

Networking Essentials

Third Edition

Jeffrey S. Beasley
Piyasat Nilkaew

Software Enclosed



Networking Essentials

Third Edition

**Jeffrey S. Beasley and
Piyasat Nilkaew**

Pearson
800 East 96th Street
Indianapolis, Indiana 46240 USA

NETWORKING ESSENTIALS, THIRD EDITION

Copyright © 2012 by Pearson Education, Inc.

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

ISBN-13: 978-0-7897-4903-1

ISBN-10: 0-7897-4903-3

Library of Congress Cataloging-in-Publication Data

Beasley, Jeffrey S., 1955-

Networking essentials / Jeffrey S. Beasley and Piyasat Nilkaew. – 3rd ed.

p. cm.

Rev. ed. of: Networking / Jeffrey S. Beasley.

Includes index.

ISBN 978-0-7897-4903-1 (hardcover w/cd)

1. Computer networks--Design and construction. 2. TCP/IP (Computer network protocol) 3. Internetworking (Telecommunication) I. Nilkaew, Piyasat. II. Beasley, Jeffrey S., 1955-. Networking. III. Title.

TK5105.5.B39 2012

004.6--dc23

2011051393

Printed in the United States of America

First Printing: March 2012

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 authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Bulk Sales

Pearson IT Certification offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales

1-800-382-3419

corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales

international@pearson.com

Associate Publisher

Dave Dusthimer

Executive Editor

Brett Bartow

Senior Development Editor

Christopher Cleveland

Managing Editor

Sandra Schroeder

Project Editor

Mandie Frank

Copy Editor

Megan Wade

Indexer

Lisa Stumpf

Proofreader

Leslie Joseph

Technical Editors

Dr. Kenneth L Hawkins

Douglas E. Maume

Peer Reviewers

DeAnnia Clements

Osman Guzide

Gene Carwile

Dr. Theodor Richardson

Publishing Coordinator

Vanessa Evans

Designer

Gary Adair

Compositor

Studio Galou LLC

Contents at a Glance

	Introduction	xxii
Chapter 1	Introduction to Computer Networks	2
Chapter 2	Physical Layer Cabling: Twisted Pair	58
Chapter 3	Physical Layer Cabling: Fiber Optics	114
Chapter 4	Wireless Networking	152
Chapter 5	Interconnecting the LANs	196
Chapter 6	TCP/IP	236
Chapter 7	Introduction to Router Configuration	286
Chapter 8	Introduction to Switch Configuration	326
Chapter 9	Routing Protocols	356
Chapter 10	Internet Technologies: Out to the Internet	398
Chapter 11	Troubleshooting	438
Chapter 12	Network Security	466
	Glossary	503
	Index	518

Table of Contents

Introduction

xxii

Chapter 1	Introduction to Computer Networks	2
1-1	INTRODUCTION	5
1-2	NETWORK TOPOLOGIES	7
	Section 1-2 Review	11
	Test Your Knowledge	12
1-3	THE OSI MODEL	12
	Section 1-3 Review	14
	Test Your Knowledge	15
1-4	THE ETHERNET LAN	15
	IP Addressing	19
	Section 1-4 Review	21
	Test Your Knowledge	22
1-5	HOME NETWORKING	22
	Securing the Home Network	34
	IP Addressing in the Home Network	36
	Section 1-5 Review	37
	Test Your Knowledge	38
1-6	ASSEMBLING AN OFFICE LAN	38
	Section 1-6 Review	43
	Test Your Knowledge	44
1-7	TESTING AND TROUBLESHOOTING A LAN	44
	Section 1-7 Review	46
	Test Your Knowledge	47
	Summary	48
	Questions and Problems	48
	Section 1-1	48
	Section 1-2	49
	Section 1-3	50
	Section 1-4	51

Section 1-5	52
Section 1-6	54
Section 1-7	55
Certification Questions	55
Chapter 2 Physical Layer Cabling: Twisted Pair	58
2-1 INTRODUCTION	61
2-2 STRUCTURED CABLING	62
Horizontal Cabling	65
Section 2-2 Review	68
Test Your Knowledge	69
2-3 UNSHIELDED TWISTED-PAIR CABLE	69
Shielded Twisted-pair Cable	72
Section 2-3 Review	72
Test Your Knowledge	72
2-4 TERMINATING CAT6/5E/5 UTP CABLES	73
Computer Communication	74
Straight-through and Crossover Patch Cables	76
Section 2-4 Review	85
Test Your Knowledge	85
2-5 CABLE TESTING AND CERTIFICATION	86
Section 2-5 Review	90
Test Your Knowledge	90
2-6 10 Gigabit Ethernet over Copper	90
Overview	91
Alien Crosstalk	91
Signal Transmission	93
Section 2-6 Review	94
Test Your Knowledge	94
2-7 TROUBLESHOOTING CABLING SYSTEMS	94
Installation	94
Cable Stretching	95
Cable Failing to Meet Manufacturer	
Specifications	95
CAT5e Cable Test Examples	96
Section 2-7 Review	103
Test Your Knowledge	104
Summary	105
Questions and Problems	105

Section 2-1	105
Section 2-3	106
Section 2-4	107
Section 2-5	109
Section 2-6	109
Certification Questions	112
Chapter 3 Physical Layer Cabling: Fiber Optics 114	
3-1 INTRODUCTION	117
3-2 THE NATURE OF LIGHT	119
Graded-Index Fiber	123
Single-Mode Fibers	124
Section 3-2 Review	125
Test Your Knowledge	125
3-3 FIBER ATTENUATION AND DISPERSION	126
Attenuation	126
Dispersion	127
Dispersion Compensation	129
Section 3-3 Review	130
Test Your Knowledge	130
3-4 OPTICAL COMPONENTS	130
Intermediate Components	132
Detectors	132
Fiber Connectorization	134
Section 3-4 Review	135
Test Your Knowledge	135
3-5 OPTICAL NETWORKING	136
Defining Optical Networking	136
Building Distribution	138
Campus Distribution	141
Section 3-5 Review	144
Test Your Knowledge	145
3-6 SAFETY	145
Section 3-6 Review	146
Test Your Knowledge	146
Summary	147
Questions and Problems	147
Section 3-1	147
Section 3-2	147

Section 3-3	148
Section 3-4	148
Section 3-5	149
Section 3-6	149
Certification Questions	150
Chapter 4 Wireless Networking	152
4-1 INTRODUCTION	154
4-2 THE IEEE 802.11 WIRELESS LAN STANDARD	155
Section 4-2 Review	162
Test Your Knowledge	162
4-3 802.11 WIRELESS NETWORKING	163
Section 4-3 Review	171
Test Your Knowledge	172
4-4 Bluetooth, WiMAX, and RFID	172
Bluetooth	172
WiMAX	174
Radio Frequency Identification	175
Section 4-4 Review	179
Test Your Knowledge	179
4-5 SECURING WIRELESS LANS	179
Section 4-5 Review	182
Test Your Knowledge	182
4-6 CONFIGURING A POINT-TO-MULTIPOINT WIRELESS LAN: A CASE STUDY	183
1. Antenna Site Survey	183
2. Establishing a Point-to-Point Wireless Link to the Home Network	184
3-4. Configuring the Multipoint Distribution/Conducting an RF Site Survey	185
5. Configuring the Remote Installations	187
Section 4-6 Review	187
Test Your Knowledge	188
Summary	189
Questions and Problems	189
Section 4-2	189
Section 4-3	190
Section 4-4	191
Section 4-5	192

Section 4-6	193
Critical Thinking	193
Certification Questions	194
Chapter 5 Interconnecting the LANs	196
5-1 INTRODUCTION	198
5-2 THE NETWORK BRIDGE	199
Section 5-2 Review	203
Test Your Knowledge	204
5-3 THE NETWORK SWITCH	204
Hub-Switch Comparison	206
Managed Switches	209
Multilayer Switches	214
Section 5-3 Review	214
Test Your Knowledge	215
5-4 THE ROUTER	215
The Router Interface: Cisco 2800 Series	216
The Router Interface—Cisco 2600 Series	217
The Router Interface—Cisco 2500 Series	218
Section 5-4 Review	220
Test Your Knowledge	220
5-5 INTERCONNECTING LANS WITH THE ROUTER	221
Gateway Address	223
Network Segments	223
Section 5-5 Review	224
Test Your Knowledge	224
5-6 CONFIGURING THE NETWORK INTERFACE—AUTO-NEGOTIATION	225
Auto-Negotiation Steps	225
Full-Duplex/Half-Duplex	226
Section 5-6 Review	228
Test Your Knowledge	228
Summary	229
Questions and Problems	229
Section 5-2	229
Section 5-3	230
Section 5-4	232
Section 5-5	232
Section 5-6	233

Critical Thinking	233
Certification Questions	234
Chapter 6	
TCP/IP	236
6-1 INTRODUCTION	238
6-2 THE TCP/IP LAYERS	239
The Application Layer	240
The Transport Layer	241
The Internet Layer	245
The Network Interface Layer	248
Section 6-2 Review	248
Test Your Knowledge	249
6-3 NUMBER CONVERSION	249
Binary-to-Decimal Conversion	249
Decimal-to-Binary Conversion	251
Hexadecimal Numbers	252
Section 6-3 Review	255
Test Your Knowledge	255
6-4 IPv4 ADDRESSING	255
Private IP Addresses	258
IP Address Assignment	258
Section 6-4 Review	259
Test Your Knowledge	259
6-5 SUBNET MASKS	259
Section 6-5 Review	266
Test Your Knowledge	266
6-6 CIDR BLOCKS	267
Section 6-6 Review	269
Test Your Knowledge	270
6-7 IPV6 ADDRESSING	270
Section 6-7 Review	273
Test Your Knowledge	273
Summary	274
Questions and Problems	274
Section 6-2	274
Section 6-3	276
Section 6-4	277
Section 6-5	278
Section 6-6	280
Section 6-7	282

Critical Thinking	282
Certification Questions	283
Chapter 7	
Introduction to Router Configuration	286
7-1 INTRODUCTION	288
7-2 ROUTER FUNDAMENTALS	289
Layer 3 Networks	290
Section 7-2 Review	296
Test Your Knowledge	296
7-3 THE CONSOLE PORT CONNECTION	296
Configuring the HyperTerminal Software (Windows)	298
Configuring the Z-Term Serial Communications Software (Mac)	300
Section 7-3 Review	302
Test Your Knowledge	302
7-4 THE ROUTER'S USER EXEC MODE (ROUTER>)	303
The User EXEC Mode	303
Router Configuration Challenge: The User EXEC Mode	305
Section 7-4 Review	308
Test Your Knowledge	308
7-5 THE ROUTER'S PRIVILEGED EXEC MODE (ROUTER#)	308
Hostname	309
Enable Secret	310
Setting the Line Console Passwords	310
Fast Ethernet Interface Configuration	311
Serial Interface Configuration	312
Router Configuration Challenge: The Privileged EXEC Mode	314
Section 7-5 Review	316
Test Your Knowledge	316
Summary	317
Questions and Problems	317
Section 7-1	317
Section 7-2	317
Section 7-3	320

Section 7-4	320
Section 7-5	321
Critical Thinking	322
Certification Questions	323
Chapter 8 Introduction to Switch Configuration	326
8-1 INTRODUCTION	328
8-2 Introduction to VLANs	329
Virtual LAN	329
Section 8-2 Review	330
Test Your Knowledge	330
8-3 Introduction to Switch Configuration	330
Hostname	331
Enable Secret	332
Setting the Line Console Passwords	332
Static VLAN Configuration	333
Networking Challenge—Switch Configuration	337
Section 8-3 Review	337
Test Your Knowledge	338
8-4 Spanning-Tree Protocol	338
Section 8-4 Review	339
Test Your Knowledge	340
8-5 Network Management	340
Configuring SNMP	341
Section 8-5 Review	344
Test Your Knowledge	344
8-6 Power over Ethernet	344
Section 8-6 Review	346
Test Your Knowledge	347
Summary	348
Questions and Problems	348
Section 8-2	348
Section 8-3	349
Section 8-4	350
Section 8-5	350
Section 8-6	352
Critical Thinking	353
Certification Questions	353

Chapter 9	Routing Protocols	356
9-1	INTRODUCTION	358
9-2	STATIC ROUTING	359
	Gateway of Last Resort	366
	Configuring Static Routes	366
	Networking Challenge: Chapter 9—	
	Static Routes	368
	Section 9-2 Review	369
	Test Your Knowledge	369
9-3	DYNAMIC ROUTING PROTOCOLS	370
	Section 9-3 Review	371
	Test Your Knowledge	371
9-4	DISTANCE VECTOR PROTOCOLS	372
	Section 9-4 Review	374
	Test Your Knowledge	374
9-5	LINK STATE PROTOCOLS	375
	Section 9-5 Review	378
	Test Your Knowledge	378
9-6	HYBRID PROTOCOLS	378
	Section 9-6 Review	379
	Test Your Knowledge	379
9-7	CONFIGURING RIP and RIPv2	379
	Configuring Routes with RIP	381
	Configuring Routes with RIP Version 2	385
	Networking Challenge—RIP V2	387
	Section 9-7 Review	388
	Test Your Knowledge	388
	Summary	389
	Questions and Problems	389
	Section 9-2	389
	Section 9-3	391
	Section 9-4	392
	Section 9-5	392
	Section 9-6	393
	Section 9-7	394
	Critical Thinking	395
	Certification Questions	395

Chapter 10 Internet Technologies: Out to the Internet

	398
10-1 INTRODUCTION	401
10-2 THE LINE CONNECTION	402
Data Channels	403
Point of Presence	404
Section 10-2 Review	406
Test Your Knowledge	407
10-3 REMOTE ACCESS	407
Analog Modem Technologies	407
Cable Modems	408
xDSL Modems	408
The Remote Access Server	410
Section 10-3 Review	411
Test Your Knowledge	411
10-4 Metro Ethernet/Carrier Ethernet	412
Ethernet Service Types	413
Service Attributes	414
Section 10-4 Review	415
Test Your Knowledge	416
10-5 NETWORK SERVICES—DHCP AND DNS	416
The DHCP Data Packets	418
DHCP Deployment	419
Network Services: DNS	420
Internet Domain Name	421
Section 10-5 Review	423
Test Your Knowledge	423
10-6 INTERNET ROUTING—BGP	424
Section 10-6 Review	426
Test Your Knowledge	427
10-7 ANALYZING INTERNET DATA TRAFFIC	427
Utilization/Errors Strip Chart	428
Network Layer Matrix	429
Network Layer Host Table	430
Frame Size Distribution	430
Section 10-7 Review	431
Test Your Knowledge	432
Summary	433
Questions and Problems	433

Section 10-2	433
Section 10-3	434
Section 10-4	434
Section 10-5	435
Section 10-6	435
Certification Questions	436
Chapter 11 Troubleshooting	438
11-1 INTRODUCTION	440
11-2 ANALYZING COMPUTER NETWORKS	441
Using Wireshark to Inspect Data Packets	442
Using Wireshark to Capture Packets	444
Section 11-2 Review	446
Test Your Knowledge	446
11-3 ANALYZING COMPUTER NETWORKS—FTP DATA PACKETS	446
Section 11-3 Review	447
Test Your Knowledge	448
11-4 ANALYZING CAMPUS NETWORK DATA TRAFFIC	448
Section 11-4 Review	450
Test Your Knowledge	450
11-5 TROUBLESHOOTING THE ROUTER INTERFACE	451
Section 11-5 Review	454
Test Your Knowledge	454
11-6 TROUBLESHOOTING THE SWITCH INTERFACE	454
Section 11-6 Review	457
Test Your Knowledge	457
11-7 TROUBLESHOOTING FIBER OPTICS—The OTDR	457
Section 11-7 Review	459
Test Your Knowledge	459
Summary	460
Questions and Problems	460
Section 11-2	460
Section 11-3	461
Section 11-4	462
Section 11-5	462

Section 11-6	462
Section 11-7	463
Certification Questions	463
Chapter 12 Network Security	466
12-1 INTRODUCTION	468
12-2 INTRUSION (HOW AN ATTACKER GAINS CONTROL OF A NETWORK)	469
Social Engineering	469
Password Cracking	470
Packet Sniffing	470
Vulnerable Software	471
Viruses and Worms	473
Section 12-2 Review	474
Test Your Knowledge	474
12-3 DENIAL OF SERVICE	475
Distributed Denial-of-service Attacks	476
Section 12-3 Review	477
Test Your Knowledge	477
12-4 SECURITY SOFTWARE AND HARDWARE	477
Antivirus Software	477
Personal Firewall	478
Firewall	484
Other Security Appliances	485
Section 12-4 Review	486
Test Your Knowledge	486
12-5 INTRODUCTION TO VIRTUAL PRIVATE NETWORK	486
VPN Tunneling Protocols	487
Configuring a Remote Access VPN Server	489
Configuring a Remote Client's VPN	
Connection	489
Cisco VPN Client	491
Section 12-5 Review	495
Test Your Knowledge	495
Summary	497
Questions and Problems	497
Section 12-2	497
Section 12-3	498

Section 12-4	498
Section 12-5	499
Critical Thinking	500
Certification Questions	500

Glossary of Key Terms	503
------------------------------	------------

Index	518
--------------	------------

ABOUT THE AUTHORS

Jeff Beasley is a professor and department head in the Information and Communications Technology program at New Mexico State University, where he teaches computer networking and many related topics. He is coauthor of *Modern Electronic Communication*, Ninth Edition and author of *Networking*, Second Edition.

Piyasat Nilkaew is a network manager at New Mexico State University with more than fifteen years of experience in network management and consulting. He has extensive expertise in deploying and integrating multi-protocol and multi-vendor data, voice, and video network solutions.

DEDICATIONS

This book is dedicated to my family, Kim, Damon, and Dana.

—Jeff Beasley

This book is dedicated to my parents, Boonsong and Pariya Nilkaew.

Thank you for your unwavering love and support that guide me through various stages of my life. Thank you for all the wisdom and values you have instilled in me to build my life's foundation. You are my best teachers and I am eternally grateful.

—Piyasat Nilkaew

ACKNOWLEDGMENTS

I am grateful to the many people who have helped with this text. My sincere thanks go to the following technical consultants:

- Danny Bosch and Matthew Peralta for sharing their expertise with optical networks and unshielded twisted pair cabling, and Don Yates for his help with the initial Net-Challenge software.
- Byron Hicks, for his helpful suggestions on the configuring, managing, and troubleshooting sections.
- Todd Bowman, CCIE#6316, for guiding me through the challenging routing protocols, wide area networking, managing a campus type network, and network security.

I would also like to thank my many past and present students for their help with this book.

- David Potts, Jonathan Trejo and Nate Murillo for their work on the Net-Challenge software; Adam Segura for his help with taking pictures of the steps for CAT6 termination; Marc Montez, Carine George-Morris, Brian Morales, Michael Thomas, Jacob Ulibarri, Scott Leppelman, and Aarin Buskirk for their help with laboratory development; and Josiah Jones and Raul Marquez Jr. for their help with the Wireshark material.
- Aaron Shapiro and Aaron Jackson for their help in testing the many network connections presented in the text.
- Paul Bueno and Anthony Bueno for reading through the early draft of the text.

Your efforts are greatly appreciated.

I appreciate the excellent feedback of the following reviewers: Phillip Davis, DelMar College, TX; Thomas D. Edwards, Carteret Community College, NC; William Hessmiller, Editors & Training Associates; Bill Liu, DeVry University, CA; and Timothy Staley, DeVry University, TX.

My thanks to the people at Pearson for making this project possible: Dave Dusthimer, for providing me with the opportunity to work on the third edition of this text and Vanessa Evans, for helping make this process enjoyable. Thanks to Christopher Cleveland, and the all the people at Pearson IT Certification, and also to the many technical editors for their help with editing the manuscript.

Special thanks to our families for their continued support and patience.

—Jeffrey S. Beasley and Piyasat Nilkaew

ABOUT THE TECHNICAL REVIEWERS

Dr. Kenneth L. Hawkins is the Program Director of Information Technology at the Hampton campus of Bryant and Stratton College. He earned his doctorate in Education from Nova Southeastern University, a master's degree in Computer Science from Boston University, a master's degree in Education from Old Dominion University, a master's degree in Management from Troy State University, and his undergraduate degree in Mathematics from Michigan Technological University. Dr. Hawkins, a retired military officer, has worked in post-secondary education for the past fourteen years as department head, campus dean, and faculty for undergraduate and graduate business and information technology courses at six Tidewater universities. A graduate of the Leadership Institute of the Virginia Peninsula, he is actively involved both professionally and socially in the community having served as district chairman for the Boy Scouts of America, educational administration consultant for a local private school, board member of two area businesses, member of the international professional society Phi Gamma Sigma and member of the Old Point Comfort Yacht Club.

Douglas E. Maume is currently the Lead Instructor for the Computer Networking program at Centura College Online. He has been conducting new and annual course reviews for both the CN and IT programs since 2006. He is also an adjunct professor for Centura College; teaching Computer Networking, Information Technology, and Business Management courses since 2001. Mr. Maume owned his own business called Wish You Were Here, Personal Postcards, creating digital postcards on location at the Virginia Beach oceanfront. He earned a Bachelor's degree in Graphic Design from Old Dominion University, and an Associate's in Applied Science degree in Graphic Design from Tidewater Community College. Mr. Maume is currently Esquire to the District Deputy Grand Exalted Ruler for Southeast Virginia in the Benevolent and Protective Order of Elks. He has been actively involved with the Elks since 1999, serving the Veteran's and Youth of the Norfolk Community. He is also the Registrar for the adult men's league; Shipps Corner Soccer Club, and has been playing competitively since 1972.

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.

As the associate publisher for Pearson IT Certification, I welcome your comments. You can email or write me directly to let me 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 I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

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

Email: feedback@pearsonitcertification.com

Mail:
Dave Dustimer
Associate Publisher
Pearson IT Certification
800 East 96th Street
Indianapolis, IN 46240 USA

READER SERVICES

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

Introduction

This book provides a look at computer networking from the point of view of the network administrator. It guides readers from an entry-level knowledge in computer networks to advanced concepts in Ethernet networks, router configuration, TCP/IP networks, routing protocols, local, campus, and wide area network configuration, network security, wireless networking, optical networks, Voice over IP, the network server, Linux networking, and industrial networks. After covering the entire text, readers will have gained a solid knowledge base in computer networks.

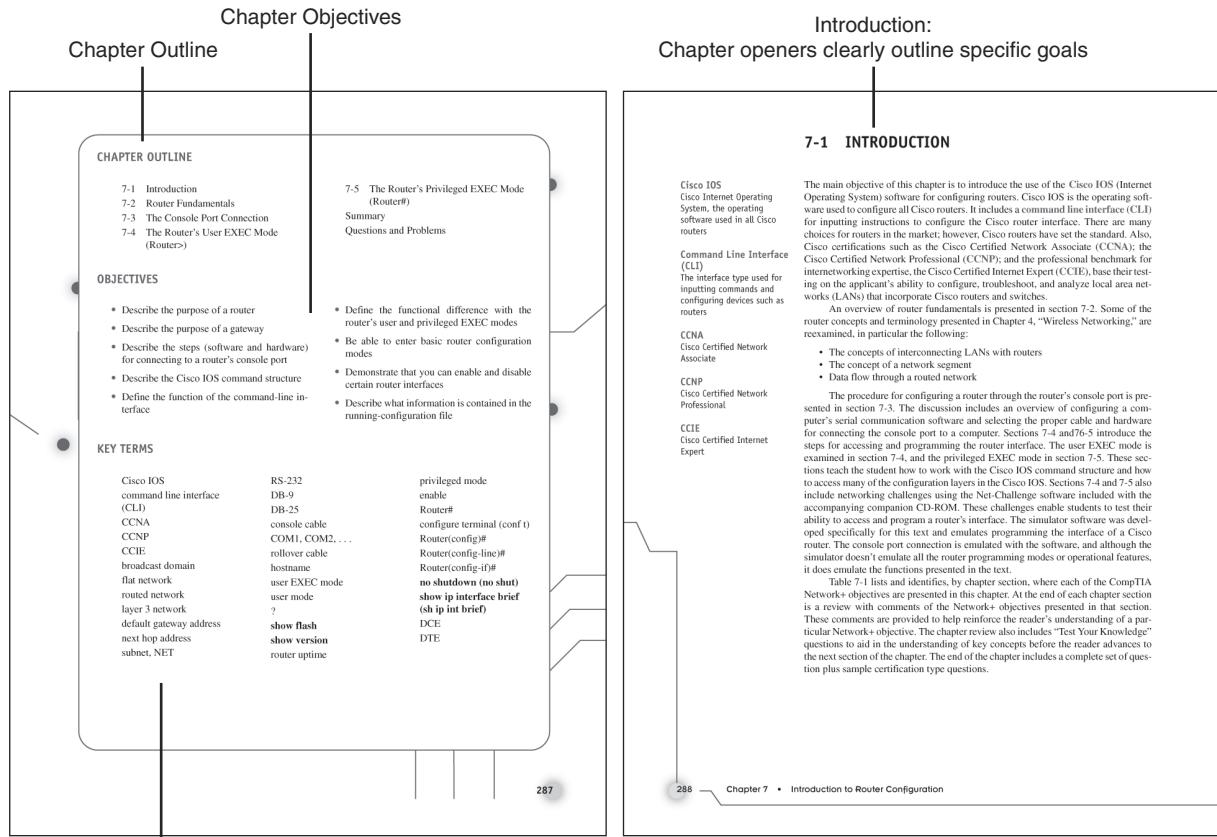
In my years of teaching, I have observed that technology students prefer to learn “how to swim” after they have gotten wet and taken in a little water. Then they are ready for more challenges. Show the students the technology, how it is used, and why, and they will take the applications of the technology to the next level. Allowing them to experiment with the technology helps them to develop a greater understanding. This book does just that.

ORGANIZATION OF THE TEXT

Thoroughly updated to reflect the latest version of CompTIA’s Network+ exam, **Networking Essentials, 3rd Edition**, is a practical, up-to-date, and hands-on guide to the basics of networking. Written from the viewpoint of a working network administrator, it requires absolutely no experience with either network concepts or day-to-day network management. This new edition splits the previous edition into two volumes. This first volume has been revised and reorganized around the needs of introductory networking students, and assumes no previous knowledge. Throughout the text, the students will gain an appreciation of how basic computer networks and related hardware are interconnected to form a network. This involves understanding the concepts of twisted pair cable, fiber optics, interconnecting LANs, configuring TCP/IP, subnet masking, basic router configuration, switch configuration and management, wireless networking, and network security.

Key Pedagogical Features

- *Chapter Outline, Network+ Objectives, Key Terms, and Introduction* at the beginning of each chapter clearly outline specific goals for the reader. An example of these features is shown in Figure P-1.



Key Terms for
this chapter

FIGURE P-1

- *Net-Challenge Software* provides a simulated, hands-on experience in configuring routers and switches. Exercises provided in the text (see Figure P-2) and on the CD challenge readers to undertake certain router/network configuration tasks. The challenges check the students' ability to enter basic networking commands and to set up router function, such as configuring the interface (Ethernet and Serial) and routing protocols (that is, RIP, and static). The software has the look and feel of actually being connected to the router's console port.

Net-Challenges are found throughout the text

to a console session, thus enabling the simulated console terminal access to all three routers. The routers are marked with their default hostnames of Router A, Router B, and Router C. This challenge tests your ability to use router commands in the User EXEC mode. Click on the Net-Challenge icon to open the software. Then click the Select Challenge button to open a list of challenges available with the software. Select the Chapter 7 - User EXEC Mode challenge. Selecting a challenge will open a check box window, as shown in Figure 7-16. The tasks in each challenge will be checked as completed, as appropriate.

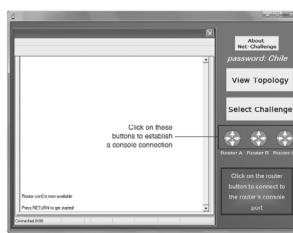


FIGURE 7-15 The Net-Challenge screen.



FIGURE 7-16 The check box for the User EXEC Net-Challenge software.

306 Chapter 7 • Introduction to Router Configuration

1. Make sure you are connected to Router A by clicking the appropriate selection button.

2. Demonstrate that you can enter the router's user EXEC mode. The router screen will display Router> when you are in the user EXEC mode.

3. Enter ? to display the help menu. Then click the Select Challenge button. The challenge simulation software. You should see that the enable, exit, and show commands are available from the Router> prompt. The Net-Challenge software displays only the available commands and options within the software. The text provided in the challenge software is the help text that the software looks up.

4. Enter exit from the Router> prompt (Router>exit). Where does this place you? You should be back at the Press RETURN screen, as shown in Figure 7-17.

5. Enter the user EXEC mode by pressing Enter.

6. Enter the command show after the Router> prompt (Router>show).

This step generates an "error unknown command" message. Include a ? after the show command to see which options are available for show. The text displayed on the terminal screen should look like Figure 7-17.



FIGURE 7-17 The display for Step 6 using the show command.

7. Enter the command show flash at the Router> prompt on the command line interface. Describe the information displayed.

8. Enter the command show version at the Router> prompt on the command line interface. Describe the information displayed.

9. Enter the command show history at the Router> prompt on the command line interface. Describe the information displayed.

Section 7-4 • THE ROUTER'S USER EXEC MODE (ROUTER>) 307

FIGURE P-2

- The textbook features and introduces how to use the *Wireshark Network Protocol Analyzer*. Examples of using the software to analyze data traffic are included throughout the text. *Numerous worked-out examples* are included in every chapter to reinforce key concepts and aid in subject mastery, as shown in Figure P-3.

Examples using the Wireshark Network Protocol Analyzer are included throughout the text

provided in the Capture folder with the text's accompanying CD-ROM. Portions of the captured data packets are shown in Figure 6-5.



FIGURE 6-4 The setup for the capture of the TCP connection.



FIGURE 6-5 An example of the three packets exchanged in the initial TCP handshake.

Packet 1 (0x0000) is the SYN or synchronizing packet. This packet is sent from the local computer on the network that wants to establish a TCP file transfer. In this example, Host A is making a TCP connection for an FTP transfer. The summary information for packet 1 specifies that this is a TCP packet, the source port is 1054 (SPT=1054), and the destination port is 21 (DPT=21). Port 1054 is an arbitrary port chosen by the client picks or is assigned by the operating system. The destination port 21 is commonly used for establishing an FTP port (see Table 6-4). The packet has a starting sequence number, 99762768, and there is no acknowledgement (ACK=0). The length of the data packet is 0 (LEN=0). This indicates that the data does not contain any data. The window size is 16384 (WS=16384). The window size indicates how many data packets can be transferred without an acknowledgement.

Packet 2 is the SYN-ACK packet from the FTP server. The sequence number SEQ = 399692546 is the sum of a new sequence number and the acknowledgement number. Host A receives the packet with SEQ=399692546 and the destination port 21 (DPT=21) and the source port for packet 2 is 1054 (DPT=1054). ACK=99762769 is an acknowledgement by host B (the FTP server) for the first TCP transmission was received. Note that this acknowledgement shows an increment of 1 from the initial sequence number specified by host A in packet 1.

Packet 3 is the acknowledgement from the local (host A) to the remote (host B) that packet 2 was received. Note that the acknowledgement is ACK=3996925467, which is an increment of 1 from the SEQ number transmitted in packet 2. This completes the initial handshake establishing the TCP connection. The next part is the data packet transfer. At this point, the two hosts can begin transferring data packets.

The last part of the TCP connection is terminating the session for each host. The final thing that happens is the sending of a FIN packet from the terminated host. This is seen in Figure 6-6. Host B sends a FIN packet to Host A indicating the data transfer is complete. Host A responds with an ACK packet acknowledging the reception of the FIN packet. Host A then sends Host B a FIN packet indicating the connection is being terminated. Host B replies with an ACK packet.

Section 6-2 • THE TCP/IP LAYERS 243

octet-3	128	64	32	16	8	4	2	1
	1	0	1	0	1	0	0	0
$(1 \times 128) + (1 \times 32) + (1 \times 8) = 128 + 32 + 8 = 168$								
octet-4	128	64	32	16	8	4	2	1
	1	1	0	0	0	0	0	0
$(1 \times 128) + (1 \times 64) = 128 + 64 = 192$								

Therefore, the dotted decimal equivalent is 192.168.32.12.

Decimal-to-Binary Conversion

The simplest way to convert a decimal number to binary is using division, repeatedly dividing the decimal number by 2 until the quotient is 0. The division steps for converting decimal numbers to binary are as follows:

- Divide the decimal number by 2. Record the remainder of 0 or 1, and write the quotient on the result of the division.
- Divide the quotient by 2 and record the remainder of 0 or 1. Write the quotient and repeat this step until the quotient is 0.
- Write the remainder numbers (0 and 1) in reverse order to obtain the binary equivalent value.

Example 6-2

Convert the decimal number 12 to binary.

Solution:

Divide 12 by 2. This equals 6 with a remainder of 0. Divide 6 by 2. This equals 3 with a remainder of 0. Divide 3 by 2. This equals 1 with a remainder of 1. Divide 1 by 2. This equals 0 with a remainder of 1. The quotient is 0; therefore, the conversion is done. Write the remainder numbers in reverse order to generate the binary equivalent value. This yields a value of 1 1 0. The calculation for this is shown:

2|12

2|6

2|3

2|1

0

You can verify the answer by converting the binary number back to decimal.

8	4	2	1
1	1	0	0
(1 × 8)	(1 × 4)	(1 × 2)	(1 × 1)
8	4	2	1

(1 × 8) + (1 × 4) = 12

Numerous worked out examples aid in subject mastery

FIGURE P-3

- Key Terms* and their definitions are highlighted in the margins to foster inquisitiveness and ensure retention. Illustrations and photos are used throughout to aid in understanding the concepts discussed. This is illustrated in Figure P-4.

Illustrations and photos enhance the text

• **DSU Port:** This T1 controller port connection is used to make the serial connection to Telco. This module has a built-in CSU/DSU module. There are five LEDs next to the RJ45 jack. These LEDs are for the following:

- TD—Transmit Data
- LP—Loop
- RD—Receive Data
- CD—Carrier Detect
- AL—Alarm

• **Ethernet Port:** This connection provides a 10/100Mbps Ethernet data link.

• **Analog Modem Ports:** This router has a 16-port analog network module.

The Router Interface—Cisco 2500 Series

Figure 5-17 shows the rear panel view (interface side) of a Cisco 2500 series router.

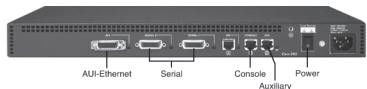


FIGURE 5-17 The rear panel view of a Cisco 2500 series router.

The following describes the function of each interface to the network.

- **Power On/Off:** Turns on/off electrical power to the router.
- **Auxiliary Input:** Used to connect a dial-in modem into the router. The auxiliary port provides an alternative way to remotely log in to the router if the network is down. This port also uses an RJ-45 connection.
- **Console Input:** Provides an RS-232 serial communications link into the router for initial router configuration. A special cable, called a *console cable*, is used to connect the console input to the serial port on a computer. The console cable uses RJ-45 plugs at both ends and requires the use of an RJ-45 to DB9 adapter for connecting to the COM1 or COM2 serial port.
- **Serial Ports:** Provides a serial data communication link into and out of the router, using V.35 serial interface cables. Figure 5-18 shows an example of a V.35 cable.
- **AUI Port:** This is a 10Mbps Ethernet port. AUI stands for “attachment unit-interface.”

218 — Chapter 5 • Interconnecting the LANs

Key Terms are defined in the margin

Test Your Knowledge

1. Which of the following are the five Spanning-Tree Protocol states?
 - a. Blocking
 - b. Listening
 - c. Selecting
 - d. Learning
 - e. Forwarding
 - f. Disabled
 - g. Passing
 - h. Cut-through
2. STP is which of the following? (select all that apply)
 - a. Link-management protocol
 - b. Replaces RIP as the routing protocol for switches
 - c. Used to minimize hops
 - d. Used to prevent loops

8-5 NETWORK MANAGEMENT

A network of moderate size has a tremendous number of data packets entering and leaving. The number of routers, switches, hubs, servers, and host computers can become staggering. Proper network management requires that all network resources be managed. This requires that proper management tools be in place.

A fundamental network management tool is **SNMP (SNMPv1)**, the Simple Network Management Protocol. SNMPv1, developed in 1988, is widely supported in most networking hardware. SNMP is a request-response User Datagram Protocol (UDP) for the exchange of data to and from port 161.

SNMP uses a **management information base (MIB)**, which is a collection of standard objects that are used to obtain configuration parameters and performance data on a networking device such as a router. For example, the MIB (*iDescr*) returns a description of the router's interfaces as demonstrated in Figure 8-3. An SNMP software tool was used to collect the interface description information. The IP address of the router is 10.10.10.1, and a *get request* (*iDescr*) was sent to port 161, the UDP port for SNMP. The descriptions of the interfaces were returned as shown.

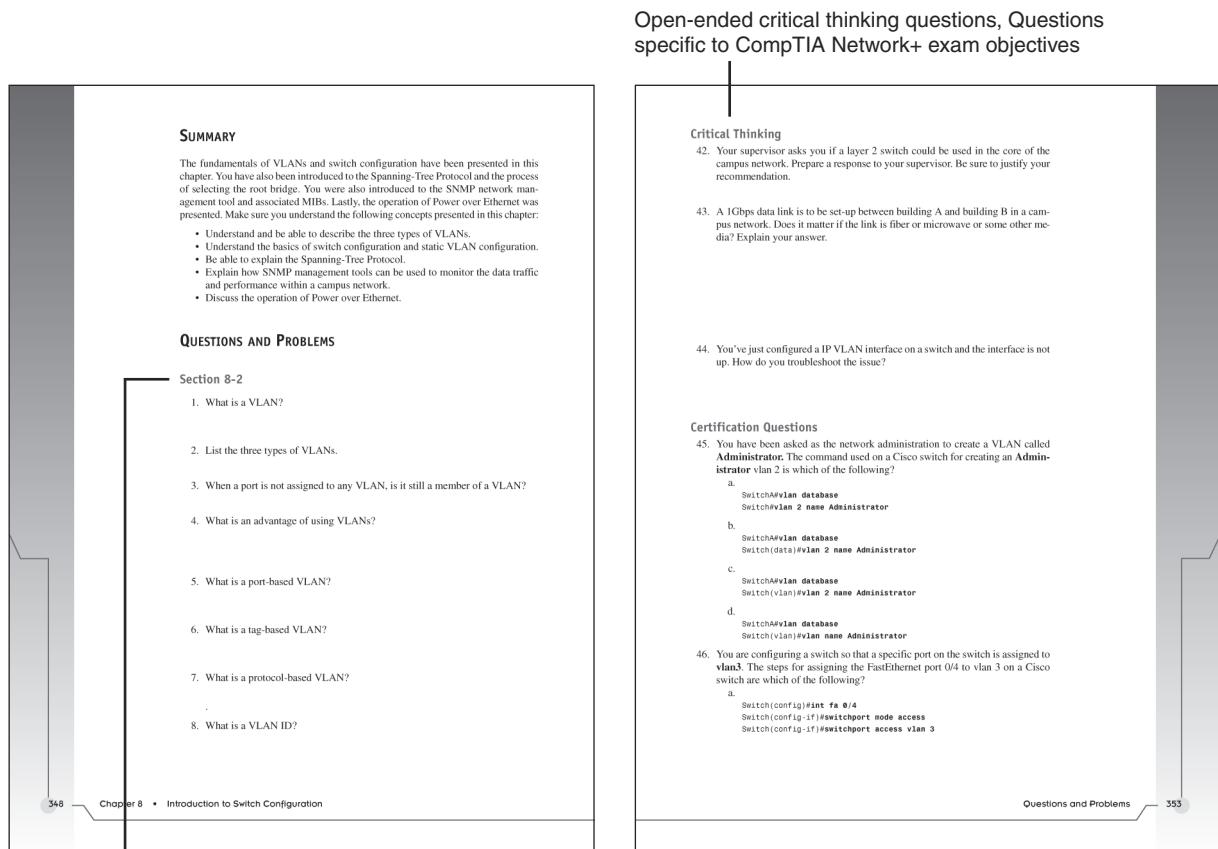
SNMP (SNMPv1)
Simple Network Management Protocol

Management Information Base (MIB)
A collection of standard objects that are used to obtain configuration parameters and performance data on a networking device

340 — Chapter 8 • Introduction to Switch Configuration

FIGURE P-4

- *Extensive Summaries, Questions and Problems, Critical Thinking, as well as Network+-specific Certification Questions are found at the end of each chapter, as shown in Figure P-5*



Summary, Questions and Problems organized by section

FIGURE P-5

- An extensive Glossary is found at the end of the book and offers quick, accessible definitions to key terms and acronyms, as well as an exhaustive Index (Figure P-6).

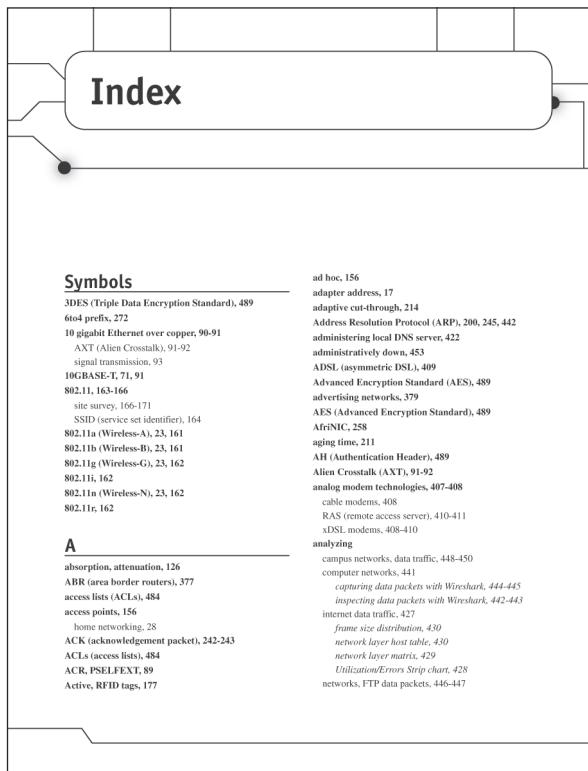
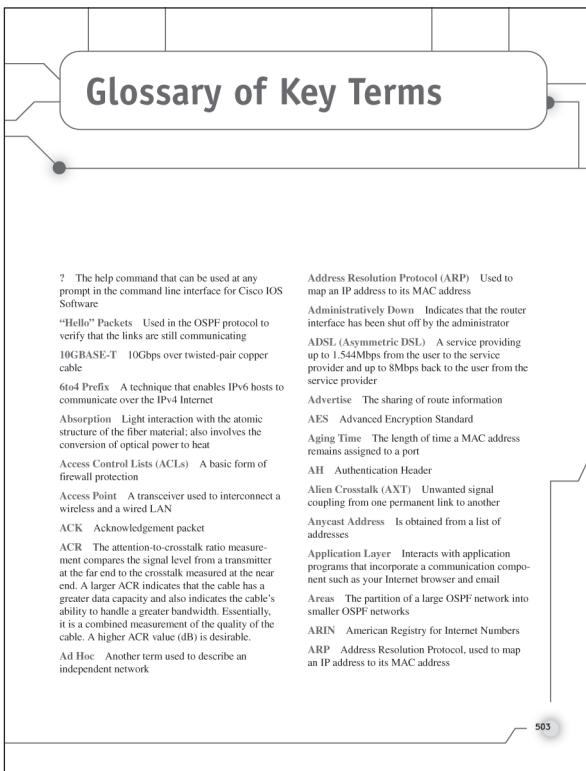


FIGURE P-6

Accompanying CD-ROM

The CD-ROM packaged with the text includes the captured data packets used in the text. It also includes the Net-Challenge Software, which was developed specifically for this text.

3

CHAPTER

Physical Layer Cabling: Fiber Optics

CHAPTER OUTLINE

- | | |
|--------------------------------------|------------------------|
| 3-1 Introduction | 3-5 Optical Networking |
| 3-2 The Nature of Light | 3-6 Safety |
| 3-3 Fiber Attenuation and Dispersion | Summary |
| 3-4 Optical Components | Questions and Problems |

OBJECTIVES

- Describe the advantages of glass fiber over copper conductors
- Describe the differences in how light travels in single- and multimode fiber
- Define *attenuation* and *dispersion* in fiber-optic cabling
- Describe the components of a fiber-optic system
- Describe the issues of optical networking, including fiber-to-the-business and fiber to-the-home
- Describe the new networking developments associated with optical Ethernet
- Understand the safety issues when working with fiber optics

KEY TERMS

refractive index	polarization mode-dispersion	fusion splicing
infrared light	zero-dispersion-wavelength	mechanical splices
optical spectrum	dispersion compensating fiber	index-matching gel
cladding	fiber Bragg grating	SC, ST, FC, LC, MT-RJ
numerical aperture	DL	SONET/SDH
multimode fiber	LED	STS
pulse dispersion	distributed feedback (DFB) laser	FTTC
graded-index fiber	dense wavelength division multiplex (DWDM)	FTTH
single-mode fiber	vertical cavity surface emitting lasers (VCSELs)	FTTB
step-index fiber	tunable laser	FTTD
long haul	fiber, light pipe, glass	optical Ethernet
mode field diameter	isolator	fiber cross-connect
scattering	received signal level (RSL)	GBIC
absorption		SFP
macrobending		XENPAK
microbending		XPAK
dispersion		X2
modal dispersion		XFP
chromatic dispersion		

continues

KEY TERMS continued

SFP+	logical fiber map	sm
IDC	physical fiber map	backbone
IC	mm	

3-1 INTRODUCTION

Recent advances in the development and manufacture of fiber-optic systems have made them the latest frontier in the field of optical networking. They are being used extensively for both private and commercial data links and have replaced a lot of copper wire. The latest networking technologies to benefit from the development in optical networking are gigabit Ethernet and 10 gigabit Ethernet.

A fiber-optic network is surprisingly simple, as shown in Figure 3-1. It is comprised of the following elements:

1. A fiber-optic transmission strand can carry the signal (in the form of a modulated light beam) a few feet or even hundreds or thousands of miles. A cable may contain three or four hair-like fibers or a bundle of hundreds of such fibers.
2. A source of invisible infrared radiation—usually a light-emitting diode (LED) or a solid-state laser—that can be modulated to impress digital data or an analog signal on the light beam.
3. A photosensitive detector to convert the optical signal back into an electrical signal at the receiver.
4. Efficient optical connectors at the light source-to-cable interface and at the cable-to-photo detector interface. These connectors are also critical when splicing the optical cable due to excessive loss that can occur at connections.

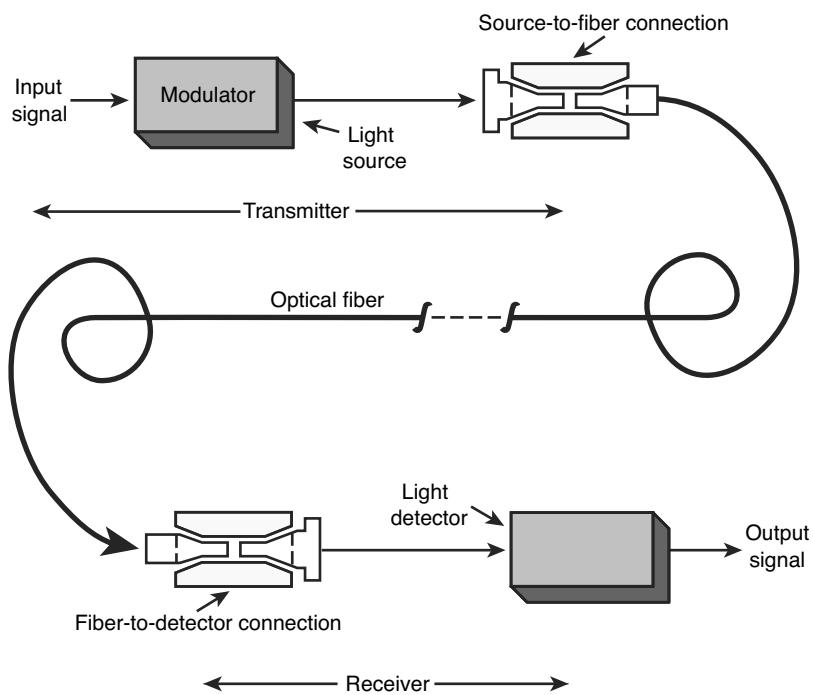


FIGURE 3-1 Fiber-optic communication system. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 781. Copyright ©2002 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

The advantages of optical communication links compared to copper conductors are enormous and include the following:

1. **Extremely wide system bandwidth:** The intelligence is impressed on the light by varying the light's amplitude. Because the best LEDs have a 5 ns response time, they provide a maximum bandwidth of about 100MHz. With laser light sources, however, data rates over 10Gbps are possible with a single-mode fiber. The amount of information multiplexed on such a system, in the hundreds of Gbps, is indeed staggering.
2. **Immunity to electrostatic interference:** External electrical noise and lightning do not affect energy in a fiber-optic strand. However, this is true only for the optical strands, not the metallic cable components or connecting electronics.
3. **Elimination of crosstalk:** The light in one glass fiber does not interfere with, nor is it susceptible to, the light in an adjacent fiber. Recall that crosstalk results from the electromagnetic coupling between two adjacent copper wires.
4. **Lower signal attenuation than other propagation systems:** Typical attenuation of a 1GHz bandwidth signal for optical fibers is 0.03 dB per 100 ft., compared to 4.0 dB for RG-58U coaxial.
5. **Lower costs:** Optical fiber costs are continuing to decline. The costs of many systems are declining with the use of fiber, and that trend is accelerating.
6. **Safety:** In many wired systems, the potential hazard of short circuits requires precautionary designs. Additionally, the dielectric nature of optic fibers eliminates the spark hazard.
7. **Corrosion:** Given that glass is basically inert, the corrosive effects of certain environments are not a problem.
8. **Security:** Due to its immunity to and from electromagnetic coupling and radiation, optical fiber can be used in most secure environments. Although it can be intercepted or tapped, it is very difficult to do so.

This chapter examines the issues of optical networking. Section 3-2 presents an overview of optical fiber fundamentals including a discussion on wavelengths and type of optical fibers. Section 3-3 examines the two distance-limiting parameters in fiber-optic transmission, attenuation, and dispersion. Optical components are presented in section 3-4. This includes the various types of connectors currently used on fiber. Optical networking is presented in section 3-5. An overview of SONET and FDDI are presented, followed by optical Ethernet. This section includes a discussion on setting up the building and campus distribution for fiber. Safety is extremely important when working with fiber. A brief overview of safety is presented in section 3-6.

Table 3-1 lists and identifies, by chapter section, where each of the CompTIA Network+ objectives are presented in this chapter. At the end of each chapter section is a review with comments of the Network+ objectives presented in that section. These comments are provided to help reinforce the reader's understanding of a particular Network+ objective. The chapter review also includes "Test Your Knowledge" questions to aid in the understanding of key concepts before the reader advances to the next section of the chapter. The end of the chapter includes a complete set of question plus sample certification type questions.

TABLE 3-1 Chapter 3 - CompTIA Network+ Objectives

Domain/ Objective Number	Domain/ Objective Description	Section Where Objective Is Covered
3.0	<i>Network Media and Topologies</i>	
3.1	Categorize standard media types and associated properties	3-2, 3-3, 3-6
3.2	Categorize standard connector types based on network media	3-4
3.7	Compare and contrast different LAN technologies	3-5
3.8	Identify components of wiring distribution	3-5
4.0	<i>Network Management</i>	
4.5	Describe the purpose of configuration management documentation	3-5

3-2 THE NATURE OF LIGHT

Before you can understand the propagation of light in a glass fiber, it is necessary to review some basics of light refraction and reflection. The speed of light in free space is 3×10^8 m/s but is reduced in other media, including fiber-optic cables. The reduction as light passes into denser material results in refraction of the light. Refraction causes the light wave to be bent, as shown in Figure 3-2. The speed reduction and subsequent refraction is different for each wavelength, as shown in Figure 3-2(b). The visible light striking the prism causes refraction at both air/glass interfaces and separates the light into its various frequencies (colors) as shown. This same effect produces a rainbow, with water droplets acting as prisms to split the sunlight into the visible spectrum of colors (the various frequencies).

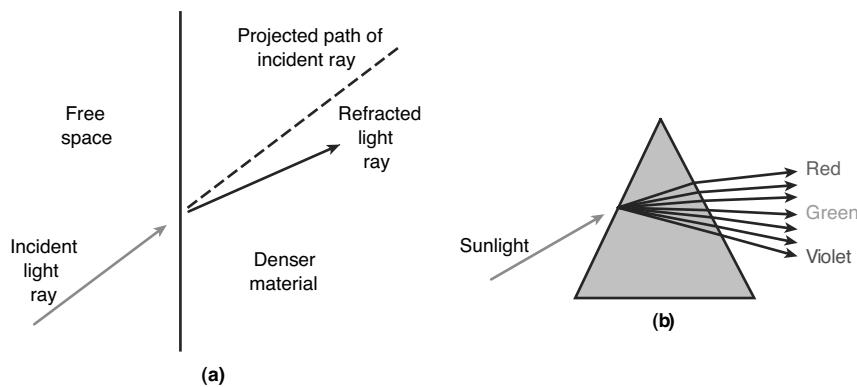


FIGURE 3-2 Refraction of light. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 782. Copyright ©2002 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

Refractive Index

Ratio of the speed of light in free space to its speed in a given material

Infrared Light

Light extending from 680 nm up to the wavelengths of the microwaves

Optical Spectrum

Light frequencies from the infrared on up

The amount of bend provided by refraction depends on the **refractive index** of the two materials involved. The refractive index, n , is the ratio of the speed of light in free space to the speed in a given material. It is slightly variable for different frequencies of light, but for most purposes a single value is accurate enough.

In the fiber-optics industry, spectrum notation is stated in nanometers (nm) rather than in frequency (Hz) simply because it is easier to use, particularly in spectral-width calculations. A convenient point of commonality is that 3×10^{14} Hz, or 300THz, is equivalent to 1 μm , or 1000 nm. This relationship is shown in Figure 3-3. The one exception to this naming convention is when discussing dense wavelength division multiplexing (DWDM), which is the transmission of several optical channels, or wavelengths, in the 1550-nm range, all on the same fiber. For DWDM systems, notations, and particularly channel separations, are stated in terahertz (THz). Wavelength division multiplexing (WDM) systems are discussed in section 3-5. An electromagnetic wavelength spectrum chart is provided in Figure 3-3. The electromagnetic light waves just below the frequencies in the visible spectrum extending from 680 nm up are called **infrared light** waves. Whereas visible light has a wavelength from approximately 430 nm up to 680 nm, infrared light extends from 680 nm up to the microwaves. The frequencies from the infrared on up are termed the **optical spectrum**.

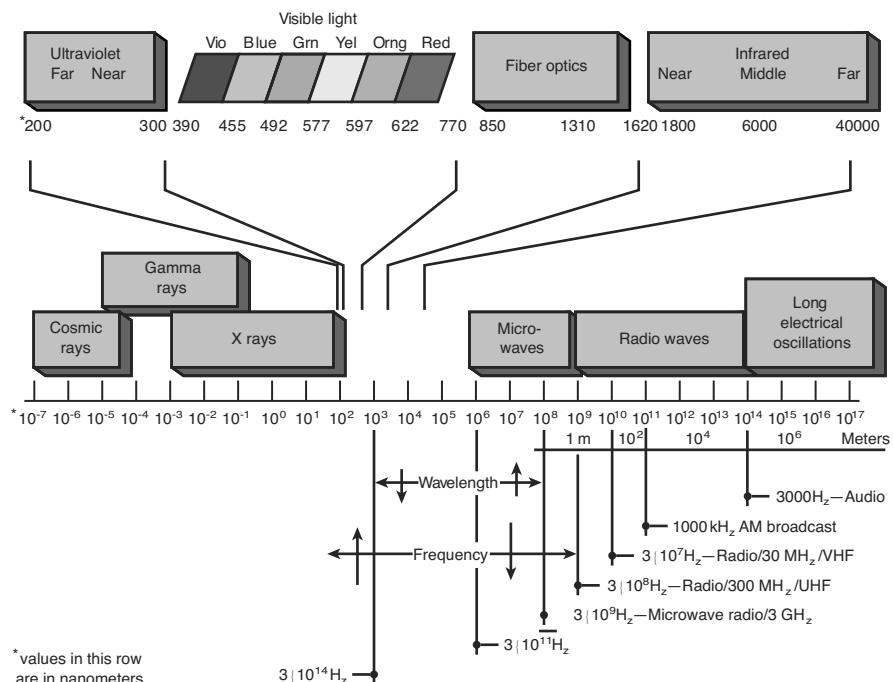


FIGURE 3-3 The electromagnetic wavelength spectrum. (From *Modern Electronic Communication 9/e*, by J.S. Beasley & G. M. Miller, 2008, p. 784. Copyright ©2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

The commonly used wavelengths in today's fiber-optic systems are

- **Multimode fiber:** (850 and 1310) nm
- **Single mode fiber:** (1310 and 1550) nm
- **Fiber to the home/business:** 1600–1625 nm

Figure 3-4 shows the typical construction of an optical fiber. The *core* is the portion of the fiber strand that carries the transmitted light. The *cladding* is the material surrounding the core. It is almost always glass, although plastic cladding of a glass fiber is available but rarely used. In any event, the refraction index for the core and the cladding are different. The cladding must have a lower index of refraction to keep the light in the core. A plastic coating surrounds the cladding to provide protection. Figure 3-5 shows examples of fiber strands from a fiber bundle.

Cladding

Material surrounding the core, which must have a lower index of refraction to keep the light in the core

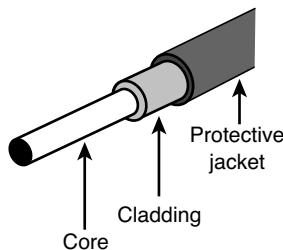


FIGURE 3-4 Single-fiber construction. (From *Modern Electronic Communication 9/e*, by J.S. Beasley & G. M. Miller, 2008, p. 785. Copyright ©2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)



FIGURE 3-5 Fiber strands (courtesy of Anixter, Inc.).

Numerical Aperture

A measure of a fiber's ability to accept light

Another measure of a fiber's light acceptance is **numerical aperture**. The numerical aperture is a basic specification provided by the manufacturer that indicates the fiber's ability to accept light and shows how much light can be off-axis and still propagate.

Several types of optical fibers are available, with significant differences in their characteristics. The first communication-grade fibers (early 1970s) had light-carrying core diameters about equal to the wavelength of light. They could carry light in just a single waveguide mode.

The difficulty of coupling significant light into such a small fiber led to development of fibers with cores of about 20 to 100 μm . These fibers support many waveguide modes and are called **multimode fibers**. The first commercial fiber-optic systems used multimode fibers with light at 800–900 nm wavelengths. A variation of the multimode fiber was subsequently developed, termed graded-index fiber. This afforded greater bandwidth capability.

As the technology became more mature, the single-mode fibers were found to provide lower losses and even higher bandwidth. This has led to their use at 1300 nm, 1550 nm, up to 1625 nm in many telecommunication and fiber-to-the home applications. The new developments have not made old types of fiber obsolete. The application now determines the type used. The following major criteria affect the choice of fiber type:

1. Signal losses
2. Ease of light coupling and interconnection
3. Bandwidth

Figure 3-6 presents a graphic of a fiber showing three modes (that is, multimode) of propagation:

- The lowest-order mode is seen traveling along the axis of the fiber.
- The middle-order mode is reflected twice at the interface.
- The highest-order mode is reflected many times and makes many trips across the fiber.

Pulse Dispersion

Stretching of received pulse width because of multiple paths taken by the light

As a result of these variable path lengths, the light entering the fiber takes a variable length of time to reach the detector. This results in a pulse-broadening or dispersion characteristic, as shown in Figure 3-6. This effect is termed **pulse dispersion** and limits the maximum distance and rate at which data (pulses of light) can be practically transmitted. You will also note that the output pulse has reduced amplitude as well as increased width. The greater the fiber length, the worse this effect will be. As a result, manufacturers rate their fiber in bandwidth per length, such as 400MHz/km. This means the fiber can successfully transmit pulses at the rate of 400MHz for 1 km, 200MHz for 2 km, and so on. In fact, current networking standards limit multimode fiber distances to 2 km. Of course, longer transmission paths are attained by locating regenerators at appropriate locations. Step-index multimode fibers are rarely used in networking due to their very high amounts of pulse dispersion and minimal bandwidth capability.

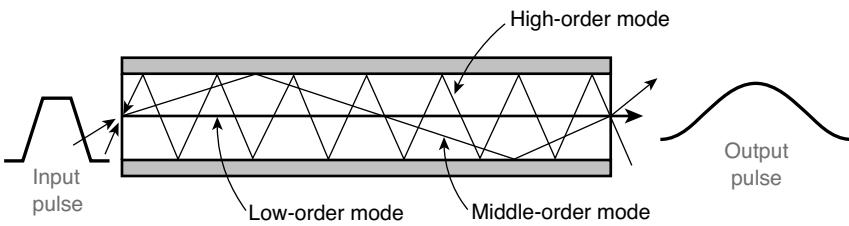


FIGURE 3-6 Modes of propagation for step-index fiber. (From *Modern Electronic Communication 9/e*, by J.S. Beasley & G. M. Miller, 2008, p. 787. Copyright ©2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

Graded-Index Fiber

In an effort to overcome the pulse-dispersion problem, the **graded-index fiber** was developed. In the manufacturing process for this fiber, the index of refraction is tailored to follow the parabolic profile shown in Figure 3-7. This results in low-order modes traveling through the constant-density material in the center. High-order modes see a lower index of refraction material farther from the core, and thus the velocity of propagation increases away from the center. Therefore, all modes, even though they take various paths and travel different distances, tend to traverse the fiber length in about the same amount of time. These fibers can therefore handle higher bandwidths and/or provide longer lengths of transmission before pulse dispersion effects destroy intelligibility and introduce bit errors.

Graded-index Fiber

The index of refraction is gradually varied with a parabolic profile

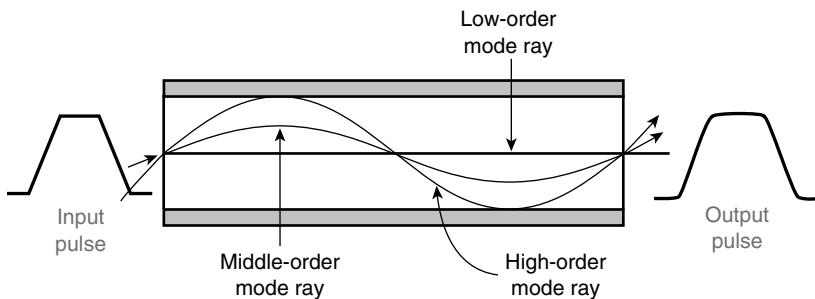


FIGURE 3-7 Modes of propagation for graded-index fiber. (From *Modern Electronic Communication 9/e*, by J.S. Beasley & G. M. Miller, 2008, p. 788. Copyright ©2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

Graded-index multimode fibers with 50 μm -diameter cores and 125 μm cladding are used in many telecommunication systems at up to 300 megabits per second (Mbps) over 50-km ranges without repeaters. Graded-index fiber with up to a 100 μm core is used in short-distance applications that require easy coupling from the source and high data rates, such as for video and high-speed local area networks (LANs). The larger core affords better light coupling than the 50 μm core and does

not significantly degrade the bandwidth capabilities. In the telecommunications industry, there are two commonly used core sizes for graded-index fiber, these being 50 μm and 62.5 μm . Both have 125 μm cladding. The large core diameter and the high NA (numerical aperture) of these fibers simplify input cabling and allow the use of relatively inexpensive connectors. Fibers are specified by the diameters of their core and cladding. For example, the fibers just described would be called 50/125 fiber and 62.5/125 fiber.

Single-Mode Fibers

Single-mode Fiber

Fiber cables with core diameters of about 7–10 μm ; light follows a single path

A technique used to minimize pulse dispersion effects is to make the core extremely small—on the order of a few micrometers. This type accepts only a low-order mode, thereby allowing operation in high-data-rate, long-distance systems. This fiber is typically used with high-power, highly directional modulated light sources such as a laser. Fibers of this variety are called **single-mode** (or monomode) **fibers**. Core diameters of only 7–10 μm are typical.

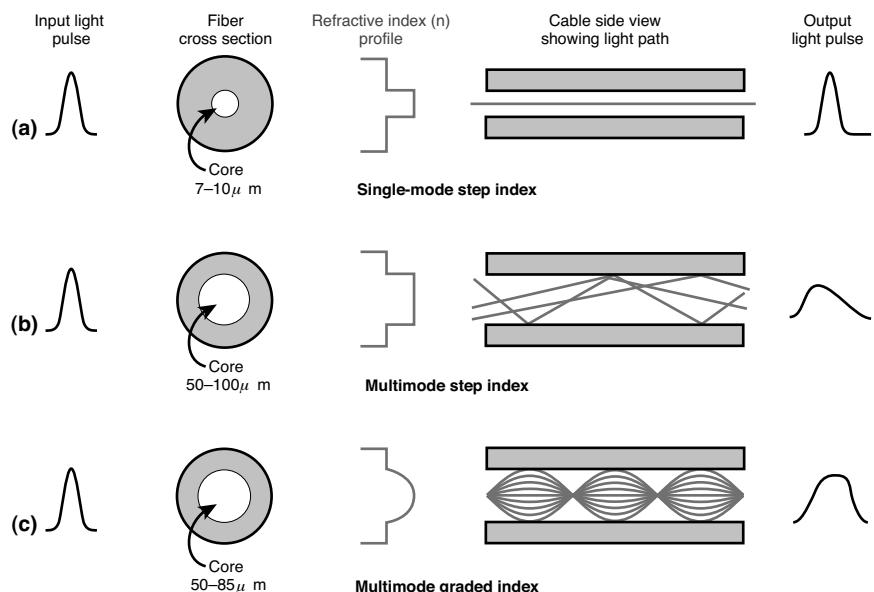


FIGURE 3-8 Types of optical fiber. (From *Modern Electronic Communication 9/e*, by J.S. Beasley & G. M. Miller, 2008, p. 789. Copyright ©2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

Long Haul

The transmission of data over hundreds or thousands of miles

Single-mode fibers are widely used in **long-haul** and wide area network (WAN) applications. They permit transmission of about 10Gbps and a repeater spacing of up to 80km. These bandwidth and repeater spacing capabilities are constantly being upgraded by new developments.

When describing the core size of single-mode fibers, the term **mode field diameter** is the term more commonly used. Mode field diameter is the actual guided optical power distribution diameter. In a typical single-mode fiber, the mode field diameter is 1 μm or so larger than the core diameter. The actual value depends on the wavelength being transmitted. In fiber specification sheets, the core diameter is stated for multimode fibers, but the mode field diameter is typically stated for single-mode fibers.

Figure 3-8 provides a graphical summary of the three types of fiber discussed, including typical dimensions, refractive index profiles, and pulse-dispersion effects.

Mode Field Diameter
The actual guided optical power distribution, which is typically a micron or so larger than the core diameter; single-mode fiber specifications typically list the mode field diameter

Section 3-2 Review

This section has covered the following **Network+** Exam objectives.

3.1 Categorize standard media types and associated properties

This section has introduced the reader to the nature of light and fiber-optics; in particular, single-mode and multimode fiber. Figure 3-4 provides a good graphical view of the composition of a fiber-optic cable. The concept of how light travels in an optical waveguide such as fiber was also presented.

Test Your Knowledge

1. What are the light waves just below the frequencies in the visible spectrum extending up called?
 - a. Sub-light waves
 - b. Infrared light waves
 - c. Refractive waves
 - d. Multimode waves
 - e. Polar waves
2. What is the material surrounding the core of an optical waveguide called?
 - a. Cladding
 - b. Aperture
 - c. Mode field
 - d. Step-index
 - e. Graded-index
3. Single-mode fiber cables have a core diameter of about 7–10 micrometers.
True or False?

3-3 FIBER ATTENUATION AND DISPERSION

There are two key distance-limiting parameters in fiber-optic transmissions: attenuation and dispersion.

Attenuation

Attenuation is the loss of power introduced by the fiber. This loss accumulates as the light is propagated through the fiber strand. The loss is expressed in dB/km (decibels per kilometer) of length. The loss, or attenuation, of the signal is due to the combination of four factors: scattering, absorption, macrobending, and microbending. Two other terms for attenuation are intrinsic and extrinsic.

Scattering

Caused by refractive index fluctuations; accounts for 96 percent of attenuation loss

Absorption

Light interaction with the atomic structure of the fiber material; also involves the conversion of optical power to heat

Macrobending

Loss due to light breaking up and escaping into the cladding

Microbending

Loss caused by very small mechanical deflections and stress on the fiber

Scattering is the primary loss factor over the three wavelength ranges. Scattering in telecommunication systems accounts for 96 percent of the loss and is the basis of the attenuation curves and values, such as that shown in Figure 3-9, and industry data sheets. The scattering is known as *Rayleigh scattering* and is caused by refractive index fluctuations. Rayleigh scattering decreases as wavelength increases, as shown in Figure 3-9.

Absorption is the second loss factor, a composite of light interaction with the atomic structure of the glass. It involves the conversion of optical power to heat. One portion of the absorption loss is due to the presence of OH hydroxyl ions dissolved in the glass during manufacture. These cause the water attenuation or OH peaks shown in Figure 3-9 and other attenuation curves.

Macrobending is the loss caused by the light mode breaking up and escaping into the cladding when the fiber bend becomes too tight. As the wavelength increases, the loss in a bend increases. Although losses are in fractions of dB, the bend radius in small splicing trays and patching enclosures should be minimal.

Microbending is a type of loss caused by mechanical stress placed on the fiber strand, usually in terms of deformation resulting from too much pressure being applied to the cable. For example, excessively tight tie wraps or clamps will contribute to this loss. This loss is noted in fractions of a dB.

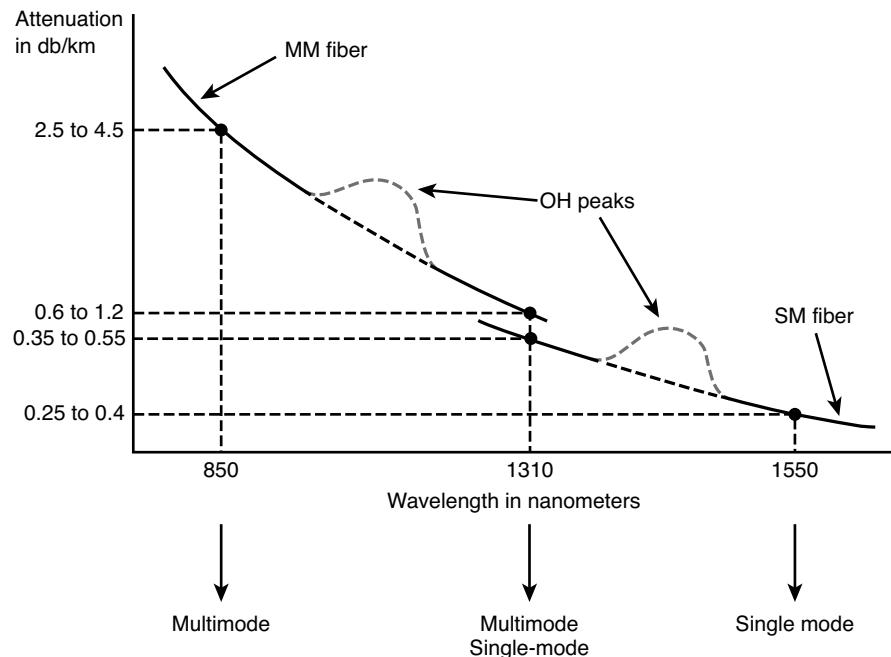


FIGURE 3-9 Typical attenuation of cabled fiber strands. (From *Modern Electronic Communication 9/e*, by J.S. Beasley & G. M. Miller, 2008, p. 792. Copyright ©2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

Dispersion

Dispersion, or pulse broadening, is the second of the two key distance-limiting parameters in a fiber-optic transmission system. It is a phenomenon in which the light pulse spreads out in time as it propagates along the fiber strand. This results in a broadening of the pulse. If the pulse broadens excessively, it can blend into the adjacent digital time slots and cause bit errors. Figure 3-10 illustrates the effects of dispersion on a light pulse.

Dispersion

Broadening of a light pulse as it propagates through a fiber strand

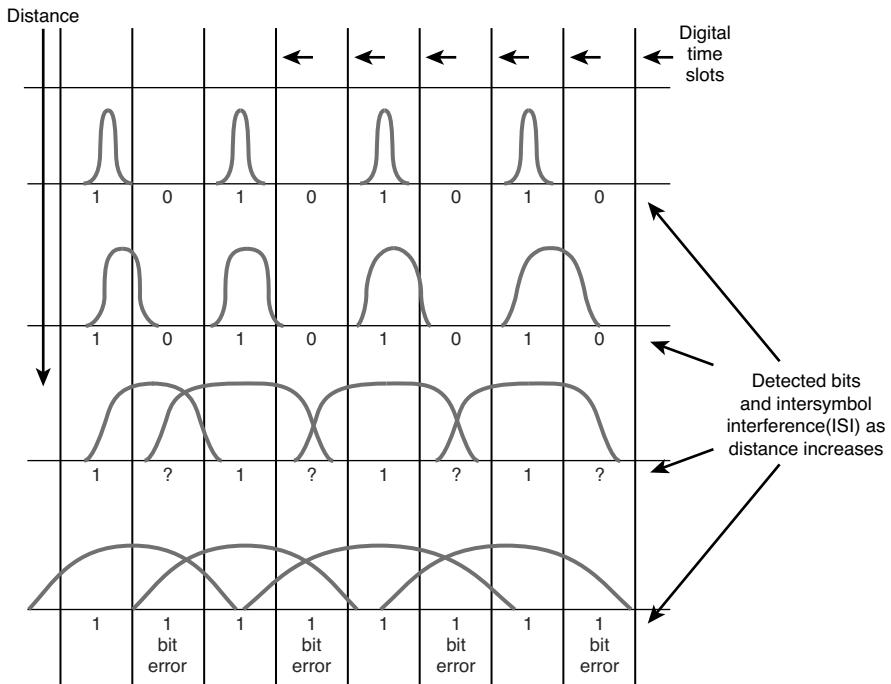


FIGURE 3-10 Pulse broadening or dispersion in optical fibers. (Adapted from *Modern Electronic Communication 9/e*, by J.S. Beasley & G. M. Miller, 2008, p. 793. Copyright ©2008 Pearson Education, Inc. Adapted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

There are three types of dispersion:

- **Modal dispersion:** The broadening of a pulse due to different path lengths taken through the fiber by different modes.
- **Chromatic dispersion:** The broadening of a pulse due to different propagation velocities of the spectral components of the light pulse.
- **Polarization mode dispersion:** The broadening of a pulse due to the different propagation velocities of the X and Y polarization components of the light pulse.

Modal dispersion occurs predominantly in multimode fiber. From a light source, the light rays can take many paths as they propagate along the fiber. Some light rays do travel in a straight line, but most take variable-length routes. As a result, the rays arrive at the detector at different times, and the result is pulse broadening. This was shown in Figures 3-6 and 3-7. The use of graded-index fiber greatly reduces the effects of modal dispersion and therefore increases the bandwidth to about 1GHz/km. On the other hand, single-mode fiber does not exhibit modal dispersion, given that only a single mode is transmitted.

A second equally important type of dispersion is chromatic. Chromatic dispersion is present in both single-mode and multimode fibers. Basically, the light source, both lasers and LEDs, produce several different wavelength light rays when generating the light pulse. Each light ray travels at a different velocity, and as a result, these rays arrive at the receiver detector at different times, causing the broadening of the pulse.

There is a point where dispersion is actually at zero, this being determined by the refractive index profile. This happens near 1310 nm and is called the **zero dispersion wavelength**. By altering the refractive index profile, this zero dispersion wavelength can be shifted to the 1550-nm region. Such fibers are called *dispersion-shifted*. This is significant because the 1550-nm region exhibits a lower attenuation than at 1310 nm. This becomes an operational advantage, particularly to long-haul carriers because with minimum attenuation and minimum dispersion in the same wavelength region, repeater and regenerator spacing can be maximized.

Polarization mode is the type of dispersion found in single-mode systems and becomes of particular concern in long-haul and WAN high-data-rate digital and high-bandwidth analog video systems. In a single-mode fiber, the single propagating mode has two polarizations, horizontal and vertical, or X axis and Y axis. The index of refraction can be different for the two components; this affects their relative velocity as shown in Figure 3-11.

Zero-dispersion Wavelength
Point where the dispersion is actually zero

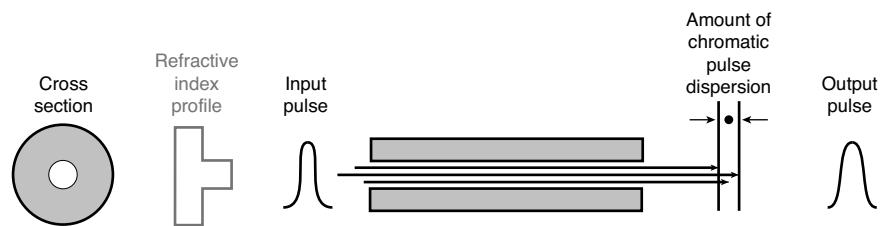


FIGURE 3-11 Polarization mode dispersion in single-mode fiber. (From *Modern Electronic Communication 9/e*, by J.S. Beasley & G. M. Miller, 2008, p. 794. Copyright ©2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

Dispersion Compensation

A considerable amount of fiber in use today was installed in the 1980s and early 1990s. This cable was called the class IVa variety. These cables were optimized to operate in the 1310-nm region, which means their zero-dispersion point was in the 1310-nm wavelength. Due to continuous network expansion needs in recent years, it is often desired to add transmission capacity to the older fiber cables by using the 1550-nm region, particularly because the attenuation at 1550 nm is less than at 1310 nm. One major problem arises at this point. The dispersion value is higher at 1550 nm, which severely limits its distance capability.

To overcome this problem, a fiber called **dispersion compensating fiber** was developed. This fiber acts like an equalizer, negative dispersion canceling positive dispersion. The fiber consists of a small coil normally placed in the equipment rack just prior to the optical receiver input. This does introduce some insertion loss (3–10 dB) and may require the addition of an optical-line amplifier.

A new device is a **fiber Bragg grating**. This technology involves etching irregularities onto a short strand of fiber, which changes the index of refraction and, in turn, reflects slower wavelengths to the output before the faster ones. This results in a compressed, or narrower, light pulse, minimizing intersymbol interference (ISI).

Dispersion Compensating Fiber
Acts like an equalizer, canceling dispersion effects and yielding close to zero dispersion in the 1550-nm region

Fiber Bragg Grating
A short strand of modified fiber that changes the index of refraction and minimizes intersymbol interference

Section 3-3 Review

This section has covered the following Network+ Exam objectives.

3.1 Categorize standard media types and associated properties

There are two key distance-limiting parameters in a fiber-optic transmission system. These are attenuation and dispersion, and these concepts were presented. Knowledge of the properties of fiber-optics is critical for planning a network installation or upgrade.

Test Your Knowledge

1. Which of the following terms refers to broadening of a light pulse as it propagates through a fiber strand?
 - a. Pulse shaping
 - b. Diffusion
 - c. Absorption
 - d. Dispersion
2. Which of the following terms is caused by refractive index fluctuations and accounts for 96% of attenuation loss?
 - a. Scattering
 - b. Absorption
 - c. Dispersion
 - d. Diffusion
3. Which of the following terms refers to loss due to light breaking up and escaping into the cladding?
 - a. Microbending
 - b. Scattering
 - c. Macrobending
 - d. Absorption

3-4 OPTICAL COMPONENTS

DL

Diode laser

LED

Light-emitting diode

Two kinds of light sources are used in fiber-optic communication systems: the diode laser (**DL**) and the high-radiance light-emitting diode (**LED**). In designing the optimum system, the special qualities of each light source should be considered. Diode lasers and LEDs bring to systems different characteristics:

1. Power levels
2. Temperature sensitivities
3. Response times
4. Lifetimes
5. Characteristics of failure

The diode laser is a preferred source for moderate-band to wideband systems. It offers a fast response time (typically less than 1 ns) and can couple high levels of useful optical power (usually several mW) into an optical fiber with a small core and a small numerical aperture. The DL is usually used as the source for single-mode fiber because LEDs have a low input coupling efficiency.

Some systems operate at a slower bit rate and require more modest levels of fiber-coupled optical power (50–250 μ W). These applications allow the use of high-radiance LEDs. The LED is cheaper, requires less complex driving circuitry than a DL, and needs no thermal or optical stabilizations.

The light output wavelength spread, or spectrum, of the DL is much narrower than that of LEDs: about 1 nm compared with about 40 nm for an LED. Narrow spectra are advantageous in systems with high bit rates since the dispersion effects of the fiber on pulse width are reduced, and thus pulse degradation over long distances is minimized.

Another laser device, called a **distributed feedback (DFB) laser**, uses techniques that provide optical feedback in the laser cavity. This enhances output stability, which produces a narrow and more stable spectral width. Widths are in the range of 0.01–0.1 nm. This allows the use of more channels in **dense wavelength division multiplex (DWDM)** systems. Another even more recent development is an entirely new class of laser semiconductors called **vertical cavity surface emitting lasers (VCSELs)**. These lasers can support a much faster signal rate than LEDs, including gigabit networks. They do not have some of the operational and stability problems of conventional lasers, however.

VCSELs have the simplicity of LEDs with the performance of lasers. Their primary wavelength of operation is in the 750–850-nm region, although development work is underway in the 1310-nm region. Reliabilities approaching 10^7 hours are projected.

Most lasers emit a fixed wavelength, but there is a class called **tunable lasers** in which the fundamental wavelength can be shifted a few nanometers, but not from a modulation point of view as in frequency modulation. Figure 3-12 shows an example of a tunable laser diode module. The primary market for these devices is in a network operations environment where DWDM is involved. Traffic routing is often made by wavelength, and, as such, wavelengths or transmitters must be assigned and reassigned to accommodate dynamic routing or networking, bandwidth on demand, seamless restoration (serviceability), optical packet switching, and so on. Tunable lasers are used along with either passive or tunable WDM filters.

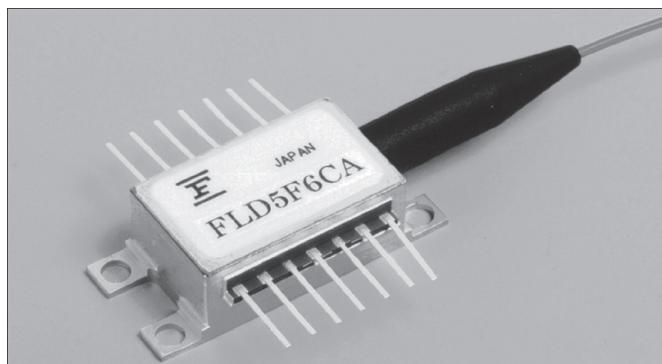


FIGURE 3-12 A tunable laser diode module (courtesy of Fujitsu Compound Semiconductor, Inc.).

Distributed Feedback (DFB) Laser

A more stable laser suitable for use in DWDM systems

Dense Wavelength Division Multiplex (DWDM)

Incorporates the propagation of several wavelengths in the 1550-nm range for a single fiber

Vertical Cavity Surface Emitting Lasers (VCSELs)

Lasers with the simplicity of LEDs and the performance of lasers

Tunable Laser

Laser in which the fundamental wavelength can be shifted a few nanometers, ideal for traffic routing in DWDM systems

Intermediate Components

Fiber, Light Pipe, Glass

Terms used to describe a fiber-optic strand

Isolator

An inline passive device that allows optical power to flow only in one direction

Received Signal Level (RSL)

The input signal level to an optical receiver

The typical fiber-optic telecommunication link (as shown previously in Figure 3-1) is a light source or transmitter and light detector or receiver interconnected by a strand of optical **fiber**, **light pipe**, or **glass**. An increasing number of specialized networks and system applications have various intermediate components along the span between the transmitter and the receiver. A brief review of these devices and their uses is provided in the list that follows.

- **Isolators:** An **isolator** is an inline passive device that allows optical power to flow in one direction only.
- **Attenuators:** Attenuators are used to reduce the **received signal level (RSL)**. They are available in fixed and variable configurations.
- **Branching devices:** Branching devices are used in simplex systems where a single optical signal is divided and sent to several receivers, such as point-to-multipoint data or a CATV distribution system.
- **Splitters:** Splitters are used to split, or divide, the optical signal for distribution to any number of places.
- **Wavelength division multiplexers:** Wavelength division multiplexers combine or divide two or more optical signals, each having a different wavelength. They are sometimes called optical beam splitters.
- **Optical-line amplifiers:** Optical-line amplifiers are analog amplifiers. Placement can be at the optical transmitter output, midspan, or near the optical receiver.

Detectors

The devices used to convert the transmitted light back into an electrical signal are a vital link in a fiber-optic system. This important link is often overlooked in favor of the light source and fibers. However, simply changing from one photodetector to another can increase the capacity of a system by an order of magnitude.

The important characteristics of light detectors are as follows:

- **Responsivity:** This is a measure of output current for a given light power launched into the diode.
- **Response speed:** This determines the maximum data rate capability of the detector.
- **Spectral response:** This determines the responsivity that is achieved relative to the wavelength at which responsivity is specified.

Optical fibers are joined either in a permanent fusion splice or with a mechanical splice (for example, connectors and camspllices). The connector allows repeated matings and unmatings. Above all, these connections must lose as little light as possible. Low loss depends on correct alignment of the core of one fiber to another, or to a source or detector. Losses for properly terminated fusion and mechanical splices is typically 0.2 dB or less. Signal loss in fibers occurs when two fibers are not perfectly aligned within a connector. Axial misalignment typically causes the greatest loss—about 0.5 dB for a 10 percent displacement. Figure 3-13 illustrates this condition as well as other loss sources.

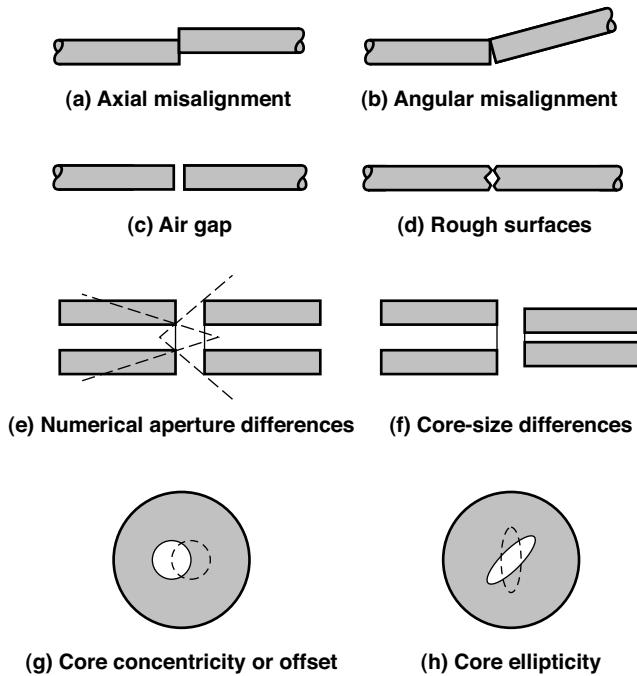


FIGURE 3-13 Sources of connection loss. (From *Modern Electronic Communication 9/e*, by J.S. Beasley & G. M. Miller, 2008, p. 806. Copyright ©2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

Angular misalignment [Figure 3-13(b)] can usually be well controlled in a connector. Most connectors leave an air gap, as shown in Figure 3-13(c). The amount of gap affects loss since light leaving the transmitting fiber spreads conically.

The losses due to rough end surfaces shown in Figure 3-13(d) are often caused by a poor cut, or “cleave,” but can be minimized by polishing or using pre-polished connectors. Polishing typically takes place after a fiber has been placed in a connector. The source of connection losses shown in Figure 3-13(d) can, for the most part, be controlled by a skillful cable splicer. There are four other situations that can cause additional connector or splice loss, although in smaller values. These are shown in Figure 3-13(e), (f), (g), and (h). These are related to the nature of the fiber strand at the point of connection and are beyond the control of the cable splicer. The effect of these losses can be minimized somewhat by the use of a rotary mechanical splice, which by the joint rotation will get a better core alignment.

With regard to connectorization and splicing, there are two techniques to consider for splicing. **Fusion Splicing** is a long-term method, in which two fibers are fused or welded together. The two ends are stripped of their coating, cut or cleaved, and inserted into the splicer. The ends of the fiber are aligned, and an electric arc is fired across the ends, melting the glass and fusing the two ends together. There are both manual and automatic fusion splicers; the choice usually depends on the number of splices to be done on a given job, technician skill levels available, and of course the budget. Typical insertion losses of less than 0.1 dB—frequently in the 0.05 dB range—can be consistently achieved.

Fusion Splicing

A long-term method where two fibers are fused or welded together

Mechanical Splices

Two fibers joined together with an air gap, thereby requiring an index-matching gel to provide a good splice

Index-matching Gel

A jellylike substance that has an index of refraction much closer to glass than to air

SC, ST, FC, LC, MT-RJ

Typical fiber connectors on the market

Mechanical splices can be permanent and an economical choice for certain fiber-splicing applications. Mechanical splices also join two fibers together, but they differ from fusion splices in that an air gap exists between the two fibers. This results in a glass-air-glass interface, causing a severe double change in the index of refraction. This change results in an increase in insertion loss and reflected power. The condition can be minimized by applying an **index-matching gel** to the joint. The gel is a jellylike substance that has an index of refraction much closer to the glass than air. Therefore, the index change is much less severe. Mechanical splices have been universally popular for repair and for temporary or laboratory work. They are quick, cheap, easy, and appropriate for small jobs. The best method for splicing depends on the application, including the expected future bandwidth (that is, gigabit), traffic, the job size, and economics. The loss in a mechanical splice can be minimized by using an OTDR to properly align the fiber when you are making the splice.

Fiber Connectorization

For fiber connectorization, there are several choices on the market such as SC, ST, FC, LC, MT-RJ, and others. The choice of the connector is typically dictated by the hardware being used and the fiber application. Figure 3-14(a–e) provides some examples of SC, ST, FC, LC, and MTRJ connectors

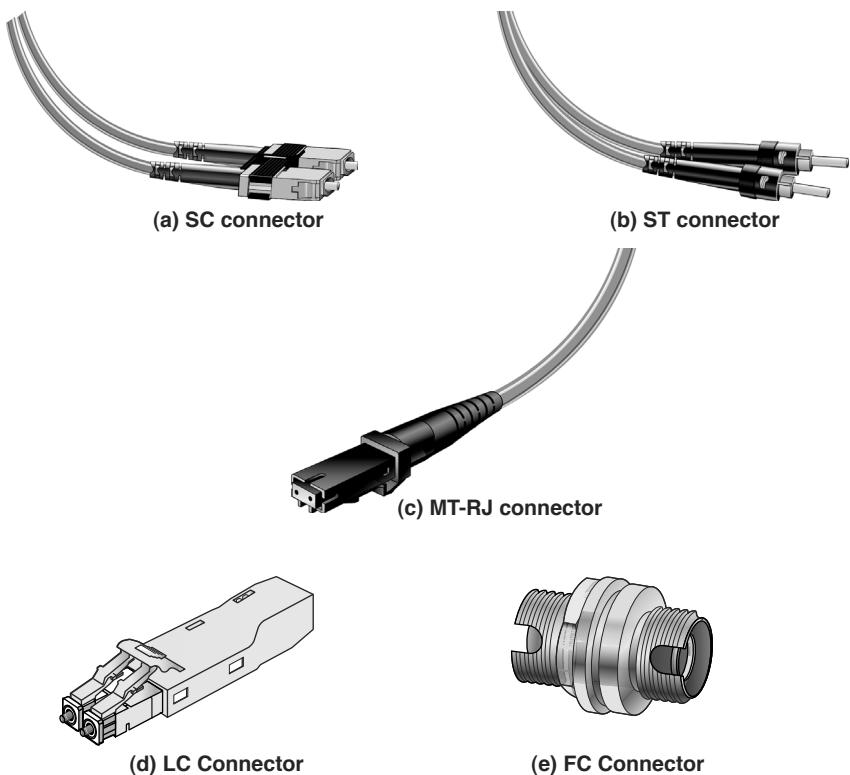


FIGURE 3-14 Typical fiber connections. [(a), (b), and (c) From *Modern Electronic Communication 9/e*, by J.S. Beasley & G. M. Miller, 2008, p. 808. Copyright ©2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ. (d) and (e) from Black Box Corporation.]

Some general requirements for fiber connectors are as follows:

- Easy and quick to install
- Low insertion loss—a properly installed connector will have as little as 0.25 dB insertion loss
- High return loss greater than 50 dB—this is increasingly important in gigabit networks, DWDM systems, high-bandwidth video, and so on
- Repeatability
- Economical

In preparing the fiber for splicing or connectorization, only the coating is removed from the fiber strand. The core and the cladding are not separable. The 125m cladding diameter is the portion that fits into the splice or connector, and therefore most devices can handle both single and multimode fiber.

Sometimes the issue arises as to the advisability of splicing together fibers of different core sizes. The one absolute rule is do *not* splice single- and multimode fiber together! Similarly, good professional work does not allow different sizes of multimode fiber to be spliced together. However, in an emergency, different sizes can be spliced together if the following is considered:

When transmitting from a small- to large-core diameter, there will be minimal, if any, increase in insertion loss. However, when the transmission is from a larger to a smaller core size, there will be added insertion loss and a considerable increase in reflected power should be expected.

Industrial practice has confirmed the acceptability of different core size interchangeability for emergency repairs in the field, mainly as the result of tests with 50 m and 62.5 m multimode fiber for a local area network.

Section 3-4 Review

This section has covered the following Network+ Exam objectives.

3.2 Categorize standard connector types based on network media

This section presented a look at optical components. Issues with connection loss are shown in Figure 3-13 and the different types of connectors are shown in Figure 3-14.

Test Your Knowledge

1. Fusion-splicing is characterized by which of the following?
 - a. A temporary method for splicing fiber
 - b. An inexpensive alternative to mechanical splices
 - c. Requires index-matching gel
 - d. A long-term method where two fibers are fused or welded together
2. The function of an attenuator is to reduce the receive signal level. True or False?

3-5 OPTICAL NETWORKING

The need for increased bandwidth is pushing the fiber-optic community into optical networking solutions that are almost beyond the imagination of even the most advanced networking person. Optical solutions for long-haul, wide area, metropolitan, campus, and local area networks are available. Cable companies are already using the high-bandwidth capability of fiber to distribute cable programming as well as data throughout their service areas.

The capital cost differences between a fiber system and a copper-based system are diminishing, and the choice of networking technology for new networks is no longer just budgetary. Fiber has the capacity to carry more bandwidth, and because the fiber infrastructure cost decreases, fiber will be chosen to carry the data. Of course, the copper infrastructure is already in place, and new developments are providing increases in data speed over copper (for example, CAT6 and CAT7). However, optical fiber is smaller and easier to install in already crowded ducts and conduits. Additionally, security is enhanced because it is difficult to tap optical fiber without detection. Will fiber replace copper in computer networks? For many years, a hybrid solution of fiber and copper is expected.

Defining Optical Networking

Optical networks are becoming a major part of data delivery in homes, in businesses, and for long-haul carriers. The telecommunications industry has been using fiber to carry long-haul traffic for many years. Some major carriers are merging with cable companies so that they are poised to provide high-bandwidth capabilities to the home. Developments in optical technologies are reshaping the way we will use fiber in future optical networks.

But there is a new slant with optical networks. Dense wave division multiplexing and tunable lasers have changed the way optical networks can be implemented. It is now possible to transport many wavelengths over a single fiber. Lab tests at AT&T have successfully demonstrated the transmission of 1,022 wavelengths over a single fiber. Such transport of multiple wavelengths opens up the possibilities to routing or switching many different data protocols over the same fiber but on different wavelengths. The development of cross-connects that allow data to arrive on one wavelength and leave on another opens other possibilities.

Synchronous optical network (SONET) and SDH were the North American and international standards for the long-haul optical transport of telecommunication for many years. SONET/SDH defined a standard for the following:

- Increase in network reliability
- Network management
- Defining methods for the synchronous multiplexing of digital signals such as DS-1 (1.544Mbps) and DS-3 (44.736Mbps)
- Defining a set of generic operating/equipment standards
- Flexible architecture

SONET/SDH

Synchronous optical network; protocol standard for optical transmission in long-haul communication/synchronous digital hierarchy

SONET/SDH specifies the various optical carrier (OC) levels and the equivalent electrical synchronous transport signals (STS) used for transporting data in a fiber-optic transmission system. Optical network data rates are typically specified in terms of the SONET hierarchy. Table 3-2 lists the more common data rates.

STS
Synchronous transport signals

TABLE 3-2 SONET Hierarchy Data Rates

Signal	Bit Rate	Capacity
OC-1 (STS-1)	51.840Mbps	28DS-Is or 1 DS-3
OC-3 (STS-3)	155.52Mbps	84DS-Is or 3 DS-3s
OC-12 (STS-12)	622.080Mbps	336 DS-1s or 12 DS-3s
OC-48 (STS-48)	2.48832Gbps	1344 DS-1s or 48 DS-3s
OC-192 (STS-192)	9.95328Gbps	5376 DS-Is or 192 DS-3s

OC: Optical carrier—DS-1: 1.544Mbps

STS: Synchronous transport signal—DS-3: 44.736Mbps

The architectures of fiber networks for the home include providing fiber to the curb (**FTTC**) and fiber to the home (**FTTH**). FTTC is being deployed today. It provides high bandwidth to a location with proximity to the home and provides a high-speed data link, via copper (twisted-pair), using VDSL (very high-data digital subscriber line). This is a cost-effective way to provide large-bandwidth capabilities to a home. FTTH will provide unlimited bandwidth to the home; however, the key to its success is the development of a low-cost optical-to-electronic converter in the home and laser transmitters that are tunable to any desired channel.

FTTC
Fiber to the curb

Another architecture in place is fiber to the business (**FTTB**). A fiber connection to a business provides for the delivery of all current communication technologies including data, voice, video, conferencing, and so on. An additional type is fiber to the desktop (**FTTD**). This setup requires that the computer has a fiber network interface card (NIC). FTTD is useful in applications such as computer animation work that has high-bandwidth requirements.

FTTH
Fiber to the home

Conventional high-speed Ethernet networks are operating over fiber. This is called **optical Ethernet** and uses the numerics listed in Table 3-3 for describing the type of network configuration. Fiber helps to eliminate the 100-m distance limit associated with unshielded twisted-pair (UTP) copper cable. This is possible because fiber has a lower attenuation loss. In a star network, the computer and the switch are directly connected. If the fiber is used in a star network, an internal or external media converter is required. The media converter converts the electronic signal to an optical signal, and vice versa. A media converter is required at both ends, as shown in Figure 3-15. The media converter is typically built in to the network interface card.

FTTB
Fiber to the business

FTTD
Fiber to the desktop

Optical Ethernet
Ethernet data running over a fiber link

TABLE 3-3 Optical Ethernet Numerics

Numeric	Description
10BASE-F	10Mbps Ethernet over fiber—generic specification for fiber
10BASE-FB	10Mbps Ethernet over fiber—part of the IEEE 10BaseF specification; segments can be up to 2 km in length
10BASE-FL	10Mbps Ethernet over fiber—segments can be up to 2 km in length; it replaces the FOIRL specification.
10BASE-FP	A passive fiber star network; segments can be up to 500 m in length
100BASE-FX	A 100Mbps fast Ethernet standard that uses two fiber strands
1000BASE-LX	Gigabit Ethernet standard that uses fiber strands using long-wavelength transmitters
1000BASE-SX	Gigabit Ethernet standard using short-wavelength transmitters
10GBASE-R	10 gigabit (10.325Gbps) Ethernet for LANs
10GBASE-W	10 gigabit (9.95328Gbps) Ethernet for WANs using OC-192 and SONET Framing

Multimode fiber—2 km length single mode—10 km length

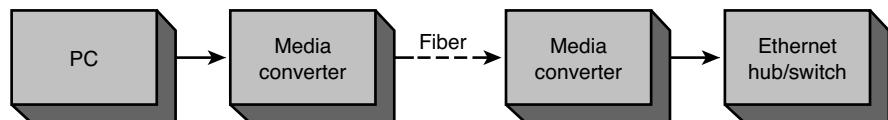


FIGURE 3-15 An example of connecting a PC to an Ethernet hub or switch via fiber. (From *Modern Electronic Communication 9/e*, by J.S. Beasley & G. M. Miller, 2008, p. 820. Copyright ©2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

Two important issues to be considered when designing a fiber network are the guidelines for the following:

- Building distribution
- Campus distribution

The following subsections discuss techniques for planning the fiber plant, the distribution of the fiber, and the equipment and connections used to interconnect the fiber. The first example is for a building distribution, the second for a campus distribution.

Building Distribution

Figure 3-16 shows an example of a simple fiber network for a building. Fiber lines consist of a minimum of two fibers, one for transmitting and one for receiving. Fiber networks work in the full-duplex mode, meaning that the links must be able to simultaneously transmit and receive; hence, the need for two fibers on each link.

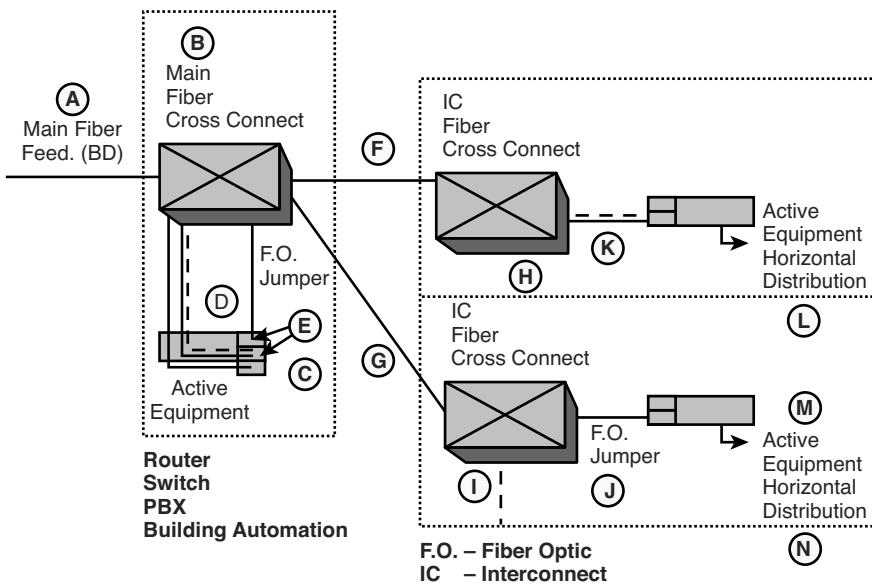


FIGURE 3-16 A simple fiber distribution in a building.

Item A is the main fiber feed for the building. This is called a *building distribution (BD)* fiber. The two fibers for the BD link terminate into a main fiber cross-connect (item B). A **fiber cross-connect** is the optical patch panel used to connect the fiber cables to the next link. The fiber cross-connect typically uses mechanical splices to make the fiber connections.

Items C and E represent the active equipment in the main distribution closet in the building. The active equipment could be a router, switch, or telephone PBX (private branch exchange). Item D shows the jumpers connecting the main fiber cross-connect (item B) to the active equipment (item C).

The active equipment will need some type of optical interface for the optical-electrical signal conversion, such as a **GBIC** (pronounced “gee-bick”). GBIC, or the Gigabit Interface Converter, is a hot-swappable transceiver that is used for transmitting and receiving higher-speed signals over fiber-optic lines. This is shown in Figure 3-17(a).

Fiber Cross-connect

Optical patch panel used to interconnect fiber cables

GBIC

Gigabit interface converter

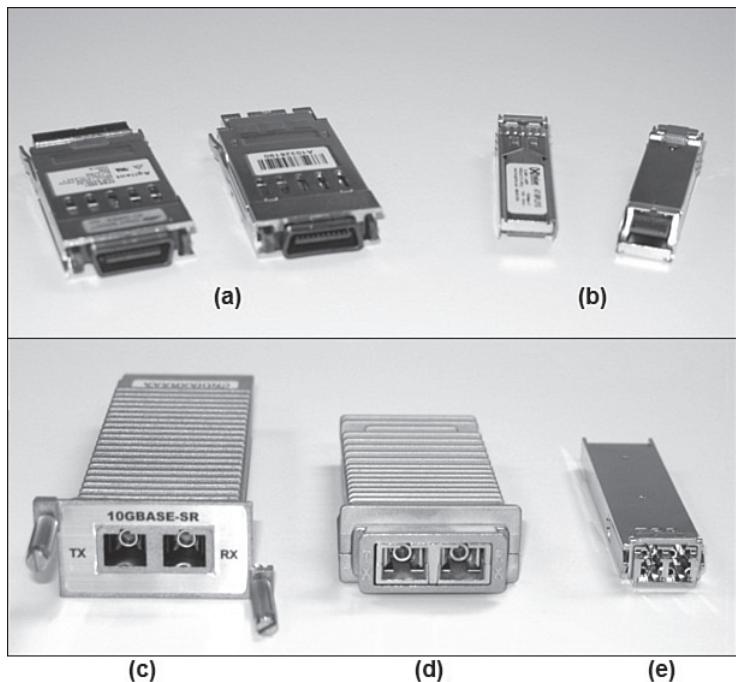


FIGURE 3-17 The Cisco (a) GBIC, (b) SFP, (c) XENPAK, (d) X2, and (e) XFP optical-to-fiber transceivers (courtesy of Cisco).

SFP

Small Form Pluggable

XENPAK, XPAK, X2, XFP, SFP+

The ten gigabit interface adapter

To increase port density on the active network equipment, the industry has been moving toward using a mini-GBIC or **SFP** (Small Form factor Pluggable). This is shown in Figure 3-17(b). The SFP is more than half the size of the GBIC shown in Figure 3-17(a). These modules are used to connect to other fiber-optic systems such as 1000Base-SX, which operates with multimode fiber in a short wavelength, and 1000Base-LX, which operates with the single-mode fiber in a longer wavelength. GBIC and SFP modules are designed to plug into interfaces such as routers and switches.

In the ten gigabits (10G) Ethernet world, several versions of optical-to-fiber transceivers have been developed. It all started with the **XENPAK**, shown in Figure 3-17(c), transceivers which were followed by the **XPAK** and the **X2**, shown in Figure 3-17(d). These later transceiver modules are smaller than the XENPAK. Then, an even smaller size module called **XFP** was developed. The **XFP**, shown in Figure 3-17(e), has lower power consumption than the XENPAK, XPAK, and X2, but it still can deliver up to 80Km in distance, which is the same as the older modules. With its small size, its lower power consumption, and its reachability, the XFP was thought to be the future of the 10G transceiver. Recently, a new type of 10G transceiver has emerged, and it is a **SFP+**. Its look and size are identical to a 1000Base SFP transceiver. To be able to deliver 10G speed in its small form factor, the working distance that the SFP+ can deliver is reduced to 40Km. So, if the distance is not of the concern, then SFP+ might be the 10G transceiver of choice. These modules support 850, 1310, and 1550 fiber wavelengths. Figure 3-17 collectively shows examples of 1000Base and 10GBase transceivers.

Referring to Figure 3-16, items F and G show the two fiber pairs patched into the main fiber cross-connect connecting to the **IDC**. These fibers (F and G) are called the interconnect (**IC**) fibers. The fibers terminate into the IDC fiber cross-connects (items H and I).

Items J and K in Figure 3-16 are fiber jumpers that connect the fiber cross-connect to the IDC active equipment. Once again, the active equipment must have a GBIC or some other interface for the optical-electrical signal conversion.

A general rule for fiber is that the distribution in a building should be limited to “2 deep.” This means that a building should have only the main distribution and the intermediate distribution that feeds the horizontal distribution to the work area.

Figure 3-18(a) and (b) illustrate an example of the “2-deep” rule. Figure 3-18(a) shows an example of a building distribution that meets the “2-deep” rule. The IDC is at the first layer, and the horizontal distribution (HD) is at the second layer. Figure 3-18(b) illustrates an example of a fiber distribution that does not meet the “2-deep” rule. In this example, the HD and work area are 3-deep, or 3 layers from the building’s main distribution.

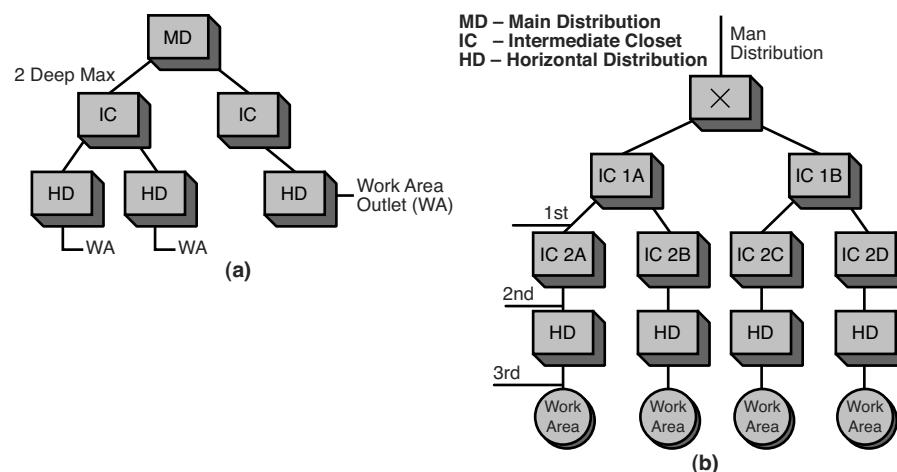


FIGURE 3-18 Examples of the “2-deep” rule: (a) the distribution meeting the requirement; (b) the distribution not meeting the requirement.

Campus Distribution

Figure 3-19 shows a map of the fiber distribution for a campus network. This map shows how the fiber is interconnected and data is distributed throughout the campus and is called a **logical fiber map**. Another style of map often used to show the fiber distribution is a **physical fiber map**, as shown in Figure 3-20. This map shows the routing of the fiber but also shows detail about the terrain, underground conduit, and entries into buildings. Both map styles are important and necessary for documentation and planning of the fiber network. This material focuses on the documentation provided in the logical fiber map.

IDC

Intermediate distribution closet

IC

Interconnect fibers branch exchange—item D shows the jumpers connecting the main fiber cross-connect (item B) to the active equipment (item C)

Logical Fiber Map

Shows how the fiber is interconnected and data is distributed throughout a campus

Physical Fiber Map

Shows the routing of the fiber but also shows detail about the terrain, underground conduit, and entries into buildings

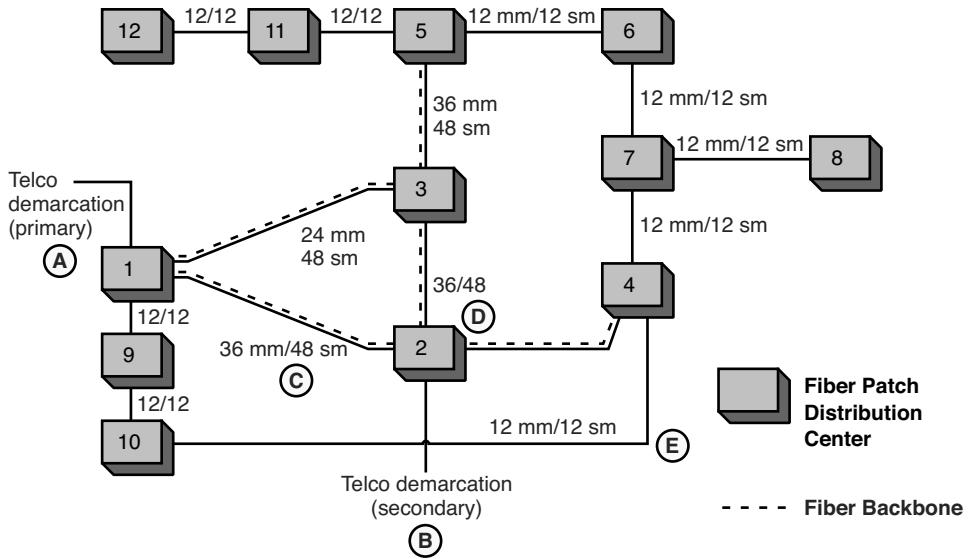


FIGURE 3-19 A logical fiber map.

mm
Multimode

sm
Single mode

Backbone
Main fiber distribution

Referring to the logical fiber map in Figure 3-19, this campus network has two connections to the Telco: the primary Telco demarcation (item A) in building 1 and the secondary Telco demarcation (item B) in building 2. These two Telco connections provide for redundant Internet and wide area network data services. If something happens in building 1 that shuts down the external data services, Internet and WAN data traffic can be switched to building 2. Also data traffic can be distributed over both connections to prevent bottlenecks. Buildings 1 and 2 are interconnected with 36 multimode (mm) and 48 single-mode (sm) fibers. This is documented on the line interconnecting buildings 1 and 2 (item C) and written as 36/48 (item D). The dotted line between buildings 1 and 2 indicates the backbone or main fiber distribution for the campus network. The bulk of the campus network data traffic travels over these fibers. The campus backbone (green dotted line) also extends from building 2 to building 4 and from building 3 to building 5.

This setup enables the data to be distributed over the campus. For example, data traffic from the primary Telco demarcation (item A) reaches building 12 by traveling via fiber through buildings 1-3-5-11-12. If the building 3 connection is down, then data traffic from the primary Telco demarcation can be routed through buildings 1-2-4-7-6-5-11-12. What happens to the data traffic for building 12 if building 5 is out of operation? In this case, data traffic to/from buildings 11 and 12 is lost.

Item E shows a fiber connection to/from buildings 4 and 10. This fiber bundle provides an alternative data path from the primary Telco demarcation to the other side of the campus network.



FIGURE 3-20 An example of a physical fiber map (courtesy of Palo Alto Utilities).

The cabling between buildings is a mix of multimode and single-mode fiber. The older fiber runs a 12/12 cable (12 multimode/12 single-mode). Fiber cables are bundled in groups of 12 fibers. For example, a 12/12 fiber will have two bundles: one bundle of multimode and one bundle of single-mode fiber. A 36/48 cable will have 3 bundles of multimode and 4 bundles of single-mode fiber. Each bundle of fibers is color-coded as listed in Table 3-4. For example, in a 36/48 fiber cable, the 3 bundles of multimode are in loose tubes that are color-coded blue/orange/green. The four bundles of single mode are in loose tubes that are color-coded brown/slate/white/red.

TABLE 3-4 The Fiber Color-code for the Twelve Fibers in a Bundle

Pair	Color
1/2	Blue/Orange
3/4	Green/Brown
5/6	Slate/White
7/8	Red/Black
9/10	Yellow/Violet
11/12	Rose/Aqua Marine

In this example, the newer fiber cabling installations were run with a 36/48 and 24/48 mix. Why the difference? The main reason is economics. The cost per foot (meter) of the new fiber is cheaper, so more fiber can be placed in a cable for the same cost per foot.

The fiber connecting the buildings is typically run either in PVC conduit, which makes it easy to add or remove fiber cables, or in trenches or tunnels. Running fiber in trenches is very expensive and significantly increases the installation cost. (*Note:* Network administrators need to be aware of any trenches being dug on campus.) Even if the budget doesn't allow for buying fiber at the time, at least have a conduit and pull line installed.

Fiber provides substantially increased bandwidth for building and campus networks and can easily handle the combined traffic of PCs, switches, routers, video, and voice services. Fiber has greater capacity, which enables faster transfer of data, minimizes congestion problems, and provides tremendous growth potential for each of the fiber runs.

Another important application of optical Ethernet is extending the reach of the Ethernet network from the local and campus network out to the metropolitan and wide area networks. Essentially, optical networking is introducing Ethernet as a viable WAN technology. Extending Ethernet into a WAN is a seamless integration of the technologies. The Ethernet extension into the WAN simply requires optical adapters such as a GBIC (gigabit interface converter) and two fiber strands, one for transmitting and one for receiving. Conventional high-speed Ethernet LANs operating over fiber use the numerics listed in Table 3-4 for describing the network configuration.

Section 3-5 Review

This section has covered the following **Network+** Exam objectives.

3.7 Compare and contrast different LAN technologies

The issues with configuring an optical network have been introduced in this chapter. The concept of optical networking is defined as well as FTTH (Fiber to the Home) and FTTB(Fiber to the Business).

3.8 Identify components of wiring distribution

A block diagram for fiber distribution in a building is provided in Figure 3-18. A logical fiber map that shows how the fiber is interconnected in a network is provided in Figure 3-19. An example of a physical fiber map showing detail such as terrain and entries into a building is provided in Figure 3-20.

4.5 Describe the purpose of configuration management documentation

Documenting a fiber-optic network becomes extremely important when trying to keep track of how the data is routed and which fibers are being used. Equally important are which fibers are available for future expansion.

Test Your Knowledge

1. What does the logical fiber map show? (select all that apply)
 - a. How data is distributed throughout a campus
 - b. The routing of the fiber
 - c. Terrain and underground conduits
 - d. How the fiber is interconnected
2. What does the physical fiber map show? (select all that apply)
 - a. The routing of the fiber
 - b. The LAN connections
 - c. Terrain issues
 - d. Router placement
3. What is the name of the optical-to-fiber interface used at 10 gigabits?
 - a. GBIC
 - b. 10GBIC
 - c. XENPAK
 - d. ZENPAK

3-6 SAFETY

Any discussion of fiber-optics or optical networking is not complete unless it addresses safety issues, even if only briefly. As the light propagates through a fiber, two factors will further attenuate the light if there is an open circuit:

1. A light beam will disperse or fan out from an open connector.
2. If a damaged fiber is exposed on a broken cable, the end will likely be shattered, which will considerably disperse the light. In addition, there would be a small amount of attenuation from the strand within the cable, plus any connections or splices along the way.

However, there are two factors that can increase the optical power at an exposed fiber end.

1. There could be a lens in a pigtail that could focus more optical rays down the cable.
2. In the newer DWDM systems, there will be several optical signals in the same fiber; although separate, they will be relatively close together in wavelength. The optical power incident on the eye will then be multiplied.

There are two factors to be aware of:

1. The eye can't see fiber-optic communication wavelength, so there is no pain or awareness of exposure. However, the retina can still be exposed and damaged. (Refer to Figure 3-3, the electromagnetic spectrum.)

2. Eye damage is a function of the optical power, wavelengths, source or spot diameter, and duration of exposure.

So for those working on fiber-optic equipment:

1. *DO NOT EVER* look into the output connector of energized test equipment. Such equipment can have higher powers than the communication equipment itself, particularly OTDRs.
2. If you need to view the end of a fiber, *ALWAYS turn off the transmitter*; particularly if you don't know whether the transmitter is a laser or LED, given that lasers are higher-power sources. If you are using a microscope to inspect a fiber, the optical power will be multiplied.

From a mechanical point of view:

1. Good work practices are detailed in safety, training, and installation manuals. **READ AND HEED.**
2. Be careful with machinery, cutters, chemical solvents, and epoxies.
3. Fiber ends are brittle and will break off easily, including the ends cut off from splicing and connectorization. These ends are extremely difficult to see and can become "lost" and/or easily embedded in your finger. You won't know until your finger becomes infected. Always account for all scraps.
4. Use safety glasses specifically designed to protect the eye when working with fiber-optic systems.
5. Obtain and *USE* an optical safety kit.
6. Keep a *CLEAN* and orderly work area.

In all cases, be sure the craft personnel have the proper training for the job!

Section 3-6 Review

This section has covered the following **Network+** Exam objectives.

- 3.1 Categorize standard media types and associated properties

Anytime you are working with fiber, you need to be careful. This section presents an overview of safety.

Test Your Knowledge

1. The eye cannot see fiber-optic communication wavelengths, so never look into the end of a fiber. True or False?
2. It is important to be very careful working with fiber ends. These ends are extremely difficult to see and can become "lost" and/or easily embedded in your finger. True or False?

SUMMARY

Chapter 3 introduced the field of fiber-optics and optical networking. The chapter has provided examples using fiber to interconnect LANs in both a building and a campus network. The major topics that the student should understand include the following:

- The advantages offered by optical networking
- The properties of light waves
- The physical and optical characteristics of optical fibers
- Attenuation and dispersion effects in fiber
- The description of the common techniques used to connect fiber
- The usage of fiber-optics in LANs, campus networks, and WANs
- System design of optical networks
- Safety considerations when working with fiber
- Analysis of OTDR waveforms

QUESTIONS AND PROBLEMS

Section 3-1

1. List the basic elements of a fiber-optic communication system.
2. List five advantages of an optical communications link.

Section 3-2

3. Define refractive index.
4. What are the commonly used wavelengths in fiber-optic systems?

5. Which part of an optical fiber carries the light?
6. What is a measure of a fiber's light acceptance?
7. Define pulse dispersion.
8. What are the typical core/cladding sizes (in microns) for multimode fiber?
9. What is the typical core size for single-mode fiber?
10. Define *mode field diameter*.

Section 3-3

11. What are the two key distance-limiting parameters in fiber-optic transmissions?
12. What are the four factors that contribute to attenuation?
13. Define *dispersion*.
14. What are three types of dispersion?
15. What is meant by the *zero-dispersion wavelength*?
16. What is a dispersion compensating fiber?

Section 3-4

17. What are the two kinds of light sources used in fiber-optic communication systems?
18. Why is a narrower spectra advantageous in optical systems?
19. Why is a tunable laser of importance in optical networking?

20. What is the purpose of an optical attenuator?
21. List two purposes of optical detectors.
22. What is the advantage of fusion splicing over mechanical splicing?

Section 3-5

23. Define: (a) FTTC; (b) FTTH; (c) FTTB; (d) FTTD.
24. What is the purpose of a GBIC?
25. What is the “2-deep” rule?
26. What is the purpose of a logical fiber map?
27. What are the typical maximum lengths for (a) multimode and (b) single-mode fiber?
28. What is FDDI?

Section 3-6

29. Why is safety an important issue in optical networking?
30. A campus network is planning to install fiber-optic cables to replace outdated coaxial cables. They have the choice of installing single-mode, multimode, or a combination of single–multimode fibers in the ground. Which fiber type should they select? Why?

31. The networking cables for a new building are being installed. You are asked to prepare a study about which cable type(s) should be used. Discuss the issues related to the cable selection.

Certification Questions

32. Which of the following are advantages of optical communication links? (select three)
 - a. Extremely wide bandwidth
 - b. Elimination of crosstalk
 - c. Elimination of attenuation
 - d. Security
33. The stretching of a received pulse is due to what? (select two)
 - a. Multiple paths taken by the light waves
 - b. Misaligned connectors
 - c. Pulse-dispersion
 - d. OTDR testing
34. The broadening of a pulse due to the different path lengths taken through the fiber by different modes is called what?
 - a. Chromatic dispersion
 - b. Polarization mode dispersion
 - c. Modal dispersion
 - d. Diffusion
35. The broadening of a pulse due to different propagation of the spectral components of the light pulse is called what?
 - a. Chromatic dispersion
 - b. Modal dispersion
 - c. Polarization mode dispersion
 - d. Diffusion
36. The broadening of a light pulse due to the different propagation velocities of the X and Y polarization components of the light pulse is called what?
 - a. Modal dispersion
 - b. Chromatic dispersion
 - c. Diffusion
 - d. Polarization mode dispersion
37. What is the data rate for OC-192?
 - a. 1.522Mbps
 - b. 155.52Mbps
 - c. 9.95Gbps
 - d. 2.488Gbps

38. What is the name of the optical-to-fiber interface used at 1 gigabit?
- XENPAK
 - GBIC
 - 10GBIC
 - ZENPAK
39. What is the “two deep” rule relative to optical networking?
- This means the horizontal distribution to the work floor can only have two 8P8C connections.
 - This means the horizontal distribution to the work floor can only have two ST connections to the fiber patch panel.
 - This is no longer an issue with high-speed, single-mode fiber and wave division multiplexing equipment.
 - This means that a building should have only the main distribution and the intermediate distribution that feeds the horizontal distribution to the work area.
40. Which type of fiber is preferred for use in modern computer networks?
- Multimode
 - Polarized mode
 - Single-mode
 - All of these answers are correct
41. What is the material surrounding the core of an optical waveguide called?
- Aperture
 - Mode field
 - Step-index
 - Cladding
 - Graded-index

Index

Symbols

3DES (Triple Data Encryption Standard), 489

6to4 prefix, 272

10 gigabit Ethernet over copper, 90-91

AXT (Alien Crosstalk), 91-92

signal transmission, 93

10GBASE-T, 71, 91

802.11, 163-166

site survey, 166-171

SSID (service set identifier), 164

802.11a (Wireless-A), 23, 161

802.11b (Wireless-B), 23, 161

802.11g (Wireless-G), 23, 162

802.11i, 162

802.11n (Wireless-N), 23, 162

802.11r, 162

A

absorption, attenuation, 126

ABR (area border routers), 377

access lists (ACLs), 484

access points, 156

home networking, 28

ACK (acknowledgement packet), 242-243

ACLs (access lists), 484

ACR, PSELFEXT, 89

Active, RFID tags, 177

ad hoc, 156

adapter address, 17

adaptive cut-through, 214

Address Resolution Protocol (ARP), 200, 245, 442

administering local DNS server, 422

administratively down, 453

ADSL (asymmetric DSL), 409

Advanced Encryption Standard (AES), 489

advertising networks, 379

AES (Advanced Encryption Standard), 489

AfriNIC, 258

aging time, 211

AH (Authentication Header), 489

Alien Crosstalk (AXT), 91-92

analog modem technologies, 407-408

cable modems, 408

RAS (remote access server), 410-411

xDSL modems, 408-410

analyzing

campus networks, data traffic, 448-450

computer networks, 441

capturing data packets with Wireshark, 444-445

inspecting data packets with Wireshark, 442-443

internet data traffic, 427

frame size distribution, 430

network layer host table, 430

network layer matrix, 429

Utilization/Errors Strip chart, 428

networks, FTP data packets, 446-447

A

- angular misalignment, 133
- antenna site survey, configuring point-to-multipoint
 - wireless LAN case study, 183
- antivirus software, 477
- anycast addresses, 272
- APNIC, 258
- appearance, home networking, 32
- application layer, 13
 - OSI (open systems interconnect) model, 13
 - TCP/IP, 240-241
- application-specific integrated circuits (ASICs), 214
- area border routers (ABR), 377
- areas, 375
- ARIN (American Registry for Internet Numbers), 258
- ARP (Address Resolution Protocol), 200, 245, 442
 - ARP cache, 201-202
 - ARP reply, 442
 - ARP table, 201
- AS (autonomous systems), 426
- ASICs (application-specific integrated circuits), 214
- ASN (AS number), 426
- assembling straight-through CAT5e/5 patch cables, 82-85
- associations, bridges, 200
- asymmetric DSL (ADSL), 409
- asymmetric operations, 407
- attenuation, 86-87
 - fiber optics, 126
 - attenuators, 132
- Authentication Header (AH), 489
- auto-negotiation, 225
 - full-duplex, 226
 - half-duplex, 226
- autonomous systems (AS), 426
- auxiliary input, 216
- AXT (Alien Crosstalk), 91-92

B

- backbone cabling, structured cabling, 63
- backbones, 142, 375
- backscatter, 175
- balanced mode, UTP, 70

C

- bandwidth, 371
- Basic Service Set (BSS), 156
- BD (building distributor), 63
- beacons, WLAN, 180
- BGP (Border Gateway Protocol), 424-426
- binary-to-decimal conversion, 249-251
- Bluetooth, 172-174
- BOOTP, 416
- Border Gateway Protocol (BGP), 424-426
- bottlenecking, UTP, 71
- BPDUs (bridge protocol data units), 338
- branching devices, 132
- bridges
 - interconnecting LANs, 199-203
 - multiport bridges, 205
 - translation bridges, 202
 - transparent bridges, 202
- bridging tables, 199
- broadband modem/gateway, home networking, 30
- broadband wireless access (BWA), 174
- broadcast, 9, 200
- broadcast domain
 - routers, 290
 - switches, 213
- broadcast storms, 200
- brute-force attack, 470
- BSS (Basic Service Set), 156
- buffer overflow, 471
- building distribution, optical networking, 138-141
- building distributor (BD), 63
- building entrance, structured cabling, 63
- but topology, 8
- BWA (broadband wireless access), 174

cabling

CAT6 horizontal link cables, terminating, 77-82
certification, 86-89
crossover patch cables, 76-77
straight-through cables, 76-77
straight-through CAT5e/5 patch cables, assembling, 82-85
structured cabling, 62-65
 backbone cabling, 63
 equipment room (ER), 63
 horizontal cabling, 63, 65-67
 structured entrance, 63
 work areas, 63
testing, 86-89
troubleshooting, 94
 cable failing to meet manufacturer specifications, 95
 cable stretching, 95
 CAT5e cable test examples, 96-100, 103
 installation, 94
UTP. *See* UTP

CAM (Content Addressable Memory), 213

campus area network (CAN), 5

campus distribution, optical networking, 141-144

campus distributor (CD), 63

campus networks, 62, 198
 analyzing data traffic, 448-450

camspllices, 132

CAN (campus area network), 5

capturing data packets with Wireshark, 444-445

Carrier Ethernet, 412-413
 Ethernet service types, 413-414
 service attributes, 414-415

case studies, configuring point-to-multipoint wireless LAN, 183
 antenna site survey, 183
 configuring multipoint distribution/conducting an RF site survey, 185
 configuring remote installations, 187
 establishing point-to-point home networks, 184

CAT5e, 69

CAT5e cable test examples, troubleshooting cabling systems, 96-100, 103

CAT6 (category 6), 40

CAT6/5E/5 UTP cables, terminating, 73-74
 computer communication, 74-76

CAT6 horizontal link cables, terminating, 77-82

CAT6a, 69, 71

CAT7, 71

CAT7a, 71

CBS (Committed Burst Size), 415

CCIE (Cisco Certified Internet Expert), 288

CCNA (Cisco Certified Network Associate), 288

CCNP (Cisco Certified Network Professional), 288

CD (campus distributor), 63
certification, cabling, 86-89

Challenge Handshake Authentication Protocol (CHAP), 487

Channel Service Unit/Data Service Unit (CSU/DSU), 401, 404

CHAP (Challenge Handshake Authentication Protocol), 487

Children's Internet Protection Act (CIPA), 486

chromatic dispersion, 128

CIDR (classless inter-domain routing), 267

CIDR blocks, TCP/IP, 267-269

CIPA (Children's Internet Protection Act), 486

CIR (Committed Information Rate), 415

Cisco 2500 series, 218-219

Cisco 2600 series, 217-218

Cisco 2800 series, 216-217

Cisco Certified Internet Expert (CCIE), 288

Cisco Certified Network Associate (CCNA), 288

Cisco Certified Network Professional (CCNP), 288

Cisco IOS, 288

Cisco Network Assistant (CNA), 209

Cisco VPN client, configuring remote client's VPN connection, 491-494

cladding, 121

class network address, 379

classes, IPv4 networks, 20

classful, 267

classful addressing, 379

CLI (command line interface), 288

CLNS (Connectionless Network Service), 377

clock rate command, 313

CNA (Cisco Network Assistant), 209

collision domains, 213

color maps, 73

color-code, fiber optics, 143

COM1, 298
COM2, 298
command line interface (CLI), 288
commands
 ipconfig, 45
 ipconfig/all, 17-18
Committed Burst Size (CBS), 415
committed information rate (CIR), 415
communications (air interface) protocol, 178
CompTIA Network+ objectives, 5
computer communication, CAT6/5E/5, 74-76
config-if, 406
Configuration BPDU, 338
configure terminal, 309, 331, 366
configuring
 HyperTerminal software (Windows), 298-300
 network interfaces, auto-negotiation, 225-226
 point-to-multipoint wireless LAN, case studies,
 183-185, 187
 remote access VPN server, 489
 remote client's VPN connection, 489-495
 RIP, 379-381
 RIP2, 379-381
 routes
 with RIP, 381-385
 with RIPv2, 385-386
 SNMP, 341-343
 static routes, 366-368
 switches. *See* switch configuration
 Z-Term Serial Communications software (Mac),
 300-302
connection-oriented protocols, 241
Connectionless Network Service (CLNS), 377
connectors, optical fibers, 132
console cables, 297
console input, 216
console port connection, 296-298
 configuring HyperTerminal software (Windows),
 298-300
 configuring Z-Term Serial communications software
 (Mac), 300-302
consoles, 310
Content Addressable Memory (CAM), 213
convergence, 371
converting hexadecimal numbers, 253
copy run start, 368
copy running-config startup-config, 333
cost, 371
 home networking, 32
country domains, 420
CRC (cyclic redundancy check), 16
cross connect, 64
crossover, 41
crossover patch cables, 76-77
crosstalk, 88
CSMA/CA (carrier sense multiple access/collision avoidance), 157
CSMA/CD (carrier sense multiple access with collision detection), 15
CSU/DSU (Channel Service Unit/Data Service Unit), 401, 404
cut-through, 214
cyclic redundancy check (CRC), 16

D

DARPA (Defense Advanced Research Projects Agency), 238
data, analyzing internet data traffic, 427
 frame size distribution, 430
 network layer host table, 430
 network layer matrix, 429
 Utilization/Errors Strip Chart, 428
data channels, 403-404
Data Communications Equipment (DCE), 312
Data Encryption Standard (DES), 489
data link layer, OSI (open systems interconnect model, 13
data packets
 capturing with Wireshark, 444-445
 DHCP, 418-419
 FTP, 446-447
 Inspecting with Wireshark, 442-443
data speed, home networking, 32
Data Terminal Equipment (DTE), 312
data traffic, campus networks, 448-450
DB-9 type connector, 296
DB-25 type connector, 296
DCE (Data Communications Equipment), 312
DDoS (distributed denial-of-service), 476

decimal-to-binary conversion, 251-252
default gateway address, 291
default version control, 386
Defense Advanced Research Projects Agency (DARPA), 238
definitions, 477
delay, 371
delay skew, NVP, 89
denial-of-service (DoS), 475-476
dense wavelength division multiplex (DWDM), 131
deployment, DHCP, 419
DES (Data Encryption Standard), 489
detectors, 132-134
deterministic networks, 7
DFB (distributed feedback) laser, 131
DHCP (Dynamic Host Configuration Protocol), 416-418
 data packets, 418-419
 deployment, 419
dictionary attack, 470
Diffie-Hellman, 489
digital subscriber line (DSL), 408
diode laser (DL), 130
direct sequence spread spectrum (DSSS), 157
directed broadcast, 476
discrete multitone (DMT), 409
dispersion, fiber optics, 127-129
dispersion compensating fiber, 129
dispersion compensation, fiber optics, 129
distance vector protocols, 372-374
distributed denial-of-service (DDoS), 476
distributed feedback (DFB) laser, 131
DL (diode laser), 130
DMT (discrete multitone), 409
DNS (domain name service), 420-421
 administering local DNS server, 422
 Internet domain name, 421
 reverse DNS, 423
domain registrars, 421
DoS (denial-of-service), 475-476
 DDoS (distributed denial-of-service), 476
DS-0, 403
DS-3, 403
DSL (digital subscriber line), 408

DSL modems, home networking, 32
DSSS (direct sequence spread spectrum), 157
DTE (Data Terminal Equipment), 312
DUAL Finite State Machine, EIGRP, 379
DWDM (dense wavelength division multiplex), 131
dynamic assignment, 210
Dynamic Host Configuration Protocol. *See* DHCP
dynamic protocols, 358
dynamic routing protocols, 370-371
dynamic VLANs, 330

E

E-LAN service type (E-LAN), 413
E-Line service type (E-Line), 413
E-Tree service type (E-Tree), 414
EAP (Extensible Authentication Protocol), 181, 487
eBGP (external BGP), 426
EBS (Excess Burst Size), 415
echo request, 443
EIA (Electronic Industries Alliance), 62
EIA/TIA 568-A, 62
EIA/TIA 568-B, 62
EIA/TIA-568-B.1, 62
EIA/TIA-568-B.2, 62
EIA/TIA-568-B.3, 62
EIGRP (Enhanced Interior Gateway Routing Protocol), 378
EIR (Excess Information Rate), 415
electromagnetic interference (EMI), 72
Electronic Industries Alliance (EIA), 62
ELTCTL (Equal Level Transverse Conversion Transfer Loss), 92
EMI (electromagnetic interference), 72
enable secret
 privileged Exec mode, routers, 310
 switch configuration, 332
encap ? command, 406
Encapsulating Security Payload (ESP), 489
encryption, home networks, 35
endpoint PSE, 345
Enhanced Interior Gateway Routing Protocol (EIGRP), 378
enterprise networks, 198, 221

- Equal Level FEXT (ELFEXT),** 89
Equal Level Transverse Conversion Transfer Loss (ELTCTL), 92
equipment room (ER), structured cabling, 63
error threshold, 214
ESP (Encapsulating Security Payload), 489
ESS (Extended Service Set), 157
Ethernet, 15-17
 - 10 gigabit Ethernet over copper, 90-91
 - AXT (Alien Crosstalk),* 91-92
 - signal transmission,* 93
 - Carrier Ethernet, 412-413
 - Ethernet service types,* 413-414
 - service attributes,* 414-415
 - IP addressing, 19-21
 - MAC address, 18
 - Metro Ethernet, 412-413
 - Ethernet service types,* 413-414
 - service attributes,* 414-415
 - optical Ethernet, 137- Ethernet frames, 16**
- Ethernet LAN Service (E-LAN),** 413
- Ethernet Line Service (E-Line),** 413
- Ethernet packet frame, components of,** 16
- Ethernet Service Definition,** 412
- Ethernet service types, 413-414**
- Ethernet Tree Service (E-Tree),** 413
- EVC (Ethernet Virtual Connection),** 412
- events, 457
- Excess Burst Size (EBS),** 415
- Excess Information Rate (EIR),** 415
- Extended Service Set (ESS),** 157
- Extensible Authentication Protocol (EAP),** 181, 487
- external BGP (eBGP), 426

F

 - F/UTP, 92**
 - far-end crosstalk (FEXT),** 89
 - Fast Ethernet Interface configuration, privileged Exec mode (routers),** 311-312
 - fast link pulse (FLP),** 225
 - fast-forward, 214**
 - FastEthernet, UTP,** 71
 - FastEthernet port (FA0/0, FA0/1, FA0/2),** 221
 - FastEthernet Ports,** 216, 295
 - FEXT (far-end crosstalk),** 89-91
 - FHSS (frequency hopping spread spectrum),** 158-159
 - fiber, 132**
 - fiber Bragg grating,** 129
 - fiber connectorization,** 134-135
 - fiber cross-connect,** 139
 - fiber optics**
 - attenuation, 126
 - cladding, 121
 - color-code, 143
 - dispersion, 127-129
 - dispersion compensation, 129
 - graded-index fiber, 123-124
 - multimode fibers, 122
 - single-mode fibers, 124
 - mode field diameter,* 125
 - troubleshooting OTDR, 457-458
 - fiber to the business (FTTB),** 137
 - fiber to the curb (FTTC),** 137
 - fiber to the desktop (FTTD),** 137
 - fiber to the home (FTTH),** 137
 - fiber to the home/business,** 121
 - fiber-optic networks,** 117
 - fiber-optic systems, wavelengths,** 121
 - File Transfer Protocol.** *See* **FTP**
 - firewall protection,** 35
 - firewalls, 484-485**
 - home networks, 35
 - personal firewalls, 478
 - Linux,* 483
 - Mac OS X,* 482
 - Windows 7,* 478-481
 - stateful firewalls, 484
 - flat networks, routers,** 290
 - flooding,** 213
 - FLP (fast link pulse),** 225
 - forward domain name service,** 420
 - fragment-free,** 214
 - frame size distribution,** 430
 - frequency hopping spread spectrum (FHSS),** 158-159
 - FTP (File Transfer Protocol),** 440
 - data packets, 446-447

FTTB (fiber to the business), 137
FTTC (fiber to the curb), 137
FTTD (fiber to the desktop), 137
FTTH (fiber to the home), 137
full channel, 86
full duplex gigabit Ethernet, UTP, 71
full-duplex, 226
full IPv6 address, 270
fusion splicing, 133

G

gateway addresses, 223
gateway of last resort, static routing, 366
gateways, 223
GBIC (gigabit interface converter), 139
Generic Routing Encapsulation (GRE), 487
gigabit Ethernet, 71
glass, 132
graded-index fiber, 123-124
GRE (Generic Routing Encapsulation), 487

H

half-duplex, 226
hand-off, 157
hardware address, 17
HC (horizontal cross-connect), 63-64
HDLC (high-level data link control), 405
“Hello” packets, 375
hex (hexadecimal numbers), 252-255
 converting, 253
HF (high-frequency), 178
high-level data link control (HDLC), 405
high-speed, 402
 data channels, 403-404
 POP (point of presence), 404-406
high-speed serial interface (HSSI), 402
home access, home networking, 33
home networking, 22-24
 access points, 28
 appearance, 32
 broadband modem/gateway, 30

cable modems, 30
cost, 32
data speed, 32
DSL modems, 32
establishing wireless connections, 34
home access, 33
hubs, 24
implementation, 32
IP addressing, 36-37
network adapters, 24
public access, 33
routers, 28
securing, 34-35
switches, 24
troubleshooting, 33-34
wired networks, 22-23, 27
wireless, 34
wireless networks, 22-23, 27
wireless routers, 28
home networks, configuring point-to-multipoint
 wireless LAN case study, 184
hop count, 371
hopping sequence, 159
horizontal cabling, structured cabling, 63, 65-67
horizontal cross-connect (HC), 63
host addresses, 20
host numbers, 20
hostname, 303
 privileged Exec mode, routers, 309-310
 switch configuration, 331
hotspots, 34
HSSI (high-speed serial interface), 402
hub-switch comparison, 206-209
hubs, 9, 24
hybrid echo cancellation circuit, 93
hybrid protocols, 378-379
HyperTerminal software, configuring, 298-300

I-J

IANA (Internet Assigned Numbers Authority), 19, 421
iBGP (internal Border Gateway Protocol), 426
IC (interconnect) fibers, 141
IC (intermediate cross-connect), 63

ICANN (Internet Corporation for Assigned Names and Numbers), 240, 421

ICMP (Internet Control Message Protocol), 44, 247

IDC (intermediate distribution closet), 141

IEEE (Institute of Electrical and Electronics Engineers), 7

IEEE 802.3an-2006 10GBASE-T, 91

IEEE 802.5 Token-Ring Network standard, 7

IEEE 802.11, 155-157, 159-162

IETF (Internet Engineering Task Force), 375

IGMP (Internet Group Message Protocol), 247

IGP (Interior Gateway Protocol), 375

IKE (Internet Key Exchange), 489

implementation, home networking, 32

inbound data traffic, 427

index-matching gel, 134

infrared light, 120

inquiry procedure, Bluetooth, 173

inspecting data packets with Wireshark, 442-443

installation, troubleshooting cabling systems, 94

interconnecting LANs, 198

 bridges, 199-203

 switches. *See* switches

 with routers. *See* routers

Interior Gateway Protocol (IGP), 375

intermediate components, fiber optics, 132

intermediate cross-connect (IC), 63

Intermediate System to Intermediate System (IS-IS), 377

intermediate systems, 377

internal Border Gateway Protocol (iBGP), 426

International Organization for Standardization, 12

Internet Assigned Numbers Authority (IANA), 421

Internet Control Message Protocol (ICMP), 44, 247

Internet Corporation for Assigned Names and Numbers (ICANN), 240, 421

Internet domain name, 421

Internet Engineering Task Force (IETF), 375

Internet Group Message Protocol (IGMP), 247

Internet Key Exchange (IKE), 489

Internet layer, TCP/IP, 245-247

Internet Protocol (IP), 245

internet routing, BGP, 424-426

Internet Security Association and Key Management Protocol (ISAKMP), 489

intranets, 21

intrusion, 469

 packet sniffing, 470-471

 password cracking, 470

 social engineering, 469

 viruses, 473-474

 vulnerable software attacks, 471-472

preventing, 472-473

 worms, 473-474

intrusion prevention system (IPS), 485

IP (Internet Protocol), 245

IP address assignment, 258

IP addresses, 20

IP addressing

 Ethernet, 19-21

 home networks, 36-37

ip helper, 418

IP internetwork, 21

ip route command, 363-365

IP security (IPsec), 471

IP tunnels, 487

ipconfig, 45

ipconfig/all command, 17-18

IPng (next generation IP), 270

IPS (intrusion prevention system), 485

IPsec, 491-492

IPsec (IP security), 471

IPv4 addressing, TCP/IP, 255-257

 IP address assignment, 258

IPv4 networks, classes, 20

IPv6 addressing, TCP/IP, 270-273

IPX (Internetworking Packet Exchange), 429

IS-IS (Intermediate System to Intermediate System), 377

ISAKMP (Internet Security Association and Key Management Protocol), 489

ISI (intersymbol interference), 129

isolating collision domains, 213

isolators, 132

ISP (internet service provider), 21

Keepalive packets, 451

L2F (Layer 2 Forwarding Protocol), 488
L2TP (Layer 2 Tunneling Protocol), 488
LACNIC, 258
LANs (local area networks), 5
interconnecting, 198
bridges, 199-203
switches. *See switches*
with routers. *See routers*
office LAN, assembling, 38-43
testing, 44-45
Token Ring topology, 7
troubleshooting, 44-45
last mile, WiMAX, 175
Layer 2 Forwarding Protocol (L2F), 488
layer 2 switch, 205
Layer 2 Tunneling Protocol (L2TP), 488
layer 3 networks, routers, 290-295
layers, TCP/IP, 239
application layer, 240-241
Internet layer, 245-247
network interface layer, 248
transport layer, 241-245
LCL (Longitudinal Conversion Loss), 92
lease time, 416
LED (light-emitting diode), 130
LF (low-frequency), 178
light, 119
infrared light, 120
numerical aperture, 122
optical spectrum, 120
pulse dispersion, 122
refraction, 119
refractive index, 120
light pipe, 132
light-emitting diode (LED), 130
line console passwords
privileged Exec mode, routers, 310-311
switch configuration, 332-333
line of demarcation, 404
link integrity tests, 42

link lights, 42

link pulses, 42

link state advertisements (LSAs), 375

link state protocols, 375-377

links, 86

Linux, personal firewalls, 483

load, 371

load balancing, 371

local area networks. *See LAN*

logical addresses, 215

logical fiber maps, 141

long-haul, single-mode fibers, 124

Longitudinal Conversion Loss (LCL), 92

loopback, static routing, 360

loss of association, wireless networking, 170

lost associations, 165

low-frequency (LF), 178

LSAs (link state advertisements), 375

M

Mac, configuring Z-Term Serial Communications software, 300-302

MAC address, 17-19

MAC address filtering, 35

Mac OS X

configuring computers in office LAN, 43

configuring remote client's VPN connection, 491

establishing wireless connections, 34

personal firewalls, 482

macrobending, 126

main cross-connect (MC), 63

main distribution frame (MDF), 63

malware, 474

MAN (metropolitan area network), 5

managed switches, 209-214

management information base (MIB), 340

Mbps (megabits per second), 40

MC (main cross-connect), 63

MD5 (Message Digest 5), 487-489

MDF (main distribution frame), 63

mechanical splices, 134

media converters, 219

MEF (Metro Ethernet Forum), 412
mesh topology, 11
messages, multicast, 206
metrics, 371
Metro Ethernet, 5, 412-413
 Ethernet service types, 413-414
 service attributes, 414-415
Metro Ethernet Forum (MEF), 412
metropolitan area network (MAN), 5
MIB (management information base), 340
microbending, 126
midspan PSE, 345
MIMO (Multiple Input Multiple Output), 161
MLS (multilayer switches), 214
mm (multimode), 142
modal dispersion, 128
mode field diameter, fiber optics, 125
modems, analog modem technologies, 407-408
 cable modems, 408
 RAS (remote access server), 410-411
 xDSL modems, 408-410
MT ACK, 419
MT Discover, 418
MT Offer, 419
MT Request, 419
multicast addresses, 247, 272
multicast messages, 206
multicasting, 247
multihomed, 425
multilayered switches, 214
multilevel encoding, 93
multimode (mm), 142
multimode fibers, 121-122
Multiple Input Multiple Output (MIMO), 161
multiplexed, 404
multipoint distribution, configuring point-to-point wireless LAN case study, 185
multiport bridges, 205
multiport repeaters, 9

near-end crosstalk (NEXT), 86-88, 91
NET (Network Entity Title), 294, 377
Net-Challenge software, 305
netstat-a, 472
netstat-b, 473
netsta-r, 360
network adapters, 24
network addresses, 20, 215
network command, 379
network congestion, UTP, 71
Network Control Protocol (NCP), 238
Network Discovery Recovery, EIGRP, 378
Network Entity Title (NET), 377
network interface card (NIC), 17
network interface layer, TCP/IP, 248
network interfaces, configuring auto-negotiation, 225-226
network layer, OSI (open systems interconnect) model, 13
network layer host table, 430
network layer matrix, 429
network numbers, 20
network operations center (NOC), 419
network security, 468
 DoS (denial-of-service), 475-476
 DDoS (distributed denial-of-service), 476
 intrusion, 469
 packet sniffing, 470-471
 password cracking, 470
 social engineering, 469
 viruses, 473-474
 vulnerable software attacks, 471-473
 worms, 473-474
 security software and hardware, 477
 antivirus software, 477
 firewalls, 484-485
 personal firewalls, 478-483
 security appliances, 485-486
 VPNs, 486-487
 tunneling protocols, 487-489
network segments, routers, 223
network services, 416-418
 DHCP
 data packets, 418-419
 deployment, 419

N

NAT (Network Address Translation), 35-36
NCP (Network Control Protocol), 238

DNS, 420-421
 administering local DNS server, 422
 Internet domain name, 421
reverse DNS, 423
network slowdowns, 200
network statements, 379
networking challenges
 RIPv2, 387
 static routes, 368-369
 switch configuration, 337
networks, analyzing, 441
 capturing data packets with Wireshark, 444-445
 FTP data packets, 446-447
 inspecting data packets with Wireshark, 442-443
NEXT (near-end crosstalk), 86-88, 91
next hop address, 294
NIC (network interface card), 17
NLOS (non-line-of-sight), 175
no ip directed-broadcast, 476
no shut command, 313, 366
no shutdown (no shut), 311
NOC (network operations center), 419
 internet data traffic, 427
nominal velocity of propagation (NVP), 89
non-internet routable IP addresses, 258
non-line-of-sight (NLOS), 175
NS record, 421
number conversion
 binary-to-decimal conversion, 249-251
 decimal-to-binary conversion, 251-252
 hexadecimal numbers, 252-255
numerical aperture, 122
numerics for Ethernet LAN cabling, 41
NVP (nominal velocity of propagation), 89
 delay skew, 89
 propagation delay, 89

O

OC (optical carriers), 137, 403
OFDM (orthogonal frequency division multiplexing), 158-159
office LAN, assembling, 38-43
Open Shortest Path First (OSPF), 375

Open System Interconnection (OSI), 377
optical carrier (OC), 137, 403
optical communication links, advantages of, 118
optical components
 detectors, 132-134
 DFB (distributed feedback) laser, 131
 DL (diode laser), 130
 DWDM (dense wavelength division multiplex), 131
 fiber connectorization, 134-135
 intermediate components, 132
 LED (light-emitting diode), 130
 tunable lasers, 131
 VCSELs (vertical cavity surface emitting lasers), 131
optical Ethernet, 137
optical fibers, connectors, 132
optical networking, 118, 136
 building distribution, 138-141
 campus distribution, 141-144
 defining, 136-138
 safety, 145-146
optical spectrum, 120
optical time-domain reflectometer (OTDR), 457-458
optical-line amplifiers, 132
organizational unit identifier (OUI), 248
organizationally unique identifier. *See OUI*
orthogonal frequency division multiplexing (OFDM), 158
Ortronics clarity twisted-pair system, 67
OSI (open systems interconnect) model, 12-14, 377
OSPF (Open Shortest Path First), 375
OTDR (optical time-domain reflectometer), 457-458
OUI (organizational unit identifier), 17, 248
outbound data traffic, 427
overloading, 36

P-Q

packet filtering, 484
packet sniffing, intrusion, 470-471
packets, 16
paging procedure, Bluetooth, 173
pairing, Bluetooth, 173
PAP (Password Authentication Protocol), 487
passive, RFID tags, 177

Passkey, Bluetooth, 173
Password Authentication Protocol (PAP), 487
password cracking, intrusion, 470
passwords, line consoles (switch configuration), 332-333
PAT (Port Address Translation), 36
patch cables, 67
path determination, 371
PC Card adapters, home networking, 26
PD (Powered Device), 345
peering, 426
personal firewalls, 478
 Linux, 483
 Mac OS X, 482
 Windows 7, 478-481
physical address, 17
physical fiber map, 141
physical layer, 13, 61
 IEEE 802.11, 156
 OSI (open systems interconnect) model, 13
physical layer cabling, 61
piconet, 173
Ping, 44, 443
ping command, 207
PoE (Power over Ethernet), 328, 344-346
 switches, 345
PoE Plus, 346
point of presence (POP), 404-406
Point-to-Point Protocol (PPP), 405, 487
Point-to-Point Tunneling Protocol (PPTP), 487
polarization mode dispersion, 128
POP (point of presence), 404-406
Port Address Translation (PAT), 36
port-based VLANs, 329
ports, 10, 41
 uplink ports, 41
 well-known ports, 240
Power over Ethernet. *See PoE (Power over Ethernet)*
Power Sourcing Equipment (PSE), 345
Power Sum NEXT (PSNEXT), 89
Power-Sum Alien Attenuation Cross-Talk Ration Far-End (PSAACRF), 92
Power-Sum Alien Near-End Cross-Talk (PSSANEXT), 92
Powered Device (PD), 345
PPP (Point-to-Point Protocol), 405, 487
PPTP (Point-to-Point Tunneling Protocol), 487
prefix length notation, 267
presentation layer, OSI (open systems interconnect) model, 13
preventing vulnerable software attacks, 472-473
private addresses, 21
privileged exec mode
 router configuration challenge, 314-316
 routers, 308-309
 enable secret, 310
 Fast Ethernet Interface configuration, 311-312
 hostname, 309-310
 line console passwords, 310-311
 serial interface configuration, 312-313
privileged mode, 308
propagation delay, 89
Protocol Dependent Modules, EIGRP, 379
protocol-based VLANs, 329
protocols, 7
 routing protocols. *See routing protocols*
 VPN tunneling protocols, 487-489
proxy servers, 484
PSAACRF (Power-Sum Alien Attenuation Cross-Talk Ratio Far-End), 91-92
PSACRF, 89
PSANEXT, 91
PSE (Power Sourcing Equipment), 345
PSELFEXT, 89
pseudorandom, 159
PSSANEXT (Power-Sum Alien Near-End Cross-Talk), 92
public access, home networking, 33
pulse dispersion, 122
PuTTY, 298

R

RADIUS (Remote Authentication Dial-In User Service), 181, 487
range extenders, 34
ranging, 408
RAS (remote access server), 410-411

- Rayleigh scattering**, 126
receive (RX), 75
received signal level (RSL), 132
refraction of light, 119
refractive index, 120
regional Internet registries (RIRs), 258
reliability, 371
Reliable Transport Protocol, EIGRP, 379
remote access, 407
 analog modem technologies, 407-408
 cable modems, 408
 RAS (remote access server), 410-411
 xDSL modems, 408-410
remote access server (RAS), 410-411
remote access VPN, 487
remote access VPN server, configuring, 489
Remote Authentication Dial-In User Service, 181
remote client's VPN connection, configuring, 489-495
remote installations, configuring point-to-multipoint wireless LAN case study, 187
Resistive Power Discovery, 346
response speed, 132
responsivity, 132
Return Loss, 91
 propagation delay, 89
 PSACR, 89
reverse DNS, 423
reverse domain name service, 420
RF site surveys, configuring point-to-multipoint wireless LAN case study, 185
RFID (radio frequency identification), 175-178
RIP (Routing Information Protocol), 373
 configuring, 379-381
 configuring routes, 381-385
RIPE NCC, 258
RIPv2
 configuring, 379-381
 configuring routes, 385-386
 networking challenges, 387
RIPv2 routing protocols, 358
RIRs (regional Internet registries), 258
RJ-45, 40-41, 73
roaming, 157
rollover cables, 298
root servers, 421
route flapping, 376
route print, 360
routed networks, 291
router configuration challenge, privileged Exec mode, 314-316
router configuration challenges, User Exec mode, 305-307
router interfaces, 216
 Cisco 2500 series, 218-219
 Cisco 2600 series, 217-218
 Cisco 2800 series, 216-217
 troubleshooting, 451-453
router rip, 379, 382
router uptime, 305
Router#, 308
Router(config)#, 310
Router(config-line)#, 311
routers, 215-216
 fundamentals of, 289-290
 layer 3 networks, 290-295
 home networking, 28
 interconnecting LANs, 221-223
 gateway addresses, 223
 network segments, 223
 privileged exec mode, 308-309
 enable secret, 310
 Fast Ethernet Interface configuration, 311-312
 hostname, 309-310
 line console passwords, 310-311
 serial interface configuration, 312-313
 router interface
 Cisco 2500 series, 218-219
 Cisco 2600 series, 217-218
 Cisco 2800 series, 216-217
 User Exec mode, 303-305
 router configuration challenge, 305-307
 wireless routers, home networking, 28
routes, configuring
 with RIP, 381-385
 with RIPv2, 385-386
Routing Information Protocol. See RIP
routing loops, 373
routing protocols, 358
 distance vector protocols, 372-374
 dynamic routing protocols, 370-371

hybrid protocols, 378-379
link state protocols, 375-377
static routing, 359
static routing protocols, 358
routing table code C, 365
routing table code S, 365
routing tables, 223
RS-232, 296
RSL (received signal level), 132
RX (receive), 75

S

safety, optical networking, 145-146
scattering attenuation, 126
SDH, 136
secure address, 210
Secure File Transfer Protocol (SFTP), 447
Secure Hash Algorithm 1 (SHA-1), 489
securing home networks, 34-35
security, WLAN, 179, 181-182. *See also network security*
beacons, 180
WPA (Wi-Fi Protected Access), 181
security appliances, 485-486
semi-active, RFID tags, 177
serial interface, 216
serial interface configuration, privileged Exec mode (routers), 312-313
serial ports (S0/0, S0/1, S0/2), 222
service attributes, Metro Ethernet/Carrier Ethernet, 414-415
Service Set Identifier (SSID), 35, 164
session layer, OSI (open systems interconnect) model, 13
SFP (Small Form factor Pluggable), 140
SFP+, 140
SFTP (Secure File Transfer Protocol), 447
sh ip int brief, 451
sh ip int brief command, 314, 451
sh ip protocol, 386
sh ip route, 364, 385
sh run command, 383-384
SHA-1 (Secure Hash Algorithm 1), 489

shielded twisted-pair. *See STP*
show controllers command, 313
show controllers serial, 313
show flash command, 305
show interface status, 440, 454
show ip interface brief, 440
show ip interface brief (s hip int brief), 312, 367
show ip protocol (show ip protocol), 382
show ip route (sh ip route), 364
show ip route static (s hip route static), 367
show mac address-table, 440
show power inline, 345
show running-config, 333, 336
show running-config (sh rum), 367
show startup-config, 333
show startup-config (sh start), 367
show version command, 305
show vlan, 334-335
signal transmission, 10 gigabit Ethernet over copper, 93
signatures, 477
Simple Network Management Protocol. *See SNMP*
single-mode (sm), 142
single-mode fibers, 121, 124
long-haul, 124
mode field diameter, 125
site survey, wireless networking, 166-171
site-to-site VPN, 487
Slotted Aloha, 178
sm (single-mode), 142
small office/home office (SOHO), 419
Smurf attack, 475
SNMP (Simple Network Management Protocol), 328, 340-341
configuring, 341-343
snmp community, 341
snmp community public ro, 341
SNMPv2, 343
SNMPv3, 343
social engineering, intrusion, 469
software
antivirus software, 477
personal firewalls, 478
Linux, 483

- Mac OS X*, 482
Windows 7, 478-481
- SOHO (small office/home office)**, 419
- SONET (synchronous optical network)**, 136
- SONET?SDH**, 136
- Spanning-Tree Protocol.** *See* STP (Spanning-Tree Protocol)
- spectral response**, 132
- SPI (stateful packet inspections)**, 35
- splitters**, 132
- spoof**, 476
- SSID (Service Set Identifier)**, 35, 164
- star topology**, 9
- stateful firewalls**, 484
- stateful packet inspections (SPI)**, 35
- static addressing**, 210
- static routes**, 424
- configuring, 366-368
 - networking challenges, 368-369
- static routing**, 359-365
- gateway of last resort, 366
 - loopback, 360
- static routing protocols**, 358
- static VLAN configuration, switch configuration**, 333-337
- static VLANs**, 330
- store-and-forward**, 213
- STP (Spanning-Tree Protocol)**, 61, 72, 328, 338-339
- straight-through cables**, 76-77
- straight-through CAT5e/5 patch cables, assembling**, 82-85
- straight-through input**, 41
- structured cabling**, 62-65
- backbone cabling, 63
 - equipment room (ER), 63
 - horizontal cabling, 63, 65-67
 - structured entrance, 63
 - work areas, 63
- STS (synchronous transport signals)**, 137
- Stubby areas**, 424
- subchannels, OFDM (orthogonal frequency division)**, 159
- subnet**, 294
- subnet masks, TCP/IP**, 259-266
- supernetting**, 267
- switch configuration**, 330-331
- enable secret, 332
 - hostname, 331
 - networking challenges, 337
 - setting line console passwords, 332-333
 - static VLAN configuration, 333-337
- switch interfaces, troubleshooting**, 454-457
- switch latency**, 213
- Switch(config)#**, 332
- Switch(config-line)#**, 332
- switches**, 10, 24
- broadcast domain, 213
 - hub-switch comparison, 206-209
 - interconnecting LANs, 204-206
 - layer 2 switches, 205
 - managed switches, 209-214
 - multilayer switches, 214
 - PoE, 345
- SYN (synchronizing packet)**, 242
- SYN ACK (Synchronizing Acknowledgement)**, 242
- SYN attack**, 475
- synchronous optical network (SONET)**, 136
- synchronous transport signals (STS)**, 137
-
- T**
- T1**, 402-403
- T3**, 403
- T568A**, 73
- T568B**, 73
- tag-based VLANs**, 329
- TCA (Topology Change Notification Acknowledgement)**, 338
- TCL (Transverse Conversion Loss)**, 92
- TCN (Topology Change Notification)**, 338
- TCO (telecommunications outlet)**, 63
- TCP (Transport Control Protocol)**, 241
- TCP/IP (Transmission Control Protocol/Internet Protocol)**, 21, 238
- CIDR blocks, 267-269
 - IPv4 addressing, 255-257
 - IP address assignment*, 258
 - IPv6 addressing, 270-273
 - layers, 239
 - application layer*, 240-241

Internet layer, 245-247
network interface layer, 248
transport layer, 241-245
subnet masks, 259-266

TCTL (Transverse Conversion Transfer Loss), 92

TDM (time division multiplexing), WiMAX, 175

TDMA (time-division multiple access), WiMAX, 175

TE (telecommunications enclosure), 63

telco, 403

telco cloud, 403

telecommunications enclosure (TE), 63

Telecommunications Industry Association (TIA), 62

telecommunications outlet (TCO), 63

telecommunications room (TR), 63

terminating

- CAT6 horizontal link cables, 77-82
- CAT6/5E/5 UTP cables, 73-74
 - computer communication*, 74-76

testing

- cabling, 86-89
- LANs, 44-45

ThinNet, 8

TIA (Telecommunications Industry Association), 62

ticks, 371

TLD (top-level domains), 420-421

token passing, 7

Token Ring hub, 8

Token Ring system, disadvantages of, 8

Token Ring topology, 7

top-level domains (TLD), 420-421

topologies, 7

- bust topology, 8
- mesh topology, 11
- star topology, 9
- token ring topology, 7

Topology Change Notification (TCN), 338

Topology Change Notification Acknowledgement (TCA), 338

totally stubby areas, 424

TR (telecommunications room), 63

traffic, analyzing internet data traffic, 427-430

transceivers, 156

translation bridges, 202

Transmission Control Protocol/Internet Protocol.
See TCP/IP

transmit (TX), 75

transparent bridges, 202

Transport Control Protocol (TCP), 241

transport layer, 13

- OSI (open systems interconnect) model, 13
- TCP/IP, 241-245

transport layer protocols, 241

Transverse Conversion Loss (TCL), 92

Transverse Conversion Transfer Loss (TCTL), 92

Triple Data Encryption Standard (3DES), 489

troubleshooting

- cabling, 94
 - cable stretching*, 95
 - cabling failing to meet manufacturer specifications*, 95
 - CAT5e cable test examples*, 96-100, 103
 - installation*, 94
- fiber optics, OTDR, 457-458
- home networks, 33-34
- LANs, 44-45
- router interfaces, 451-453
- switch interfaces, 454-457

tunable lasers, 131

tunneling protocols, VPNs, 487-489

tunnels, 487

twisted-pair cable, categories for, 70

TX (transmit), 75

U

U-NII (unlicensed national information infrastructure), 159

UDP (User Datagram Protocol), 244

UHF (ultra-high frequency), 178

ultra-high frequency (UHF), 178

UNI (user-network interface), 412

unicast, 417

unicast addresses, 272

unshielded twisted pair. See UTP

uplink port, 41

USB interface, 216

User Datagram Protocol (UDP), 244

User Exec mode, routers, 303-305

- router configuration challenges, 305-307

user mode, 303
user-network interface (UNI), 412
Utilization/Errors Strip Chart, 428
UTP (unshielded twisted-pair), 69-70
 balanced mode, 70
 bottlenecking, 71
 crossover patch cables, 76-77
 FastEthernet, 71
 full duplex gigabit Ethernet, 71
 network congestion, 71
 straight-through cables, 76-77
UTP cabling, 61

V

V.44/V.34, 407
V.92/V.90, 407
variable length subnet masking, 363
variable length subnet masks (VLSMs), 376
VCSELs (vertical cavity surface emitting lasers), 131
VFL (visual fault locator), 457
VIC-4FXS/DID, 217
virtual local area networks. *See* **VLANs**
viruses, 473-474
visual fault locator (VFL), 457
VLAN Tag Preservations, 415
VLANS (virtual local area networks), 328-329
 dynamic VLANs, 330
 port-based, 329
 protocol-based, 329
 static, 330
 configuring, 333-337
 tag-based, 329
VLSMs (variable length subnet masks), 376
voice interface card, 217
VPNs (virtual private networks), 35
 remote access VPNs, 487-489
 remote client's VPN connection, configuring, 489-495
 security, 486-487
 tunneling protocols, 487-489
 site-to-site VPNs, 487
vulnerable software attacks, intrusion, 471-472
 preventing, 472-473

W

WAN interface card, 217
WANs (wide area networks), 5, 401
wavelength division multipliers, 132
web filter appliance, 485
well-known ports, 240
WEP (wired equivalent privacy), 180
Wi-Fi, 161
Wi-Fi Alliance, 23
Wi-Fi Protected Access (WPA), 181
wide area network. *See* **WAN**
WiMAX (Worldwide Interoperability for Microwave Access), 174-175
 last mile, 175
Windows, configuring HyperTerminal software, 298-300
Windows 7
 configuring computers in office LAN, 42
 configuring remote client's VPN connection, 489
 establishing wireless connections, 34
 personal firewalls, 478-481
Windows Vista
 configuring computers in office LAN, 42
 configuring remote client's VPN connection, 489
 establishing wireless connections, 34
Windows XP
 configuring computers in office LAN, 43
 configuring remote client's VPN connection, 490
 establishing wireless connections, 34
wire speed routing, 214
wire-maps, 77
wired networks, 22-23, 27
wireless connections, establishing home networking, 34
wireless local area network. *See* **WLAN**
wireless networking, 802.11, 155-166
 site survey, 166-171
 SSID (service set identifier), 164
wireless networks, 22-23, 27
 home networking, 34
wireless routers, 24
 home networking, 28

wireless technologies

- Bluetooth, 172-174
 - inquiry procedure*, 173
- RFID (radio frequency identification), 175-178
- WiMAX (Worldwide Interoperability for Microwave Access), 174-175

Wireless-N adapter, 27**Wireshark, 441-442**

- capturing data packets, 444-445
- inspecting data packets, 442-443

wiring color schemes for T568A and T568B, 73**WLAN (wireless local area network), 154**

- configuring point-to-multipoint wireless LAN, case study, 183-187
- ESS (Extended Service Set), 157
- IEEE 802.11, 155-162
- security, 179-182
 - beacons*, 180
 - WPA (*Wi-Fi Protected Access*), 181

WO (work area outlet), 64**work areas, structured cabling, 63****workstations, 64****worms, 473-474****WPA (Wi-Fi Protected Access), 181****write memory (wr m), 368**

X-Z**xDSL modems, 408-410****XENPAK, 140****XFP, 140****XPAK, 140****Z-Term Serial Communications software, configuring, 300, 302****zero dispersion wavelength, 129**