

Save 10%
on Exam
Voucher

See Inside

EXAM CRAM

CompTIA[®]

Network+

N10-009



Exam Alerts



Cram
Sheet



Flash
Cards



Practice
Tests



EMMETT DULANEY

FREE SAMPLE CHAPTER |



CompTIA® Network+ N10-009 Exam Cram

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, Key Term flash card application, a Cram Sheet, and more!

To access the companion website, simply follow these steps:

1. Go to www.pearsonITcertification.com/register.
2. Enter the **print book ISBN**: 9780135340837.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to pearsonitp.ehelp.org.

This page intentionally left blank

EXAM ✓ **CRAM**

**CompTIA[®]
Network+
N10-009
Exam Cram**

Emmett Dulaney



Pearson

CompTIA® Network+ N10-009 Exam Cram

Copyright © 2025 by Pearson Education, Inc.

Hoboken, New Jersey

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.

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

ISBN-13: 978-0-13-534083-7

ISBN-10: 0-13-534083-7

Library of Congress Control Number: 2024939808

\$PrintCode

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification 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.

Special Sales

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

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

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

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

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

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

GM K12, Early Career and Professional Learning

Soo Kang

Director, ITP Product Management

Brett Bartow

Executive Editor

Nancy Davis

Development Editor

Ellie Bru

Managing Editor

Sandra Schroeder

Senior Project Editor

Tonya Simpson

Copy Editor

Chuck Hutchinson

Indexer

Timothy Wright

Proofreader

Barbara Mack

Technical Editor

Chris Crayton

Publishing Coordinator

Cindy Teeters

Cover Designer

Chuti Prasertsith

Compositor

codeMantra

Contents at a Glance

	Introduction	xviii
CHAPTER 1	Networking Models, Ports, Protocols, and Services	1
CHAPTER 2	Network Topologies, Architectures, and Types	43
CHAPTER 3	Network Addressing, Routing, and Switching	61
CHAPTER 4	Network Implementations	127
CHAPTER 5	Cabling Solutions and Issues	181
CHAPTER 6	Wireless Solutions	239
CHAPTER 7	Cloud Computing Concepts and Options	269
CHAPTER 8	Network Operations	289
CHAPTER 9	Network Security	385
CHAPTER 10	Network Troubleshooting	449
	Cram Sheet	531
	Index	551

Online

Glossary

Table of Contents

Introduction	xviii
-------------------------------	--------------

CHAPTER 1

Networking Models, Ports, Protocols, and Services	1
The OSI Networking Model	2
The OSI Seven-Layer Model	3
Comparing OSI to the Four-Layer TCP/IP Model	8
Identifying the OSI Layers at Which Various Network Components Operate	9
Data Encapsulation/Decapsulation and OSI	10
Ports, Protocols, Services, and Traffic Types	13
Connection-Oriented Protocols Versus Connectionless Protocols	14
Internet Protocol	14
Transmission Control Protocol	15
User Datagram Protocol	16
Internet Control Message Protocol	17
IPsec	18
Generic Routing Encapsulation	19
File Transfer Protocol (FTP)	20
Secure File Transfer Protocol (SFTP)	21
Secure Shell (SSH)	22
Telnet	22
Simple Mail Transfer Protocol (SMTP)	23
Domain Name System (DNS)	23
Dynamic Host Configuration Protocol (DHCP)	23
Trivial File Transfer Protocol (TFTP)	24
Hypertext Transfer Protocol (HTTP)	25
Network Time Protocol (NTP)	25
Simple Network Management Protocol (SNMP)	26
Lightweight Directory Access Protocol (LDAP)	30
Hypertext Transfer Protocol Secure (HTTPS)	31
Server Message Block (SMB)	31
Syslog	31
Simple Mail Transfer Protocol Secure (SMTPS)	32
Lightweight Directory Access Protocol over SSL (LDAPS)	32
Structured Query Language (SQL) Server	33

Remote Desktop Protocol (RDP)	33
Session Initiation Protocol (SIP)	34
Understanding Port Functions	34
Traffic Types	36
What's Next?	41
CHAPTER 2	
Network Topologies, Architectures, and Types	43
Network Topologies	44
Star/Hub and Spoke	45
Mesh Topology	46
Hybrid Topology	47
Point to Point	48
Spine and Leaf	48
Three-Tier Hierarchical Model	49
Collapsed Core	52
Traffic Flows	53
Older Topologies: Bus and Ring	54
What's Next?	59
CHAPTER 3	
Network Addressing, Routing, and Switching	61
IPv4 Network Addressing	62
An Overview of IPv4	63
IP Address Classes	63
Subnet Mask Assignment	64
Subnetting	65
Identifying the Differences Between IPv4 Public and Private Networks	66
Classless Interdomain Routing	68
Default Gateways	68
Assigning IP Addresses	70
Identifying MAC Addresses	74
Routing and Switching Technologies	79
The Default Gateway	79
Routing Tables	80
Static Routing	81
Default Route	82
Switching Methods	82

Dynamic Routing	85
Route Selection	89
Address Translation	90
First Hop Redundancy Protocol (FHRP)	93
Virtual IP	94
Subinterfaces	94
Virtual Local-Area Networks	95
Interface Configuration and Switch Management	101
Voice VLAN	103
Trunking	103
The Spanning Tree Protocol (STP)	103
Maximum Transmission Unit (MTU)	105
Network Services	108
Dynamic Host Configuration Protocol	108
The DHCP Process	110
DHCP and DNS Suffixes	111
DHCP Relays and IP Helpers	112
Domain Name Service (DNS)	112
The DNS Namespace	114
Types of DNS Entries	117
DNS Records	117
DNS in a Practical Implementation	119
Time Protocols	120
What's Next?	125

CHAPTER 4

Network Implementations	127
Common Networking Devices	128
Router	129
Switch	131
Firewall	134
IDS/IPS	136
Load Balancer	138
Proxy Server	139
Network-Attached Storage (NAS)	141
Storage-Area Networks	142
Wireless Access Point	144
Wireless LAN Controller	145
Applications/Content Delivery Network	145

VPNs	146
Quality of Service	151
Time To Live (TTL)	153
Networking Use Cases	156
Software-Defined Networking	157
Virtual Extensible Local-Area Network (VXLAN)	162
Zero Trust Architecture (ZTA)	163
Secure Access Secure Edge (SASE)/Security Service Edge (SSE)	165
Infrastructure as Code (IaC)	166
IPv6 Addressing	169
Comparing IPv4 and IPv6 Addressing	174
What's Next?	179

CHAPTER 5

Cabling Solutions and Issues	181
General Media Considerations	182
Broadband Versus Baseband Transmissions	183
Simplex, Half-Duplex, and Full-Duplex Modes	184
Data Transmission Rates	184
Wired Versus Wireless	185
Types of Wired Network Media	187
Types of Media Connectors	195
Media Couplers/Converters	201
TIA/EIA 568A and 568B Wiring Standards	202
Straight-Through Versus Crossover Cables	203
Rollover and Loopback Cables	205
Ethernet Copper and Fiber Standards	206
Multiplexing Options	210
Troubleshooting Common Cable Connectivity Issues	214
Limitations, Considerations, and Issues	216
Throughput, Speed, and Distance	216
Cabling Specifications/Limitations	217
Cabling Considerations	218
Cabling Issues	218
Signal Degradation	219
Interference	220
Improper Termination	220
Incorrect Pinout	221

Bad Ports	221
Open/Short	222
LED Status Indicators	222
Duplexing Issues	223
TX/RX Reversed	223
Dirty Optical Cables	224
Interface Issues	224
Hardware Issues	227
Power over Ethernet Issues	227
Transceiver Issues	228
Common Tools	229
Cable Crimpers, Strippers, and Snips/Cutters	229
Punchdown Tools	230
Tone Generator	230
Loopback Adapter	231
TDR/OTDR	231
Multimeter	232
Cable Tester	233
Wire Map	234
Tap	234
Fusion Splicer	234
Spectrum Analyzer	234
Fiber Light Meter	234
What's Next?	237

CHAPTER 6

Wireless Solutions	239
Understanding Wireless Basics	240
Wireless Channels and Frequencies	240
Speed, Distance, and Bandwidth	246
Channel Bonding	247
MIMO/MU-MIMO/Directional/Omnidirectional	248
Network Types	251
Establishing Communications Between Wireless Devices	253
Guest Networks	255
Configuring the Wireless Connection	256
Autonomous and Lightweight Access Points	262
What's Next?	267

CHAPTER 7	
Cloud Computing Concepts and Options	269
Cloud Concepts	270
Service Models	271
Software as a Service	271
Platform as a Service	272
Infrastructure as a Service	273
Deployment Models	276
Private Cloud	276
Public Cloud	276
Hybrid Cloud	276
Multitenancy	278
Elasticity	279
Scalability	279
Network Functions Virtualization (NFV)	279
Cloud Connectivity Options	280
Virtual Private Cloud (VPC)	281
Cloud Gateways	282
Network Security, Groups, and Lists	283
What's Next?	288
CHAPTER 8	
Network Operations	289
Physical Installation Factors	290
Components of Wiring Distribution	291
Using Uninterruptible Power Supplies	299
Beyond the UPS	300
Environmental Factors	301
Organizational Processes and Procedures	305
Wiring and Port Locations	310
Physical and Logical Network Diagrams	313
Baseline/Golden Configurations	316
Policies, Procedures, Configurations, and Regulations	318
Labeling	330
Monitoring Network Performance	334
Common Performance Metrics	335
SNMP	339
Network Performance, Load, and Stress Testing	343
Network Device Logs	345

Disaster Recovery and High Availability	360
Backups	361
Backup Best Practices	365
Cold, Warm, Hot, and Cloud Sites	365
High-Availability Approaches and Recovery Concepts	367
Active-Active Versus Active-Passive.	369
DR Testing	370
Network Access and Management Methods	375
Site-to-Site VPN	376
Client-to-Site VPN	377
Connection Methods	378
Jump Box	380
In-Band Versus Out-of-Band Management	381
What's Next?	383

CHAPTER 9

Network Security	385
Common Security Concepts	386
Encryption	388
Access Control	388
Mandatory Access Control.	389
Discretionary Access Control	389
Rule-Based Access Control	390
Role-Based Access Control	390
Defense in Depth	393
Separation of Duties	398
Deception Technologies: Honeypots and Honeynets	399
RADIUS and TACACS+	400
Kerberos Authentication	401
Local Authentication.	403
Lightweight Directory Access Protocol	403
Using Certificates.	404
Identity and Access Management (IAM)	405
Security Assertion Markup Language (SAML)	406
Multifactor Authentication Factors	407
Auditing and Regulatory Compliance	408
Additional Access Control Methods	410
Risk Management.	415

Penetration Testing	416
Security Information and Event Management	417
Common Networking Attacks	421
Denial-of-Service and Distributed Denial-of-Service Attacks	422
Other Common Attacks	424
Vulnerabilities and Prevention	431
Applying Network Security	436
Disposing of Assets	437
Secured Versus Unsecured Protocols	437
Key Management	438
Hardening Best Practices	440
Wireless Security	444
Working with Zones	445
What's Next?	448

CHAPTER 10

Network Troubleshooting 449

Troubleshooting Steps and Procedures	450
Identify the Problem	451
Establish a Theory of Probable Cause	453
Test the Theory to Determine the Cause	454
Establish a Plan of Action	454
Implement the Solution or Escalate	455
Verify Full System Functionality	456
Document Findings, Actions, Outcomes, and Lessons Learned Throughout the Process	457
Troubleshooting Common Networking Issues	460
Common Considerations	461
Common Problems to Be Aware Of	462
Hardware Failure	474
Network Performance Issues	475
Wireless Issues	476
Site Surveys	481
Factors Affecting Wireless Signals	481
Troubleshooting AP Coverage	483
Troubleshooting Tools	489
Toner	490
Cable Tester	490

Taps	490
Visual Fault Locator	491
Wi-Fi Analyzer	491
Protocol Analyzer	493
Speed Tester	494
Port Scanner	494
LLDP and CDP	497
NetFlow Analyzer	498
TFTP Server	498
Terminal Emulator	498
IP Scanner	498
Command-Line Tools	498
The Trace Route Utility (tracert/traceroute)	500
ping	504
ARP	510
The netstat Command	512
ipconfig	518
ifconfig	521
nslookup	522
dig	523
The tcpdump Command	525
The route Utility	525
nmap	526
Basic Networking Device Commands	526
What's Next?	530
Cram Sheet	531
Index	551
Online	
Glossary	

About the Author

Emmett Dulaney (CompTIA Network+, Cloud+, Security+, A+, and others) has been the author of several books on certifications and operating systems over the past 25 years. He is a columnist for *Certification Magazine* and a professor at a small university in Indiana. He is currently the editor of a journal devoted to business education (and the business of education).

Dedication

For Harrison, Teresea, Wolfgang, and Elijah: never stop networking

—Emmett Dulaney

Acknowledgments

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

About the Technical Reviewer

Chris Crayton, MCSE, CISSP, CASP+, PenTest+, Project+, CySA+, Cloud+, S+, N+, A+, ITF+ is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He has also been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge.

We Want to Hear from You!

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

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

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

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

Email: community@informit.com

Reader Services

Register your copy of *CompTIA Network+ N10-009 Exam Cram* for convenient access to downloads, updates, and corrections as they become available.

To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780135340837 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

Introduction

Welcome to *CompTIA Network+ N10-009 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 N10-009. As such, it is easy to find the information required for each of the specified CompTIA Network+ objectives. The objective focus design used by this Exam Cram is an important feature because the information you need to know is easily identifiable and accessible. To see what we mean, compare the CompTIA objectives to the book's layout, and you can see that the facts are right where you would expect them to be.

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

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

About the Network+ Exam

The Network+ (N10-009 Edition) exam is the newest iteration of several versions of the exam. The new Network+ objectives are aimed toward those who have at least 9 to 12 months of experience in the IT networking field. While it is helpful if Network+ candidates have A+ certification (or its equivalent), it is not required, and this should not discourage those who do not.

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

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

CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (that is, objectives) and specific topics under each general topic (that is, subobjectives) for the CompTIA Network+ N10-009 exam. This table also lists the chapter in which each exam topic is covered.

TABLE I-1 CompTIA Network+ Exam Topics

Chapter	N10-009 Exam Objective	N10-009 Exam Subobjective
1 (Networking Models, Ports, Protocols, and Services)	1.0 Networking Concepts	1.1 Explain concepts related to the Open Systems Interconnection (OSI) reference model.
		1.4. Explain common networking ports, protocols, services, and traffic types.
2 (Network Topologies, Architectures, and Types)	1.0 Networking Concepts	1.6 Compare and contrast network topologies, architectures, and types.
3 (Network Addressing, Routing, and Switching)	1.0 Networking Concepts	1.7 Given a scenario, use appropriate IPv4 network addressing.
	2.0 Network Implementation	2.1 Explain characteristics of routing technologies.
	3.0 Network Operations	2.2 Given a scenario, configure switching technologies and features.
		3.4 Given a scenario, implement IPv4 and IPv6 network services.

Chapter	N10-009 Exam Objective	N10-009 Exam Subobjective
4 (Network Implementations)	1.0 Networking Concepts	1.2 Compare and contrast networking appliances, applications, and functions. 1.8 Summarize evolving use cases for modern network environments.
5 (Cabling Solutions and Issues)	1.0 Networking Concepts 5.0 Network Troubleshooting	1.5 Compare and contrast transmission media and transceivers. 5.2 Given a scenario, troubleshoot common cabling and physical interface issues.
6 (Wireless Solutions)	2.0 Network Implementation	2.3 Given a scenario, select and configure wireless devices and technologies.
7 (Cloud Computing Concepts and Options)	1.0 Networking Concepts	1.3 Summarize cloud concepts and connectivity options.
8 (Network Operations)	2.0 Network Implementation 3.0 Network Operations	2.4 Explain important factors of physical installations. 3.1 Explain the purpose of organizational processes and procedures. 3.2 Given a scenario, use network monitoring technologies. 3.3 Explain disaster recovery (DR) concepts. 3.5 Compare and contrast network access and management methods.
9 (Network Security)	4.0 Network Security	4.1 Explain the importance of basic network security concepts. 4.2 Summarize various types of attacks and their impact to the network. 4.3 Given a scenario, apply network security features, defense techniques, and solutions.
10 (Network Troubleshooting)	5.0 Network Troubleshooting	5.1 Explain the troubleshooting methodology. 5.3 Given a scenario, troubleshoot common issues with network services. 5.4 Given a scenario, troubleshoot common performance issues. 5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.

Booking and Taking the Network+ Certification Exam

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

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

What to Expect from the Exam

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

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

Most of the questions on the Network+ exam require you to choose a single correct answer, but a few require multiple answers. When there are multiple

correct answers, a message at the bottom of the screen prompts you to “Choose all that apply.” Be sure to read these messages.

A Few Exam-Day Details

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

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

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

After the Test

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

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. ExamAlerts, Tips, and Notes found throughout each chapter are designed to pull out exam-related hotspots. These can be your best friends when preparing for the exam.
- ▶ **Use the questions to assess your knowledge:** Don't just read the chapter content; use the exam questions to find out what you know and what you don't. If you struggle, study some more, review, and then assess your knowledge again.
- ▶ **Review the exam objectives:** Develop your own questions and examples for each topic listed. If you can develop and answer several questions for each topic, you should not find it difficult to pass the exam.

Good luck!

Companion Website

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

To access this companion website, follow these steps:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: 9780135340837.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

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

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

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by accessing the registration code that comes with the book. You can access the code in these ways:

- ▶ You can get your access code by registering the print ISBN 9780135340837 on <https://www.pearsonitcertification.com/register>. Make sure to use the print book ISBN, regardless of whether you purchased an eBook or the print book. After you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the **Access Bonus Content** link.
- ▶ If you purchase the Premium Edition eBook and Practice Test directly from the Pearson IT Certification website, the code will be populated on your account page after purchase. Just log in at <https://www.pearsonitcertification.com>, click **Account** to see details of your account, and click the **Digital Purchases** tab.

Note

After you register your book, your code can always be found in your account under the Registered Products tab.

Once you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

- Step 1.** Open this book's companion website as shown on the first page of the book.
- Step 2.** Click the Practice Exams button.
- Step 3.** Follow the instructions listed there for both installing the desktop app and using the web app.

Note that if you want to use the web app only at this point, just navigate to <https://www.pearsontestprep.com>, log in using the same credentials used to register your book or purchase the Premium Edition, and register for this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

Customizing Your Exams

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

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

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

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

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

Updating Your Exams

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

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

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

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

Assessing Exam Readiness

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

Figure Credits

Figures 1.3, 3.5, 3.9, 6.2, 6.4, 6.5, 8.13, 9.3, 10.2, 10.3: Linksys Holdings, Inc

Figures 3.2–3.4, 4.3, 4.4, 5.15, 8.9–8.12, 10.4: Microsoft Corporation

Chapter 10, Cram Quiz under “Troubleshooting Common Networking Issues,” screenshot of Internet Protocol Version 4 (TCP/IPv4) Properties: Microsoft Corporation

CHAPTER 2

Network Topologies, Architectures, and Types

This chapter covers the following official Network+ objective:

- ▶ 1.6 Compare and contrast network topologies, architectures, and types.

For more information on the official CompTIA Network+ exam topics, see the “About the Network+ Exam” section in the Introduction.

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

This chapter reviews general network considerations, such as the various topologies used on today’s networks, *local-area networks* (LANs), and *wide-area networks* (WANs).

Network Topologies

- **1.6 Compare and contrast network topologies, architectures, and types.**

CramSaver

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

1. Which topology is commonly known as a hub and spoke model?
2. With which topology does every node have a direct connection to every other node?
3. True or false: Traffic flows entering and leaving a datacenter are known as East-West traffic.
4. True or false: In the three-tier hierarchical model, the access/edge layer ensures data is delivered to edge/end devices.

Answers

1. The star topology is commonly known as a hub and spoke model as it utilizes a centralized switch, or hub, and devices extend from it.
2. With a mesh topology, every node has a direct connection to every other node.
3. False. Traffic flows entering and leaving a datacenter are known as North-South traffic. East-West traffic refers to network traffic that flows within a datacenter between servers.
4. True. In the three-tier hierarchical model, the access/edge layer is the place where switches connect to and ensure data is delivered to edge/end devices.

A *topology* refers to a network's physical and logical layout. A network's *physical topology* refers to the actual layout of the computer cables and other network devices. A network's *logical topology* refers to the way in which the network appears to the devices that use it. Network topology diagrams are used to identify network components and how they are physically or logically connected.

Several topologies are in use on networks today. Some of the more common topologies are the star/hub and spoke, mesh, and hybrid models. The following sections provide an overview of each as well as look at some older topologies you may encounter.

Star/Hub and Spoke

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

Using a separate cable to connect to the hub or switch allows the network to be expanded without disruption. A break in any single cable does not cause the entire network to fail. Figure 2.1 shows a star/hub and spoke topology.

ExamAlert

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

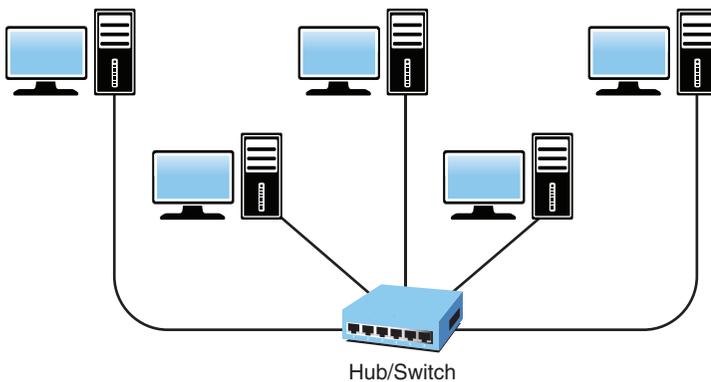


FIGURE 2.1 Star/Hub and Spoke Topology

The star/hub and spoke topology is the most widely implemented network design in use today, but it is not without shortcomings. Because all devices connect to a centralized hub or switch, this creates a single point of failure for the network. If the hub or switch fails, any device connected to it cannot access the network. Because of the number of cables required and the need for network devices, the cost of a star/hub and spoke network is often higher than other topologies. Table 2.1 summarizes the advantages and disadvantages of the star/hub and spoke topology.

TABLE 2.1 **Advantages and Disadvantages of the Star/Hub and Spoke Topology**

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

Mesh Topology

When it comes to the *mesh topology*, it is helpful to differentiate between a wired and wireless implementation, so we focus on the former here and the latter in Chapter 6, “Wireless Solutions.” Mesh incorporates a unique network design in which each computer on the network connects to every other, creating a point-to-point connection between every device on the network. Since this is often done physically, the term *wired mesh* or *wired mesh topology* is sometimes used. The purpose of the mesh design is to provide a high level of *redundancy*. If one network cable fails, the data always has an alternative path to get to its destination; each node can act as a relay.

The wiring for a mesh network can be complicated, as illustrated by Figure 2.2. Furthermore, the cabling costs associated with the mesh topology can be high, and troubleshooting a failed cable can be tricky. As a result, the mesh topology is not the first choice for many wired networks but is more popular with servers/routers.

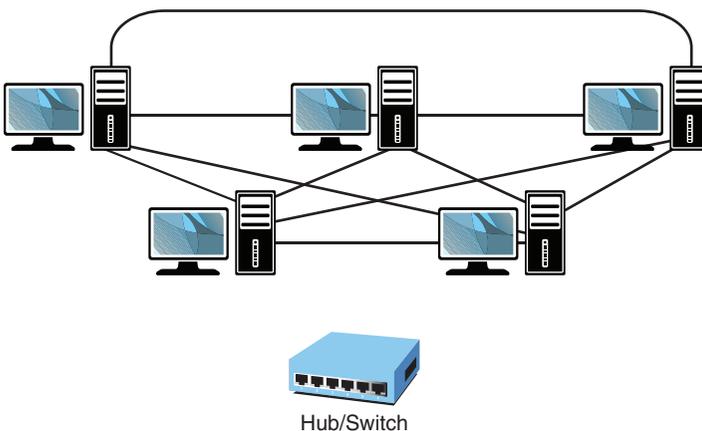
FIGURE 2.2 **Mesh Topology**

Table 2.2 summarizes the advantages and disadvantages of the mesh topology.

ExamAlert

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

Note

Fault tolerance is a process or capability of a network or system to continue working after there is a problem. It refers to a network or system's ability to continue operating after a malfunction or failure.

TABLE 2.2 **Advantages and Disadvantages of the Mesh Topology**

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

Hybrid Topology

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

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

Many of the topologies found in large networking environments are a hybrid of physical topologies. An example of a hybrid topology is the star/hub and spoke bus—a combination of the star/hub and spoke topology and the bus topology (explored further later in this chapter). Figure 2.3 shows how this might look in a network implementation.

ExamAlert

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

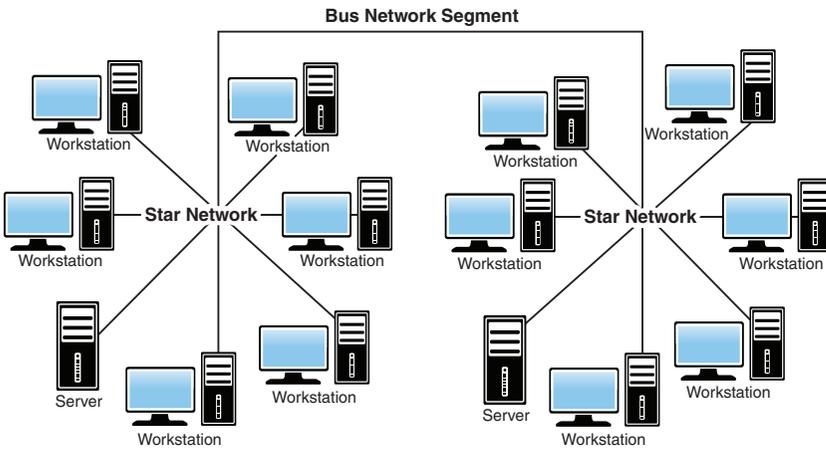


FIGURE 2.3 A Star/Hub and Spoke Bus Topology

Point to Point

A *point to point* (often written with hyphens: *point-to-point*) networking topology is a network configuration where two devices or nodes are directly connected to each other. In this topology, there is a dedicated communication link between the two endpoints, and data flows directly between them without the involvement of any intermediary devices. While the distinction can be nitpicky, mesh and star/hub and spoke networks are used to connect multiple devices to a network, while point-to-point topology is used to connect two devices.

It might not be the ideal choice for larger, more complex networks. In such cases, more scalable and flexible topologies like star/hub and spoke or mesh networks are typically preferred, since they can accommodate multiple devices and provide greater redundancy and fault tolerance.

Note

More information on point to point, as it relates to wireless networking, is provided in Chapter 6.

Spine and Leaf

Tiered models of computer network architecture are a way of organizing and structuring a network infrastructure into distinct layers (or *tiers*), each with specific functions and responsibilities. These models help simplify network design, management, and scalability.

A two-tier model that Cisco promotes for switches is the *spine and leaf* model. In this model, the spine is the *backbone* of the network, just as it would be in a skeleton and is responsible for interconnecting all the leaf switches in a full-mesh topology. Thanks to the mesh, every leaf is connected to every spine, and the path is randomly chosen so that the traffic load is evenly distributed among the top-tier switches. If one of the switches at the top tier were to fail, there would only be a slight degradation in performance throughout the datacenter.

Because of the design of this model, no matter which leaf switch is connected to a server, the traffic always has to cross the same number of devices to get to another server. This keeps latency at a steady level.

Note

Latency is the typical amount of time that it takes for packets of data to travel from one computer or system to the next. The higher the latency, the worse the experience when it comes to real-time video conferencing, webinars, gaming, and so on.

When *top-of-rack (ToR) switching* is incorporated into the network architecture, switches located within the same rack are connected to an in-rack network switch, which is connected to aggregation switches (usually via fiber cabling). The big advantage of this setup is that the switches within each rack can be connected with cheaper copper cabling and the cables to each rack are all that need to be fiber.

ExamAlert

Remember that in a spine and leaf model, the spine is the backbone of the network and is responsible for interconnecting all the leaf switches in a full-mesh topology. Know, as well, that all data flows require the same number of hops, they incorporate a full-mesh switching topology, and they use software-defined networking (SDN) to direct traffic, rather than blocking ports using the Spanning Tree Protocol (STP).

Three-Tier Hierarchical Model

Just as the spine and leaf is a two-tiered model, it is possible to improve system performance, as well as to improve security, by implementing an n -tiered model (wherein the n - can be one of several different numbers).

If we were looking at a database, for example, with a one-tier model, or single-tier environment, the database and the application exist on a single system. This is common on desktop systems running a standalone database. Early UNIX

implementations also worked in this manner; each user would sign on to a terminal and run a dedicated application that accessed the data. With two-tier architecture, the client workstation or system runs an application that communicates with the database that is running on a different server. This common implementation works well for many applications. With *three-tiered architecture*, otherwise known as a three-tier hierarchical model, security is enhanced. In this model, the end user is effectively isolated from the database by the introduction of a middle-tier server. This server accepts requests from clients, evaluates them, and then sends them on to the database server for processing. The database server sends the data back to the middle-tier server, which then sends the data to the client system. Becoming common in business today, this approach adds both capability and complexity.

While the examples are of database tiering, this same approach can be taken with devices such as routers, switches, and other servers. In a three-tiered model of routing and switching, the three tiers would be the core, the distribution/aggregation layer, and the access/edge. We walk through each of the layers present in this scenario.

Core Layer

The *core* layer is the backbone: the place where switching and routing meet (switching ends, routing begins). It provides high-speed, highly redundant forwarding services to move packets between distribution layer devices in different regions of the network. The core switches and routers would be the most powerful in the enterprise (in terms of their raw forwarding power) and would be used to manage the highest-speed connections (such as 100 Gigabit Ethernet). Core switches also incorporate internal firewall capability as part of their features, helping with segmentation and control of traffic moving from one part of the network to another.

Distribution/Aggregation Layer

The *distribution layer*, or *aggregation layer* (sometimes called the workgroup layer), is the layer in which management takes place. This is the place where Quality of Service (QoS) policies are managed, filtering is done, and routing takes place. Distribution layer devices can be used to manage individual branch-office WAN connections, and this is considered to be smart (usually offering a larger feature set than switches used at the access/edge layer). Lower latency and larger MAC address table sizes are important features for switches used at this level because they aggregate traffic from thousands of users rather than hundreds (as access/edge switches do).

Access/Edge Layer

Switches that allow end users and servers to connect to the enterprise are called access switches or edge switches, and the layer where they operate in the three-tiered model is known as the *access layer*, or *edge layer*. Devices at this layer may or may not provide Layer 3 switching services; the traditional focus is on minimizing the cost of each provisioned Ethernet port (known as “cost-per-port”) and providing high port density. Because the focus is on connecting client nodes, such as workstations to the network, this is sometimes called the desktop layer.

Note

As was discussed in Chapter 1, “Networking Models, Ports, Protocols, and Services,” a switch can work at either Layer 2 (the data link layer) or Layer 3 (the network layer) of the OSI model. When it filters traffic based on the MAC address, it is called a Layer 2 switch, since MAC addresses exist at Layer 2 of the OSI model (if it operated only with IP traffic, it would be a Layer 3 switch).

Table 2.3 highlights each of the layers of the three-tier hierarchical model.

TABLE 2.3 **Three-tier Hierarchical Model Layers**

Layer	Core	Distribution	Access
Description	Backbone of the network, provides high-speed connectivity between distribution layers and serves as a transit for all traffic	Aggregates traffic from access layer devices and distributes it to the appropriate destinations, provides policy enforcement and access control	Interfaces directly with end devices such as computers, printers, and IP phones, provides connectivity to the network
Function	Provides high-speed, low-latency forwarding of packets between distribution layer devices	Aggregates and filters traffic, enforces security policies, implements VLANs, routing protocols, and Quality of Service (QoS)	Delivers network services to end devices, such as Ethernet ports, wireless access points, and VLANs
Scale	Typically has the highest capacity and fastest speeds, often utilizes high-performance networking equipment	Capacity and performance requirements are moderate, often use Layer 3 switches and routers for routing and filtering	Usually consists of a large number of ports to accommodate end devices, employs switches with basic Layer 2 functionality

Layer	Core	Distribution	Access
Redundancy	Redundancy and high availability are critical, often implemented using redundant links and protocols like Virtual Router Redundancy Protocol (VRRP)	Redundancy is important but may not be as critical as in the core, often utilizes redundant uplinks and EtherChannel bundles	Redundancy is essential to ensure connectivity for end devices, typically implemented using redundant switches and network paths
Traffic flow	Handles transit traffic between distribution layer devices, typically high-speed and low-latency	Aggregates and filters traffic from access layer devices before forwarding it to the core or other distribution layer devices	Facilitates traffic between end devices and the rest of the network, including user data, management traffic, and control messages
Examples	High-speed routers, switches with large forwarding tables, MPLS networks	Layer 3 switches, VLANs, Quality of Service (QoS) policies, access control lists (ACLs)	Ethernet switches, wireless access points, Power over Ethernet (PoE) switches

ExamAlert

Remember: The core layer is the backbone of the network (where the fastest routers and switches operate to manage separate networks), whereas the distribution/aggregation layer (between the access/edge and core layers) is the “boundary” layer where ACLs and Layer 3 switches operate to properly manage data between VLANs and subnetworks. The access/edge layer is the place where switches connect to and ensure data is delivered to edge/end devices, such as computers and servers.

Collapsed Core

With a *collapsed core* architecture, the three-tier model becomes a two-tier model as the core and distribution layers are combined. While a three-tier model is necessary for complex installations that require access by multiple sites, devices, and users, the collapsed core approach is commonly used in datacenters and enterprise networks.

By collapsing the core and distribution layers into a single layer, the streamlined design provides both advantages and trade-offs. Advantages include simplicity, cost savings (via a reduced number of network devices and switches), efficient communication (with fewer layers, there are fewer network hops between devices), and scalability (it can scale relatively well for medium-sized networks and datacenters with a moderate number of devices). Disadvantages include limited redundancy (a failure at the collapsed core layer could

potentially impact the entire network), scalability constraints (it is not ideal for extremely large networks or datacenters with high traffic demands), and potential bottlenecks (there is a risk of network congestion if not properly designed and managed).

Traffic Flows

Traffic flows within a datacenter typically occur within the framework of one of two models: East-West or North-South. The names may not be the most intuitive, but the East-West traffic model means that data is flowing among devices within a specific datacenter, whereas North-South means that data is flowing into the datacenter (from a system physically outside the datacenter) or out of it (to a system physically outside the datacenter).

The naming convention comes from the way diagrams are drawn: data staying within the datacenter is traditionally drawn on the same horizontal line (East-to-West), while data leaving or entering is typically drawn on a vertical line (North-to-South). With the increase in virtualization being implemented at so many levels, the East-West traffic has increased in recent years. Table 2.4 summarizes the traffic flow possibilities.

Note

Network Functions Virtualization (NFV) is a network architecture concept that uses the proven technologies of IT virtualization. It delivers the network services needed to support an infrastructure independent from hardware by decoupling network functions from proprietary hardware appliances. This is covered in more detail in Chapter 7, “Cloud Computing Concepts and Options.”

TABLE 2.4 **Traffic Flow Options**

Traffic Flow	Description	Characteristics	Examples
North-South	Refers to the traffic flow between a client and external resources	Typically involves communication between internal users or devices and external networks or services	Internet browsing, accessing cloud services
East-West	Relates to the traffic flow between internal resources within a network	Occurs within the boundaries of a datacenter or local network, involving communication between servers, virtual machines, or applications	Inter-server communication, database queries

ExamAlert

East-West traffic is a concept referring to network traffic flow within a datacenter between servers. North-South refers to data transfers between the datacenter and outside the network.

Older Topologies: Bus and Ring

There are two topologies that have been removed from this iteration of the CompTIA Network+ exam objectives that you will very likely encounter in the workplace: bus and ring. For that reason, it is highly suggested that you be aware of them, and coverage of them is included at the end of this chapter rather than in with the exam fodder.

A *bus topology* uses a trunk or backbone to connect all the computers on the network, as shown in Figure 2.4. Systems connect to this backbone using *T connectors* or taps (known as a vampire tap, if you must pierce the wire). To avoid signal reflection, a physical bus topology requires that each end of the physical bus be terminated, with one end also being grounded. Note that a hub or switch is not needed in this installation, and loose or missing terminators from a bus network disrupt data transmissions.

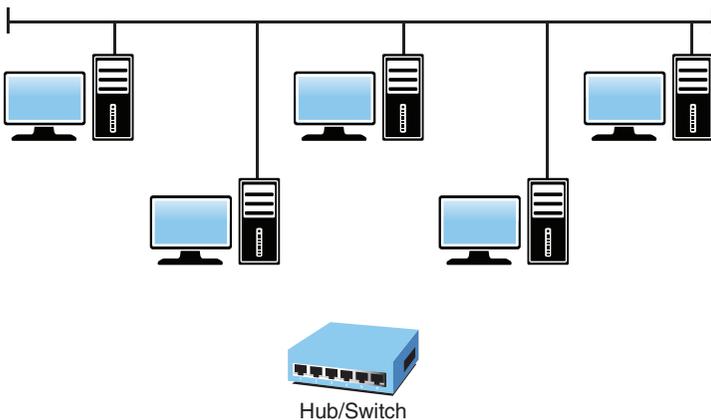


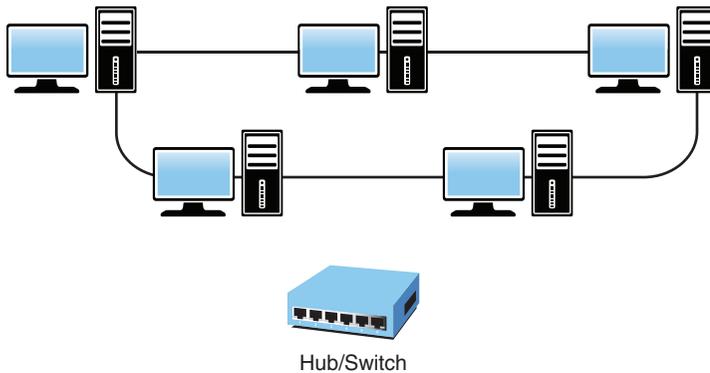
FIGURE 2.4 Physical Bus Topology

Table 2.5 summarizes the advantages and disadvantages of the bus topology.

TABLE 2.5 **Advantages and Disadvantages of the Bus Topology**

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

The *ring topology* is a logical ring, meaning that the data travels in a circular fashion from one computer to another on the network. It is not a physical ring topology. Figure 2.5 shows the logical layout of a ring topology. Note that a hub or switch is not needed in this installation either.

FIGURE 2.5 **Logical Design of a Ring Topology**

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

Ring networks can be set up in a fault-tolerant design, meaning that they have primary and secondary rings. If one ring fails, data can use the second ring to reach its destination. Naturally, the addition of the second ring adds to the cost of the network as well as the complexity. Table 2.6 summarizes the advantages and disadvantages of the ring topology.

TABLE 2.6 **Advantages and Disadvantages of the Ring Topology**

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

Cram Quiz

1. You have been asked to install a network that will give the network users the greatest amount of fault tolerance. Which of the following network topologies would you choose?
 - A. Star/hub and spoke
 - B. Ring
 - C. Mesh
 - D. Bus
2. Which of the following topologies allows for network expansion with the least amount of disruption for the current network users?
 - A. Bus
 - B. Ring
 - C. LAN
 - D. Star/hub and spoke
3. Which network topology offers the greatest level of redundancy but has the highest implementation cost?
 - A. Wireless mesh
 - B. Wired mesh
 - C. Hybrid star
 - D. Bus network
4. What traffic pattern refers to data that travels outside the datacenter or enterprise?
 - A. East-to-West
 - B. North-to-South
 - C. On-premises
 - D. West-to-South

5. What layer in three-tier hierarchical model network architecture is considered the backbone of a network?
- A. Core layer
 - B. Distribution/aggregation layer
 - C. Access/edge layer
 - D. Application layer
6. Which topology utilizes a dedicated connection between two endpoints?
- A. Mesh
 - B. Spine and leaf
 - C. Point to point
 - D. Star
7. Which topology is commonly used in datacenter environments for high scalability and flexibility?
- A. Ad hoc
 - B. Hybrid
 - C. Star
 - D. Spine and leaf
8. This network architecture includes simplicity, cost savings (via a reduced number of network devices and switches), efficient communication (with fewer layers, there are fewer network hops between devices), and scalability (it can scale relatively well for medium-sized networks and datacenters with a moderate number of devices). Which network architecture is being described?
- A. Collapsed core
 - B. NFV
 - C. ToR switching
 - D. Four-tier hierarchical model
9. Which layer in the three-tier hierarchical model network architecture facilitates traffic between end devices and the rest of the network?
- A. Core layer
 - B. Distribution layer
 - C. Point-to-point layer
 - D. Access layer

Cram Quiz Answers

- 1. C.** A mesh network uses a point-to-point connection to every device on the network. This creates multiple points for the data to be transmitted around the network and therefore creates a high degree of redundancy. The star/hub and spoke, ring, and bus topologies do not offer the greatest amount of fault tolerance.
- 2. D.** On a star/hub and spoke network, each network device uses a separate cable to make a point-to-point connection to a centralized device, such as a hub or a switch. With such a configuration, a new device can be added to the network by attaching the new device to the hub or switch with its own cable. This process does not disrupt the users who are currently on the network. Answers A and B are incorrect because the addition of new network devices on a ring or bus network can cause a disruption in the network and cause network services to be unavailable during the installation of a new device.
- 3. B.** The wired mesh topology requires each computer on the network to be individually connected to every other device. This configuration provides maximum reliability and redundancy for the network. However, it is very costly to implement because of the multiple wiring requirements.
- 4. B.** North-South refers to data transfers between the datacenter and outside of the network. East-West traffic is a concept referring to network traffic flow within a datacenter between servers. On-premises can be thought of as the old, traditional approach: the data and the servers are kept in-house. Although West-to-South is a direction, it is not a valid specified data path.
- 5. A.** The core layer is the backbone of the network where the fastest routers and switches operate to manage separate networks. The distribution/aggregation layer is between the access/edge and core layers. This is the “boundary” layer where ACLs and Layer 3 switches operate. The access/edge layer is the place where switches connect to and ensure data is delivered to edge/end devices. The application layer is the seventh and top layer of the OSI reference model.
- 6. C.** Point-to-point topology involves a direct link between two devices, providing a dedicated connection for communication. It’s commonly used in WAN connections, such as leased lines or serial connections.
- 7. D.** Spine and leaf topology is prevalent in datacenters due to its scalability and high-performance characteristics. It consists of spine switches interconnected with leaf switches, offering multiple paths and high bandwidth for data traffic.
- 8. A.** With a collapsed core architecture, the three-tier model becomes a two-tier model as the core and distribution layers are combined. By collapsing the core and distribution layers into a single layer, the streamlined design provides both advantages and trade-offs. Advantages include simplicity, cost savings (via a reduced number of network devices and switches), efficient communication (with fewer layers, there are fewer network hops between devices), and scalability (it can scale relatively well for medium-sized networks and datacenters with a moderate number of devices). Network Functions Virtualization (NFV) is a technology that allows for the virtualization of a replica of a network’s physical topology and the way it behaves without changing the logical topology and the way that devices are managed. NFV allows for the virtualization of network functions such

as routers, firewalls, and switches, resulting in increased flexibility and scalability. When top-of-rack (ToR) switching is incorporated into the network architecture, switches located within the same rack are connected to an in-rack network switch, which is connected to aggregation switches (usually via fiber cabling). There is no such thing as the four-tier hierarchical model.

9. **D.** The access layer in three-tier hierarchical model network architecture facilitates traffic between end devices and the rest of the network, including user data, management traffic, and control messages. The core layer is the backbone of the network, provides high-speed connectivity between distribution layers, and serves as a transit for all traffic. The distribution layer aggregates and filters traffic; enforces security policies; and implements VLANs, routing protocols, and Quality of Service (QoS). Point to point is not a layer in the three-tier hierarchical model. It is a network configuration where two devices or nodes are directly connected to each other. In this topology, there is a dedicated communication link between the two endpoints, and data flows directly between them without the involvement of any intermediary devices.
-

What's Next?

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

This page intentionally left blank

This page intentionally left blank

Index

Numerics

4G, 186
5G, 186
10BASE-T, 206
10GBASE-LR/10GBASE-SR, 209
10GBASE-T, 208
40GBASE-T, 207–209
66 block, 295–296
100BASE-FX, 207
100BASE-TX, 206–207
110 block, 295–296
568A and 568B wiring standards,
202–203
802.1Q, 95, 96, 101–102
802.1X, 410
802.11a, 241
802.11ac, 243, 245
802.11ax, 244, 245
802.11b/g, 243
802.11h, 242
1000BASE-LX/1000-BASE-SX, 209
1000BASE-T, 207–208

A

AAA (authentication, accounting, and
authorization), 102
absorption, 482
access control, 388, 392–393
802.1X, 410
discretionary, 389–390
EAP (Extensible Authentication
Protocol), 410–411

access control

- geofencing, 413–414
- mandatory, 389
- network, 411–412
- role-based, 390–391
- rule-based, 390
- vestibule, 414

access/edge layer, 51**ACL (access control list), 140–141, 389, 443, 473****active-active, 369****active-passive, 369****ad hoc discovery, 354****ad hoc network, 251****address class, IPv4, 63–64****address pool, 23, 109****address translation, 90**

NAT (Network Address Translation), 90–92

PAT (Port Address Translation), 92

administrative distance, 89**agent, SNMP (Simple Network Management Protocol), 27–28****agreement**

- non-disclosure, 320
- privileged user, 325
- service-level, 320

AH (Authentication Header), 18, 150**algorithm, SPF (shortest path first), 86****antenna**

- AP (access point), 477
- coverage, 249–250
- directional, 250
- isotropic, 249
- MIMO (multiple input, multiple output), 243, 248
- MU-MIMO (multiuser multiple input, multiple output), 248
- omnidirectional, 249–250
- placement, 4445
- polarization, 250
- ratings, 248–249

antivirus software, 431–432**anycast, 37****anycast address, 173****AP (access point), 144–145. See also antenna**

- antenna, 477
- association, 253, 254
- authentication, 254, 259–260
- autonomous, 262
- BSSID (basic service set identifier), 254–255
- client dissociation, 479
- coverage, troubleshooting, 483–485
- ESSID (extended service set identifier), 254–255
- lightweight, 262
- reassociation, 253
- roaming misconfiguration, 485
- rogue, 427
- SSID (service set identifier), 254–255, 258
- thick/thin, 477

APC (angled physical contact), 199**API (application programming interface), 351, 379****APIPA (Automatic Private IP Addressing), 73–74****application, logs, 347****application layer, OSI (Open Systems Interconnection) model, 7****ARP (Address Resolution Protocol), 510–512**

- poisoning, 429
- spoofing, 428–429

asset

- disposal, 437
- inventory, documentation, 306
- tags, 415

association, 253, 254**asymmetric key cryptography, 403****attack/s**

- ARP poisoning, 429
- brute force, 430
- disassociation, 430

DoS (denial-of-service), 422
 buffer overflow, 423
 distributed reflective, 423
 fraggle, 422
 ICMP flood, 424
 ping of death, 423
 smurf, 423
 SYN flood, 423
 evil twin, 427
 logic bomb, 426
 MAC flooding, 426
 on-path, 430
 phishing, 427–428
 ransomware, 428
 rouge DHCP server, 426–427
 social engineering, 424–426
 spoofing, 428
 ARP, 428–429
 DNS, 429
 VLAN hopping, 430–431
 zero-day, 387

attenuation, 191

auditing, 408

AUP (acceptable use policy), 319, 446

authentication
 AP (access point), 254, 259–260
 WEP (Wired Equivalent Privacy), 259
 WPA (Wi-Fi Protected Access), 259–261
 WPA-PSK (Wi-Fi Protected Access with Pre-Shared Key), 259
 de-, 430
 Kerberos, 401–403
 local
 certificates, 404–405
 LDAP (Lightweight Directory Access Protocol), 403–404
 multifactor, 406, 407–408
 preshared keys, 445
 RADIUS (Remote Authentication Dial-In User Service), 400

TACACS (Terminal Access Controller Access Control System), 400–401
 time-based, 407–408

authorization, 405

autonomous AP, 262

availability, 355, 387

B

backbone, 49, 50

backup, 361, 363

best practices, 365

cloud, 364

configuration, 328

differential, 362

full, 361–362

incremental, 362–363

band steering, 241

bandwidth, 152, 184, 336

speed tester, 494

tester, 217–218

versus throughput, 217

troubleshooting, 463

baseband transmission, 183

baseline/golden configuration, 316–317

BCP (business continuity plan), 320

best-effort delivery, 14, 17

BGP (Border Gateway Protocol), 86

Bix, 296

black box/unknown environment test, 416–417

BNC (Bayonet Neill-Concelman connector), 195–196

BOOTP (BOOT Protocol), 73

bottlenecking, troubleshooting, 463

bottom-to-top troubleshooting, 453

BPDU (bridge protocol data unit), 104

bps (bits per second), 216

branching, 169

broadband transmission, 183

broadcast

broadcast, 37, 66

- BOOTP, 73
- domain, 65
- storm, 465

brute force attack, 430

BSSID (basic service set identifier), 254–255

buffer overflow, 423

buffering, 6

bus topology, 54–55

BYOD (bring-your-own-device) policy, 261–262, 318, 396, 473

C

CA (certificate authority), 404, 471

cable

- copper, 187
 - coax, 191–192
 - DAC (direct attach copper), 192–193
 - twisted-pair, 188–190
- crimper, 229–230
- cross-connects, 291
- crossover, 203–205
- damaged, 218
- Ethernet standards, 207
 - 10BASE-T, 206
 - 10GBASE-LR/10GBASE-SR, 209
 - 10GBASE-T, 208
 - 40GBASE-T, 207–209
 - 100BASE-FX, 207
 - 100BASE-TX, 206–207
 - 1000BASE-LX/1000-BASE-SX, 209
 - 1000BASE-T, 207–208
- fiber-optic, 193
 - cladding, 193
 - modes, 194
- horizontal, 291, 292–293
- loopback, 206
- maps, 308

media connectors

- 568A and 568B wiring standards, 202–203
- BNC (Bayonet Neill-Concelman), 195–196
- fiber, 198–200
- F-type, 197–198
- RJ-11, 195–196
- RJ-45, 197

media converter, 201–202

patch, 293

plenum-rated, 195, 312

rollover, 205

tester, 233, 490

troubleshooting common

- connectivity issues, 215–216, 217–219
 - bad ports, 221–222, 223
 - dirty optical cables, 224
 - improper termination, 220–221
 - incorrect pinout, 221
 - interface issues, 224–226
 - interference, 220
 - signal degradation, 219–220
 - TX/RX reversed, 223–224
- vertical, 291, 293

caching, 140

calculator, CIDR, 68

captive portal, 256, 446

capturing, 317

CDMA (code-division multiple access), 185–186

CDN (content delivery network), 145–146

CDP (Cisco Discovery Protocol), 497

cellular technology, 185

4G, 186

5G, 186

GSM (Global System for Mobile Communications), 185–186

LTE (Long-Term Evolution), 186

central repository, 169

certificates, 404–405

change management,
documentation, 327

channel/s, 242, 244–245, 255

- bonding, 247–248
- overlap, 242–243, 482
- width, 240–241

CIA triad, 387

CIDR (classless interdomain routing),
66, 68

- calculator, 68
- slash, 68

circuit switching, 84

cladding, 193

client

- DNS, 113
- server protocol, FTP, 21
- to-site VPN, 377–378

cloud/cloud computing, 269

- backups, 364
- bursting, 277
- community, 277
- connectivity options, 280–281
- deployment models, 277–278
- elasticity, 279
- gateway, 282
- hybrid, 276–277
- IaC (Infrastructure as Code), 166–169
- multitenancy, 278
- NSG (network security group), 284–285
- private, 276
- public, 276
- scalability, 279
- security, 283–285
- service models, 274–275
 - IaaS (Infrastructure as a Service), 273–274
 - PaaS (Platform as a Service), 272–273
 - SaaS (Software as a Service), 271–272
- virtual private, 281–282

clustering, 369

coax cable, thicknet, 191

cold site, 366

collapsed core architecture, 52–53

collision domain, 65

command/s

- arp, 510–512
 - dig, 523–524
 - hostname, 510
 - ip route, 468
 - ipconfig, 243, 521–522
 - ipconfig / all, 518–521
 - ipconfig / release, 470
 - iwconfig, 243
 - log management, 349
 - netstat, 512–514
 - netstat -a, 495–496, 515–516
 - netstat -e, 514
 - netstat -r, 516
 - netstat -s, 517–518
 - nslookup, 522–523
 - ping, 222, 468, 494, 504–505, 508–509
 - “Destination Host Unreachable” error message, 505–506
 - expired TTL message, 508
 - “Request Timed Out” error message, 506–507
 - route, 525–526
 - route add, 82
 - route print, 80
 - show, 526–527
 - show interface, 80
 - SNMP (Simple Network Management Protocol), 28
 - tcpdump, 525
 - traceroute, 134, 500–504
 - tracert, 87
 - troubleshooting, 498–500
- communities, SNMP (Simple Network Management Protocol), 29**
- community cloud, 277**

compliance, regulatory

compliance, regulatory, 409

confidentiality, 136, 387

configuration

backup, 328

management, documentation, 328

monitoring, 355

production, 328

congestion/contention, troubleshooting, 462

connectionless protocols, 14

ICMP (Internet Control Message Protocol), 17

IP (Internet Protocol), 14–15

UDP (User Datagram Protocol), 16–17

connection-oriented protocols, 14, 15–16

console, 379

consultancy, documentation, 306

content filtering, 440

content switch, 133–134

contract work, documentation, 306

Control Plane Policing, 441

conversion

decimal-to-binary, 63

media, 201–202

copper cable, 187

coax, 191

thicknet, 191

thin, 191–192

DAC (direct attach copper), 192–193

twisted-pair, 188

categories, 189–190

shielded, 188

unshielded, 188

core layer, 50

CoS (class of service), 152

CRC (cyclic redundancy check), 225, 337–338

CRL (certificate revocation list), 404

cross-connects, 291–292

crossover cable, 203–205

crosstalk, 191

cryptography, 402

asymmetric key, 403

key management, 438–440

secret key, 402

symmetric key, 402

cut-through switching, 132

CVE (common vulnerabilities and exposures), 388

CVSS (Common Vulnerability Scoring System), 387

CWDM (coarse wavelength-division multiplexing), 210

cybersecurity insurance, 416

D

DAC (direct attach copper), 192–193

DAC (discretionary access control), 389–390

DAI (Dynamic ARP Inspection), 441

dashboard, SIEM, 417

data. See also transmission

integrity, 387

at rest, 388

sovereignty requirements, 409

in transit, 388

data flow control, 6

data link layer

OSI (Open Systems Interconnection) model, 4

VLAN, 96

data rate, 246–247

datagram packet switching, 83–84

dB loss, 219

DCI (Data Center Interconnect), 163

deauthentication, 430

decapsulation, GRE (Generic Routing Encapsulation), 20. See also encapsulation

decimal-to-binary conversion, 63

decommissioning, 326

default gateway, 68–70, 79–80

default port, 34–35

default route, 82, 467–468

default subnet mask, 64–65

defense in depth, 393

network segmentation, 393–397

screened subnet, 397–398

separation of duties, 398

deployment model, 277–278

hybrid cloud, 276–277

private cloud, 276

public cloud, 276

device/s. See also router; switch/switching

bring-your-own-, 396

conflicting, 478

IoT/IIoT, 394–395

mapping to OSI model, 9

DFS (Dynamic Frequency Selection), 242

DHCP (Dynamic Host Configuration Protocol), 23–24, 70–71, 108–109, 110–111

address pool, 109, 472

advantages, 109

and DNS suffixes, 111

expired address, troubleshooting, 470

IP helper, 112

lease, 71

lease time, 109

relays, 112

reservation, 109–110

rogue server, 426

rogue server, troubleshooting, 471

scopes, 71, 109

server, 71

snooping, 442

version 6, 110

DHCP6, 73

diagram

network layer, 308

physical/logical network, 313–316

rack, 308

dialog modes, 184

differential backup, 362

dig command, 523–524

directional antenna, 250

disassociation attack, 430

disaster recovery, 319–320, 361

backups, 361, 363

best practices, 365

cloud, 364

differential, 362

full, 361–362

incremental, 362–363

cold site, 366

hot site, 366–367

snapshots, 364–365

testing, 370

disposing of assets, 437

distance-vector routing protocol, 85–86, 88

distributed reflective DoS attack, 423

distribution/aggregation layer, 50

DLP (data loss prevention), 319

DNS (Domain Name System), 23, 71, 112–114

authoritative server, 118–119

clients, 113

FQDN (fully qualified domain name), 115

namespace, 114–116

over HTTPS, 119

over TLS, 120

practical implementation, 119–120

records, 117–119

root server, 115

spoofing, 429

suffixes, 111

troubleshooting, 468

types of entries, 117

DNSSEC (Domain Name System Security Extensions), 119

documentation, 306

change management, 327

- configuration management, 328
- network, 306–307, 309
 - baseline/golden configuration, 316–317
 - cable maps and rack diagrams, 308
 - floor plan, 307
 - IDF/MDF, 308
 - physical and logical diagrams, 313–316
 - server configuration, 308
 - services, 309
 - standard operating procedures, 310
 - topology, 307
 - wireless survey report, 309
 - wiring schematics, 310, 312
- troubleshooting, 457

DoH (DNS over HTTPS), 119–120**DoS (denial-of-service) attacks, 422**

- buffer overflow, 423
- distributed reflective, 423
- fraggle, 422
- ICMP flood, 424
- ping of death, 423
- smurf, 423
- SYN flood, 423

DoT (DNS over TLS), 120**dotted-decimal format, 64–65****downgrading, 353****driver, updates, 353****DTIM (Delivery Traffic Indication Message), 261****DTLS (Datagram Transport Layer Security), 151****duplicate IP address, troubleshooting, 469****duplicate MAC address, troubleshooting, 469–470****DWDM (dense wavelength-division multiplexing), 210****dynamic addressing, 70–73. See also DHCP (Dynamic Host Configuration Protocol)****dynamic inventory, 168****dynamic routing, 5, 82, 85–89****E**

EAP (Extensible Authentication Protocol), 410–411**East-West traffic model, 53****eavesdropping, 401****EIA/TIA (Electronic Industries Alliance/Telecommunications Industry Association), 188, 202–203****EIGRP, 86****EIRP (Effective Isotropic Radiated Power), 478****elasticity, 279****email**

- phishing, 427–428
- usage policy, 319

EMI (electromagnetic interference), 220**employee**

- onboarding/offboarding policies, 318–321
- phishing, 427–428
- training, 415

encapsulation, 10–11, 20

- GRE (Generic Routing Encapsulation), 19
- Layer 2, 162–163

encryption, 7, 388, 478**environment, telecommunications/computer room**

- fire suppression, 301
- heat/temperature, 301
- humidity, 301

EOL (end-of-life), 325–326**EOS (end-of-support), 325–326****equipment**

- decommissioning, 326
- port-side exhaust/intake, 298
- rack size, 297–298

error checking, 5

ESP (Encapsulating Security Payload), 18, 150

ESSID (extended service set identifier), 254–255

Ethernet

- 10BASE-T, 206
- 10GBASE-LR/10GBASE-SR, 209
- 10GBASE-T, 208
- 40GBASE-T, 207–209
- 100BASE-FX, 207
- 100BASE-TX, 206–207
- 1000BASE-LX/1000-BASE-SX, 209
- Fast, 207
- Fibre Channel over, 143
- Gigabit, 207–208
- Power over, 218–219, 227

EUI-48, 76

EUI-64, 76

event log, 346, 408

evil twin attack, 427

exploit, 353

external threats, 387

F

Fast Ethernet, 207

fault detection, 337

fault tolerance, 47, 368

FCoE (Fibre Channel over Ethernet), 143

FDM (frequency-division multiplexing), 183

FHRP (First Hop Redundancy Protocol), 93

fiber connectors, 198–200

fiber light meter, 234

fiber transceiver, 200

fiber-optic cable, 193
 cladding, 193
 modes, 194

Fibre Channel, 143

file hashing, 444

FileZilla, 20–21

filtering

- content, 440
- MAC, 412–413
- MAC address, 257
- URL, 440

fire suppression, 301

firewall, 134–135, 136

- hardware, 135
- rules, 443
- troubleshooting, 472–473
- web application, 136

firmware, updates, 352

floor plan, 307

flow control, 101

FQDN (fully qualified domain name), 115

fraggle attack, 422

fragmentation, 15

fragment-free switching, 132

frame

- giant, 224
- jumbo, 105
- runt, 105, 224, 462

FTP (File Transfer Protocol), 20–21, 430

F-type connector, 197–200

full backup, 361–362

full-duplex mode, 184

fusion splicer, 234

G

gateway, 282–283

GBIC (gigabit interface converter) module, 200

Gbps (gigabits per second), 184

GDPR (General Data Protection Regulation), 409

geofencing, 413–414

giant frame, 224

Gigabit Ethernet, 207–208

golden configuration, 316–317

goodput, 247

GPS (Global Positioning System), 121

gray box/partially known environment test, 416–417

GRE (Generic Routing Encapsulation), 19–20, 174–175

guest network, 255–256

GUI (graphical user interface), 379

H

half-duplex mode, 184

hardening best practices, 440–444

hardware. *See also* tool/s

decommissioning, 326

disposal, 437

firewall, 135

redundant, 368

troubleshooting, 227, 228, 474–475

header, GRE (Generic Routing Encapsulation), 19–20

heat, 301

heat map, 309, 481

high availability

active-active, 369

active-passive, 369

high throughput, 247

history logs, 349

honeynet, 399

honeypot, 399

hops, 87, 90

horizontal cable, 291, 292–293

host, 62

hostname command, 510

hot site, 366–367

HTML (Hypertext Markup Language), 25

HTTP (Hypertext Transfer Protocol), 25

HTTPS (Hypertext Transfer Protocol Secure), 31

hub-and-spoke topology, 45–46, 315

humidity, 301

HVAC (heating, ventilation, and air conditioning), 191, 195, 301

hybrid cloud, 276–277

hybrid topology, 47

I

IaC (Infrastructure as Code), 166–169

IAM (identity and access management), 405

identity lifecycle management, 405

SAML (Security Assertion Markup Language), 406–407

SSO (single sign-on), 405

IANA (Internet Assigned Numbers Authority), 66, 67

ICMP (Internet Control Message Protocol), 17

ICMP flood, 424

ICS (industrial control systems), 395–396

IDC (insulation displacement connector), 294

identity federation, 406

IDF (intermediate distribution frame), 296, 308

IDS (intrusion detection system), 136–138

IEEE 802.1Q, 95, 96, 101–102

IEEE 802.1X, 326

IETF (Internet Engineering Task Force), RFC (Request For Comments), 15

IIoT (Industrial Internet of Things), 394–395

IKE (Internet Key Exchange), 18–19

implicit deny, 136

in-band management, 381

incident response, 319

incremental backup, 362–363

independent routing, 83

infrastructure network, 251

integrity, 387

interface. See also port/s

- administratively down, 225
- monitoring, 338
- troubleshooting, 224–226

interference

- electromagnetic, 220
- radio frequency, 433–434
- troubleshooting, 220
- wireless, 481–482

internal threats, 387**international export policy, 319****Internet**

- gateway, 282–283
- satellite, 186–187
- usage policy, 318

IoT (Internet of Things), 394–395**IP (Internet Protocol), 14–15****ip route command, 468****IP scanner, 498****ipconfig / all command, 518–521****ipconfig / release command, 470****ipconfig command, 243, 521–522****IPS (intrusion prevention system), 136–138****IPsec, 18–19, 150–151****IPv4, 62. See also address translation**

- address classes, 63–64
- APIPA (Automatic Private IP Addressing), 73–74
- CIDR (classless interdomain routing), 66, 68
 - calculator, 68
 - slash, 68
- comparison with IPv6, 174
- decimal-to-binary conversion, 63
- default gateway, 68–70
- duplicate address, troubleshooting, 469
- dynamic addressing, 70–73
- expired address, troubleshooting, 470
- local loopback, 64
- octet, 63

- private address ranges, 67
- static addressing, 70
- subnet mask, 63
 - default, 64–65
 - troubleshooting, 469
 - variable-length, 66
- subnetting, 65–66

IPv6, 169

- address exhaustion, 170
- anycast address, 173
- comparison with IPv4, 174
- compatibility requirements, 174–175
- identifying IPv6 addresses, 170–172
- link-local address, 172
- multicast address, 173
- RA (Router Advertisement) guard, 441
- site-local address, 172–173
- unicast address, 172

iSCSI (Internet Small Computer Systems Interface), 143**ISO (International Organization for Standardization), 28. See also OSI (Open Systems Interconnection) model****isolation, 445****isotropic antenna, 249****ISP (Internet service provider), 67, 119, 186****iwconfig command, 243**

J**jitter, 337, 464–465****jumbo frame, 102, 105****jump box, 380–381**

K**Kerberos, 401–403****key management, 438–440, 445****Krone, 296**

L

labeling, 330

LACP (Link Aggregation Control Protocol), 97

latency, 90, 151–152, 336, 463–464

Layer 2 switch, 133

LDAP (Lightweight Directory Access Protocol), 30, 403–404

LDAPS (Lightweight Directory Access Protocol over SSL), 32

lease, **DHCP (Dynamic Host Configuration Protocol)**, 71

lightweight AP, 262

link-local address, 172

link-state routing protocol, 86, 88–89

LLC (logical link control) layer, 4

LLDP (Link Layer Discovery Protocol), 497

load balancer, 138–139, 368

load test, 344

local authentication

- certificates, 404–405
- LDAP (Lightweight Directory Access Protocol), 403–404

local loopback, 64

lockable environment, 298–299, 414–415

log management command, 349

logic bomb, 426

logical network diagram, 313–316

log/s

- aggregation, 349–350
- application, 347
- event, 346
- history, 349
- management, 349–350
- security, 346–347
- syslog, 31–32, 350
- system, 348

looking-glass site, 217–218, 494

loopback adapter, 231

loopback cable, 206

low optical link budget, troubleshooting, 468

LWAPP (Lightweight Access Point Protocol), 477

M

MAC (mandatory access control), 389

MAC (media access control) layer, 4

MAC address, 74–75

- BSSID (basic service set identifier), 254–255
- duplicate, troubleshooting, 469–470
- EUI-48, 76
- EUI-64, 76
- filtering, 257, 412–413
- NIC, 75
- OUI (organizationally unique identifier), 75
- universal LAN MAC address, 75

MAC flooding, 426

major update, 353

malware, 431–433

MAM (mobile application management), 396–397

management system, **SNMP (Simple Network Management Protocol)**, 27

mapping network devices to OSI model, 9

Mbps (megabits per second), 184

MDF (main distribution frame), 296, 308

MDI-X (medium-dependent interface crossed), 133

MDM (mobile device management), 318, 396–397

media connector

- 568A and 568B wiring standards, 202–203
- BNC (Bayonet Neill-Concelman), 195–196
- fiber, 198–200
- F-type, 197–198

- RJ-11, 195–196
 - RJ-45, 197
 - transceivers, 200–201
 - media converter, 201–202**
 - membership, VLAN, 97–98**
 - mesh network, 251, 252**
 - mesh topology, 46–47**
 - message logging, syslog, 31–32**
 - methodology, troubleshooting, 450–451**
 - document findings, actions, outcomes, and lessons learned, 457
 - establish a plan of action, 454–455
 - establish a theory of probable cause, 453–454
 - identify the problem, 451–452
 - approach multiple problems individually, 453
 - determine if anything has changed, 452
 - duplicate the problem if possible, 453
 - identify symptoms, 452
 - implement the solution or escalate, 455–456
 - test the theory to determine the cause, 454
 - verify full system functionality, 456
 - metrics, 89–90, 335–337**
 - MFA (multifactor authentication), 406, 407–408**
 - MIB (management information base), 340–341**
 - MIBs (Management Information Bases), 28**
 - MIMO (multiple input, multiple output) antenna, 243, 248**
 - minor update, 353**
 - Miredo, 92**
 - mobile device, onboarding, 318**
 - monitoring**
 - configuration, 355
 - events, 408
 - interface, 338
 - network
 - availability, 355
 - performance, 334–335, 337
 - traffic analysis, 354–355
 - power, 338
 - security, 337–338
 - motion detection, 414**
 - MOU (memorandum of understanding), 320**
 - MPO (multifiber push-on) connector, 199–200**
 - MTBF (mean time between failures), 367**
 - MTTR (mean time to recovery), 367**
 - MTU (maximum transmission unit), 15, 90, 105, 222**
 - multicast address, 173**
 - multicast flooding, 465**
 - multicasting, 37, 261**
 - multilayer switch, 133**
 - multimeter, 232–233**
 - multimode fiber, 194**
 - multipathing, 368**
 - multiplexing, 210**
 - coarse wavelength-division, 210
 - dense wavelength-division, 210
 - multitenancy, 278**
 - MU-MIMO (multiuser multiple input, multiple output) antenna, 248**
 - MySQL, 33**
-
- ## N
- NAC (network access control), 396, 411–412**
 - NAC (network admission control), 326**
 - namespace, DNS (Domain Name System), 114–116**
 - NAS (network-attached storage), 141–142**
 - NAT (Network Address Translation), 90–92, 283**
 - NDA (non-disclosure agreement), 320**

NetFlow analyzer, 498**netstat -a command, 495–496, 515–516****netstat command, 512–514****netstat -e command, 514****netstat -r command, 516****netstat -s command, 517–518****network layer**

diagram, 308

OSI (Open Systems Interconnection)

model, 5, 19

network/s. See also transmission; VPN; wireless network

access, 375–376

client-to-site VPN, 377–378

jump box, 380–381

site-to-site VPN, 376–377

access control, 411–412

backbone, 49, 50

connection methods, 378–380

content delivery, 145–146

controller, 390, 412

discovery, 354

documentation, 306–307, 309

baseline/golden configuration, 316–317

cable maps and rack diagrams, 308

floor plan, 307

IDF/MDF, 308

physical and logical diagrams, 313–316

standard operating procedures, 310

topology, 307

wireless survey report, 309

wiring schematics, 310, 312, 313

guest, 255–256

hardening best practices, 440–444

installation. *See also* cable; equipment; wiring closet

port-side exhaust/intake, 298

rack size, 297–298

monitoring. *See also* log/s

availability, 355

port mirroring, 351

traffic analysis, 354–355

node, 62

performance

metrics, 335–337

monitoring, 334–335

test, 343–344

physical installation, 290–291

policies, 318

private, 66–67

procedures, 324–325

public, 66–67

quarantine, 411

regulations, 328–329

segmentation, 393–397

software-defined. *See* SDN (software-defined networking)

storage-area, 142

topology, 44

bus, 54–55

collapsed core, 52–53

hybrid, 47

mesh, 46–47

point to point, 48

ring, 55–56

spine and leaf, 48–49

star/hub and spoke, 45–46

three-tier hierarchical, 49–52

troubleshooting, 461

ACL (access control list), 473

address pool exhaustion, 472

asymmetrical routing, 465

bandwidth/throughput capacity, 463

blocked ports, services, or addresses, 472

bottlenecking, 463

broadcast storm, 465

CA (certificate authority), 471

congestion/contention, 462

default route, 467–468

- DNS issues, 468
- duplicate IP address, 469
- duplicate MAC address, 469–470
- firewall, 472–473
- hardware, 474–475
- incorrect gateway, 468–469
- incorrect subnet mask, 469
- jitter, 464–465
- latency, 463–464
- licensed feature issues, 473
- low optical link budget, 468
- missing route, 467
- multicast flooding, 465
- NTP, 472
- packet loss, 464
- rogue DHCP server, 471
- route selection, 467
- routing loops, 467
- virtual private. *See* VPN (virtual private network)
- zones, 445–446

NFV (Network Functions Virtualization), 53–54, 279–280

NIC (network interface card), 75, 369

NIST (National Institute of Standards and Technology)

- Digital Identity Guidelines, 324
- SP 800–145, 270

Nmap, 496

NMS (network management system), 27

node, 62

North-South traffic model, 53

NOS (network operating system), 317

NSG (network security group), 284–285

nslookup command, 522–523

NTP (Network Time Protocol), 25, 120–121

- stratum, 120
- troubleshooting, 472

NTS (Network Time Security), 121

O

octet, 63

OFDM (orthogonal frequency-division multiplexing), 247

offboarding, 318–321

omnidirectional antenna, 249–250

onboarding, 318–321

open/short faults, troubleshooting, 222

OSI (Open Systems Interconnection) model, 1, 2, 7–8. *See also* protocols

- application layer, 7
- comparing with TCP/IP model, 8–9
- data link layer, 4
- encapsulation/decapsulation, 10–11
- mapping to network devices, 9
- network layer, 5, 19
- physical layer, 36
- presentation layer, 6–7
- session layer, 6
- transport layer, 5–6

OT (operational technology), 395–396

OTDR (optical time-domain reflectometer), 232

OUI (organizationally unique identifier), 75

out-of-band management, 381, 382

P

PaaS (Platform as a Service), 272–273

packet, 5, 83

- capture, 338
- drops, 224
- fragmentation, 15
- loss, troubleshooting, 464
- MTU (maximum transmission unit), 105
- TTL (time to live), 153

packet switching, 83–84

PAM (privileged access management), 406

partial mesh network, 47

passive reconnaissance

passive reconnaissance, 416

password

 policies, 321–324

 policy, 319, 442

PAT (Port Address Translation), 92

patch cables, 293

patch management, 351–352, 443

patch panel, 294

PDU (power distribution unit), 300

PDU (protocol data unit), 11

penetration test, 369, 416–417

performance

 baseline, 316–317

 metrics, 345

 network

 metrics, 335–337

 monitoring, 334–335

 test, 343–344

 wireless, troubleshooting, 476–480

personal software policy, 319

phishing, 427–428

physical address, 74. See also MAC address

physical layer

 OSI model, 4

 troubleshooting, 3

physical network diagram, 313–316

physical security, 414–415

ping of death, 423

ping utility, 17, 222, 468, 494, 504–505, 508–509

 “Destination Host Unreachable”

 error message, 505–506

 expired TTL message, 508

 “Request Timed Out” error message, 506–507

PKI (public key infrastructure), 444

playbooks, 167–168

plenum, 191, 195

PoE (Power over Ethernet), 218–219, 227

point to point network, 48

point-to-point network, 251–252

poison reverse, 88

polarization, 250

policy/ies, 318. See also procedures; regulations

 antivirus, 432–433

 BYOD (bring-your-own-device), 261–262, 396

 employee onboarding/offboarding, 318–321

 network, 318

 ownership, 321

 password, 321–324

 safety, 321

POP3 (Post Office Protocol version 3), 23

port/s

 aggregation, 369

 –based VLAN, 97–98

 binding, 97

 default, 34–35

 functions, 34–35

 MDI (medium-dependent interface), 133

 MDI-X (medium-dependent interface crossed), 133

 mirroring, 101, 351

 scanner, 494–496

 security, 102

 state, 104–105

 TCP/UDP, 35–36

 troubleshooting, 221–222, 472

 TX/RX, 201

 well-known, 35

posture assessment, 412

power management

 PDU (power distribution unit), 300

 threats, 300

 UPS (uninterruptible power supply), 299

prefix length, 89

presentation layer, OSI (Open Systems Interconnection) model, 6–7

preshared keys, 445

private address ranges, 67

private cloud, 276

private network, 66–67

privileged user agreement, 325

procedures

network, 324–325

remote-access, 326

for reporting violations, 326

production configuration, 328

protocol/s, 13, 497. See also DHCP (Dynamic Host Configuration Protocol)

analyzer, 493–494

-based VLAN, 97

BOOTP (BOOT Protocol), 73

connectionless, 14

connection-oriented, 14

DHCP (Dynamic Host Configuration Protocol), 23–24

EAP (Extensible Authentication Protocol), 410–411

FHRP (First Hop Redundancy Protocol), 93

FTP (File Transfer Protocol), 20–21

GRE (Generic Routing Encapsulation), 19–20

HTTP (Hypertext Transfer Protocol), 25

HTTPS (Hypertext Transfer Protocol Secure), 31

ICMP (Internet Control Message Protocol), 17

IP (Internet Protocol), 14–15

IPsec, 18–19

LDAP (Lightweight Directory Access Protocol), 30

LDAPS (Lightweight Directory Access Protocol over SSL), 32

LLDP (Link Layer Discovery Protocol), 497

NTP (Network Time Protocol), 25, 120–121

ports, 34–36

RDP (Remote Desktop Protocol), 33

reliable, 16

secured versus unsecured, 437–438

SFTP (Secure File Transfer Protocol), 21–22

SIP (Session Initiation Protocol), 34

SMB (Server Message Block), 31

SMTP (Simple Mail Transfer Protocol), 23

SMTSPS (Simple Mail Transfer Protocol Secure), 32

SNMP (Simple Network Management Protocol), 26, 339–340, 342–343

agents, 27–28

communities, 29

components, 26–27

management systems, 27

MIB (management information base), 340–341

MIBs (Management Information Bases), 28

traps, 340

version 3, 29–30

versions, 341–342

SSH (Secure Shell), 22

STP (Spanning Tree Protocol), 103–104

BPDU (bridge protocol data unit), 104

port state, 104–105

TCP (Transmission Control Protocol), 15–16

Telnet, 22–23

TFTP (Trivial File Transfer Protocol), 24–25

UDP (User Datagram Protocol), 16–17

proxy server, 139–141

PTP (Precision Time Protocol), 121

public cloud, 276

public network, 66–67

punchdown block, 294

Bix, 296

punchdown block

- Krone, 296
- type 66, 295
- type 110, 296

punchdown tool, 230, 294

purging, 437

Q

QoS (Quality of Service), 151–152, 396

- CoS (class of service), 152
- DSCP (Differentiated services code point), 152

quarantine network, 411

R

RA (Router Advertisement) guard, 441

rack

- diagrams, 308
- size, 297–298

RADIUS (Remote Authentication Dial-In User Service), 400

RAID, 141, 368

ransomware, 428

RBAC (role-based access control), 390–391

RBAC (rule-based access control), 390

RDP (Remote Desktop Protocol), 33, 35

reassociation, 253

reflection, 482

regulations, 328–329, 395, 408–409

- compliance, 409
- data sovereignty requirements, 409
- GDPR (General Data Protection Regulation), 409
- wireless, 241–242

reliable protocol, 16

remote access, procedures, 326

repeater, 484

report/ing

- audit and assessment, 310
- wireless survey, 309

reservation, 109–110

resolvers, 113

reusable tasks, 167–168

RF (radio frequency) amplifier, 484

RFC (Request For Comments), 15

RFC 792, 17

RFC 821, 23

RFC 854, 22

RFC 1350, 24

RFC 2068, 25

RFC 8484, 120

RFI (radio frequency interference), 433–434

RFID (radio frequency identifier), 296, 433–434

ring topology, 55–56

risk management, 415–416

RJ-11 connector, 195–196

RJ-45 connector, 197

roaming misconfiguration, 485

rogue AP, 427

rogue DHCP server, 426–427

rollover cable, 205

root DNS server, 115

route add command, 82

route command, 525–526

route print command, 80

route redistribution, 85

route selection, 5

router, 129–131

- default gateway, 79–80
- GBIC (gigabit interface converter) module, 200
- SFP (small form-factor pluggable) module, 200
- SOHO (small office/home office), 129
- wireless broadband, 256–257, 258–262

routing, 5

- administrative distance, 89
- asymmetrical, troubleshooting, 465

- dynamic, 82, 85–89
 - FHRP (First Hop Redundancy Protocol), 93
 - hops, 87, 90
 - latency, 90
 - loops, 87–88, 467
 - metric, 89–90
 - MTU (maximum transmission unit), 90
 - poison reverse, 88
 - prefix length, 89
 - route selection, 89–90, 467
 - split horizon, 88
 - static, 81–82
 - subinterface, 94
 - troubleshooting, missing route, 467
 - TTL (time to live), 87
 - VIP (virtual IP) address, 94
 - routing protocol**
 - BGP (Border Gateway Protocol), 86
 - distance-vector, 85–86, 88
 - EIGRP, 86
 - link-state, 86, 88–89
 - OSPF (Open Shortest Path First), 86
 - routing table, 80–81, 467**
 - RPO (recovery point objective), 367–368**
 - RSSI (Received Signal Strength Indication), 477**
 - RTO (recovery time objective), 367–368**
 - runt, 105, 224, 462**
- S**
-
- SaaS (Software as a Service), 271–272**
 - SAML (Security Assertion Markup Language), 406–407**
 - SAN (storage-area network), 142**
 - SASE (Secure Access Service Edge), 165–166**
 - satellite technology, 186–187**
 - SCADA (supervisory control and data acquisition), 395–396**
 - scalability, cloud, 279**
 - scheduled network discovery, 354**
 - scopes, 71, 109**
 - screened subnet, 397–398**
 - SDN (software-defined networking), 157**
 - application layer, 155–157
 - control layer, 157
 - infrastructure layer, 157
 - management plane, 158
 - SD-WAN (software-defined wide-area network), 158–160**
 - central policy management, 161–162
 - zero-touch provisioning, 160–161
 - secret key cryptography, 402**
 - security. *See also* attack/s; cryptography**
 - access control, 388, 392–393
 - 802.1X, 410
 - discretionary, 389–390
 - mandatory, 389
 - rule-based, 390
 - authentication. *See also* local authentication
 - Kerberos, 401–403
 - multifactor, 407–408
 - RADIUS (Remote Authentication Dial-In User Service), 400
 - TACACS (Terminal Access Controller Access Control System), 400–401
 - CIA triad, 387
 - cloud, 283–285
 - defense in depth, 393
 - honeypots and honeynets, 399
 - network segmentation, 393–397
 - screened subnet, 397–398
 - separation of duties, 398
 - encryption, 388
 - geofencing, 413–414
 - groups, 136
 - IAM (identity and access management), 405

- identity lifecycle management, 405
- SAML (Security Assertion Markup Language), 406–407
- SSO (single sign-on), 405
- logs, 346–347
- MAC filtering, 412–413
- monitoring, 337–338
- penetration test, 416–417
- physical, 414–415
- posture assessment, 412
- procedures, 325
- training, 415
- wireless, antenna placement and power levels, 4445
- segmentation, 5, 98–99**
- self-healing, 252**
- separation of duties, 398**
- server**
 - access control, role-based, 390–391
 - authoritative DNS, 118–119
 - BOOTP, 73
 - content, 134
 - DHCP, 71, 471
 - documentation, 308
 - FTP, 20–21
 - network controller, 390
 - nonauthoritative DNS, 118–119
 - NTP, 121
 - proxy, 139–141
 - reverse proxy, 141
 - root DNS, 115
 - SQL (Structured Query Language), 33
 - TFTP, 498
- service/s**
 - addressing, 5
 - documentation, 309
 - troubleshooting, 472–473
- session layer, OSI (Open Systems Interconnection) model, 6**
- SFP (small form-factor pluggable) module, 200**
- SFTP (Secure File Transfer Protocol), 21–22**
- show commands, 526–527**
- show interface command, 80**
- SIEM (security information and event management), 350, 417**
- signal strength, 228**
- single-mode fiber, 194**
- SIP (Session Initiation Protocol), 34**
- site survey, 309, 481**
- site-local address, 172–173**
- site-to-site VPN, 376–377**
- SLA (service-level agreement), 320**
- SLAAC (Stateless Address Auto Configuration), 110**
- slash, 68**
- SMB (Server Message Block), 31**
- SMTP (Simple Mail Transfer Protocol), 23**
- SMTSPS (Simple Mail Transfer Protocol Secure), 32**
- smurf attack, 423**
- snapshots, 364–365**
- snips, 229–230**
- SNMP (Simple Network Management Protocol), 26, 339–340, 342–343, 441**
 - agents, 27–28
 - communities, 29
 - components, 26–27
 - management systems, 27
 - MIB (management information base), 28, 340–341
 - traps, 340
 - version 3, 29–30
 - versions, 341–342
- SNMPv2c, 29**
- social engineering, 424–426**
- software**
 - antivirus, 431–432
 - defined network. *See* SDN (software-defined networking)
 - LG (looking-glass), 218

- management, 326
- patch management, 351–352
- procedures, 325
- spectrum analyzer, 234**
- speed tester, 494**
- SPF (shortest path first) algorithm, 86**
- spine and leaf topology, 48–49**
- split horizon, 88**
- SPOF (single point of failure), 367**
- spoofing, 428**
 - ARP, 428–429
 - DNS, 429
- SQL (Structured Query Language), 33**
- SSE (Security Service Edge), 165–166**
- SSH (Secure Shell), 21, 22, 378–379**
- SSID, 478**
- SSID (service set identifier), 254–255, 258**
- SSL (Secure Sockets Layer), 151**
- SSO (single sign-on), 401, 405**
- STA (station), 253**
- standard operating procedures, 310**
- star topology, 45–46**
- stateful/stateless, 173**
- static addressing, 70**
- static routing, 5, 81–82**
- statistics, capturing, 317**
- storage**
 - area network, 142
 - box, lockable, 298–299
 - iSCSI (Internet Small Computer Systems Interface), 143
 - network-attached, 141–142
- store-and-forward switching, 132**
- STP (shielded twisted-pair), 188**
- STP (Spanning Tree Protocol), 103–104**
 - BPDU (bridge protocol data unit), 104
 - port state, 104–105
 - troubleshooting, 466–467
- stratum, 120**
- stress test, 344–345**

- subinterface, 94**
- subnet**
 - IPv4, 65–66
 - mask, 63, 64–65
 - screened, 397–398
- suffix, DNS, 111**
- SVI (Switch Virtual Interface), 99–100**
- switch/switching, 82–83, 99–100, 131–132**
 - cabling, 133–134
 - circuit, 84
 - comparison of methods, 84–85
 - content, 133–134
 - Layer 2, 133
 - multilayer, 133
 - packet, 83–84
 - top-of-rack, 49
 - troubleshooting, 466–467
- symmetric key cryptography, 402**
- SYN flood, 423**
- syslog, 31–32, 350**
- system logs, 348**

T

- tabletop exercise, 370**
- TACACS (Terminal Access Controller Access Control System), 400–401**
- tap, 490–491, 494**
- TCP (Transmission Control Protocol), 5, 15–16**
 - ports, 35–36
 - three-way handshake, 16
- tcpdump command, 525**
- TCP/IP**
 - model, 1, 8–9
 - Windows configuration options, 71–72
- TDM (time-division multiplexing), 183**
- TDMA (time-division multiple access), 185–186**
- TDR (time-domain reflectometer), 231–232**

telecommunications/computer room

telecommunications/computer room, 291. See also wiring closet

- environmental factors
 - fire suppression, 301
 - heat, 301
 - humidity, 301
- HVAC (heating, ventilation, and air conditioning), 301
- lockable environment, 298–299, 414–415
- patch panel, 294
- power management
 - PDU (power distribution unit), 300
 - threats, 300
 - UPS (uninterruptible power supply), 299
- rack size, 297–298

Telnet, 22–23

TEMPEST, 433–434

Teredo, 92

terminal emulator, 498

test/ing

- bandwidth, 217–218
- disaster recovery, 370
- load, 344
- penetration, 369, 416–417
- performance, 343–344
- stress, 344–345
- throughput, 216–217
- validation, 370

TFTP (Trivial File Transfer Protocol), 24–25

thicknet, 191

thick/thin AP, 477

thin client computing, 33

thin coax, 191–192

threats

- external, 387
- internal, 387

three-tier hierarchical model, 49–50, 51–52

- access/edge layer, 51
- core layer, 50
- distribution/aggregation layer, 50

three-way handshake, TCP (Transmission Control Protocol), 16

throughput, 216, 336

- versus bandwidth, 217
- goodput, 247
- high, 247
- tester, 216–217
- troubleshooting, 463
- wireless, 246–247

ticket, Kerberos, 403

time protocols. See also protocols

- NTP (Network Time Protocol), 120–121, 472
- NTS (Network Time Security), 121
- PTP (Precision Time Protocol), 121

time synchronization, 120

time-based authentication, 407–408

TLS (Transport Layer Security), 7, 31, 151

toner/toner probe, 230–231, 490

tool/s

- cable crimper, 229–230
- cable tester, 233
- fiber light meter, 234
- fusion splicer, 234
- IaC (Infrastructure as Code), 168
- loopback adapter, 231
- multimeter, 232–233
- OTDR (optical time-domain reflectometer), 232
- punchdown, 230, 294
- SIEM (security information and event management), 350, 417
- snips, 229–230
- spectrum analyzer, 234
- toner probe, 230–231
- troubleshooting, 489–490
 - cable tester, 490
 - CDP (Cisco Discovery Protocol), 497

- command-line, 498–500
- IP scanner, 498
- LLDP (Link Layer Discovery Protocol), 497
- NetFlow analyzer, 498
- ping utility, 504–509
- port scanner, 494–496
- protocol analyzer, 493–494
- speed tester, 494
- taps, 490–491
- terminal emulator, 498
- TFTP server, 498
- toner, 490
- VFL (visual fault locator), 491
- Wi-Fi analyzer, 491–493
- wire map, 234
- wire stripper, 229–230
- topology, 44**
 - bus, 54–55
 - collapsed core, 52–53
 - hub-and-spoke, 315
 - hybrid, 47
 - logical, 313
 - mesh, 46–47
 - physical, 313
 - point to point, 48
 - ring, 55–56
 - spine and leaf, 48–49
 - star/hub and spoke, 45–46
 - three-tier hierarchical, 49–50, 51–52
 - access/edge layer, 51
 - core layer, 50
 - distribution/aggregation layer, 50
- top-to-bottom troubleshooting, 453**
- TPC (Transmit Power Control), 242**
- traceroute command, 134, 500–504**
- tracert command, 87**
- traffic, 36**
 - anycast, 37
 - broadcast, 37
 - East-West, 53
 - monitoring, 354–355
 - multicast, 37
 - North-South, 53
 - unicast, 37
- training**
 - documentation, 306
 - employee, 415
- transceiver, 200**
 - fiber, 200
 - troubleshooting, 228
- transmission. See also cable**
 - baseband, 183
 - bps (bits per second), 216
 - broadband, 183
 - full-duplex mode, 184
 - half-duplex mode, 184
 - rates, 184–185
 - simplex mode, 184
 - throughput, 216
 - wired versus wireless, 185
- transport layer, OSI (Open Systems Interconnection) model, 5–6**
- traps, SNMP (Simple Network Management Protocol), 340**
- troubleshooting, 450–451**
 - bottom-to-top approach, 453
 - cable connectivity issues, 215–216, 217–219
 - bad ports, 221–222
 - dirty optical cables, 224
 - duplexing issues, 223
 - improper termination, 220–221
 - incorrect pinout, 221
 - interface issues, 224–226
 - interference, 220
 - LED status indicators, 222
 - open/short faults, 222
 - signal degradation, 219–220
 - TX/RX reversed, 223–224
 - common network issues, 461
 - ACL (access control list), 473
 - address pool exhaustion, 472
 - asymmetrical routing, 465

troubleshooting

- bandwidth/throughput capacity, 463
- blocked ports, services, or addresses, 472
- bottlenecking, 463
- broadcast storm, 465
- BYOD (bring-your-own-device) issues, 473
- CA (certificate authority), 471
- congestion/contention, 462
- DNS issues, 468
- duplicate IP address, 469
- duplicate MAC address, 469–470
- expired IP address, 470
- firewall, 472–473
- hardware, 474–475
- incorrect subnet mask, 469
- jitter, 464–465
- latency, 463–464
- licensed feature issues, 473
- missing route, 467
- multicast flooding, 465
- NTP, 472
- packet loss, 464
- rogue DHCP server, 471
- route selection, 467
- routing loops, 467
- switching, 466–467
- VNAN, 468
- document findings, actions, outcomes, and lessons learned, 457
- documentation, 306
- establish a plan of action, 454–455
- establish a theory of probable cause, 453–454
- hardware
 - PoE (Power over Ethernet), 227
 - transceiver issues, 228
- identify the problem, 451–452
 - approach multiple problems individually, 453
 - determine if anything has changed, 452
 - duplicate the problem if possible, 453
 - identify symptoms, 452
- implement the solution or escalate, 455–456
- in-band management, 381
- network/s
 - default route, 467–468
 - low optical link budget, 468
 - show commands, 526–527
 - unresponsive service, 473
 - wireless, 476–480
- out-of-band management, 381–382
- physical layer, 3
- test the theory to determine the cause, 454
- tools, 489–490
 - ARP (Address Resolution Protocol), 510–512
 - cable tester, 490
 - CDP (Cisco Discovery Protocol), 497
 - command-line, 498–500
 - dig command, 523–524
 - IP scanner, 498
 - ipconfig / all command, 518–521
 - ipconfig command, 521–522
 - LLDP (Link Layer Discovery Protocol), 497
 - NetFlow analyzer, 498
 - netstat -a command, 515–516
 - netstat command, 512–514
 - netstat -e command, 514
 - netstat -r command, 516
 - netstat -s command, 517–518
 - nslookup command, 522–523
 - ping utility, 504–509
 - port scanner, 494–496
 - protocol analyzer, 493–494
 - route command, 525–526
 - speed tester, 494
 - taps, 490–491
 - tcpdump, 525

- terminal emulator, 498
- TFTP server, 498
- toner, 490
- VFL (visual fault locator), 491
 - Wi-Fi analyzer, 491–493
- top-to-bottom approach, 453
- using wiring schematics, 313
- verify full system functionality, 456
- wireless, 243
- trunking, VLAN, 96, 103**
- TTL (time to live), 17, 87, 153**
- tunneling, 91–92, 174–175**
- twinax, 192**
- twisted-pair cable, 188**
 - categories, 189–190
 - shielded, 188
 - unshielded, 188

U

- UDP (User Datagram Protocol), 5, 14, 16–17, 25, 35–36**
- unicast, 37**
- unicast address, 172**
- universal LAN MAC address, 75**
- unresponsive service, troubleshooting, 473**
- UPC (ultra-physical contact), 199**
- updates**
 - driver, 353
 - firmware, 352
 - major versus minor, 353
 - software, 351–352
- UPS (uninterruptible power supply), 299**
 - power-relate threats, 300
 - reasons for using, 299
- URL (uniform resource locator), 25, 31, 140, 440**
- user account policy, 319**
- utilization, 336**
- UTP (unshielded twisted-pair), 188**

V

- validation test, 370**
- VC (virtual console), 102**
- versions, SNMP (Simple Network Management Protocol), 341–342**
- vertical cable, 291, 293**
- VFL (visual fault locator), 491**
- VIP (virtual IP) address, 94**
- virtual terminal protocol, Telnet, 22–23**
- virtual-circuit packet switching, 83**
- virus, 431–433**
- VLAN (virtual local-area network), 95**
 - 802.1Q, 95, 96, 101–102
 - advantages, 95–96
 - database, 96
 - default, 101
 - hopping, 430–431
 - MAC address-based, 98
 - membership, 97–98
 - pooling, 145
 - port binding, 97
 - port-based, 97–98
 - private, 441
 - protocol-based, 97
 - segmentation, 98–99
 - SVI (Switch Virtual Interface), 99–100
 - troubleshooting, 468
 - trunking, 96, 103
 - voice, 103
- VLSM (Variable Length Subnet Masking), 66**
- voice VLAN, 103**
- VoIP (Voice over IP), 34**
- VPC (virtual private cloud), 281–282**
- VPN (virtual private network), 146–147**
 - client-to-site, 377–378
 - components, 147–148
 - connection types, 148
 - pros and cons, 149–150
 - site-to-site, 376–377

VRRP (Virtual Router Redundancy Protocol)

VRRP (Virtual Router Redundancy Protocol), 370

vulnerability, 387. See also attack/s

patch, 353

scan, 369, 387

VXLAN (virtual extensible local-area network), 162–163

W

WAF (web application firewall), 136

war chalking, 427

war driving, 427

well-known ports, 35

WEP (Wired Equivalent Privacy), 259

white box/known environment test, 416–417

Wi-Fi 6e, 246

Wi-Fi analyzer, 491–493

windowing, 6

Windows

ipconfig / release command, 470

TCP/IP configuration options, 71–72

tracert command, 500–504

wire map, 234

wire stripper, 229–230

wireless network, 185

absorption, 482

ad hoc, 251

antenna

coverage, 249–250

directional, 250

omnidirectional, 249–250

polarization, 250

ratings, 248–249

antenna placement and power levels, 445

AP (access point), 144–145

association, 253, 254

authentication, 254, 259–260

BSSID (basic service set identifier), 254–255

coverage, troubleshooting, 483–485

ESSID (extended service set identifier), 254–255

reassociation, 253

rogue, 427

SSID (service set identifier), 254–255, 258

thick/thin, 477

band steering, 241

captive portals, 479

cellular technology, 185

4G, 186

5G, 186

GSM (Global System for Mobile Communications), 185–186

LTE (Long-Term Evolution), 186

channel/s, 242, 244–245, 255, 478

bonding, 247–248

overlap, 242–243, 482

width, 240–241

configuring the wireless connection, 256–262

data rate, 246–247

encryption, 478

geofencing, 413–414

guest, 255–256

infrastructure, 251

insufficient coverage, 481

interference, 481–482

isolation, 445

mesh, 251, 252

monitoring, 339

obstacles, 483

performance issues, troubleshooting, 476–480

point-to-point, 251–252

reflection, 482

regulations, 241–242

router, 256–257, 258–262

satellite technology, 186–187

signal strength, 228

site survey, 481

STA (station), 253

ZTA (zero trust architecture)

standards, 246
802.11, 254
802.11a, 241, 243
802.11ac, 243, 245
802.11ax, 244, 245
802.11b/g, 243
802.11h, 242

throughput, 246–247

troubleshooting, 243

types, 252

war chalking, 427

war driving, 427

wireless survey report, 309

wiring closet, 291

FDP (fiber distribution panel), 295

IDF (intermediate distribution
frame), 296

MDF (main distribution frame), 296
punchdown block, 294

wiring schematics, 310, 312, 313

WLC (wireless LAN controller), 145

**WPA (Wi-Fi Protected Access),
259–261**

**WPA-PSK (Wi-Fi Protected Access
with Pre-Shared Key), 259**

X-Y-Z

zero-day attack, 387

zero-touch provisioning, 160–161

zones, 445–446

**ZTA (zero trust architecture),
163–165**