.** Cable trays run overhead and can be used to carry cabling throughout the building. They usually have open bottoms like wire shelving or have solid bottoms to blend in easier with the aesthetics of the environment.
 3. **D.** Power inverters are used to step power up from one voltage (low) to another (high). The opposite of this is a power converter, which goes from a higher voltage to a lower one.
-

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 7, “Cabling and Wiring,” focuses on the media and connectors used in today’s networks and how they fit into wiring closets.

This page intentionally left blank

Index

Symbols

4G, 204
10 Gigabit standard, 266-268
10BASE2 standard, 263
10BASE-T standard, 263-264
10GBASE-ER/EW, 267
10GBASE-SR/SW, 266
10GBASE-T, 268
66 blocks (punchdown), 248
100BASE-T standard, 265
110 blocks (punchdown), 248
802.11 standards
 WLANs, 305-306
 802.11ac, 307
 802.11n, 307
 DSSS, 308
 FHSS, 308
 OFDM, 308
1000BASE-T standard, 266

A

AAA (authentication, accounting, and authorization), 156
access control, 391
 ACEs (access control entries), 392
 DAC (discretionary access control), 392
 MAC (mandatory access control), 391
 RBAC (role-based access control), 393
 RBAC (rule-based access control), 392
access methods
 IEEE 802.3x, 260-261
 VPNs, 386
access points, rogue, 423
accounting, 433
ACE (access control entry), 392
ACL (access control list), 129, 392
 misconfigured, 550

ad hoc wireless topology

ad hoc wireless topology, 23

addresses. *See also* MAC addresses

- DNAT (Destination Network Address Translation), 115
- NAT (Network Address Translation), 113-114
- PAT (Port Address Translation), 114
- SNAT (Static Network Address Translation), 115

addressing. *See* IP addresses

ADSL (asymmetric DSL), 192

AES (Advanced Encryption Standard), 313

AH (Authentication Header) protocol, 389

air conditioning, 541

analog modems, 137

antennas, wireless networks, 284

- configuration, 300
- coverage, 286
- isotropic, 285
- ratings, 285-286
- signal quality, 287-288

AP (access point), 22, 136-137, 279-281

- BSA (basic service area), 283
- BSS (basic service set), 282
- BSSID (basic service set identifier), 282
- ESS (extended service set), 282
- ESSID (extended service set identifier), 282
- rogue, 316
- SSID (service set identifier), 282
- troubleshooting, 283-284

APIDS (application protocol-based intrusion detection system), 140, 460

APIPA (Automatic Private IP Addressing), 110

application documentation, 328

Application layer (Layer 7) of OSI model, 46

application level firewalls, 456

ARP (Address Resolution Protocol), 45, 82-83

- poisoning, 423
- proxy ARP, 484

ARP issues, 552

ARP utility, 518-520

ASCII (American Standard Code for Information Interchange), 46

ASIC (application-specific integrated circuit), 375

ASN (autonomous system number), 126

association, wireless networks, 297

asymmetric DSL, 192

ATM (Asynchronous Transfer Mode), 45, 185-186

attenuation

- cabling, 224
- troubleshooting, 491

AUP (acceptable use policy), 412

authentication, 431

- cryptography, 436
- Kerberos, 435-438
- multifactor, 448
- passwords, 433-435
- PKI, 438-441
 - digital signatures, 441
 - private keys, 439
 - public keys, 439
 - secure email, 441
 - uses, 440
- port authentication, 133
- PPTP, 388
- remote authentication protocols, 442-444
- SNMPv3, 69
- two-factor, 448
- wireless networks, 298

authorization, 431

B

backdoor attacks, 422

backups, 338

- best practices, 406
- differential backups, 404
- full backups, 403-404
- incremental, 402, 404
- tape rotations, 405
- UPS (uninterruptible power supplies), 407-408

bandwidth, 127

- monitoring and, 345

- banner grabbing, 552**
- baseband, 221**
 - versus broadband
 - DOCSIS, 221-222
 - IEEE, 221-222
- baselines in documentation, 335-336**
- battery backup, 407**
- baud rates, 269**
- BCP (business continuity planning), 411**
- beacons, wireless transmission, 293-294**
- behavior-based intrusion detection system, 139**
- BGP (Border Gateway Protocol), 47, 126**
- biometrics, 448**
- bit rates, 269**
- blackouts, 407**
- blocking, 276**
- bluejacking, 424**
- bluesnarfing, 424**
- BNC connectors, 232**
- bonding, IEEE 802.3x, 262**
- BOOTP, 110**
- BPDU (bridge protocol data unit), 131**
- BPL (broadband over power lines), 221**
- BRI (Basic Rate Interface), 178**
 - PRI comparison, 178
- bridges, 297**
- broadband, 198, 221**
 - BPL (broadband over power lines), 221
 - versus baseband
 - DOCSIS, 221-222
 - IEEE, 221-222
- broadcast addresses, IPv4, 102**
- broadcast storms, troubleshooting, 484**
- brownouts, 408**
- BSA (basic service area), 283**
- BSID (basic service set identifier), 282**
- BSS (basic service set), 282**

buffering

- buffer overflow, 421
- OSI Transport layer, 45

bus compatibility, 496**bus topology, 17-18****butt set, 545****BWA (broadband wireless access), 295****BYOD (bring your own device) policies, 337, 412****C**

CA (certificate authority), 438**cable certifier, 254, 543****cable Internet access, 195-196**

- troubleshooting, 196-197

cable modems, 33, 195**cable tester, 543****cabling**

- 568A wiring standards, 240
- 568B wiring standards, 240
- attenuation, 224
- baseband, 221
- broadband, 221
- broadband versus baseband, 222
- cable trays, 215
- coaxial, 225, 228-229
- copper wire, 225
- cross connects, 244
- crossover, 145, 240, 242
- CSU/DSU (channel service unit/data service unit), 251
- data transmission rates, 224-225
- demarcation point, 249-250
- dialog modes, 223
- distribution, 244
- fiber-optic, 225, 230-231
- horizontal, 244-245
- hubs, 145
- installation verification, 251-252
- loopback, 243
- media interference, 223
- NOC (network operations center), 244
- patch panels, 215, 247-248
- plenium, 232

cabling

- punchdown blocks
 - 66 blocks, 248
 - 110 blocks, 248
- PVC cables, 232
- RG-6 cables, 235
- RG-59 cables, 235
- rollover, 243
- straight-through, 240, 242
- switches, 145
- termination verification, 251-252
- tools, 252-254
- troubleshooting, 488-490
 - attenuation, 491
 - bad wiring, 493
 - connectors, 492
 - crosstalk, 490-491
 - dB loss, 493
 - echo, 492
 - EMI/RFI, 491
 - placement, 494
 - shorts, 493
 - split pairs, 493
 - TX/RX reversed, 494
- twisted-pair, 226-228
- UTP (unshielded twisted-pair), 223
- vertical, 246
- wiring closets, 248

caching, 378-379

CBF (critical business functions), 411

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), 313

CDMA (code division-multiple access), 188

cellular Internet access, 204-205

centralized computing, 15

certificates, 438

chain of custody, security incident response, 468

change management procedures, 339

channel bonding, 262

channels, wireless networks, 289-290

CHAP (Challenge Handshake Authentication Protocol), 187, 443

chip creep, 540

CIDR (classless interdomain routing), 100

circuit-level firewalls, 456

circuit switching, 176

cladding, cable, 230

classes, IP addresses, 95

client/server networking model, 14

client-side filters, 138

clients

- connectivity, troubleshooting, 496-501
- VPNs, 385

cloud computing, 161

- community clouds, 165
- hybrid clouds, 165
- IaaS and, 163
- PaaS and, 163
- private clouds, 164
- public clouds, 164
- SaaS and, 163
- SANs (storage-area networks), 170-171
- virtualization and, 167
 - firewalls, 169
 - NICs, 169
 - routers, 168
 - software defined networking, 169
 - switches, 168

CNAME (Canonical Name), 61

coaxial, 225

coaxial cable, 224-225, 228-229

cold sites, 409-410

cold spares, 409

cold swapping, 409

collisions, 270

command-line utilities, troubleshooting and, 507

- ARP, 518-520
- dig utility, 531-532
- host utility, 533
- ifconfig utility, 529-530
- ipconfig utility, 527-528
- nbtstat utility, 526
- netstat command, 520-524
- nslookup utility, 530-531
- pathping utility, 518
- ping utility, 513-517
- route utility, 533-534
- trace route utility, 509-512

- communications establishment, wireless, 296, 298**
- community clouds, 165**
- compatibility, network planning, 33**
- compliance, segmentation and, 380**
- configuration**
 - documentation, 340
 - interfaces, switches, 156-157
 - monitoring, 347
 - WLANs, 299-303
- connection-oriented protocols versus connectionless, 72**
- connectivity**
 - loss, 273
 - troubleshooting, 496
 - media connection, 496-497
 - physical connection, 496
 - TCP/IP configuration, 497-501
- connectors**
 - BNC, 232
 - F-Type, 235
 - fiber, 235
 - RJ-11, 233
 - RJ-45, 234
 - RJ-48C, 234
 - RS-232, 237
 - troubleshooting, 492
 - USB (universal serial bus), 238
- content filters, 138**
- converters, 238-239**
- copper wire cabling, 225**
- CoS (class of service), 369**
- couplers, 238-239**
- critical assets, 411**
- critical nodes, 411**
- CRL (certificate revocation list), 438**
- cross connects, 244**
- crossover cabling, 145, 240, 242**
- crosstalk, troubleshooting, 490-491**
- cryptography, 436-437**
- CSMA/CD (carrier sense multiple access with collision avoidance), 262, 270**
 - IEEE 802.3x, 260-262
- CSU/DSU (channel service unit/data service unit), 251**

- customer premise equipment, 275-276**
- cut-through switching, 144**
- CWDM (coarse wavelength-division multiplexing), 183**

D

- DAC (discretionary access control), 392**
- data flow, OSI Transport layer, 45**
- Data Link layer (Layer 2) of OSI model, 44**
- data rate, wireless transmission, 292**
- data transmission rates, 224-225**
- datagram packet switching, 176**
- dB loss, troubleshooting, 493**
- DCE (data circuit-terminating equipment), 184**
- DCS (distributed control system), 12**
- DDoS (distributed Dos) attacks, 419, 550**
- decapsulation, 269**
- default gateways, 100**
- default VLAN, 156**
- demarc, 36**
- demarcation point, 36, 249-250**
- DES (Data Encryption Standard), 443**
- Destination Host Unreachable error message, 514**
- devices**
 - density, 281
 - network
 - access points, 136-137
 - analog modems, 137
 - chart, 147
 - content filters, 138
 - firewalls, 138-139
 - hubs, 140-141, 145
 - IDS (intrusion detection systems), 139
 - IPS (intrusion prevention systems), 140
 - load balancer, 141
 - packet shapers, 142
 - routers, 142
 - switches, 143-146
 - VPN concentrator, 147

- network planning, 32
- placement, 216
- UC (Unified Communication), 372

DHCP (Dynamic Host Configuration Protocol), 47, 51

- access points, 137
- advantages, 52
- dynamic IP addresses, 108
- process, 53
- relays, 54
- reservations, 52
- suffixes, 54

DHCPDISCOVER packet, 53

DHCPOFFER packet, 54

DHCPREQUEST packet, 54

dialog modes, 223

dialup Internet access, 198-200

differential backups, 404

dig utility, 531-532

digital signatures, 441

distance-vector routing, 122, 124

distributed computing, 15

distribution frames

- IDF (intermediate distribution frame), 214
- MDF (main distribution frame), 214

DMZ (demilitarized zone), 458

DNAT (Destination Network Address Translation), 115

DNS (Domain Name Service), 47, 56, 108, 274

- CNAME (Canonical Name), 61
- entries, 60
- FQDN (fully qualified domain name), 56
- HOSTS file, 56
- implementation, 62-63
- IPv4 address, 61
- IPv6 address, 61
- MX (Mail Exchange), 61
- NS (Name Server), 61
- PTR (Pointer), 61
- resolution, 57
- SOA (Start of Authority), 61
- suffixes, 54
- TCP/IP-based networks, 56
- troubleshooting, 488

DNS namespace, 58-60

DOCSIS (Data Over Cable Service Interface Specification), 222

documentation

- applications, 328
- baselines, 335-336
- configuration, 340
- equipment, 328
- network services, 328
- policies, 336, 338
- procedures, 329, 338-340
- regulations, 340-341
- security incident response, 467
- server configuration, 328
- topologies, 332-334
- topology, 328
- troubleshooting, 478-479
- wiring layout, 328-331

DoS (denial-of-service) attacks, 419-420, 550

- buffer overflow, 421
- DRDoS, 421
- Fraggles, 420
- ICMP flood, 421
- ping of death, 420
- Smurfing, 420
- SYN flood, 420

downgrading versus upgrading, 364

DRDoS (distributed reflective DoS), 421

driver updates, 363

DSCP (differentiated services code), 369

DSL (digital subscriber line), 33, 192

- ADSL (asymmetric DSL), 192
- HDSL (high bit rate DSL), 192-193
- IDSL (ISDN DSL), 193
- RADSL (rate-adaptive DSL), 193
- SDSL (symmetric DSL), 192
- speeds, 193
- troubleshooting, 194-195
- VHDSL (very high bit rate DSL), 192-193

DSSS (direct-sequence spread-spectrum), 295, 308

DTE (data terminal equipment), 184

DUAL (Diffusing Update Algorithm), 123

DWDM (dense wavelength-division multiplexing), 182

dynamic addresses, 108-109

dynamic routing, 122

- distance-vector routing, 122, 124
- hybrid routing protocols, 126
- link-state routing, 125

E

EAP (Extensible Authentication Protocol), 313, 443

eavesdropping, 422

EBCDIC (Extended Binary Coded Decimal Interchange Code), 46

echo, troubleshooting, 492

EDFAs (erbium doped fiber amplifiers), 182

Edge (enhanced data rates for GSM evolution), 205

eDiscovery, 467

EIGRP (Enhanced Interior Gateway Routing Protocol), 123

electrical safety, 209

email usage policy, 337

emergency exits, 212

EMI (electromagnetic interference), 223, 491

encapsulation, 269, 396

encryption, 46

- AES (Advanced Encryption Standard), 313
- SNMPv3, 69
- VPNs, 385

environment, network planning, 32

environmental monitoring, 347, 540

equipment

- cable management, 215
- customer premise equipment, 275-276
- device placement, 216
- distribution frames
 - IDF (intermediate distribution frame), 214
 - MDF (main distribution frame), 214
- documentation, 328

- network planning, 32
- power management, 216
- rack systems, 216

error checking, 45

error messages

- Destination Host Unreachable, 514
- Request Timed Out, 514
- TTL (Time To Live), 516
- Unknown Host, 515

ESD (electrostatic discharge), 209

ESP (Encapsulating Security Payload) protocol, 389

ESS (extended service set), 282

ESSID (extended service set identifier), 282

Ethernet

- 10BASE2 standard, 263
- 10BASE-T standard, 263-264
- 10 Gigabit standard, 266-268
- 100BASE-T standard, 265
- 1000BASE-T standard, 266
- over HDMI, 222
- over power lines, 221
- PPoE, 395

event logs, 355-358

evil twin attacks, 423

Expired TTL message, 516

F

FAP (fair access policy), 276

FCoE (Fiber Channel over Ethernet), 171

FCP (Fiber Channel Protocol), 171

FDM (frequency-division multiplexing), 221

feature updates, 364

FEXT (far end crosstalk) interference, 490-491

FHSS (frequency-hopping spread-spectrum), 294-295, 308

fiber connectors, 235

fiber issues, troubleshooting, 486-487

fiber-optic cabling, 225, 230-231

Fibre Channel, 171

filters

- client-side, 138
- content filters, 138
- server-side, 138

FIOS, 33**fire suppression**

- extinguishers, 210-211
- fixed systems, 211

firewalls, 138-139, 451-453

- application level, 456
- circuit-level, 456
- comparing, 457
- misconfigured, 549
- packet-filtering, 454, 456
- stateful, 453
- stateless, 453
- VF (virtual firewall), 169

firmware

- unpatched, 550
- updates, 363

four-post racks, 217**fox and hound, 541****FQDN (fully qualified domain name), 56****Fraggles, 420****fragment free switching, 145****Frame Relay, 183**

- DCE (data circuit-terminating equipment), 184
- DTE (data terminal equipment), 184
- PAD (packet assembler/disassembler), 183
- PVC (permanent virtual circuit), 184
- SVC (switched virtual circuit), 184

free-standing racks, 217**FTP (File Transfer Protocol), 47, 75-76****F-Type connectors, 235****full backups, 403-404****full-duplex mode, 223****G****gateways, troubleshooting, 487****GBIC (gigabit interface converter) module, 486****GFS rotation (grandfather, father, son), 405****GIF files, 46****global unicast addresses, IPv6, 105****goodput, wireless transmission, 292****graphics files, 46****GRE (generic routing encapsulation), 396****H****half-duplex mode, 223****hardware**

- firewalls, 138
- OSI Layer 1, 43
- troubleshooting, 494

HDSL (high bit rate DSL), 192-193**HIDS (host-based intrusion detection system), 140, 460****high-density devices, 141****HomePlug Powerline Alliance, 222****honeynets, 376-377**

- security and, 461

honeypots, 376-377

- security and, 461

hop counts, 126**horizontal cabling, 244-245****host utility, 533****hot sites, 409-410****hot spares, 408****hot swapping, 408****hotspots, 203****HSPA+ (Evolved High Speed Packet Access), 205****HSRP (Hot Standby Router Protocol), 133****HTML (Hypertext Markup Language), 78****HTTP (Hypertext Transfer Protocol), 47, 78****HTTPS (Hypertext Transfer Protocol Secure), 47, 79****hubs, 20, 140-141**

- cabling, 145

HVAC systems, 209**hybrid clouds, 165****hybrid routing protocols, 126****hybrid topologies, 27**

-
- I**
- IaaS (Infrastructure as a Service), 162-163**
 - ICA (Independent Computing Architecture), 397**
 - ICMP (Internet Control Message Protocol), 81, 420**
 - ICMP flood, 421**
 - ICS (Industrial Control System), 12**
 - IDF (intermediate distribution frame), 214**
 - wiring closets, 248
 - IDS (intrusion detection system), 139, 459-460**
 - IDSL (ISDN DSL), 193**
 - IEEE (Institute of Electrical and Electronics Engineers), 258**
 - 802.2 standards, 259-263
 - 802.3 standards, 263
 - 802.3x standards, 259-263
 - IETF (Internet Engineering Task Force), 435-438**
 - ifconfig utility, 529-530**
 - IGMP (Internet Group Management Protocol), 85**
 - IIS (Internet Information Services), 79**
 - IMAP (Internet Message Access Protocol), 47**
 - IMAP4 (Internet Message Access Protocol Version 4), 79**
 - incident response, security, 466**
 - chain of custody, 468
 - documentation, 467
 - eDiscovery, 467
 - first responders, 466
 - securing the area, 467
 - incremental backups, 402, 404**
 - independent routing, 175**
 - infrared wireless networking, 295-296**
 - infrastructure wireless topology, 22**
 - inside threats, 416**
 - installation safety, 210**
 - interface monitoring, 347**
 - interfaces**
 - configuration, switches, 156-157
 - errors, 273
 - troubleshooting, 274
 - interference, media, 223**
 - Internet access, 191**
 - broadband, 198
 - cable, 195-197
 - cellular, 204-205
 - dialup, 198-200
 - DSL (digital subscriber line), 192
 - ADSL (asymmetric DSL), 192
 - HDSL (high bit rate DSL), 192-193
 - IDSL (ISDN DSL), 193
 - RADSL (rate-adaptive DSL), 193
 - SDSL (symmetric DSL), 192
 - speeds, 193
 - troubleshooting, 194-195
 - VHDSL (very high bit rate DSL), 192-193
 - PSTN (Public Switched Telephone Network), 201**
 - satellite, 201-203**
 - wireless, 203-204**
- Internet usage policy, 336**
- IP addresses, 94**
 - APIPA (Automatic Private IP Addressing), 110
 - BOOTP, 110
 - CIDR (classless interdomain routing), 100
 - classes, 95
 - default gateways, 100
 - duplication, 488
 - dynamic, 108-109
 - IPv4, 95
 - broadcast address, 102
 - IPv6 comparison, 107
 - multicast address, 102
 - public versus private networks, 98-99
 - unicast address, 102
 - IPv6, 102-103
 - identification, 103, 105
 - link-local, 105
 - site-local, 106
 - unicast, 105
 - unicast, global, 105
 - static, 107
 - static addressing, 51

IP addresses

- subnet masks, 97
- subnetting and, 97-98
- TCP/IP and, 94
- VIP (virtual IP address), 133

IP (Internet Protocol), 73

- troubleshooting, 486

IP helpers, 54**ipconfig utility, 527-528****IPMI (Intelligent Platform Management Interface), 157****IPsec (IP Security) protocol, 45, 389-390****IPS (intrusion prevention system), 140, 459****IPv4, 95**

- broadcast address, 102
- IPv6 comparison, 107
- multicast address, 102
- public versus private networks, 98-99
- unicast address, 102

IPv6, 102-103

- identification, 103, 105
- IPv4 comparison, 107
- link local addresses, 105
- site-local addresses, 106
- unicast addresses, 105

IrDA (Infrared Data Association), 295**ISDN (Integrated Services Digital Network), 176-177**

- BRI (Basic Rate Interface), 178
- BRI/PRI comparison, 178
- PRI (Primary Rate Interface), 178

ISDN DSL, 193**IS-IS (Intermediate System-to-Intermediate System), 45, 125****ISO (International Organization for Standardization), 68, 152****isotropic antennas, 285****ISPs (Internet Service Provider), 99, 138****ITS (intelligent transportation system), 375****J****JPEG files, 46****K****Kerberos, 435-438****L****L2TP (Layer 2 Tunneling Protocol), 386-389****LACP (Link Aggregation Control Protocol), 152****LANs (local area networks), 10-11**

- 10 Gigabit standard, 266-268
- 10BASE2 standard, 263
- 10BASE-T standard, 263-264
- 100BASE-T standard, 265
- 1000BASE-T standard, 266

latency

- QoS and, 369
- routing, 127

LDAP (Lightweight Directory Access Protocol), 85**leased lines, T-carrier lines, 179-180****legacy systems, segmentation and, 375****LG (looking glass) software, 546****line tester, 543****link local addresses, IPv6, 105****link-state routing, 125****link status, 347****LLC (logical link control), 259****LLC (Logical Link Control) layer of OSI Layer 2, 44****load balancing, 141**

- segmentation and, 377-378

load tests, 354**logging, performance monitoring and, 355-358****logical topology, 332-334****looking glasses, 546****loopback cabling, 243****LSAs (link-state advertisements), 125****LTE (Long-Term Evolution), 204****M****MAC (mandatory access control), 391****MAC address-based VLANs, 153**

- MAC addresses, 111**
 - NICs, viewing, 112
 - OUI (organizational unique identifier), 112
 - universal LAN MAC address, 112
- MAC filtering, 398**
- MAC (Media Access Control) layer of OSI Layer 2, 44**
- macro viruses, 416-418**
- maintenance monitoring, 347**
- malicious users, 551**
- malware, 416, 550**
 - Trojan horses, 418-419
 - viruses, 417-418
 - macro virus, 418
 - nonoverwriting virus, 418
 - overwriting virus, 418
 - polymorphic virus, 418
 - resident virus, 417
 - stealth virus, 418
 - variant virus, 417
 - worms, 418-419
- MAM (mobile application management), 412**
- MAN (metropolitan-area network), 12, 225**
- man-in-the-middle attacks, 422**
- mantraps, 463**
- MD5 (message digest 5), 443**
- MDF (main distribution frame), 214**
 - wiring closets, 248
- MD-IDS (misuse-detection IDS), 139**
- MDI (Medium-Dependent Interface) ports, 145**
- MDI-X (Medium-Dependent Interface Crossed) ports, 145**
- MDM (mobile device management), 412**
- media**
 - cable based, 225
 - compatibility, 496
 - IEEE 802.3x, 263
 - connectors
 - BNC, 232
 - fiber, 235
 - F-Type, 235
 - RJ-11, 233
 - RJ-45, 234
 - RJ-48C, 234
 - RS-232, 237
 - USB (universal serial bus), 238
 - converters, 238-239
 - couplers, 238-239
 - interference, 223
- media tester, 543**
- medianets, 13**
- memory, monitoring and, 346**
- mesh topology, 503-504**
- Metro-Ethernet, 188**
- MGCP (Media Gateway Control Protocol), 87**
- MIB (Management Information Base), 68**
- MIDI files, 46**
- MIMO (multiple input, multiple output) antennas, 284**
- MLA (master license agreement), 411**
- mobile data service, 204**
- modems**
 - analog, 137
 - cable modems, 195
- modulation, 270**
- MOU (memorandum of understanding), 411**
- MP3 files, 46**
- MPEG files, 46**
- MPLS (Multiprotocol Label Switching), 45, 188**
- MSAU (multistation access unit), 19**
- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), 443**
- MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2), 443**
- MSDS (material safety data sheet), 208**
- MTU (maximum transmission unit), 73**
 - black hole, 485
- multicast addresses, IPv4, 102**
- multifactor authentication, 448**
- multilayer switches, 146-147**

Multilink PPP, 187
multimeter, 544
multimode fiber cabling, 231
MUMIMO (multiuser multiple input, multiple output) antennas, 284
MX (Mail Exchange), 61

N

NaaS (network as a service), 378
NAC (network access control), 396
namespaces, DNS, 58-60
narrowband transmission, 294
NAS (network-attached storage), 171
NAT (Network Address Translation), 113-114, 169, 198, 452
nbtstat utility, 526
netstat command, 520-524
network admission procedures, 339
Network layer (Layer 3) of OSI model, 44
network monitoring procedures, 338
network policies, 412
network qualification tester, 545
network services, documentation, 328
network usage policy, 336
networks
 centralized, 15
 collisions, 270
 CSMA/CD, 270
 decapsulation, 269
 devices
 access points, 136-137
 analog modems, 137
 chart, 147
 content filters, 138
 firewalls, 138-139
 hubs, 140-141, 145
 IDS (intrusion detection system), 139
 IPS (intrusion prevention system), 140
 load balancer, 141
 packet shapers, 142
 routers, 142
 switches, 143-146
 VPN concentrator, 147
 distributed computing, 15
 encapsulation, 269
 hubs, 20
 LANs, 10-11
 MANs, 12
 medianets, 13
 models
 client/server, 14
 peer-to-peer, 13-14
 modulation, 270
 NFC (near-field communications), 11
 numbering systems, 269
 open, 315
 optimization
 QoS (Quality of Service), 368-369
 real-time services, 371
 UC (unified communication), 372
 video, 370
 VoIP (Voice over IP), 370
 PANs, 11
 planning, 32
 SANs, cloud computing and, 170-171
 SCADA/ICS, 12
 software-defined, 169
 SOHO, 32-33, 36-38
 switches, 20
 TCP/IP suite, 270
 topologies
 bus, 17-18
 hybrid, 27
 ring, 18-19
 star, 20
 wired mesh, 21-22
 wireless, 22-27
 WANs, 11
 wavelength, 270
 WPANs, 11
new user addition procedures, 338
newsgroups, 84
NEXT (near end) interference, 490-491
NFC (near-field communications), 11
NFS (Network File System), 46
NICs (network information cards)
 MAC address viewing, 112
 virtual versus physical, 169
NID (network interface device), 36
NIDS (network-based intrusion detection system), 139, 459

NIST (National Institute of Standards and Technology), 162

NIU (network interface unit), 275

NMS (network management system), 66-67

NNTP (Network News Transfer Protocol), 84

NOC (network operations center), 244

nonoverwriting virus, 418

NOS (network operating system), 138, 335

NS (Name Server), 61

nslookup utility, 530-531

NTP (Network Time Protocol), 47, 83-84

numbering systems, 269

O

OCx (Optical Carrier), 181

OFDM (orthogonal frequency-division multiplexing), 295, 308

OLT (optical line termination), 182

ONU (optical network unit), 182

open networks, 315

OS (operating system)

NOS (network operating system), 138

OS updates, 363

OSI (Open Systems Interconnect) model, 41-42, 152

Application layer (Layer 7), 46

Data Link layer (Layer 2), 44

LLC layer, 44

MAC layer, 44

network components, 48

Network layer (Layer 3), 44

Physical layer (Layer 1), 43

Presentation layer (Layer 6), 46

Session layer (Layer 5), 46

summary table, 47

Transport layer (Layer 4), 45

OSPF (Open Shortest Path First), 45, 125

OTDR (optical time domain reflectometer), 254, 544

OUI (organizational unique identifier), 111, 552

overwriting virus, 418

ownership policy, 337

P

PaaS (Platform as a Service), 162-163

packet abuse, 423

packet-filtering firewalls, 454, 456

packet shapers, 142

packet sniffers, 348

packet switching, 175

datagram packet switching, 176

virtual-circuit packet switching, 175

PAD (packet assembler/disassembler), 183

PAN (personal area network), 11

PAP (Password Authentication Protocol), 444

password attacks, 421

password policies, 433-435

PAT (Port Address Translation), 114

patch panels, 247-248

patches, 362

vulnerability, 364

pathping utility, 518

PCI DSS (Payment Card Industry Data Security Standard), 380

peer-to-peer networking model, 13-14

penetration testing, 411

performance monitoring, 344-345

event logs, 355-358

load tests, 354

packet sniffers, 348

performance tests, 353

port scanners, 351-352

reasons for, 345-347

stress tests, 354

throughput testing, 349-350

performance optimization

caching, 378-379

network segmenting, 379

perimeter network, 458

personal software policy, 337

phishing, 426

Physical layer (Layer 1) of OSI model, 43

physical security

physical security, 446-448

physical security controls, 462

physical topology, 332-334

PIDS (protocol-based intrusion detection system), 140, 460

PIN access, 447

ping of death, 420

ping utility, 513-517

PKI (public key infrastructure), 438, 440-441

digital signatures, 441

private keys, 439

public keys, 439

secure email, 441

uses, 440

plenum cabling, 232

PoE (Power over Ethernet), switches and, 157

point of demarcation, 36, 275

point-to-point wireless topology, 24-25

policies and procedures

documentation, 336, 338

passwords, 433-435

risk-related, 411-412

polymorphic viruses, 418

PON (passive optical network), 182

POP3 (Post Office Protocol version 3), 47, 79

port authentication, 133

port-based VLANs, 152

port binding, 152

port mirroring, 132, 156

port scanners, 351-352

ports

configuration, troubleshooting, 485

functioning, 88, 90

MDI, 145

MDI-X, 145

RI (ring-in), 19

RO (ring-out), 19

posture assessment, 396

POTS (plain old telephone service), 187

power

management, 216

monitoring, 347

spikes, 407

surges, 408

troubleshooting, 486

PPoE (Point-to-Point Protocol over Ethernet), 395

PPP (Point-to-Point Protocol), 187, 395

PPTP (Point-to-Point Tunneling Protocol), 386-388

Presentation layer (Layer 6) of OSI model, 46

PRI (Primary Rate Interface), 178

BRI comparison, 178

private clouds, 164

private keys, 439

private networks, segmentation and, 375-376

procedures, documentation, 329, 338-340

protocol abuse, 423

protocol analyzer, 542-543

protocol-based VLANs, 152

protocols, 71

AH, 389

ARP (Address Resolution Protocol), 82-83

connection-oriented versus connectionless, 72

ESP, 389

FCP (Fiber Channel Protocol), 171

FTP (File Transfer Protocol), 75-76

HTTP (Hypertext Transfer Protocol), 78

HTTPS (Hypertext Transfer Protocol Secure), 79

ICMP (Internet Control Message Protocol), 81

IGMP (Internet Group Management Protocol), 85

IMAP4 (Internet Message Access Protocol Version 4), 79

IP (Internet Protocol), 73

IPsec, 389-390

L2TP, 386-389

LDAP (Lightweight Directory Access Protocol), 85

MGCP (Media Gateway Control Protocol), 87

NNTP (Network News Transfer Protocol), 84

NTP (Network Time Protocol), 83-84
 POP3 (Post Office Protocol Version 3), 79
 PPP (Point-to-Point Protocol), 395
 PPTP, 386-388
 RARP (Reverse Address Resolution Protocol), 83
 RDP (Remote Desktop Protocol), 87
 RDS (Remote Desktop Services), 87
 remote access, 394-396
 remote authentication, 442-444
 remote-control, 397
 RTP (Real-time Transport Protocol), 87
 SCP (Secure Copy Protocol), 84
 secured versus unsecured, 444
 SFTP (Secure File Transfer Protocol), 76-77
 SIP (Session Initiation Protocol), 86
 SLIP, 395
 SMB (Server Message Block), 88
 SMTP (Simple Mail Transfer Protocol), 78
 SSH (Secure Shell), 80
 TCP (Transmission Control Protocol), 73-74
 Telnet, 80
 TFTP (Trivial File Transfer Protocol), 77
 TLS (Transport Layer Security), 85
 UDP (User Datagram Protocol), 74
 VPNs, 386
proxy ARP, 484
proxy servers, 128-130
PSTN (Public Switched Telephone Network), 176, 201
PtMP (point-to-multipoint) wireless topology, 25-26
PTR (Pointer), 61
public clouds, 164
public keys, 439
public networks, segmentation and, 375-376
punchdown blocks
 66 blocks, 248
 110 blocks, 248
punchdown tools, 247

PVC cabling, 232
PVC (permanent virtual circuit), 184

Q

QoS (Quality of Service), 368-369
 CoS (class of service), 369
 DSCP (differentiated services code), 369
 traffic shaping, 369

R

rack systems, 216
RADIUS, 441-442
RADSL (rate-adaptive DSL), 193
RARP (Reverse Address Resolution Protocol), 45, 83
RAS (remote access service), 394
rate adaptive DSL, 193
RBAC (role-based access control), 393
RBAC (rule-based access control), 392
RDP (Remote Desktop Protocol), 87, 397
RDS (Remote Desktop Services), 87, 397
real-time services, 371
recovery
 backups
 best practices, 406
 differential backups, 404
 full backups, 403-404
 incremental backups, 404
 tape rotations backups, 405
 UPS, 407-408
 cold sites, 409-410
 cold spares, 409
 cold swapping, 409
 hot sites, 409-410
 hot spares, 408
 hot swapping, 408
 warm sites, 409-410
regulations, documentation, 340-341
remote access, 394-396
 NAC (network access control), 396
 PPoE (Point-to-Point Protocol over Ethernet), 395

remote access

- PPP (point-to-point protocol), 395
- procedures, 339
- RAS (remote access service), 394
- SLIP (Serial Line Interface Protocol), 395

remote-control protocols, 397**Request Timed Out error message, 514****reservations, 52****resident virus, 417****resolution, DNS, 57****reverse proxy server, 130****RF (radio frequency), 280**

- channels, 289-290

RFI (radio frequency interference), 491**RG-6 cables, 235****RG-59 cables, 235****RI (ring-in) port, 19****ring topology, 18-19****RIP (Routing Information Protocol), 45, 123****risk, policies and procedures, 411-412****RJ-11 connectors, 233****RJ-45 connectors, 234****RJ-48C connectors, 234****RO (ring-out) port, 19****rogue access points, 423****rogue APs, 316****rollover cabling, 243****route problems, troubleshooting, 484****route utility, 533-534****routers, 142**

- availability, 133
- configuration, troubleshooting, 274
- proxy servers, 128-130
- STP (Spanning Tree Protocol), 130-131
- trunking, 132
- virtual, 168
- wireless, 34

routing

- administrative distance, 127
- bandwidth, 127
- costs, 127
- hop counts, 126

independent routing, 175

latency, 127

loop, 483

metrics, 126-127

MTU (maximum transmission unit), 126

route selection, 44

TCP/IP

default gateway, 119

dynamic routing, 122-126

metrics, 126-127

routing tables, 120

static routing, 121

RS-232 connectors, 237**RSPAN (Remote Switched Port Analyzer), 156****RTP (Real-time Transport Protocol), 47, 87, 371****RTSP (Real Time Streaming Protocol), 371****RX (receiver port), 486****S****SaaS (Software as a Service), 162-163****safety practices, 208**

- electrical safety, 209
- emergency exits, 212
- ESD (electrostatic discharge), 209
- fire suppression
 - extinguishers, 210-211
 - fixed systems, 211
- HVAC systems, 209
- installation safety, 210
- MSDS (material safety data sheet), 208

sampling size, 270**SANs (storage-area networks), 170-171****satellite Internet access, 201-203****satellites, troubleshooting, 277****SCADA (Supervisory Control And Data Acquisition), 12, 375****SCP (Secure Copy Protocol), 84****SCSI (Small Computer System Interface), 170****SDSL (symmetric DSL), 192**

secure email, 441**security**

authentication

Kerberos, 435-438

multifactor, 448

passwords, 433-435

PKI, 438-441

remote authentication protocols,
442-444

two-factor, 448

configuration, 299

DMZ (demilitarized zone), 458

firewalls, 452-453

application level, 456

circuit-level, 456

comparing, 457

packet-filtering, 454-456

stateful, 453

stateless, 453

honeynets, 461

honeypots, 461

IDS (intrusion detection system),
459-460

incident response, 466

chain of custody, 468

documentation, 467

eDiscovery, 467

first responders, 466

securing the area, 467

IPS (intrusion prevention
system), 459

mantraps, 463

monitoring, 346

network planning, 33

physical, 446-448

physical controls, 462

policies, 412

troubleshooting, 276

prevention measures, 426-428

procedures, 338

protocols, 444

RADIUS, 441-442

segmentation and, 380

switch ports, 461

TACACS, 441-442

threats, 416

ARP poisoning, 423

backdoor attacks, 422

bluejacking, 424

bluesnarfing, 424

DDoS, 419

DoS, 419-421

eavesdropping, 422

evil twin attacks, 423

inside threats, 416

malware, 416-419

man-in-the-middle attacks, 422

managing, 549-552

packet abuse, 423

password attacks, 421

phishing, 426

protocol abuse, 423

rogue access points, 423

session hijacking, 424

social engineering, 422

spoofing, 423

VLAN hopping, 425

weaknesses, advertising, 423

WEP attacks, 424

WPA attacks, 424

WPS attacks, 424

zero-day attacks, 425

UTM devices, 452-453

video monitoring, 463

vulnerabilities, 426-428

vulnerability scanners, 462

WLANs, 311

open networks, 315

rogue APs, 316

topologies, 316

WEP (wired equivalent privacy),
311-312WPA (Wi-Fi protected
access), 312

WPA Enterprise, 314

WPA2 (Wi-Fi protected
access), 313**security guard, 463****segmentation, 150, 374**

compliance, 380

honeynets, 376-377

honeypots, 376-377

legacy systems, 375

load balancing and, 377-378

OSI Transport layer, 45

performance optimization

caching, 378-379

network segmenting, 379

segmentation

- private networks, 375-376
- public networks, 375-376
- SCADA systems, 375
- security and, 380
- testing labs, 377
- VLANs, 154
- server rail racks, 216**
- server-side filters, 138**
- servers**
 - configuration documentation, 328
 - proxy servers, 128-130
 - VPNs, 386
- service addressing, OSI Transport layer, 45**
- services, documentation, 328**
- session hijacking, 424**
- Session layer (Layer 5) of OSI model, 46**
- SFP (small form-factor pluggable) module, 486**
- SFTP (Secure File Transfer Protocol), 76-77**
- shorts, troubleshooting, 493**
- SIEM (security information and event management), 347**
- signature-based intrusion detection system, 139**
- simplex mode, 223**
- single-mode fiber cabling, 231**
- SIP (Session Initiation Protocol), 13, 47, 86**
- site-local addresses, 106**
- SLA (service level agreement), 411**
- SLIP (Serial Line Interface Protocol), 395**
- SMB (Server Message Block), 46-47, 88**
- SMTP (Simple Mail Transfer Protocol), 47, 78, 146**
- Smurfing, 420**
- SNAT (Static Network Address Translation), 115**
- SNMP (Simple Network Management Protocol), 65**
 - agents, 67
 - commands, 67
 - communities, 68
 - components, 65
 - information bases, 67
 - NMS (network management system), 66-67
 - SNMPv3, 69
 - switches and, 157
- SOA (Start of Authority), 61**
- social engineering, 422**
- software**
 - personal software policy, 337
 - procedures, 339
- software defined networking, 169**
- SOHO (small office/home office)**
 - networks, 32-33, 36-38
 - routers, 142
- SONET (Synchronous Optical Network), 181**
- sound files, 46**
- SOW (statement of work), 411**
- SPB (shortest path bridging), 127**
- speed tests, 546**
- split horizon, 274**
- split pairs, troubleshooting, 493**
- SPOF (single point of failure), 411**
- spoofing, 423**
- spread spectrum, 294**
 - DSSS (direct-sequence spread-spectrum), 295
 - FHSS (frequency-hopping spread-spectrum), 294-295
- spyware, 417**
- SSH (Secure Shell), 47, 80, 397**
 - SFTP and, 77
- SSID (service set identifier), 203, 282**
- SSL (Secure Sockets Layer), 79**
- star topology, 20**
 - troubleshooting, 502
- static addressing, 51, 107**
- static routing, 121**
- stealth virus, 418**
- store-and-forwarding switching, 145**
- STP (shielded twisted-pair) cabling, 224-226**
- STP (Spanning Tree Protocol), 130-131**
 - switches, 155

straight-through cabling, 240, 242

stress tests, 354

subnet masks, 97, 487

subnetting, 97-98

SVC (switched virtual circuit), 184

swipe cards, 447

switches, 20, 143-144

cabling, 145

interface configuration, 156-157

loop, 483

management, 157

managing, 157

multilayer, 146

PoE (Power over Ethernet), 157

port authentication, 133

port mirroring, 132

speed, 299

STP (Spanning Tree Protocol), 155

virtual, 168

VLANs, 150-154

WANs, 174

circuit switching, 176

method comparison, 176

packet switching, 175

switchport security, 461

symmetric DSL, 192

symmetric key cryptography, 437

SYN flood, 420

T

T connectors, 17

T-carrier lines, 179-180

TACACS (Terminal Access Controller Access Control System), 441-442

tape rotations, backups, 405

TCP (Transmission Control Protocol), 45, 73-74

TCP/IP (Transmission Control Protocol/Internet Protocol), 94

client configuration, 109

configuration, troubleshooting, 497-501

default gateway, 119

dynamic routing, 122

distance-vector routing, 122-124

hybrid routing protocols, 126

link-state routing, 125

filtering, 399

four-layer model, 48

routing metrics, 126-127

routing tables, 120

static routing, 121

suite, 270

TDM (time-division multiplexing), 221

TDR (time domain reflectometer), 253, 543

Telnet, 80

Terminal Services, 87

testing

labs, 377

load tests, 354

penetration testing, 411

performance tests, 353

stress tests, 354

throughput, 349-350

TFTP (Trivial File Transfer Protocol), 77

thin client computing, 87, 397

threats

ARP poisoning, 423

backdoor attacks, 422

bluejacking, 424

bluesnarfing, 424

DDoS (distributed DoS) attack, 419

DoS (denial-of-service) attack, 419-420

buffer overflow, 421

DRDoS, 421

Fraggles, 420

ICMP flood, 421

ping of death, 420

Smurfing, 420

SYN flood, 420

eavesdropping, 422

evil twin attacks, 423

malware, 416

Trojan horses, 418-419

viruses, 417-418

worms, 418-419

man-in-the-middle attacks, 422

managing, 549-552

packet abuse, 423

password attacks, 421

phishing, 426

protocol abuse, 423

rogue access points, 423

threats

- session hijacking, 424
- social engineering, 422
- spoofing, 423
- VLAN hopping, 425
- weaknesses, advertising, 423
- WEP attacks, 424
- WPA attacks, 424
- WPS attacks, 424
- zero-day attacks, 425

threats to security. *See* security, threats**throttling, 276****throughput testing, 349-350****TIFF files, 46****TKIP (Temporal Key Integrity Protocol), 312****TLS (Transport Layer Security), 46, 85, 316****toner probes, 541-542****tools**

- butt set, 545
- cable tester, 543
- cabling, 252-254
- environmental monitors, 540
- looking glasses, 546
- media tester, 543
- multimeter, 544
- network qualification tester, 545
- OTDR (optical time domain reflectometer), 544
- protocol analyzer, 542-543
- speed tests, 546
- TDR (time domain reflectometer), 543
- toner probes, 541-542
- voltage event recorder, 539
- wire crimpers, 538-539
- wire snips, 538-539
- wire strippers, 538-539
- wireless detection, 546

topologies, 316

- bus, 17-18
- documentation, 328, 332-334
- hybrid, 27
- IEEE 802.3x, 263
- logical, 332-334
- mesh, 503-504
- OSI Layer 1, 43

- physical, 332-334
- ring, 18-19
- star, 20, 502
- wired mesh, 21-22
- wireless, 22
 - ad hoc wireless topology, 23
 - infrastructure wireless topology, 22
 - point-to-point networks, 24-25
 - PtMP (point-to-multipoint), 25-26
 - wireless mesh networks, 26-27

trace route utility, 509-512**tracert, 122****traffic shaping, 142, 369****transmission rates, 224-225****Transport layer (Layer 4) of OSI model, 45****Trojan horses, 417-419****troubleshooting**

- AP coverage, 283-284
- broadcast storms, 484
- cabling, 488-490
 - attenuation, 491
 - bad wiring, 493
 - connectors, 492
 - crosstalk, 490-491
 - dB loss, 493
 - echo, 492
 - EMI/RFI, 491
 - placement, 494
 - shorts, 493
 - split pairs, 493
 - TX/RX reversed, 494
- client connectivity, 496
 - media connection, 496-497
 - physical connection, 496
 - TCP/IP configuration, 497-501
- command-line utilities and, 507
 - ARP utility, 518-520
 - dig, 531-532
 - host, 533
 - ifconfig, 529-530
 - ipconfig, 527-528
 - nbtstat, 525
 - netstat command, 520-524
 - nslookup, 530-531
 - pathping utility, 518

- ping utility, 513-517
- route, 533-534
- trace route utility, 509-512
- common problems, 483-488
- customer premise equipment, 275-276
- dialup Internet, 199-200
- DNS, 488
- documentation, 478-479
- DSL, 194-195
- escalate, 476-477
- fiber issues, 486-487
- gateway, 487
- hardware, 494
- implement solution, 476-477
- Internet access
 - cable, 196-197
- IP address duplication, 488
- IP issues, 486
- mismatched MTU, 485
- MTU black hole, 485
- plan of action, 476
- port configuration, 485
- power issues, 486
- probable cause theory, 475
- problem identification, 473
 - changes, 474
 - symptoms, 474
- proxy ARP, 484
- route problems, 484
- routing loop, 483
- satellite, 277
- security policies, 276
- subnet mask, 487
- switching loop, 483
- system functionality verification, 478
- theory testing, 475
- VLANs, 501-502
 - topology, 502-504
- WANs, 273-275
- wiring, 488-490
 - attenuation, 491
 - bad wiring, 493
 - connectors, 492
 - crosstalk, 490-491
 - dB loss, 493
 - echo, 492
 - EMI/RFI, 491
 - placement, 494

- schematics, 331
- shorts, 493
- split pairs, 493
- TX/RX reversed, 494
- WLANs, 318-320
 - signal interference, 322-323

trunking, 132, 152

- tagging and, 156
- VLAN trunking, 132

TTL (Time to Live), 81**TTLS (Tunneled Transport Layer Security), 316****twisted-pair cabling, 226-228****two-factor authentication, 448****two-post racks, 217****U****UC (unified communication) devices, 372****UDP (User Datagram Protocol), 45, 74****unicast addresses**

- IPv4, 102
- IPv6, 105

universal LAN MAC address, 112**Unknown host error message, 515****updates, 362**

- drivers, 363
- features, 364
- firmware, 363
- major versus minor, 364
- OS, 363

upgrading versus downgrading, 364**UPS (uninterruptible power supply), 157, 216, 407-408****URLs (uniform resource locators), 78, 129****USB (universal serial bus) connectors, 238****user account policy, 337****user awareness and training, 411****utilities**

- ARP, 518-520
- dig, 531-532
- host, 533
- ifconfig, 529-530

- ipconfig, 527-528
- nbstat, 526
- netstat command, 520-524
- nslookup, 530-531
- pathping, 518
- ping, 513-517
- route, 533-534
- trace route, 509-512

UTM (Unified Threat Management), 452-453

UTP (unshielded twisted-pair) cabling, 223-226

- connection, 195

V

variant virus, 417

VC (virtual consoles), 156

vertical cabling, 246

VF (virtual firewall), 169

VHDSL (very high bit rate DSL), 192-193

video, network optimization and, 370

violations, reporting procedures, 339

VIP (virtual IP address), 133

virtual-circuit packet switching, 175

virtual networks, VNICs (virtual network interface cards), 168

virtualization

- cloud computing, 167
- firewalls, 169
- implementation, 167
- NICs, 169
- routers, 168
- software defined networking, 169
- switches, 168

viruses, 416-418

- macro viruses, 416-418
- nonoverwriting virus, 418
- overwriting virus, 418
- polymorphic virus, 418
- resident virus, 417
- stealth virus, 418
- variant virus, 417

VLAN hopping, 425

VLAN pooling, 281

VLAN trunking, 132

VLANs (virtual local-area networks)

- benefits, 151
- default, 156
- MAC address-based, 153
- membership, 152-153
- port-based, 152
- protocol-based, 152
- segmentation, 154
- switches, 150-154
- troubleshooting, 501-502
- topology, 502-504

VM (virtual machine), 379

VNIC (virtual network interface cards), 168-169

VoIP (Voice over IP), 157, 370

- SIP (Session Initiation Protocol), 86

voltage event recorder, 539

VPNs (Virtual Network Protocol), TCP/IP filtering, 399

VPNs (virtual private networks), 385

- access methods, 386
- benefits, 386
- client, 385
- concentrators, 147
- disadvantages, 386
- host-to-host tunnel, 390
- host-to-site tunnel, 390
- IPsec protocol, 389-390
- L2TP, 388-389
- MAC filtering, 398
- PPTP, 387-388
- protocols, 386
- remote access, 394-396
- remote-control protocols, 397
- server, 386
- site-to-site tunnel, 390

VRRP (Virtual Router Redundancy Protocol), 133

VTC (video teleconferencing), 13

VTP (VLAN Trunking Protocol), 132, 151

vulnerabilities, 426-428

- patches, 364
- scanners, 462
- scanning, 411

W**WANs (wide area networks), 11**

- ATM (Asynchronous Transfer Mode), 185-186
- CDMA (code division-multiple access), 188
- DWDM (dense wavelength-division multiplexing), 182
- Frame Relay, 183-184
- GSM (Global System for Mobile Communications), 188
- Internet access, 191
 - broadband, 198
 - cable, 195-197
 - cellular, 204-205
 - dialup, 198-200
 - DSL, 192-195
 - PTSN, 201
 - satellite, 201-203
 - wireless, 203-204
- ISDN, 177
 - BRI, 178
 - BRI/PRI comparison, 178
 - PRI, 178
- leased lines
 - T-carrier lines, 179-180
- Metro-Ethernet, 188
- MPLS (Multiprotocol Label Switching), 188
- Multilink PPP, 187
- OCx (Optical Carrier), 181
- OLT (optical line termination), 182
- ONUs (optical network units), 182
- PON (passive optical network), 182
- PPP (Point-to-Point Protocol), 187
- SONET (Synchronous Optical Network), 181
- summary of technologies, 186
- switching methods, 174
 - circuit switching, 176
 - comparison, 176
 - packet switching, 175
- troubleshooting, 273-275

war driving, 423**warm sites, 409-410****warm swap, 409****wavelengths, 270****weaknesses, advertising, 423****WEP (wired equivalent privacy), 311-312****WEP attacks, 424****WiMAX (Worldwide Interoperability for Microwave Access), 204****windowing, OSI Transport layer, 45****WINS (Windows Internet Network Service), 63****wire crimpers, 252, 538-539****wire snips, 253, 538-539****wire strippers, 253, 538-539****wired mesh topology, 21-22****wireless access point, 22****wireless bands, 299****wireless controllers, 281****wireless detection, 546****wireless Internet access, 203-204****wireless mesh networks, 26-27****wireless monitoring, 348****wireless networks, 279**

- AP (access points), 279

wireless routers, 34**wireless topologies, 22**

- ad hoc wireless topology, 23
- AP (access points), 22
- infrastructure wireless topology, 22
- point-to-point networks, 24-25
- PtMP (point-to-multipoint) networks, 25-26
- wireless mesh networks, 26-27

wiring. *See also* cabling

- closets, 248
- layout documentation, 328-331
- troubleshooting, 488-490
 - attenuation, 491
 - bad wiring, 493
 - connectors, 492
 - crosstalk, 490-491
 - dB loss, 493
 - echo, 492
 - EMI/RFI, 491
 - placement, 494
 - shorts, 493
 - split pairs, 493
 - TX/RX reversed, 494

WISP (wireless Internet service provider)

WISP (wireless Internet service provider), 25

WLAN (wireless local-area network), 25, 280

802.11 standards, 305-306

802.11ac, 307

802.11n, 307

DSSS and, 308

FHSS and, 308

OFDM and, 308

antennas, 284

coverage, 286

ratings, 285-286

signal quality, 287-288

APs (access points), 280-281

BSA, 283

BSS, 282

BSSID, 282

ESS, 282

ESSID, 282

SSID, 282

troubleshooting, 283-284

association, 297

authentication, 298

beacons, 293-294

BWA, 295

communication establishment,
296-298

configuration, 299-303

data rate, 292

goodput, 292

infrared, 295-296

OFDM, 295

RF channels, 289-290

security, 311

open networks, 315

rogue APs, 316

topologies, 316

WEP, 311-312

WPA, 312

WPA Enterprise, 314

WPA2, 313

spread spectrum, 294

DSSS, 295

FHSS, 294-295

troubleshooting, 318-320

signal interference, 322-323

WMI (Windows Management Instrumentation), switches, 157

WMS (warehouse management system), 375

workgroup hubs, 141

worms, 417-419

WPA (Wi-Fi protected access), 312

WPA attacks, 424

WPA Enterprise, 314

WPA2 (Wi-Fi protected access), 313

WPAN (wireless personal area network), 11

WPS attacks, 424

Z

zero-day attacks, 425