

Written by Networking Authority Todd Lammle



**Includes Real-World Scenarios, Written Labs,  
and Leading-Edge Exam Prep Software Featuring:**

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards for PCs, Pocket PCs,  
and Palm Handhelds
- Entire Book in PDF

CompTIA®

Network



®

STUDY GUIDE



**AUTHORIZED**

**Exam N10-004**

**Todd Lammle**





# CompTIA Network+ Study Guide

## N10-004 Exam Objectives

OBJECTIVE	CHAPTER
<b>1.0 NETWORK TECHNOLOGIES</b>	
1.1 Explain the function of common networking protocols TCP; FTP; UDP; TCP/IP suite; DHCP; TFTP; DNS; HTTP(S); ARP; SIP (VoIP); RTP (VoIP); SSH; POP3; NTP; IMAP4; Telnet; SMTP; SNMP2/3; ICMP; IGMP; TLS	6
1.2 Identify commonly used TCP and UDP default ports TCP ports: FTP – 20, 21; SSH – 22; TELNET – 23; SMTP – 25; DNS – 53; HTTP – 80; POP3 – 110; NTP – 123; IMAP4 – 143; HTTPS – 443 UDP ports: TFTP – 69; DNS – 53; BOOTPS/DHCP – 67; SNMP – 161	6
1.3 Identify the following address formats IPv6; IPv4; MAC addressing	7
1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes Addressing Technologies: Subnetting; Classful vs. classless (e.g. CIDR, Supernetting); NAT; PAT; SNAT; Public vs. private; DHCP (static, dynamic APIPA) Addressing schemes: Unicast; Multicast; Broadcast	7, 8
1.5 Identify common IPv4 and IPv6 routing protocols Link state: OSPF; IS-IS Distance vector: RIP; RIPv2; BGP Hybrid: EIGRP	10
1.6 Explain the purpose and properties of routing IGP vs. EGP; Static vs. dynamic; Next hop; Understanding routing tables and how they pertain to path selection; Explain convergence (steady state)	9
1.7 Compare the characteristics of wireless communication standards 802.11 a/b/g/n: Speeds; Distance; Channels; Frequency Authentication and encryption: WPA; WEP; RADIUS; TKIP	12
<b>2.0 NETWORK MEDIA AND TOPOLOGIES</b>	
2.1 Categorize standard cable types and their properties Type: CAT3, CAT5, CAT5e, CAT6; STP, UTP; Multimode fiber, single-mode fiber; Coaxial: RG-59; RG-6; Serial; Plenum vs. Non-plenum Properties: Transmission speeds; Distance; Duplex; Noise immunity (security, EMI); Frequency	3

<b>OBJECTIVE</b>	<b>CHAPTER</b>
2.2 Identify common connector types RJ-11; RJ-45; BNC; SC; ST; LC; RS-232	3
2.3 Identify common physical network topologies Star; Mesh; Bus; Ring; Point to point; Point to multipoint; Hybrid	1
2.4 Given a scenario, differentiate and implement appropriate wiring standards 568A; 568B; Straight vs. cross-over; Rollover; Loopback	3
2.5 Categorize WAN technology types and properties Type: Frame relay; E1/T1; ADSL; SDSL; VDSL; Cable modem; Satellite; E3/T3; OC-x; Wireless; ATM; SONET; MPLS; ISDN BRI; ISDN PRI; POTS; PSTN Properties: Circuit switch; Packet switch; Speed; Transmission media; Distance	16
2.6 Categorize LAN technology types and properties Types: Ethernet; 10BaseT; 100BaseTX; 100BaseFX; 1000BaseT; 1000BaseX; 10GBaseSR; 10GBaseLR; 10GBaseER; 10GBaseSW; 10GBaseLW; 10GBaseEW; 10GBaseT Properties: CSMA/CD; Broadcast; Collision; Bonding; Speed; Distance	4
2.7 Explain common logical network topologies and their characteristics Peer to peer; Client/server; VPN; VLAN	1
2.8 Install components of wiring distribution Vertical and horizontal cross connects; Patch panels; 66 block; MDFs; IDF; 25 pair; 100 pair; 110 block; Demarc; Demarc extension; Smart jack; Verify wiring installation; Verify wiring; termination	3
<b>3.0 NETWORK DEVICES</b>	
3.1 Install, configure and differentiate between common network devices Hub; Repeater; Modem; NIC; Media converters; Basic switch; Bridge; Wireless access point; Basic router; Basic firewall; Basic DHCP server	5
3.2 Identify the functions of specialized network devices Multilayer switch; Content switch; IDS/IPS; Load balancer; Multifunction network devices; DNS server; Bandwidth shaper; Proxy server; CSU/DSU	5
3.3 Explain the advanced features of a switch PoE; Spanning tree; VLAN; Trunking; Port mirroring; Port authentication	11
3.4 Implement a basic wireless network Install client; Access point placement; Install access point—Configure appropriate encryption, Configure channels and frequencies, Set ESSID and beacon—Verify installation	12



Exam specifications and content are subject to change at any time without prior notice and at CompTIA's sole discretion. Please visit CompTIA's website ([www.comptia.org](http://www.comptia.org)) for the most current information on their exam content.

OBJECTIVE	CHAPTER
<b>4.0 NETWORK MANAGEMENT</b>	
4.1 Explain the function of each layer of the OSI model Layer 1 – physical; Layer 2 – data link; Layer 3 – network; Layer 4 – transport; Layer 5 – session; Layer 6 – presentation; Layer 7 – application	2
4.2 Identify types of configuration management documentation Wiring schematics; Physical and logical network diagrams; Baselines; Policies, procedures, and configurations; Regulations	20
4.3 Given a scenario, evaluate the network based on configuration management documentation Compare wiring schematics, physical and logical network diagrams, baselines, policies and procedures and configurations to network devices and infrastructure; Update wiring schematics, physical and logical network diagrams, configurations and job logs as needed	20
4.4 Conduct network monitoring to identify performance and connectivity issues using the following: Network monitoring utilities (e.g. packet sniffers, connectivity software, load testing, throughput testers); System logs, history logs, event logs	20
4.5 Explain different methods and rationales for network performance optimization Methods: QoS; Traffic shaping; Load balancing; High availability; Caching engines; Fault tolerance Reasons: Latency sensitivity; High bandwidth applications—VoIP, Video applications—Uptime	20
4.6 Given a scenario, implement the following network troubleshooting methodology Information gathering – identify symptoms and problems; Identify the affected areas of the network; Determine if anything has changed; Establish the most probable cause; Determine if escalation is necessary; Create an action plan and solution identifying potential effects; Implement and test the solution; Identify the results and effects of the solution; Document the solution and the entire process	19
4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution Physical issues: Cross talk; Nearing crosstalk; Near end crosstalk; Attenuation; Collisions; Shorts; Open impedance mismatch (echo); Interference Logical issues: Port speed; Port duplex mismatch; Incorrect VLAN; Incorrect IP address; Wrong gateway; Wrong DNS; Wrong subnet mask—Issues that should be identified but escalated: Switching loop, Routing loop, Route problems, Proxy arp, Broadcast storms; Wireless Issues: Interference (bleed, environmental factors), Incorrect encryption, Incorrect channel, Incorrect frequency, ESSID mismatch, Standard mismatch (802.11 a/b/g/n); Distance; Bounce; Incorrect antenna placement	19

<b>OBJECTIVE</b>	<b>CHAPTER</b>
<b>5.0 NETWORK TOOLS</b>	
5.1 Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality Traceroute; Ipconfig; Ifconfig; Ping; Arp ping; Arp; Nslookup; Hostname; Dig; Mtr; Route; Nbtstat; Netstat	17
5.2 Explain the purpose of network scanners Packet sniffers; Intrusion detection software; Intrusion prevention software; Port scanners	18
5.3 Given a scenario, utilize the appropriate hardware tools Cable testers; Protocol analyzer; Certifiers; TDR; OTDR; Multimeter; Toner probe; Butt set; Punch down tool; Cable stripper; Snips; Voltage event recorder; Temperature monitor	18
<b>6.0 NETWORK SECURITY</b>	
6.1 Explain the function of hardware and software security devices Network based firewall; Host based firewall; IDS; IPS; VPN concentrator	15
6.2 Explain common features of a firewall Application layer vs. network layer; Stateful vs. stateless; Scanning services; Content filtering; Signature identification; Zones	15
6.3 Explain the methods of network access security Filtering: ACL—MAC filtering, IP filtering—Tunneling and encryption—SSL VPN, VPN, L2TP, PPTP, IPSEC— Remote access—RAS, RDP, PPPoE, PPP, VNC, ICA	13
6.4 Explain methods of user authentication PKI; Kerberos; AAA—RADIUS, TACACS+—Network access control—802.1x—CHAP; MS-CHAP; EAP	13
6.5 Explain issues that affect device security Physical security; Restricting local and remote access; Secure methods vs. unsecure methods—SSH, HTTPS, SNMPv3, SFTP, SCP; TELNET, HTTP, FTP, RSH, RCP, SNMPv1/2	15
6.6 Identify common security threats and mitigation techniques Security threats: DoS; Viruses; Worms; Attackers; Man in the middle; Smurf; Rogue access points; Social engineering (phishing) Mitigation techniques: Policies and procedures; User training; Patches	14



Exam specifications and content are subject to change at any time without prior notice and at CompTIA's sole discretion. Please visit CompTIA's website ([www.comptia.org](http://www.comptia.org)) for the most current information on their exam content.

# CompTIA Network+<sup>®</sup>

## Study Guide







# CompTIA Network+®

## Study Guide



Todd Lammle



Wiley Publishing, Inc.

Acquisitions Editor: Jeff Kellum  
Development Editor: Susan Herman  
Technical Editors: Steven Johnson and Derek Lewis  
Production Editor: Christine O'Connor  
Copy Editor: Tiffany Taylor  
Production Manager: Tim Tate  
Vice President and Executive Group Publisher: Richard Swadley  
Vice President and Publisher: Neil Edde  
Project Manager 1: Laura Moss-Hollister  
Associate Producer: Shawn Patrick  
Media Quality Assurance: Angie Denny  
Book Designer: Judy Fung, Bill Gibson  
Compositor: Craig Woods, Happenstance Type-O-Rama  
Proofreader: Publication Services, Inc.  
Indexer: Jack Lewis  
Project Coordinator, Cover: Lynsey Stanford  
Cover Designer: Ryan Sneed  
Copyright © 2009 by Wiley Publishing, Inc., Indianapolis, Indiana  
Published simultaneously in Canada  
ISBN: 978-0-470-42747-7

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Limit of Liability/Disclaimer of Warranty:** The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data.

Lammle, Todd.

CompTIA Network+ study guide (Exam N10-004) / Todd Lammle. — 1st ed.

p. cm.

ISBN 978-0-470-42747-7 (paper/cd-rom) -- ISBN 978-0-470-42748-4 (cloth/cd-rom) 1. Computer networks—Examinations—Study guides. 2. Electronic data processing personnel--Certification. I. Title.

TK5105.5.L3555 2009

004.6076—dc22

2009001904

**TRADEMARKS:** Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. Network+ is a registered trademark of The Computing Technology Industry Association, Inc. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

10 9 8 7 6 5 4 3 2 1

Sybex is an independent entity from CompTIA and is not affiliated with CompTIA in any manner. Neither CompTIA nor Sybex warrants that use of this publication will ensure passing the relevant exam. Network+ is either a registered trademark or trademark of CompTIA in the United States and/or other countries.

The logo of the CompTIA Authorized Quality Curriculum (CAQC) program and the status of this or other training material as “Authorized” under the CompTIA Authorized Quality Curriculum program signifies that, in CompTIA’s opinion, such training material covers the content of the CompTIA’s related certification exam. CompTIA has not reviewed or approved the accuracy of the contents of this training material and specifically disclaims any warranties of merchantability or fitness for a particular purpose. CompTIA makes no guarantee concerning the success of persons using any such “Authorized” or other training material in order to prepare for any CompTIA certification exam.

The contents of this training material were created for the CompTIA Network+ exam covering CompTIA certification objectives that were current as of 2008.

#### How to Become CompTIA Certified:

This training material can help you prepare for and pass a related CompTIA certification exam or exams. In order to achieve CompTIA certification, you must register for and pass a CompTIA certification exam or exams.

In order to become CompTIA certified, you must:

1. Select a certification exam provider.
2. Register for and schedule a time to take the CompTIA certification exam(s) at a convenient location.
3. Read and sign the Candidate Agreement, which will be presented at the time of the exam(s).
4. Take and pass the CompTIA certification exam(s).

For more information about CompTIA’s certification process, and to learn more about their industry acceptance, benefits, or program news, please visit <http://www.comptia.org/certification>.

CompTIA is a non-profit information technology (IT) trade association. CompTIA’s certifications are designed by subject matter experts from across the IT industry. Each CompTIA certification is vendor-neutral, covers multiple technologies, and requires demonstration of skills and knowledge widely sought after by the IT industry.

To contact CompTIA with any questions or comments please email them at:

[questions@comptia.org](mailto:questions@comptia.org)

Sybex is an independent entity from CompTIA and is not affiliated with CompTIA in any manner. Neither CompTIA nor Sybex warrants that use of this publication will ensure passing the relevant exam. Network+ is either a registered trademark or trademark of CompTIA in the United States and/or other countries.



Dear Reader,

Thank you for choosing *CompTIA Network+ Study Guide*. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than thirty years later, we're still committed to producing consistently exceptional books. With each of our titles we're working hard to set a new standard for the industry. From the paper we print on, to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an email at [nedde@wiley.com](mailto:nedde@wiley.com), or if you think you've found a technical error in this book, please visit <http://sybex.custhelp.com>. Customer feedback is critical to our efforts at Sybex.

Best regards,

A handwritten signature in black ink, appearing to read 'Neil Edde', with a stylized, flowing script.

Neil Edde  
Vice President and Publisher  
Sybex, an Imprint of Wiley

# Acknowledgments

Monica Lammle's writing style, editing ability, encouragement, and dedication to ensuring that my books are concise yet highly readable has been invaluable to the success of this and many other projects.

Susan Herman was the development editor of this, the newest book in the Sybex CompTIA series. Thank you, Susan, for having the patience of Job, and for working so hard on this book with me. I'm so happy (and relieved) that you took on the job and, most of all, that you didn't run screaming from the room the next day!

Jeff Kellum is instrumental to my success in the Cisco world and is my acquisitions editor for this new CompTIA Network+ book. Jeff, thanks for your guidance and continued patience for all our books we've published together!

In addition, Christine O'Connor was an excellent production editor and she worked really hard to get the book done as quickly as possible, without missing the small mistakes that are so easy to over look. I am always very pleased when I hear that she will be working with me on a new project. Tiffany Taylor was latest copy editor, and she was patient, helpful, and detailed, but yet worked extremely hard to get this book out the shelf as fast as possible, and for that I thank her tremendously.

Steven Johnson literally hashed and rehashed each topic in this guide with me at all hours of the day and night, scrutinizing the material until we both agreed it was verifiably solid. Thank you, Steve!

I also want to mention Patrick Conlan, who tech-edited my CCNA book and is writing the Sybex Cisco Network Professional's Advanced Internetworking Guide. Pat was very helpful in throwing ideas at me for this book, and was the photographer for all the pictures I put in this book.

# About the Author

**Todd Lammle**, CompTIA Network+, CCSI, CCNA/CCNP, CCSP/CCVP, MCSE, CEH/CHFI, FCC RF Licensed, is the authority on Network Certification and internetworking. He is a world-renowned author, speaker, trainer, and consultant. Todd has over 25 years of experience working with LANs, WANs, and large licensed and unlicensed wireless networks. He's president and CEO of GlobalNet Training and Consulting, Inc., a network-integration and training firm based in Dallas, Texas. You can reach Todd through his forum at [www.lammle.com](http://www.lammle.com).





# Contents at a Glance

<i>Introduction</i>	<i>xxvii</i>
<i>Assessment Test</i>	<i>xlvi</i>
<b>Chapter 1</b>	<b>Introduction to Networks 1</b>
<b>Chapter 2</b>	<b>The Open Systems Interconnection Specifications 33</b>
<b>Chapter 3</b>	<b>Networking Topologies, Connectors, and Wiring Standards 61</b>
<b>Chapter 4</b>	<b>The Current Ethernet Specifications 97</b>
<b>Chapter 5</b>	<b>Networking Devices 131</b>
<b>Chapter 6</b>	<b>Introduction to Internet Protocol (IP) 177</b>
<b>Chapter 7</b>	<b>IP Addressing 215</b>
<b>Chapter 8</b>	<b>IP Subnetting, Troubleshooting IP, and Introduction to NAT 241</b>
<b>Chapter 9</b>	<b>Introduction to IP Routing 287</b>
<b>Chapter 10</b>	<b>Routing Protocols 311</b>
<b>Chapter 11</b>	<b>Switching and Virtual LANs (VLANs) 339</b>
<b>Chapter 12</b>	<b>Wireless Technologies 377</b>
<b>Chapter 13</b>	<b>Authentication and Access Control 423</b>
<b>Chapter 14</b>	<b>Network Threats and Mitigation 463</b>
<b>Chapter 15</b>	<b>Physical and Hardware Security 499</b>
<b>Chapter 16</b>	<b>Wide Area Networks 545</b>
<b>Chapter 17</b>	<b>Command-Line Tools 575</b>
<b>Chapter 18</b>	<b>Software and Hardware Tools 629</b>
<b>Chapter 19</b>	<b>Network Troubleshooting 659</b>
<b>Chapter 20</b>	<b>Management, Monitoring, and Optimization 699</b>
<b>Appendix A</b>	<b>Subnetting Class A 731</b>
<b>Appendix B</b>	<b>About the Companion CD 741</b>
<b>Glossary</b>	<b>745</b>
<i>Index</i>	<i>791</i>



# Contents

*Introduction* *xxvii*

*Assessment Test* *xlvi*

## **Chapter 1 Introduction to Networks 1**

First Things First: What's a Network?	2
The Local Area Network (LAN)	3
Common Network Components	5
Virtual LANs (VLANs)	8
Wide Area Network (WAN)	9
Virtual Private Networks (VPNs)	10
Network Architecture: Peer-to-Peer or Client/Server?	11
Physical Network Topologies	13
Bus Topology	14
Star Topology	15
Ring Topology	16
Mesh Topology	17
Point-to-Point Topology	18
Point-to-Multipoint Topology	19
Hybrid Topology	20
Topology Selection, Backbones, and Segments	21
Selecting the Right Topology	21
Summary	22
Exam Essentials	23
Written Labs	24
Review Questions	25
Answers to Review Questions	29
Answers to Written Labs	31

## **Chapter 2 The Open Systems Interconnection Specifications 33**

Internetworking Models	34
The Layered Approach	35
Advantages of Reference Models	35
The OSI Reference Model	36
The Application Layer	37
The Presentation Layer	39
The Session Layer	39
The Transport Layer	39
The Network Layer	45
The Data Link Layer	48
The Physical Layer	50

	Introduction to Encapsulation	51
	Summary	52
	Exam Essentials	52
	Written Lab	53
	Review Questions	54
	Answers to Review Questions	58
	Answers to Written Lab	60
<b>Chapter 3</b>	<b>Networking Topologies, Connectors, and Wiring Standards</b>	<b>61</b>
	Physical Media	63
	Coaxial Cable	64
	Twisted-Pair Cable	66
	Fiber-Optic Cable	69
	Serial Cables	73
	Properties of Cables	75
	Transmission Speeds	75
	Distance	76
	Duplex	76
	Noise Immunity (Security, EMI)	76
	Frequency	77
	Wiring Standards	77
	568A vs. 568B	77
	Straight-Through Cable	78
	Crossover Cable	78
	Rollover Cable	79
	Hardware Loopback	80
	Installing Wiring Distributions	82
	Vertical and Horizontal Cross-Connects	82
	Patch Panels	83
	Verifying Correct Wiring Installation	86
	Verifying Proper Wiring Termination	86
	Summary	87
	Exam Essentials	87
	Written Lab	88
	Review Questions	89
	Answers to Review Questions	93
	Answers to Written Lab	95
<b>Chapter 4</b>	<b>The Current Ethernet Specifications</b>	<b>97</b>
	Network Basics	98
	Ethernet Basics	100
	Collision Domain	100
	Broadcast Domain	100

	CSMA/CD	101
	Half- and Full-Duplex Ethernet	102
	Ethernet at the Data Link Layer	104
	Binary to Decimal and Hexadecimal Conversion	104
	Ethernet Addressing	108
	Ethernet Frames	108
	Channel Bonding	111
	Ethernet at the Physical Layer	111
	Summary	116
	Exam Essentials	116
	Written Lab	118
	Review Questions	121
	Answers to Review Questions	125
	Answers to Written Lab	127
<b>Chapter 5</b>	<b>Networking Devices</b>	<b>131</b>
	Common Network Connectivity Devices	132
	Hub	133
	Repeater	134
	Modem	134
	Network Interface Card (NIC)	136
	Transceiver (Media Converter)	137
	Bridge	139
	Switch	140
	Wireless Access Point (AP)	141
	Router	142
	Firewall	143
	Dynamic Host Configuration Protocol (DHCP) Server	144
	Other Specialized Devices	147
	Multilayer Switch	147
	Content Switch	148
	Intrusion Detection or Prevention System (IDS/IPS)	148
	Load Balancer	149
	Multifunction Network Devices	149
	Domain Name Service (DNS) Server	149
	Bandwidth Shaper	154
	Proxy Server	155
	Channel Service Unit/Data Service Unit (CSU/DSU)	156
	Network Segmentation	157
	Switches and Bridges at the Data Link Layer	163
	Hubs at the Physical Layer	165
	Summary	166
	Exam Essentials	166
	Written Lab	168

	Review Questions	169
	Answers to Review Questions	173
	Answers to Written Lab	175
<b>Chapter 6</b>	<b>Introduction to Internet Protocol (IP)</b>	<b>177</b>
	Introducing TCP/IP	179
	A Brief History of TCP/IP	179
	TCP/IP and the DoD Model	180
	The Process/Application Layer Protocols	182
	The Host-to-Host Layer Protocols	190
	The Internet Layer Protocols	195
	Data Encapsulation	200
	Summary	204
	Exam Essentials	205
	Written Lab	206
	Review Questions	207
	Answers to Review Questions	211
	Answers to Written Lab	213
<b>Chapter 7</b>	<b>IP Addressing</b>	<b>215</b>
	IP Terminology	216
	The Hierarchical IP Addressing Scheme	217
	Network Addressing	218
	Private IP Addresses	222
	Broadcast Addresses	223
	Internet Protocol Version 6 (IPv6)	225
	Why Do We Need IPv6?	225
	The Benefits of and Uses for IPv6	226
	IPv6 Addressing and Expressions	227
	Shortened Expression	228
	Address Types	229
	Special Addresses	230
	Summary	230
	Exam Essentials	231
	Written Lab	232
	Review Questions	233
	Answers to Review Questions	237
	Answers to Written Lab	239
<b>Chapter 8</b>	<b>IP Subnetting, Troubleshooting IP, and Introduction to NAT</b>	<b>241</b>
	Subnetting Basics	242
	How to Create Subnets	243
	Subnet Masks	244

	Classless Inter-Domain Routing (CIDR)	245
	Subnetting Class C Addresses	247
	Subnetting Class B Addresses	256
	Troubleshooting IP Addressing	264
	Determining IP Address Problems	267
	Introduction to Network Address Translation (NAT)	271
	Types of Network Address Translation	273
	NAT Names	273
	How NAT Works	274
	Summary	275
	Exam Essentials	276
	Written Labs	277
	Review Questions	278
	Answers to Review Questions	283
	Answers to Written Labs	285
<b>Chapter 9</b>	<b>Introduction to IP Routing</b>	<b>287</b>
	Routing Basics	288
	The IP Routing Process	291
	Testing Your IP Routing Understanding	297
	Static and Dynamic Routing	298
	Summary	301
	Exam Essentials	301
	Written Lab	303
	Review Questions	304
	Answers to Review Questions	308
	Answers to Written Lab	310
<b>Chapter 10</b>	<b>Routing Protocols</b>	<b>311</b>
	Routing Protocol Basics	312
	Administrative Distances	313
	Classes of Routing Protocols	315
	Distance-Vector Routing Protocols	316
	Routing Information Protocol (RIP)	317
	RIP Version 2 (RIPv2)	318
	VLSM and Discontiguous Networks	319
	EIGRP	321
	Border Gateway Protocol (BGP)	323
	Link-State Routing Protocols	324
	Open Shortest Path First (OSPF)	325
	Intermediate System to Intermediate System (IS-IS)	327
	IPv6 Routing Protocols	328
	RIPng	329
	EIGRPv6	329
	OSPFv3	329

	Summary	330
	Exam Essentials	330
	Written Lab	331
	Review Questions	332
	Answers to Review Questions	336
	Answers to Written Lab	338
<b>Chapter 11</b>	<b>Switching and Virtual LANs (VLANs)</b>	<b>339</b>
	Networking Before Layer 2 Switching	340
	Switching Services	344
	Limitations of Layer 2 Switching	345
	Bridging vs. LAN Switching	345
	Three Switch Functions at Layer 2	346
	Spanning Tree Protocol (STP)	351
	Spanning-Tree Port States	352
	STP Convergence	353
	Virtual LANs (VLANs)	354
	VLAN Basics	354
	VLAN Memberships	358
	Static VLANs	358
	Dynamic VLANs	359
	Identifying VLANs	359
	VLAN Identification Methods	360
	Switching and Network Security	362
	Port Security/Authentication	362
	How VLANs Enhance Network Security	362
	Two Additional Advanced Features of Switches	363
	Power over Ethernet (PoE)	364
	Port Mirroring/Spanning	366
	Summary	367
	Exam Essentials	368
	Written Lab	369
	Review Questions	370
	Answers to Review Questions	374
	Answers to Written Lab	376
<b>Chapter 12</b>	<b>Wireless Technologies</b>	<b>377</b>
	Introduction to Wireless Technology	378
	The 802.11 Standards	381
	2.4GHz (802.11b)	382
	2.4GHz (802.11g)	383
	5GHz (802.11a)	384
	5GHz (802.11h)	385
	2.4GHz/5GHz (802.11n)	385



Comparing 802.11 Standards	387
Wireless LAN Modulation Techniques	387
Range Comparisons	388
Wireless Network Components	389
Wireless Access Points	389
Wireless Network Interface Card (NIC)	390
Wireless Antennas	391
Installing a Wireless Network	393
Ad hoc Mode: Independent Basic Service Set (IBSS)	393
Infrastructure Mode: Basic Service Set (BSS)	394
Design Considerations with Large Wireless Networks	396
Installing and Configuring Hardware	398
Wireless Security	406
Open Access	407
Service Set Identifiers (SSIDs), Wired Equivalent	
Privacy (WEP), and Media Access Control (MAC)	
Address Authentication	407
Remote Authentication Dial In User Service (RADIUS)	408
Temporal Key Integrity Protocol (TKIP)	409
Wi-Fi Protected Access (WPA) or WPA 2 Pre-Shared Key	410
Summary	412
Exam Essentials	412
Written Lab	414
Review Questions	415
Answers to Review Questions	419
Answers to Written Lab	421

## **Chapter 13 Authentication and Access Control 423**

Security Filtering	425
Access Control Lists	426
Tunneling	427
Encryption	432
Remote Access	436
Managing User Account and Password Security	439
Network Resource-Sharing Security Models	439
Managing User Accounts	440
Managing Passwords	443
User-Authentication Methods	447
Public Key Infrastructure (PKI)	447
Kerberos	448
Authentication, Authorization, and Accounting (AAA)	449
Network Access Control (NAC)	451
Challenge Handshake Authentication Protocol (CHAP)	451

	MS-CHAP	452
	Extensible Authentication Protocol (EAP)	452
	Summary	453
	Exam Essentials	453
	Written Lab	454
	Review Questions	455
	Answers to Review Questions	459
	Answers to Written Lab	461
<b>Chapter 14</b>	<b>Network Threats and Mitigation</b>	<b>463</b>
	Recognizing Security Threats	464
	Denial of Service (DoS)	465
	Viruses	468
	Worms	471
	Attackers and Their Tools	471
	Rogue Access Points	474
	Social Engineering (Phishing)	475
	Understanding Mitigation Techniques	476
	Active Detection	476
	Passive Detection	476
	Proactive Defense	477
	Policies and Procedures	477
	Security Policies	478
	Security Training	483
	Patches and Upgrades	484
	Updating Antivirus Components	486
	Fixing an Infected Computer	488
	Summary	488
	Exam Essentials	489
	Written Lab	490
	Review Questions	491
	Answers to Review Questions	495
	Answers to Written Lab	497
<b>Chapter 15</b>	<b>Physical and Hardware Security</b>	<b>499</b>
	Using Hardware and Software Security Devices	500
	Defining Firewalls	502
	Network-Based Firewalls	503
	Host-Based Firewalls	503
	Firewall Technologies	503
	Access Control Lists (ACL)	504
	Demilitarized Zone (DMZ)	506
	Protocol Switching	507

Dynamic Packet Filtering	508
Proxy Services	509
Firewalls at the Application Layer vs. the Network Layer	511
Stateful vs. Stateless Network-Layer Firewalls	512
Application-layer Firewalls	513
Scanning Services and Other Firewall Features	514
Content Filtering	515
Signature Identification	515
Zones	516
Intrusion-Detection and -Prevention Systems	518
Network-Based IDS	519
Host-Based IDS	521
VPN Concentrators	522
Understanding Problems Affecting Device Security	523
Physical Security	523
Logical Security Configurations	525
Restricting Local and Remote Access	527
Secure and Unsecure Application Protocols	529
Summary	534
Exam Essentials	534
Written Lab	536
Review Questions	537
Answers to Review Questions	541
Answers to Written Lab	543
<b>Chapter 16 Wide Area Networks</b>	<b>545</b>
What's a WAN?	547
Defining WAN Terms	547
The Public Switched Telephone Network (PSTN)	548
WAN Connection Types	549
Bandwidth or Speed	551
T-Series Connections	551
The T1 Connection	552
The T3 Connection	553
Transmission Media	553
Wired Connections	554
Wireless Technologies	555
Broadband Services	556
DSL Technology and xDSL	557
Cable Modem	559
WAN Protocols	560
Integrated Services Digital Network (ISDN)	560
Frame Relay Technology	562

	Asynchronous Transfer Mode (ATM)	565
	Multi Protocol Label Switching (MPLS)	565
	Summary	567
	Exam Essentials	567
	Written Lab	568
	Review Questions	569
	Answers to Review Questions	572
	Answers to Written Lab	574
<b>Chapter 17</b>	<b>Command-Line Tools</b>	<b>575</b>
	Using <i>Traceroute</i>	577
	Using <i>ipconfig</i> and <i>ifconfig</i>	578
	Using the <i>ipconfig</i> Utility	578
	Using the <i>ifconfig</i> Utility	582
	Using the <i>ping</i> Utility	583
	Using the Address Resolution Protocol (ARP)	586
	The Windows ARP Table	586
	Using the <i>arp</i> Utility	587
	Using the <i>nslookup</i> Utility	590
	Resolving Names with the Hosts Table	592
	Using the <i>Mtr</i> Command	593
	Using the <i>Route</i> Command	594
	Using the <i>route</i> Command Options	595
	Some Examples of the <i>route</i> Command	597
	Using the <i>nbtstat</i> Utility	597
	The <i>-a</i> Switch	598
	The <i>-A</i> Switch	600
	The <i>-c</i> Switch	600
	The <i>-n</i> Switch	601
	The <i>-r</i> Switch	601
	The <i>-R</i> Switch	602
	The <i>-S</i> Switch	602
	The <i>-s</i> Switch	603
	Using the <i>netstat</i> Utility	603
	The <i>-a</i> Switch	606
	The <i>-e</i> Switch	607
	The <i>-r</i> Switch	608
	The <i>-s</i> Switch	608
	The <i>-p</i> Switch	608
	The <i>-n</i> Switch	610
	Using the File Transfer Protocol (FTP)	612
	Starting FTP and Logging In to an FTP Server	613
	Downloading Files	614
	Uploading Files	616

	Using the Telephone Network ( <i>Telnet</i> ) Utility	617
	How to Enable Telnet in Vista	617
	Don't Use Telnet, Use Secure Shell (SSH)	618
	Summary	619
	Exam Essentials	619
	Written Lab	620
	Review Questions	621
	Answers to Review Questions	626
	Answers to Written Lab	628
<b>Chapter 18</b>	<b>Software and Hardware Tools</b>	<b>629</b>
	Understanding Network Scanners	630
	Packet Sniffers	630
	Intrusion Detection and Prevention Software (IDS/IPS)	632
	Port Scanners	634
	Identifying Hardware Tools	637
	Cable Testers	637
	Protocol Analyzer	639
	Certifiers	640
	Time-Domain Reflectometer (TDR)	640
	Optical Time-Domain Reflectometer (OTDR)	641
	Multimeter	642
	Toner Probe	642
	Butt Set	644
	Punch-Down Tool	644
	Cable Stripper/Snips	646
	Voltage Event Recorder	647
	Temperature Monitor	648
	Summary	649
	Exam Essentials	649
	Written Lab	650
	Review Questions	651
	Answers to Review Questions	655
	Answers to Written Lab	657
<b>Chapter 19</b>	<b>Network Troubleshooting</b>	<b>659</b>
	Narrowing Down the Problem	661
	Are There Any Cabling Issues? Did You Check the Super Simple Stuff?	662
	Is Hardware or Software Causing the Problem?	665
	Is It a Workstation or a Server Problem?	666
	Which Segments of the Network Are Affected?	667
	Is It Bad Cabling?	667

	Troubleshooting Steps	672
	Step 1: Information Gathering—Identify Symptoms and Problems	672
	Step 2: Identify the Affected Areas of the Network	673
	Step 3: Determine if Anything Has Changed	674
	Step 4: Establish the Most Probable Cause	675
	Step 5: Determine if Escalation Is Necessary	678
	Step 6: Create an Action Plan and Solution, Identifying Potential Effects	680
	Step 7: Implement and Test the Solution	683
	Step 8: Identify the Results and Effects of the Solution	683
	Step 9: Document the Solution and the Entire Process	684
	Troubleshooting Tips	685
	Don't Overlook the Small Stuff	685
	Prioritize Your Problems	685
	Check the Software Configuration	686
	Don't Overlook Physical Conditions	686
	Don't Overlook Cable Problems	687
	Check for Viruses	687
	Summary	688
	Exam Essentials	688
	Written Lab	690
	Review Questions	691
	Answers to Review Questions	695
	Answers to Written Lab	697
<b>Chapter 20</b>	<b>Management, Monitoring, and Optimization</b>	<b>699</b>
	Managing Network Documentation	702
	Schematics and Diagrams	703
	Baselines	709
	Policies, Procedures, and Regulations	711
	Monitoring the Network and Optimizing Its Performance	713
	Network Monitoring and Logging	713
	Reasons to Optimize Your Network's Performance	716
	How to Optimize Performance	718
	Summary	721
	Exam Essentials	722
	Written Lab	723
	Review Questions	724
	Answers to Review Questions	728
	Answers to Written Lab	730