PEARSON IT

CYBERSECURITY CURRICULUM



SIXTH EDITION

NETWORKING ESSENTIALS

A CompTIA® Network+ N10-008 Textbook

Save 10% on Exam Voucher
See Inside

JEFFREY S. BEASLEY
PIYASAT NILKAEW

NETWORKING ESSENTIALS: SIXTH EDITION A COMPTIA NETWORK+ N10-008 TEXTBOOK

INSTRUCTOR EDITION

JEFFREY S. BEASLEY AND PIYASAT NILKAEW



Pearson

Networking Essentials: Sixth Edition

Instructor Edition

Copyright © 2022 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

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: 978-0-13-745582-9
ISBN-10: 0-13-745582-8

Library of Congress Control Number: 2021913557

ScoutAutomatedPrintCode

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.

Special Sales

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

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

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

EDITOR-IN-CHIEF
Mark Taber

DIRECTOR, ITP PRODUCT MANAGEMENT
Brett Bartow

DEVELOPMENT EDITOR
Marianne Bartow

MANAGING EDITOR
Sandra Schroeder

PROJECT EDITOR
Mandie Frank

COPY EDITOR
Kitty Wilson

INDEXER
Ken Johnson

PROOFREADER
Abigail Manheim

TECHNICAL EDITOR
Chris Crayton

PEER REVIEWERS
DeAnnia Clements
Osman Guzide
Gene Carwile
Dr. Theodor Richardson

PUBLISHING COORDINATOR
Cindy Teeters

DESIGNER
Chuti Prasertsith

COMPOSITOR
codeMantra

CREDITS

Figure 1-8 Screenshot of The command prompt in Windows 10 © Microsoft 2020
Figure 1-9 Screenshot of A typical text screen result when entering the ipconfig /all command in the command window. © Microsoft 2020
Figure 1-15 courtesy for Linksys
Figure 1-18 courtesy Zoom Telephonics, Inc.
Figure 1-19 courtesy for Linksys
Figure 1-27 Screenshot of (a) An example of displaying the IP address for computer 1 using the ipconfig command in Windows and (b) an example of the displayed IP address in macOS for the built-in Ethernet connection © Microsoft 2020
Figure 2-34 Screenshot of DTX-1800 certification report: Failure due to a termination problem. ©Fluke Corporation
Figure 2-35 Screenshot of DTX-1800 certification report: Failure due to excessive insertion loss. ©Fluke Corporation
Figure 2-36 Screenshot of The certification report for Test 1, showing that a short jumper cable passes the CAT5e link test. ©Fluke Corporation
Figure 2-37 Screenshot of The results for Test 2, showing that the cable failed the CAT5e link test. ©Fluke Corporation
Figure 2-38 Screenshot of The Test 3 CAT5e link test, showing failures with attenuation. ©Fluke Corporation
Figure 2-39 Screenshot of A CAT5e link test, showing failures with delay skew (Test 4). ©Fluke Corporation
Unnumbered Figure 2-1 Screenshot of Answer the following questions related to the certification report shown here. ©Fluke Corporation
Unnumbered Figure 2-2 Screenshot of Answer the following questions related to the certification report shown here. ©Fluke Corporation
Unnumbered Figure 2-3 Screenshot of Answer the following questions related to the certification report shown here - OMNI Scanner. ©Fluke Corporation
Figure 4-7 Screenshot of An example of the information displayed when an association is formed between a client and an access point. © Microsoft 2020
Figure 4-8 Screenshot of An example of a lost association. © Microsoft 2020
Figure 4-18 Screenshot of The window for configuring Bluetooth settings on a Mac. © 2020 Apple Inc
Figure 4-19 Screenshot of The Mac window showing the settings for a file transfer. © 2020 Apple Inc
Figure 4-20 Screenshot of The Mac window showing that a text file is coming in from another Bluetooth device. © 2020 Apple Inc
Figure 4-28 Screenshot of The excellent signal quality measured for the multipoint distribution. © Microsoft 2020
Figure 4-29 Screenshot of The poor signal quality measured at the remote site near the lake. © Microsoft 2020
Figure 5-7 Screenshot of The data traffic captured by computer 2 for the LAN using a hub. © Microsoft 2020
Figure 5-8 Screenshot of The data traffic captured by computer 2 for the LAN using a switch. © Microsoft 2020
Figure 5-9 Screenshot of The startup menu of a Cisco Catalyst switch in the CNA software. © Microsoft 2020
Figure 5-10 Screenshot of The highlighted ports showing the current connections and the location of the stacked switches icon. © Microsoft 2020
Figure 5-11 Screenshot of The window listing the MAC addresses currently connected to a switch. © Microsoft 2020
Figure 5-13 Screenshot of Configuring an IP address on an interface. © Microsoft 2020
Figure 5-19 Screenshot of Putty configuration © 1997-2020 Simon Tatham
Figure 5-20 Screenshot of The HyperTerminal Connect To dialog © 1997-2020 Simon Tatham
Figure 5-21 Screenshot of The Properties dialogs for configuring the serial port connection PuTTY © 1997-2020 Simon Tatham
Figure 5-23 Screenshot of The macOS dialog for configuring the settings for the serial interface. © 2020 Apple Inc
Figure 5-24 Screenshot of The macOS dialog for setting the serial port to PL2303-000. © 2020 Apple Inc
Figure 5-25 Screenshot of The macOS window listing the serial communication link settings. © 2020 Apple Inc
Figure 6-6 Screenshot of An example of the three packets exchanged in the initial TCP handshake. © Microsoft 2020
Figure 6-8 Screenshot of An example of the four-packet TCP connection termination. © Microsoft 2020
Figure 6-10 Screenshot of An example of a UDP packet transfer. © Microsoft 2020
Figure 6-12 Screenshot of Captured packets showing the (a) ARP request and the (b) ARP reply. © Microsoft 2020
Figure 6-13 Screenshot of The details of the ARP broadcast packet. © Microsoft 2020
Figure 6-14 Screenshot of An example of the use of hex numbers in data packets. © Microsoft 2020
Figure 7-3 Screenshot of The TCP/IP dialog for setting the default gateway address for computer A1. © Microsoft 2020
Figure 7-6 Screenshot of The Net-Challenge screen. © Microsoft 2020
Figure 7-7 Screenshot of The check box window for the Net-Challenge software User EXEC Mode challenge. © Microsoft 2020

Figure 7-8 Screenshot of The display for step 6, using the show command. © Microsoft 2020

Figure 7-11 Screenshot of The network topology for Net-Challenge. The arrows indicate where to click to display the router IP address configurations. © Microsoft 2020

Figure 7-14 Screenshot of An example of the port management options available with a Cisco switch: (a) Speed auto-negotiation option; (b) Duplex auto option. © Microsoft 2020

Figure 9-1a Screenshot of Setting the default gateway address or default static route on a host computer (PC). © Microsoft 2020

Figure 9-1b Screenshot of Setting the default gateway address or default static route on a host computer (macOS). © Microsoft 2020

FIG10-4 Screenshot of Captured DHCP packets. © Microsoft 2020

FIG10-9 Screenshot of An example of using an SNMP software management tool to obtain descriptions of a router's interfaces using the MIB ifDescr. © Microsoft 2020

FIG10-11 Screenshot of Using an SNMP software management tool to obtain interface speed settings. © Microsoft 2020

FIG10-12 Screenshot of An example of using SNMP to collect data traffic statistics. © Microsoft 2020

FIG10-23 Screenshot of Initializing Wireshark to capture data packets from a network. © Microsoft 2020

FIG10-24 Screenshot of Starting a capture. © Microsoft 2020

FIG10-25 Screenshot of The captured packets showing the ping from computer 1 to computer 2. © Microsoft 2020

FIG10-26 Screenshot of Computer 2 replying to computer 1 with its MAC address. © Microsoft 2020

FIG10-27 Screenshot of Computer 1 is sending an echo request to computer 2. © Microsoft 2020

FIG10-28 Screenshot of The echo reply received by computer 1. © Microsoft 2020

FIG10-30 Screenshot of (a) The beginning of the FTP data packet transfer and the request for an ASCII data transfer by the client. (b) The FTP data packet transfer and the closing of the FTP transfer. © Microsoft 2020

FIG10-31 Screenshot of Figure for problems 64–68. © Microsoft 2020

FIG11-9 Screenshot of Windows Firewall in Windows 10. © Microsoft 2020

FIG11-10 Screenshot of Windows 10 Firewall status. © Microsoft 2020

FIG11-11 Screenshot of Windows 10 allowed apps. © Microsoft 2020

FIG11-12 Screenshot of Windows 10 advanced firewall settings. © Microsoft 2020

FIG11-13 Screenshot of Windows 10 echo request properties. © Microsoft 2020

FIG11-14 Screenshot of Windows 10 echo request protocols and ports. © Microsoft 2020

FIG11-15 Screenshot of macOS firewall. © 2020 Apple Inc

FIG11-16 Screenshot of macOS advanced settings. © 2020 Apple Inc

FIG11-17 Screenshot of Linux iptables © The Netfilter's webmasters

FIG11-19 Screenshot of An example of setting WEP encryption on a wireless client. © Microsoft 2020

FIG11-26 Screenshot of The traceroute from the VPN server to the VPN remote client. © Microsoft 2020

FIG11-27 Screenshot of The first window, the VPN Client status window, is displayed after starting the VPN client software. © Cisco systems

FIG11-28 Screenshot of The connection screen for establishing a VPN link. © Cisco systems

FIG11-29 Screenshot of The initial handshake screen for the VPN client. © Cisco systems

FIG11-30 Screenshot of The menu showing that the VPN client has successfully connected to the virtual private network. © Cisco systems

FIG11-31 Screenshot of The Preferences window for the VPN client. © Cisco systems

FIG11-32 Screenshot of The Statistics window (a) and Route Details window (b) for the VPN client. © Cisco systems

FIG12-1 Screenshot of Enabling Hyper-V © Microsoft 2020

FIG12-2 Screenshot of Using Hyper-V Manager © Microsoft 2020

FIG12-3 Screenshot of Creating a virtual switch in Hyper-V © Microsoft 2020

FIG12-4 Screenshot of Specifying the name of a virtual switch © Microsoft 2020

FIG12-5 Screenshot of Creating a virtual machine © Microsoft 2020

FIG12-6 Screenshot of Specifying the name and location of a virtual machine. © Microsoft 2020

FIG12-7 Screenshot of Specifying the generation of the virtual machine © Microsoft 2020

FIG12-8 Screenshot of Specifying the desired memory size for a VM. © Microsoft 2020

FIG12-9 Screenshot of Selecting the connection name of the virtual switch. © Microsoft 2020

FIG12-10 Screenshot of Specifying a virtual hard disk name, location, and size. © Microsoft 2020

FIG12-11 Screenshot of The options for installing the VM's operating system. © Microsoft 2020

FIG12-12 Screenshot of Starting the new VM. © Microsoft 2020

FIG12-13 Screenshot of The final VM screen, showing that the machine is up. © Microsoft 2020

Peter Mell (NIST), Tim Grance (NIST), The NIST Definition of Cloud Computing, SP 800-145

Cover Artistdesign29/Shutterstock

CONTENTS AT A GLANCE

	Introduction	xxiii
1	Introduction to Computer Networks	2
2	Physical Layer Cabling: Twisted-Pair	62
3	Physical Layer Cabling: Fiber Optics	124
4	Wireless Networking	172
5	Interconnecting the LANs	228
6	TCP/IP	290
7	Introduction to Router Configuration	354
8	Introduction to Switch Configuration	404
9	Routing Protocols	444
10	Managing the Network Infrastructure	524
11	Network Security	590
12	Cloud Computing and Virtualization	676
13	Codes and Standards	706
	Glossary	742
	Index	764

Online Only Elements:

Net-Challenge Software

Wireshark Captures

Network+ quizzes

CONTENTS

Introduction xxiii

CHAPTER 1 Introduction to Computer Networks 2

Chapter Outline 3
Objectives 3
Key Terms 3
1-1 Introduction 4
1-2 Network Topologies 6
Section 1-2 Review 11
Test Your Knowledge 11
1-3 The OSI Model 12
Section 1-3 Review 15
Test Your Knowledge 15
1-4 The Ethernet LAN 16
IP Addressing 20
Section 1-4 Review 22
Test Your Knowledge 23
1-5 Home Networking 24
Securing a Home Network 33
IP Addressing in a Home Network 34
Section 1-5 Review 36
Test Your Knowledge 38
1-6 Assembling an Office LAN 38
Diagram the Network 39
Connect the Network Devices 40
Configure the Computers to Operate on the LAN 44
Section 1-6 Review 44
Test Your Knowledge 45
1-7 Testing and Troubleshooting a LAN 45
Section 1-7 Review 48
Test Your Knowledge 49
Summary 50
Questions and Problems 50
Certification Questions 59

CHAPTER 2 Physical Layer Cabling: Twisted-Pair 62

Chapter Outline 63
Objectives 63
Key Terms 63
2-1 Introduction 65
2-2 Structured Cabling 66
Horizontal Cabling 69
Section 2-2 Review 73
Test Your Knowledge 73
2-3 Twisted-Pair Cable 74
Unshielded Twisted-Pair Cable 74
Shielded Twisted-Pair Cable 76
Section 2-3 Review 77
Test Your Knowledge 77
2-4 Terminating Twisted-Pair Cables 78
Computer Communication 79
Straight-Through and Crossover Patch Cables 82
Section 2-4 Review 90
Test Your Knowledge 91
2-5 Cable Testing and Certification 92
Section 2-5 Review 96
Test Your Knowledge 97
2-6 10 Gigabit Ethernet over Copper 97
Overview 98
Alien Crosstalk 98
Signal Transmission 100
Section 2-6 Review 101
Test Your Knowledge 101
2-7 Troubleshooting Cabling Systems 102
Cable Stretching 102
Cable Failing to Meet Manufacturer Specifications 102
CAT5e Cable Test Examples 104
Section 2-7 Review 111
Test Your Knowledge 111
Summary 112
Questions and Problems 112
Certification Questions 121

CHAPTER 3 Physical Layer Cabling: Fiber Optics 124

Chapter Outline 125
Objectives 125
Key Terms 125
3-1 Introduction 126
3-2 The Nature of Light 129
Graded-Index Fiber 133
Single-Mode Fibers 134
Section 3-2 Review 135
Test Your Knowledge 135
3-3 Fiber Attenuation and Dispersion 136
Attenuation 136
Dispersion 137
Dispersion Compensation 139
Section 3-3 Review 140
Test Your Knowledge 140
3-4 Optical Components 141
Intermediate Components 142
Detectors 143
Fiber Connectorization 145
Section 3-4 Review 146
Test Your Knowledge 147
3-5 Optical Networking 147
Defining Optical Networking 148
Building Distribution 151
Campus Distribution 154
Optical Link Budget 157
Section 3-5 Review 158
Test Your Knowledge 159
3-6 Safety 160
Section 3-6 Review 161
Test Your Knowledge 162
3-7 Troubleshooting Fiber Optics: The OTDR 162
Section 3-7 Review 164
Test Your Knowledge 164
Summary 165
Questions and Problems 165
Certification Questions 169

CHAPTER 4 Wireless Networking 172

Chapter Outline 173
Objectives 173
Key Terms 173
4-1 Introduction 174
4-2 The IEEE 802.11 Wireless LAN Standard 175
Section 4-2 Review 184
Test Your Knowledge 185
4-3 802.11 Wireless Networking 185
Section 4-3 Review 195
Test Your Knowledge 196
4-4 Bluetooth, WiMAX, RFID, and Mobile Communications 197
Bluetooth 197
WiMAX 199
Radio Frequency Identification 200
Mobile (Cellular) Communications 204
Section 4-4 Review 205
Test Your Knowledge 206
4-5 Configuring a Point-to-Multipoint Wireless LAN: A Case Study 206
Step 1: Conducting an Antenna Site Survey 207
Step 2: Establishing a Point-to-Point Wireless Link to the Home Network 208
Steps 3 and 4: Configuring the Multipoint Distribution and Conducting an RF Site Survey 209
Step 5: Configuring the Remote Installations 211
Section 4-5 Review 212
Test Your Knowledge 212
4-6 Troubleshooting Wireless Networks 213
Access Point Hardware Issues 213
Wireless Router Issues 213
Wireless Compatibility 213
Signal Strength Problems 214
Wireless Coverage 214
Extending the Wireless Range 214
Frequency Interference Problems 214
Wireless Channel Utilization 214
Load Issues 215
SSID Issues 215
Securing Wi-Fi Issues 215
Cable Issues 215
Deauthentication/Disassociation Attacks 215

DHCP Issues 216
Wireless Printer Issues 216
Section 4-6 Review 216
Test Your Knowledge 216
Summary 217
Questions and Problems 217
Critical Thinking 224
Certification Questions 224

CHAPTER 5 Interconnecting the LANs 228

Chapter Outline 229
Objectives 229
Key Terms 229
5-1 Introduction 230
5-2 The Network Bridge 232
Section 5-2 Review 236
Test Your Knowledge 237
5-3 The Network Switch 237
Hub and Switch Comparison 239
Managed Switches 242
Multilayer Switches 247
Section 5-3 Review 247
Test Your Knowledge 248
5-4 The Router 249
The Router Interface 250
Quality of Service 251
Section 5-4 Review 253
Test Your Knowledge 254
5-5 The Console Port Connection 254
Configuring the PuTTY Software (Windows) 256
Configuring the ZTerm Serial Communications Software (Mac) 259
Section 5-5 Review 261
Test Your Knowledge 261
5-6 Interconnecting LANs with the Router 262
Gateway Address 265
Network Segments 265
Section 5-6 Review 266
Test Your Knowledge 266

5-7 Interconnecting LANs and WANs 267
Three-Tiered LAN Architecture 267
Core 268
Distribution/Aggregation Layer 269
Access/Edge Layer 269
Traffic Flow 269
Data Center Architecture 269
WAN High-Speed Serial Connections 270
Data Channels 270
Point of Presence 271
Metro Optical Ethernet/Carrier Ethernet 273
Ethernet Service Types 274
Service Attributes 276
Section 5-7 Review 277
Test Your Knowledge 277
Summary 279
Questions and Problems 279
Critical Thinking 287
Certification Questions 287

CHAPTER 6 TCP/IP 290

Chapter Outline 291
Objectives 291
Key Terms 291
6-1 Introduction 292
6-2 The TCP/IP Layers 294
The Application Layer 295
The Transport Layer 296
The Internet Layer 301
The Network Interface Layer 304
Section 6-2 Review 304
Test Your Knowledge 305
6-3 Number Conversion 306
Binary-to-Decimal Conversion 306
Decimal-to-Binary Conversion 307
Hexadecimal Numbers 309
Converting Hexadecimal 309
Section 6-3 Review 312
Test Your Knowledge 312

6-4 IPv4 Addressing 312
Section 6-4 Review 316
Test Your Knowledge 316
6-5 Subnet Masks: Subnetting and Supernetting 317
Subnetting 318
Alternative Technique to Derive the Subnets: Magic Number 323
Subnet Masking Examples 324
Gateway IP Address 326
Section 6-5 Review 327
Test Your Knowledge 327
6-6 Supernetting, CIDR Blocks, and VLSM 328
Section 6-6 Review 332
Test Your Knowledge 332
6-7 IPv6 Addressing 333
Transitioning to IPv6 335
CIDR for IPv6 337
Section 6-7 Review 338
Test Your Knowledge 339
Summary 340
Questions and Problems 340
Critical Thinking 349
Certification Questions 350

CHAPTER 7 Introduction to Router Configuration 354

Chapter Outline 355
Objectives 355
Key Terms 355
7-1 Introduction 356
7-2 Router Fundamentals 358
Layer 3 Networks 359
Section 7-2 Review 364
Test Your Knowledge 365
7-3 The Router's User EXEC Mode (Router>) 366
The User EXEC Mode 366
Router Configuration Challenge: User EXEC Mode 369
Section 7-3 Review 372
Test Your Knowledge 372
7-4 The Router's Privileged EXEC Mode (Router#) 373
The hostname Command 374

The enable secret Command 375
Setting the Line Console Passwords 375
FastEthernet Interface Configuration 376
Serial Interface Configuration 377
Router Configuration Challenge: Privileged EXEC Mode 380
Section 7-4 Review 382
Test Your Knowledge 382
7-5 Configuring the Network Interface: Auto-negotiation 383
Auto-negotiation Steps 384
Full-Duplex/Half-Duplex 384
Section 7-5 Review 386
Test Your Knowledge 387
7-6 Troubleshooting the Router Interface 387
Section 7-6 Review 392
Test Your Knowledge 392
Summary 393
Questions and Problems 393
Critical Thinking 399
Certification Questions 400

CHAPTER 8 Introduction to Switch Configuration 404

Chapter Outline 405
Objectives 405
Key Terms 405
8-1 Introduction 406
8-2 Introduction to VLANs 407
Virtual LANs 407
Section 8-2 Review 409
Test Your Knowledge 410
8-3 Introduction to Switch Configuration 410
Hostname 411
Enable Secret 412
Setting the Line Console Passwords 412
Static VLAN Configuration 414
VLAN Subinterfaces 418
Networking Challenge: Switch Configuration 419
Section 8-3 Review 420
Test Your Knowledge 421

8-4 Spanning Tree Protocol 422
Section 8-4 Review 424
Test Your Knowledge 425
8-5 Power over Ethernet 425
Section 8-5 Review 428
Test Your Knowledge 429
8-6 Troubleshooting the Switch Interface 429
Section 8-6 Review 434
Test Your Knowledge 435
Summary 436
Questions and Problems 436
Critical Thinking 440
Certification Questions 441

CHAPTER 9 Routing Protocols 444

Chapter Outline 445
Objectives 445
Key Terms 445
9-1 Introduction 446
9-2 Static Routing 447
Gateway of Last Resort 454
Configuring Static Routes 454
Networking Challenge: Static Routes 458
Section 9-2 Review 458
Test Your Knowledge 459
9-3 Dynamic Routing Protocols 460
Section 9-3 Review 462
Test Your Knowledge 463
9-4 Distance Vector Protocols 463
Section 9-4 Review 465
Test Your Knowledge 466
9-5 Configuring RIP and RIPv2 466
Configuring Routes with RIP 468
Configuring Routes with RIPv2 473
Networking Challenge: RIPv2 474
Section 9-5 Review 475
Test Your Knowledge 476
9-6 Link State Protocols 476
Section 9-6 Review 480

Test Your Knowledge 480
9-7 Configuring the Open Shortest Path First (OSPF) Routing Protocol 481
Networking Challenge: OSPF 485
Section 9-7 Review 486
Test Your Knowledge 487
9-8 Advanced Distance Vector Protocol: Configuring Enhanced Interior Gateway Routing Protocol (EIGRP) 487
Configuring Routes with EIGRP 488
Networking Challenge: EIGRP 494
Section 9-8 Review 495
Test Your Knowledge 495
9-9 Internet Routing with Border Gateway Protocol (BGP) 496
Configuring BGP 496
Section 9-9 Review 498
Test Your Knowledge 498
9-10 IPv6 Routing 499
IPv6 Static Routing 499
RIP for IPv6 499
OSPF for IPv6 500
EIGRP for IPv6 501
BGP for IPv6 501
Section 9-10 Review 502
Test Your Knowledge 503
Summary 504
Questions and Problems 504
Critical Thinking 520
Certification Questions 520

CHAPTER 10 Managing the Network Infrastructure 524

Chapter Outline 525
Objectives 525
Key Terms 525
10-1 Introduction 527
10-2 Domain Name and IP Address Assignment 528
Section 10-2 Review 531
Test Your Knowledge 531
10-3 IP Address Management with DHCP 531
The DHCP Data Packets 534
DHCP Deployment 535

Section 10-3 Review 537
Test Your Knowledge 537
10-4 Scaling a Network with NAT and PAT 537
Section 10-4 Review 539
Test Your Knowledge 539
10-5 Domain Name System (DNS) 539
DNS Resource Records 541
Section 10-5 Review 546
Test Your Knowledge 546
10-6 Network Management Protocols 546
Configuring SNMP 547
Section 10-6 Review 551
Test Your Knowledge 552
10-7 Analyzing Network Traffic 552
Section 10-7 Review 559
Test Your Knowledge 559
10-8 Network Analyzer: Wireshark 560
Downloading and Installing Wireshark 560
Using Wireshark to Capture Packets 561
Using Wireshark to Inspect Data Packets 562
Section 10-8 Review 565
Test Your Knowledge 565
10-9 Analyzing Computer Networks: FTP Data Packets 566
Section 10-9 Review 567
Test Your Knowledge 567
10-10 Troubleshooting IP Networks 568
Verifying Network Settings 570
Investigating IP Address Issues 570
Finding Subnet Mask Issues 570
Looking for Gateway Issues 571
Identifying Name Resolution Issues 571
Investigating DHCP Issues 571
Checking for Blocked TCP/UDP Ports 573
Section 10-10 Review 573
Test Your Knowledge 573
Summary 574
Questions and Problems 574
Certification Questions 587

CHAPTER 11 Network Security 590

Chapter Outline 591
Objectives 591
Key Terms 591
11-1 Introduction 592
11-2 Intrusion: How Attackers Gain Control of a Network 594
Social Engineering 595
Password Cracking 596
Packet Sniffing 597
Packet Sniffing Attacks 598
Vulnerable Software 599
Preventing Vulnerable Software Attacks 600
Malware 602
Section 11-2 Review 604
Test Your Knowledge 605
11-3 Denial-of-Service 606
Distributed Denial-of-Service Attacks 608
Section 11-3 Review 609
Test Your Knowledge 609
11-4 Security Software and Hardware 610
Personal Firewalls 610
Antivirus/Anti-malware Software 610
Configuring Firewall Settings for Windows 10 611
Configuring Firewall Settings for macOS 615
Configuring Firewall Settings for Linux 616
Firewalls 617
Other Security Appliances 619
Computer Forensics 621
Section 11-4 Review 622
Test Your Knowledge 622
11-5 Managing Network Access 623
Section 11-5 Review 625
Test Your Knowledge 625
11-6 Router Security 626
Router Access 626
Router Services 628
Logging 630
Section 11-6 Review 631
Test Your Knowledge 631

11-7 Switch Security 631
Switch Port Security 633
Dynamic ARP Inspection 635
STP Special Features 635
Section 11-7 Review 637
Test Your Knowledge 637
11-8 Wireless Security 637
Section 11-8 Review 641
Test Your Knowledge 642
11-9 Remote Access and VPN Technologies 642
Analog Modem Technologies 643
Cable Modems 644
xDSL Modems 644
Remote Access Server 647
Virtual Private Network 647
VPN Tunneling Protocols 648
Configuring a Remote Client's VPN Connection 652
Configuring a Windows 10 VPN Client 652
Configuring a macOS VPN Client 652
Configuring a Cisco VPN Client 653
Section 11-9 Review 658
Test Your Knowledge 658
11-10 Physical Security 659
Access Control Hardware 660
Detection Methods 661
Asset Disposal 662
Internet of Things (IoT) Security Devices 662
Section 11-10 Review 663
Test Your Knowledge 663
Summary 664
Questions and Problems 664
Critical Thinking 674
Certification Questions 674

CHAPTER 12 Cloud Computing and Virtualization 676

Chapter Outline 677
Objectives 677
Key Terms 677
12-1 Introduction 678

12-2 Virtualization 679
Setting Up Virtualization on Windows 10 682
Section 12-2 Review 691
Test Your Knowledge 691
12-3 Cloud Computing 692
Cloud Computing Service Models 694
Cloud Infrastructures 696
Section 12-3 Review 697
Test Your Knowledge 698
12-4 Enterprise Storage 698
Section 12-4 Review 700
Test Your Knowledge 700
Summary 701
Questions and Problems 701
Certification Questions 704

CHAPTER 13 Codes and Standards 706

Chapter Outline 707
Objectives 707
Key Terms 707
13-1 Introduction 708
13-2 Safety Standards and Codes 708
Design and Construction Requirements for Exit Routes (29 CFR 1910.36) 709
Maintenance, Safeguards, and Operational Features for Exit Routes (29 CFR 1910.37) 710
Emergency Action Plans (29 CFR 1910.38) 710
Fire Prevention Plans (29 CFR 1910.39) 711
Portable Fire Extinguishers (29 CFR 1910.157) 712
Fixed Extinguishing Systems (29 CFR 1910.160) 713
Fire Detection Systems (29 CFR 1910.164) 714
Employee Alarm Systems (29 CFR 1910.165) 715
Hazard Communication (29 CFR 1910.1200) 716
HVAC Systems 717
Door Access 717
Section 13-2 Review 718
Test Your Knowledge 718
13-3 Industry Regulatory Compliance 718
FERPA 719
FISMA 719
GDPR 719

GLBA 719
HIPAA 720
PCI DSS 720
International Export Controls 720
Section 13-3 Review 722
Test Your Knowledge 722
13-4 Business Policies, Procedures, and Other Best Practices 723
Memorandum of Understanding 723
Service-Level Agreement 724
Master Service Agreement 724
Master License Agreement 724
Non-Disclosure Agreement 725
Statement of Work 725
Acceptable Use Policy 725
Incident Response Policy 725
Password Policy 726
Privileged User Agreement 726
Standard Operating Procedure 726
Onboarding and Offboarding Policies 727
Other Best Practices 727
Section 13-4 Review 728
Test Your Knowledge 728
13-5 Business Continuity and Disaster Recovery 729
Section 13-5 Review 732
Test Your Knowledge 732
Summary 733
Questions and Problems 733
Certification Questions 739

Glossary 742

Index 764

Online Only Elements:

Net-Challenge Software
Wireshark Captures
Network+ quizzes

ABOUT THE AUTHORS

Jeffrey S. Beasley is a professor emeritus in the Information and Communications Technology program at New Mexico State University, where he taught computer networking and many related topics. He is coauthor of *Modern Electronic Communication*, ninth edition, the author of *Networking,* second edition, and *co-author of Networking Essentials,* fifth edition, and *A Practical Guide to Advanced Networking*.

Piyasat Nilkaew is the director of Computing and Networking Infrastructure at New Mexico State University and has more than 20 years of experience in network management and consulting. He has extensive expertise in deploying and integrating multiprotocol and multivendor data, voice, and video network solutions. He is co-author of *Networking Essentials,* fifth edition, and *A Practical Guide to Advanced Networking.*

ABOUT THE TECHNICAL REVIEWER

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

DEDICATIONS

This book is dedicated to my family: Kim, Damon/Heather, and Dana/Sam. —Jeff Beasley

This book is dedicated to my family: Boonsong, Pariya, June, Ariya, and Atisat. —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
- Don Yates for his help with the initial Net-Challenge software

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

- Abel Sanchez, Kathryn Sager, and Joshua Cook for their work on the Net-Challenge software; Adam Segura for his help 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; Josiah Jones and Raul Marquez Jr. for their help with the Wireshark material; and Ariya Nilkaew for her help with revising and editing many of the captured pictures

- Aaron Shapiro and Aaron Jackson for their help testing the many network connections presented in the text
- Paul Bueno and Anthony Bueno for reading through an early draft of the text

Your efforts are greatly appreciated.

We appreciate the excellent feedback of the following reviewers: Phillip Davis, DelMar College, Texas; Thomas D. Edwards, Carteret Community College, North Carolina; William Hessmiller, Editors & Training Associates; Bill Liu, DeVry University, California; and Timothy Staley, DeVry University, Texas.

Our thanks to the people at Pearson for making this project possible. Thanks to Brett Bartow for providing us with the opportunity to work on the sixth edition and for helping make this process enjoyable. Thanks to Marianne Bartow, to all the people at Pearson IT Certification, and also to the many technical editors for their help editing the manuscript.

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

—Jeffrey S. Beasley and Piyasat Nilkaew

WE WANT TO HEAR FROM YOU!

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

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

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

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

Email: community@informit.com

READER SERVICES

Register your copy of *Networking Essentials*, Sixth Edition at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account.* Enter the product ISBN 9780137455928 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

INTRODUCTION

This book provides a look at computer networking from the point of view of a network administrator. It guides readers from an entry-level knowledge of computer networks to advanced concepts related to 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; network servers; and Linux networking. After reading the entire text, you will have gained a solid knowledge base in computer networks.

In our years of teaching, we 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. In this book, we therefore show you the technology, how it is used, and why, and you can take the applications of the technology to the next level. Allowing you to experiment with the technology helps you develop a greater understanding.

ORGANIZATION OF THE TEXT

This book has been thoroughly updated to reflect the latest version of the CompTIA Network+ exam. *Networking Essentials,* sixth edition, is a practical, up-to-date, and hands-on guide to the basics of networking. Written from the viewpoint of the network administrator, it requires absolutely no previous experience with either network concepts or day-to-day network management. Throughout the text, you will gain an appreciation of how basic computer networks and related hardware are interconnected to form a network. You will come to understand the concepts of twisted-pair cable, fiber optics, LANs interconnection, TCP/IP configuration, subnet masking, basic router configuration, switch configuration and management, wireless networking, and network security.

The textbook's companion website contains laboratory exercises, the Net-Challenge software, Wireshark captures, and the Network+ terminology quizzes.

Key Pedagogical Features

- The *Chapter Outline, Network+ Objectives, Key Terms,* and *Introduction* at the beginning of each chapter clearly outline specific goals for you, the reader. Figure I-1 shows an example of these features.

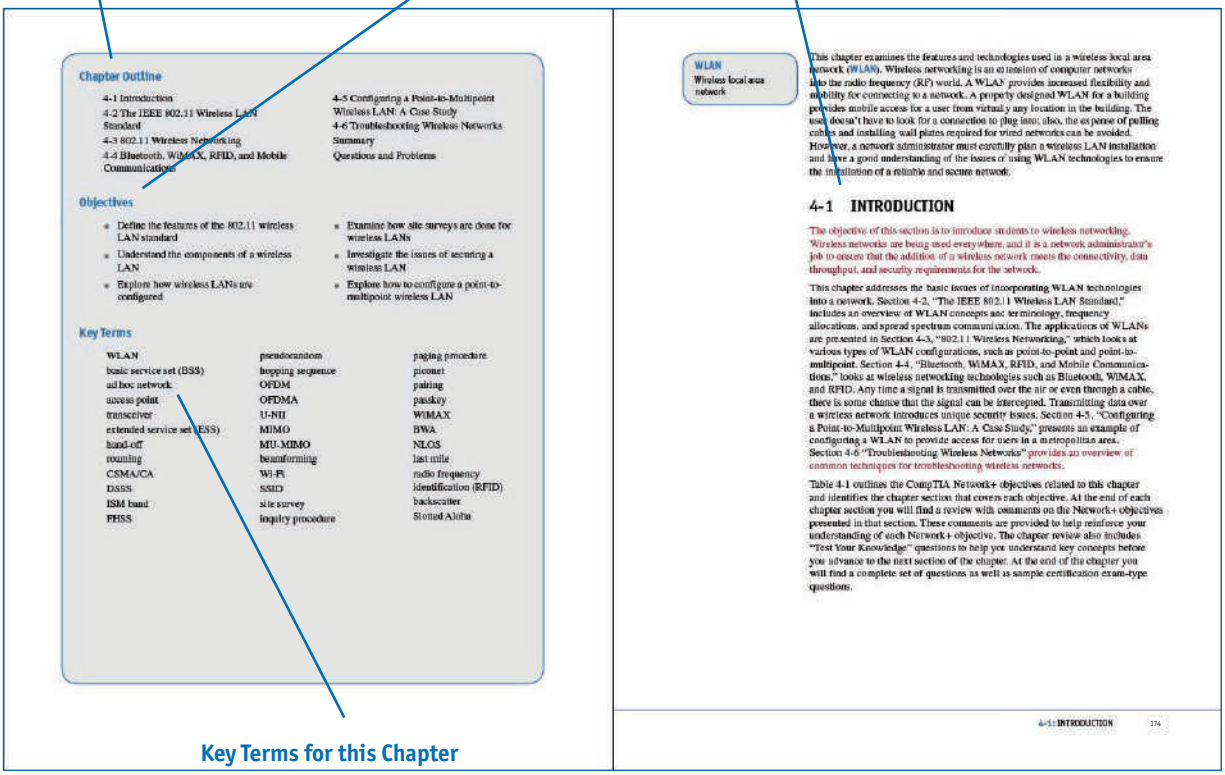


FIGURE I-1

- The *Net-Challenge software* provides simulated hands-on experience configuring routers and switches. Exercises provided in the text (see Figure I-2) and companion website challenge you to undertake certain router/network configuration tasks. These challenges help you check your ability to enter basic networking commands and to set up router functions, such as configuring the interface (Ethernet and serial) and routing protocols (for example, RIP, static). The software has the look and feel of actually being connected to a router's console port.

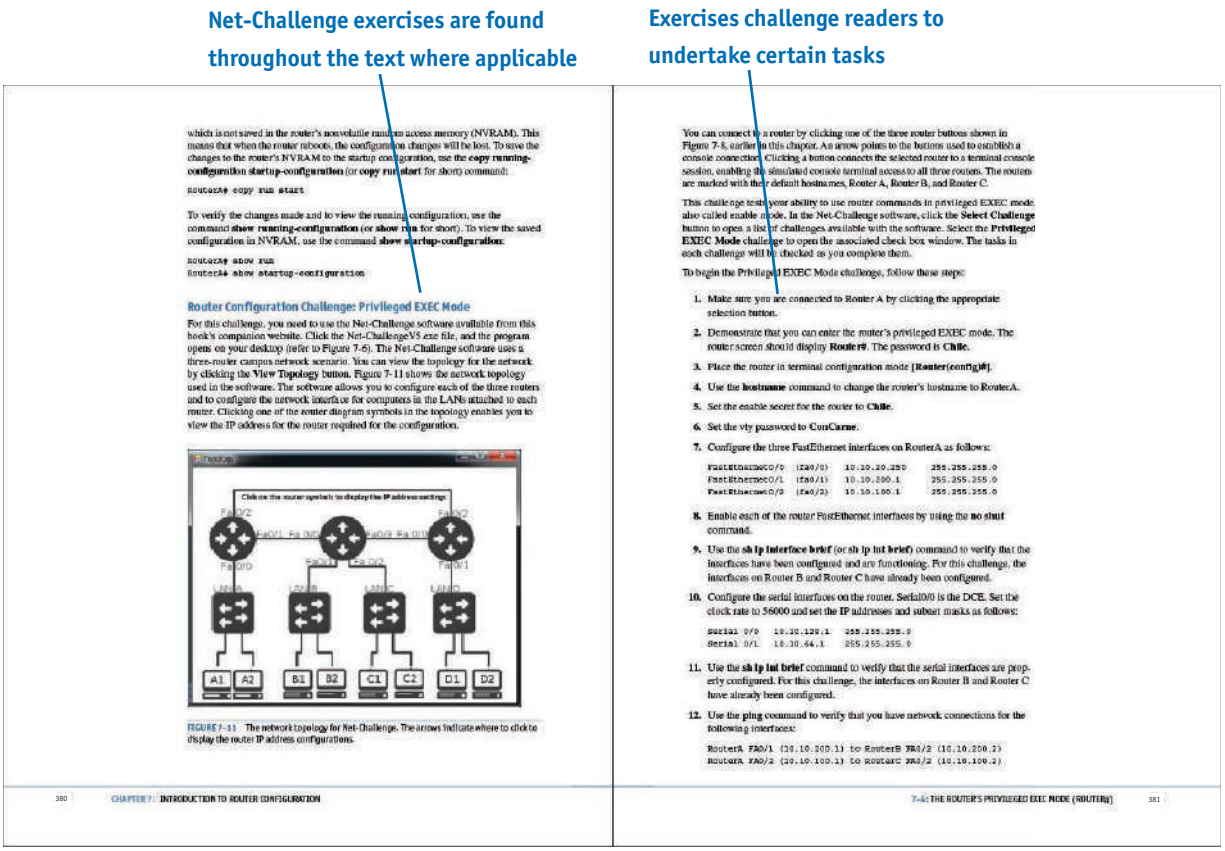
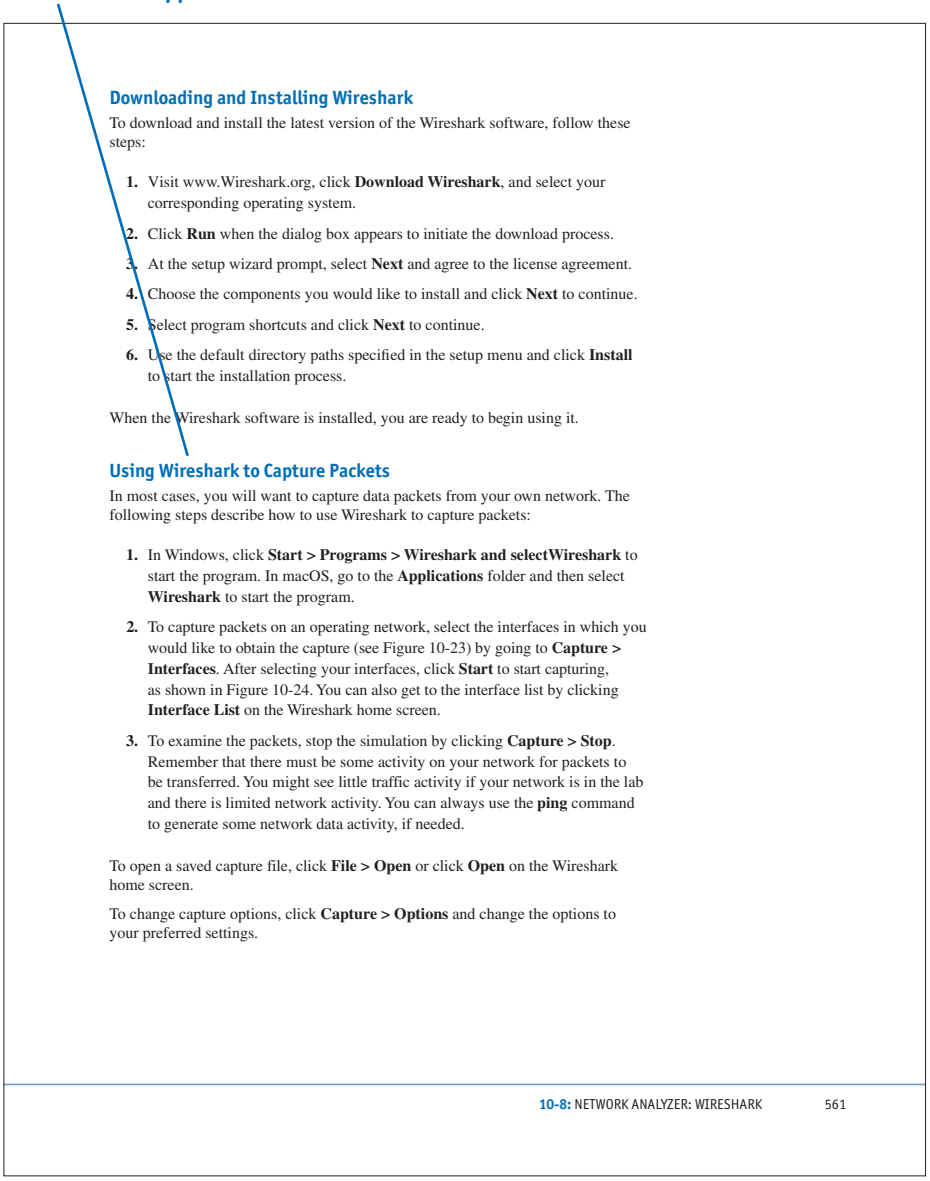


FIGURE I-2

- 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 I-3.

Examples using the Wireshark protocol analyzer are included throughout the text where applicable



Downloading and Installing Wireshark

To download and install the latest version of the Wireshark software, follow these steps:

1. Visit www.Wireshark.org, click **Download Wireshark**, and select your corresponding operating system.
2. Click **Run** when the dialog box appears to initiate the download process.
3. At the setup wizard prompt, select **Next** and agree to the license agreement.
4. Choose the components you would like to install and click **Next** to continue.
5. Select program shortcuts and click **Next** to continue.
6. Use the default directory paths specified in the setup menu and click **Install** to start the installation process.

When the Wireshark software is installed, you are ready to begin using it.

Using Wireshark to Capture Packets

In most cases, you will want to capture data packets from your own network. The following steps describe how to use Wireshark to capture packets:

1. In Windows, click **Start > Programs > Wireshark and selectWireshark** to start the program. In macOS, go to the **Applications** folder and then select **Wireshark** to start the program.
2. To capture packets on an operating network, select the interfaces in which you would like to obtain the capture (see Figure 10-23) by going to **Capture > Interfaces**. After selecting your interfaces, click **Start** to start capturing, as shown in Figure 10-24. You can also get to the interface list by clicking **Interface List** on the Wireshark home screen.
3. To examine the packets, stop the simulation by clicking **Capture > Stop**. Remember that there must be some activity on your network for packets to be transferred. You might see little traffic activity if your network is in the lab and there is limited network activity. You can always use the **ping** command to generate some network data activity, if needed.

To open a saved capture file, click **File > Open** or click **Open** on the Wireshark home screen.

To change capture options, click **Capture > Options** and change the options to your preferred settings.

FIGURE I-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 (see Figure I-4).

Key terms are highlighted in the text and defined in the margin

Extended Service Set (ESS)
A network with multiple access points to extend user mobility

Hand-off
The process in which a user's computer establishes an association with another access point

Roaming
The term used to describe a user's ability to maintain network connectivity while moving through the workplace

CSMA/CA
Carrier sense multiple access with collision avoidance

The users (clients) in the wireless LAN can communicate with other members of the network as long as a link is established with the access point. For example, data traffic from PC-A to PC-E first passes through the access point and then to PC-E in the wired LAN.

The problem with a basic service set is that mobile users can travel outside the radio range of a station's wireless link if there is only one access point. One solution is to add multiple access points to the network. Multiple access points extend the range of mobility of a wireless client in the LAN. This arrangement is called an **extended service set (ESS)**. In the example of an ESS in Figure 4-3, the mobile computer establishes an authorized connection with the access point that has the strongest signal level (for example, AP-1). As the user moves, the strength of the signal from AP-1 decreases. At some point, the signal strength from AP-2 exceeds that from AP-1, and the wireless bridge establishes a new connection with AP-2. This is called a **hand-off**. The hand-off is an automatic process for the wireless client adapter in 802.11, and the term used to describe this is **roaming**.

Network access in 802.11 uses a technique called carrier sense multiple access with collision avoidance (CSMA/CA). In **CSMA/CA**, the client station listens for other users of the wireless network. If the channel is quiet (that is, no data transmission is occurring), the client station can transmit. If the channel is busy, the station(s) must wait until transmission stops. Each client station uses a unique random back-off time. This technique prevents client stations from trying to gain access to the wireless channel as soon as it becomes quiet. Currently four physical layer technologies are being used in 802.11 wireless networking: direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), infrared, and orthogonal frequency-division multiplexing (OFDM). DSSS is used in 802.11b/g/n wireless networks, and OFDM is used in 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax.

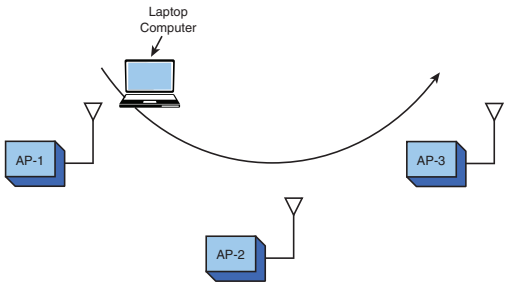


FIGURE 4-3 An example of an extended service set used for increased user mobility.

FIGURE I-4

- A *Summary, Questions and Problems, Critical Thinking*, and *Certification Questions* are provided at the end of each chapter, as shown in Figure I-5

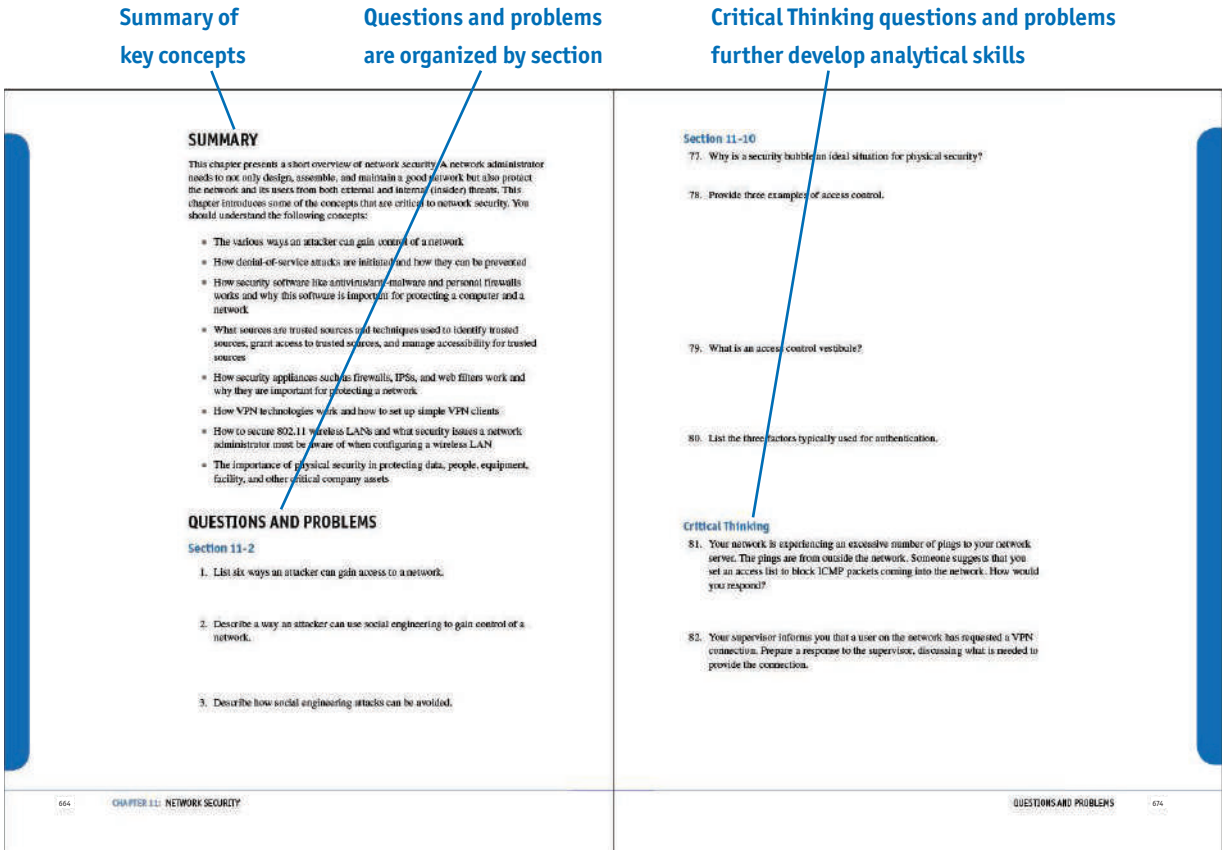


FIGURE I-5

- An extensive *Glossary* at the end of the book offers quick, accessible definitions to key terms and acronyms, and this book also includes an exhaustive *Index* (see Figure I-6).

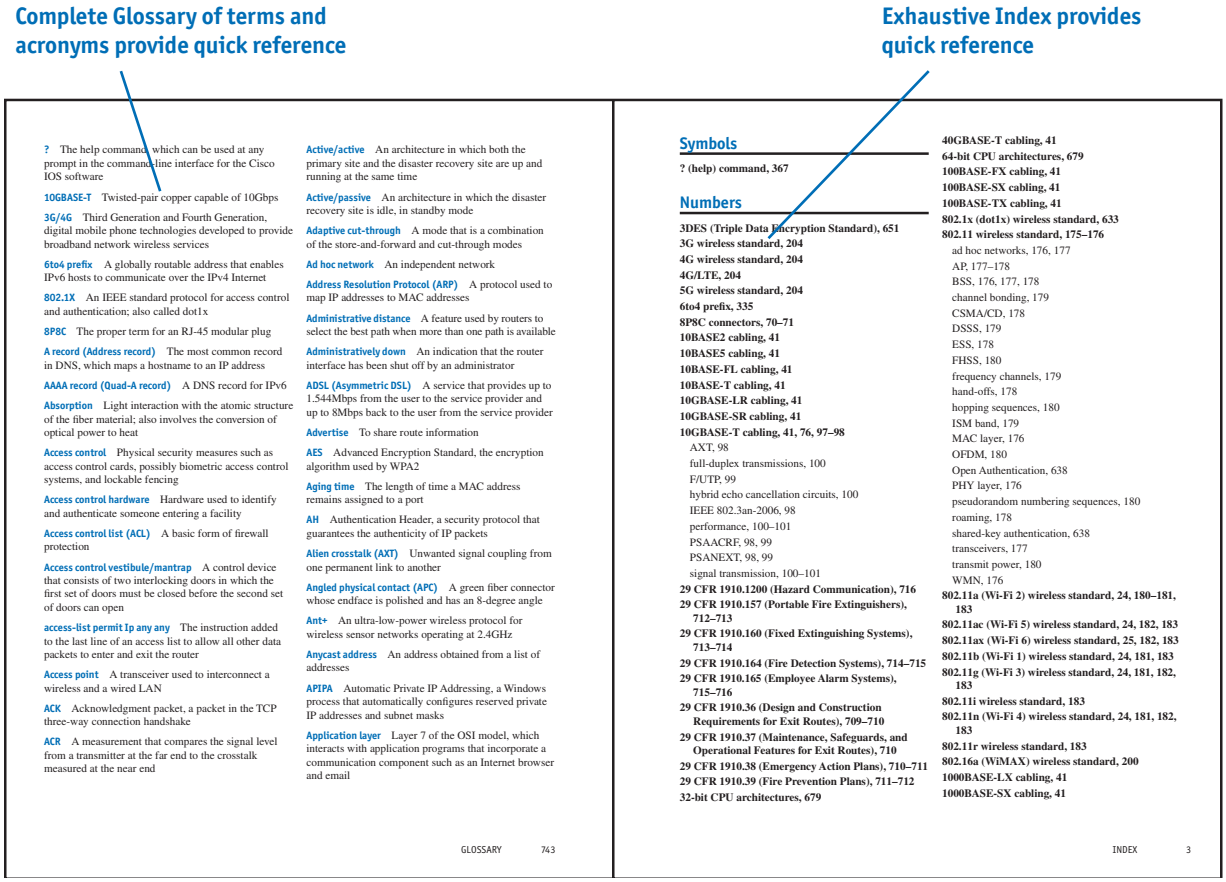


FIGURE I-6

Companion Website

The companion website includes the captured data packets used throughout the book. It also includes the NetChallenge software, which was developed specifically for this text. The companion website also includes chapter-based quiz modules for you to test your knowledge and all of the key terms in an online flash card application. Finally, you can access your 10% off Network+ exam voucher from the companion website.

CHAPTER 1

Introduction to Computer Networks

Chapter Outline

1-1 Introduction
1-2 Network Topologies
1-3 The OSI Model
1-4 The Ethernet LAN
1-5 Home Networking
1-6 Assembling an Office LAN
1-7 Testing and Troubleshooting a LAN
Summary
Questions and Problems

Objectives

- Explain the various LAN topologies
- Define the function of a networking protocol
- Describe CSMA/CD for the Ethernet protocol
- Describe the structure of an Ethernet frame
- Define the function of a network interface card
- Describe the purpose of a MAC address on a networking device
- Discuss how to determine the MAC address for a computer
- Discuss the fundamentals of IP addressing
- Discuss the issues involved in configuring a home network
- Discuss the issues involved in assembling an office LAN

Key Terms

local area network (LAN)
protocol
topology
Token Ring network
Token passing
IEEE
deterministic
Token Ring hub
bus topology
star topology
hub
multiport repeater
broadcast
switch
port
mesh topology
OSI model
physical layer
data link layer
network layer
transport layer
session layer
presentation layer
application layer
CSMA/CD
frame
network interface card (NIC)
MAC address
organizationally unique identifier (OUI)
Ethernet address, physical address, hardware address, or adapter address
ipconfig /all
IANA
IP address
network number
host number
host address
ISP
private addresses
intranet
IP internetwork
TCP/IP
wired network
wireless network
Wi-Fi Alliance
wireless router
range extender
hotspot
service set identifier (SSID)
firewall protection
stateful packet inspection (SPI)
virtual private network (VPN)
network address translation (NAT)

Key Terms continued

overloading
port address translation (PAT)
port forwarding (or port mapping)
CAT6 (Category 6)
RJ-45
Mbps
numerics
crossover
straight-through
uplink port
link light
link integrity test
link pulses
client
peer
peer-to-peer network
client/server network
ping
ICMP
ipconfig

1-1 INTRODUCTION

Each day, computer users use their computers for browsing the Internet, sending and retrieving email, scheduling meetings, sharing files, preparing reports, exchanging images, downloading music, and checking the current prices of auction items. A network connects computers with the goal of sharing their resources. The networks around the world that are connected together form the Internet. Networking requires that computers be able to access multiple networks and share their resources. This chapter looks at the various types of computer networks that are in use today.

This book introduces the essentials involved in implementing modern computer networks, stepping you through the various modern networking technologies. The accompanying textbook web link takes you to the Net-Challenge simulator software developed specifically for this text. This software gives you invaluable insight into the inner workings of computer networking and the experience of configuring routers and switches for use in computer networks.

The ease of connecting to the Internet and the dramatic decrease in the cost of computer systems have led to an explosion in the use of computer systems. Organizations such as corporations, colleges, and government agencies have acquired large numbers of single-user computer systems. Such systems might be dedicated to word processing, scientific computation, or process control, or they might be general-purpose computers that perform many tasks. Interconnection of locally distributed computer networks enables users to exchange information (data) with other network members. It also makes possible resource sharing, enabling many to access expensive equipment such as file servers and high-quality graphics printers as well as more powerful computers for tasks too complicated for the local computer to process.

The networks in use today can be generally categorized based on their geographic span:

- **Personal area network (PAN):** A PAN is the smallest type of network and has a limited span, interconnecting personal devices such as those that are Bluetooth enabled.

- **Local area network (LAN):** A LAN is a network commonly used to interconnect and share computer resources inside a building or multiple buildings in a limited area.
- **Campus area network (CAN):** A CAN—often called simple an *enterprise network*—spans multiple buildings in a campus environment such as a university or another large organization.
- **Metropolitan area network (MAN):** A MAN spans multiple buildings in a city area.
- **Wide area network (WAN):** A WAN is much larger than the other network types and can span many areas, such as cities, states, or countries.

Local Area Network (LAN)
A network of users that share computer resources in a limited area

Table 1-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 1-1 **Chapter 1 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section(s) Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.1	Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.	1-3, 1-4
1.2	Explain the characteristics of network topologies and network types.	1-2, 1-5, 1-7
1.3	Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	1-6
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes.	1-4, 1-5
1.5	Explain common ports and protocols, their application, and encrypted alternatives.	1-3, 1-7
1.6	Explain the use and purpose of network services.	1-5, 1-7
1.7	Explain basic corporate and datacenter network architecture.	1-3
1.8	Summarize cloud concepts and connectivity options	1-4, 1-5, 1-6
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	1-2, 1-4, 1-5, 1-6
2.2	Compare and contrast routing technologies and bandwidth management concepts.	1-5

Domain/Objective Number	Domain/Objective Description	Section(s) Where Objective Is Covered
2.3	Given a scenario, configure and deploy common Ethernet switching features.	1-3, 1-4, 1-5, 1-6
2.4	Given a scenario, install and configure the appropriate wireless standards and technologies.	1-5
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	1-3, 1-4, 1-5
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	1-5, 1-6
4.0	**Network Security**	
4.3	Given a scenario, apply network hardening techniques.	1-5
4.5	Explain the importance of physical security.	1-6
5.0	**Network Troubleshooting**	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	1-5, 1-6
5.3	Given a scenario, use the appropriate network software tools and commands.	1-3, 1-4, 1-5, 1-7
5.4	Given a scenario, troubleshoot common wireless connectivity issues.	1-5, 1-6

1-2 NETWORK TOPOLOGIES

This chapter presents the networking topologies commonly used in computer networks today. It is important for students to understand the structure of the star topology. Students should also understand the Token Ring and bus topologies even though they are seldom used today.

Protocol
A set of rules established for users to exchange information

Topology
The architecture of a network

Token Ring Network
A network topology configured in a logical ring that complements the token passing protocol

A LAN is defined in terms of the **protocol** and the **topology** used for accessing the network. The networking protocol is the set of rules established for users to exchange information. The topology is the network architecture used to interconnect the networking equipment. The most common architectures for LANs are the point-to-point, ring, bus, and star/hub-and-spoke architectures, as illustrated in Figure 1-1.

The simplest network topology is a point-to-point architecture, where two computers are connected directly together. In this topology, communication flows only between the two computers. Figure 1-2 shows an example of a LAN configured using the ring topology. This topology is predominantly used by **Token Ring networks**, in which a token (indicated with the letter T in the network diagram) is placed in the data channel and circulates around the ring (hence the

name *Token Ring*). If a user wants to transmit, the computer waits until it has control of the token. This technique, called **token passing**, is based on the IEEE 802.5 Token Ring Network standard. (**IEEE** is the Institute of Electrical and Electronics Engineers.) A Token Ring network is a **deterministic** network, which means each station connected to the network is ensured access for transmission of its messages at regular or fixed time intervals.

Token Passing
A technique in which an electrical token circulates around a network, and control of the token enables the user to gain access to the network

IEEE
Institute of Electrical and Electronics Engineers, one of the major standards-setting bodies for technological development

Deterministic
A type of network in which access to the network is provided at fixed time intervals

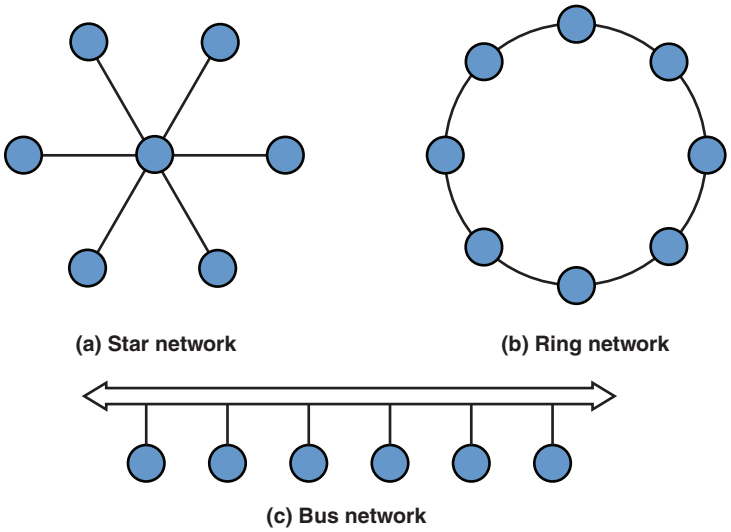


FIGURE 1-1 Network topologies. (From *Modern Electronic Communication* 9/e, by G. M. Miller & J. S. Beasley, © 2008 Pearson Education, Inc. Upper Saddle River, NJ.)

One disadvantage of the Token Ring topology is that if an error changes the token pattern, the token may stop circulating. In addition, ring networks rely on each system to relay the data to the next user. A failed station can cause data traffic to cease. Token Ring networks also have disadvantages in terms of troubleshooting and maintenance. In order to remove a device from a Token Ring network or add a device to the network, the Token Ring path must be temporarily broken (that is, the path must be interrupted). This results in downtime for the network. One way to fix this issue is by attaching all the computers to a central **Token Ring hub**, which is a device that manages the passing of the token rather than relying on individual computers to pass it, thereby improving the reliability of the network.

Token Ring Hub
A hub that manages the passing of the token in a Token Ring network

It is important to note that Token Ring has been replaced by Ethernet technology in almost all modern computer networks.

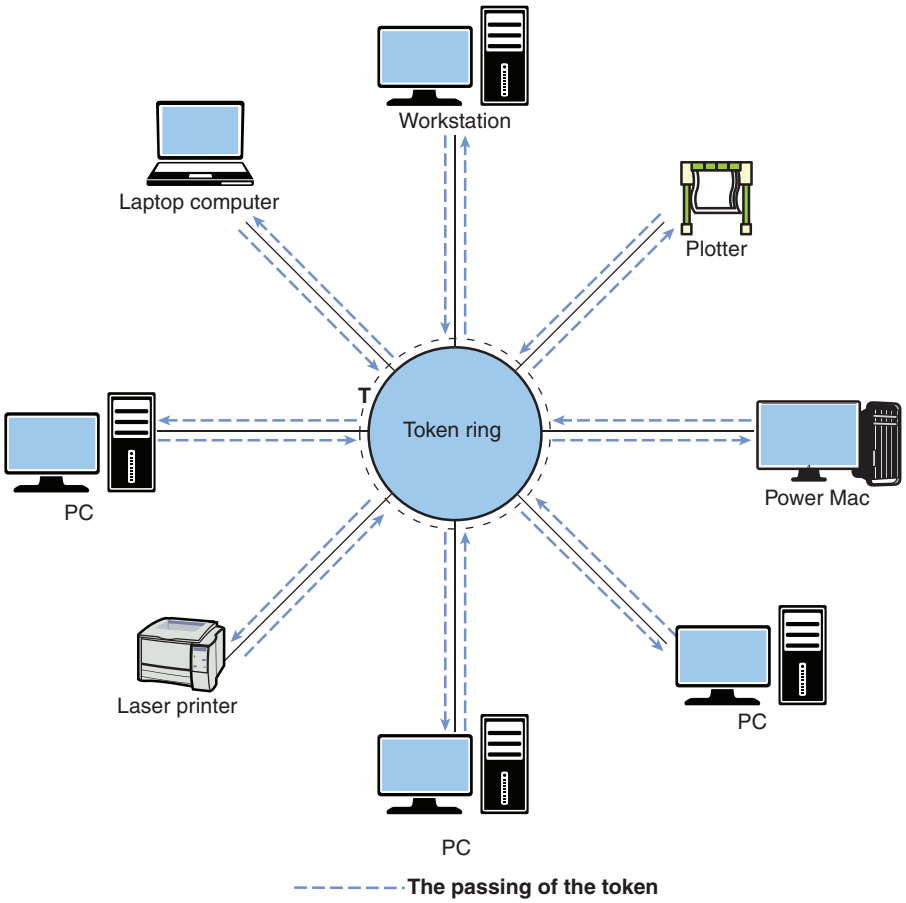


FIGURE 1-2 The Token Ring network topology.

Bus Topology
A system in which the computers share the media (coaxial cable) for data transmission

Figure 1-3 illustrates a **bus topology**, in which the computers share the media (coaxial cable) for data transmission. In this topology, a coaxial cable (called *ThinNet*) is looped through each networking device to facilitate data transfer.

In a bus topology, all LAN data traffic is carried over a common coaxial cable link. In Figure 1-3, for example, if computer 1 is printing a large file, the line of communications is between computer 1 and the printer. However, in a bus system, all networking devices can see computer 1's data traffic to the printer, and the other devices have to wait for pauses in transmission or until transmission is complete before they can initiate their own transmissions. If more than one computer's data is placed on the network at the same time, the data is corrupted and has to be retransmitted. This means that the use of a shared coaxial cable in a bus topology prevents data transmission from being very bandwidth efficient. This is one reason—but not the only reason—bus topologies are seldom used in modern computer networks.

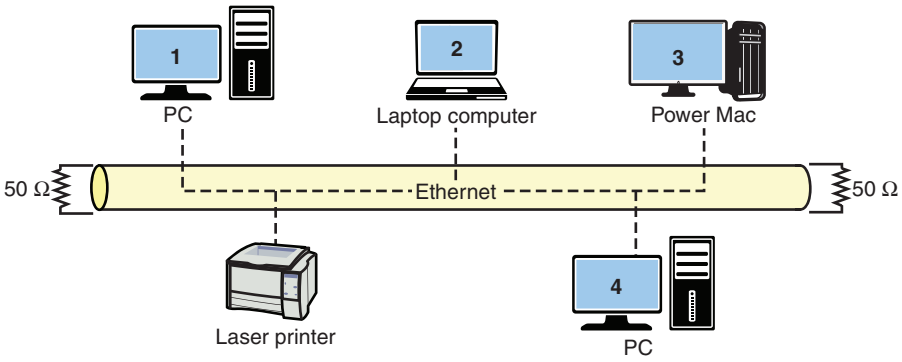


FIGURE 1-3 The bus topology.

The **star topology** (also called hub-and-spoke topology), illustrated in Figure 1-4, is the most common networking topology in today's LANs. Twisted-pair cables with modular plugs are used to connect the computers and other networking devices (see Chapter 2, "Physical Layer Cabling: Twisted-Pair"). At the center of a star network is either a switch or a hub that connects the network devices and facilitates the transfer of data. For example, if computer 1 in Figure 1-4 wants to send data to the network laser printer, the hub or switch provides the network connection. If a hub is used, computer 1's data is sent to the **hub**, which then forwards it to the printer. However, a hub is a **multiport repeater**, which means the data it receives is **broadcast** and seen by all devices connected to its ports. Therefore, the hub broadcasts computer 1's data traffic to all networking devices that are interconnected in the star network. Figure 1-4 shows this data traffic path as solid black arrowed lines going to all networking devices. Much as with the bus topology, all data traffic on the LAN is being seen by all computers. Because a hub broadcasts all data traffic to the devices connected to its network ports, this device is of limited use in a large network.

To minimize unnecessary data traffic and isolate sections of a network, you can use a **switch** at the center of a star network, as shown in Figure 1-4. Each networking device, such as a computer, has a hardware or physical address. (This concept is fully detailed in Section 1-4, "The Ethernet LAN.") A switch stores the hardware or physical address for each device connected to its ports. The storage of the address enables the switch to directly connect two communicating devices without broadcasting the data to all devices connected to its **ports**.

Star Topology
The most common networking topology in today's LANs, where all networking devices connect to a central switch or hub

Hub
A device that broadcasts the data it receives to all devices connected to its ports

Multiport Repeater
Another name for a hub

Broadcast
Transmission of data by a hub to all devices connected to its ports

Switch
A device that forwards a frame it receives directly out the port associated with its destination address

Port
A physical input/output interface to networking hardware

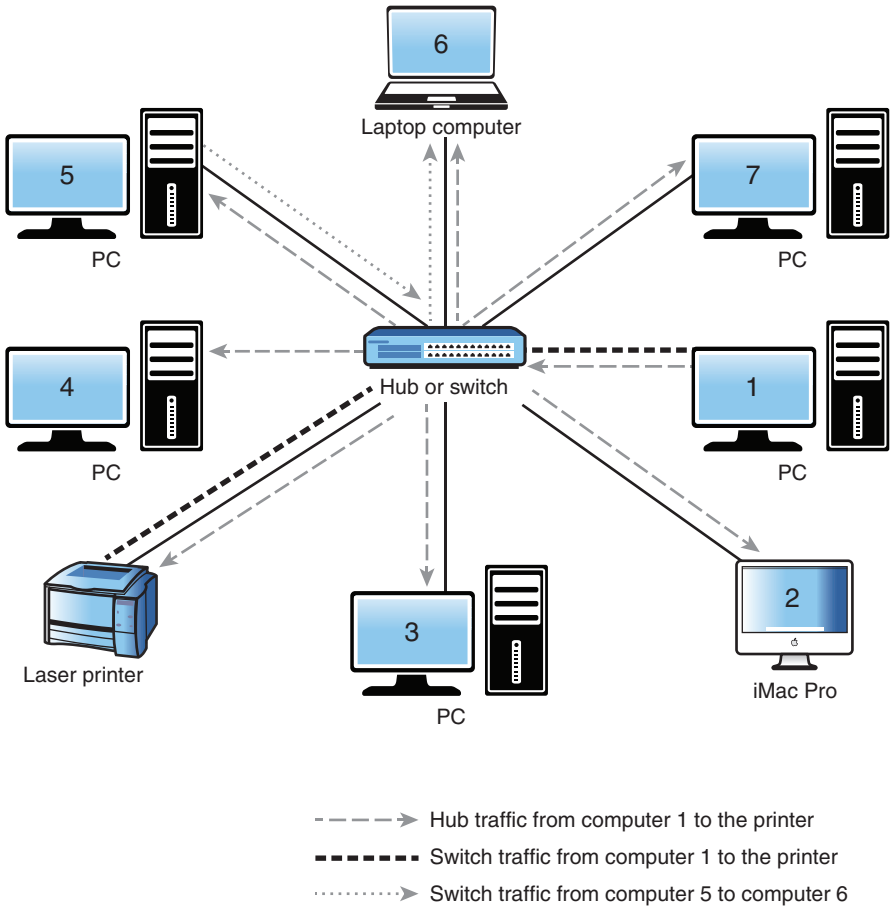


FIGURE 1-4 The star topology.

For example, if a switch is used instead of a hub, the data from computer 1 is transmitted directly to the printer, and the other computers do not see the data traffic. The dotted lines in Figure 1-4 indicate the traffic path for a switched network. The use of a switched connection greatly improves the efficiency of the available bandwidth. It also permits additional devices in the LAN to simultaneously communicate with each other without tying up network resources. For example, while computer 1 is printing a large file, computers 5 and 6 can communicate with each other, as illustrated by the dashed line in Figure 1-4. During troubleshooting and maintenance, individual computers can be removed without negatively affecting the network in a star or extended star topology. Also, the upgrade from a hub to a switched topology can be accomplished without requiring a change in the cable infrastructure and therefore requires minimal downtime and expense.

Mesh Topology
A topology in which all networking devices are directly connected to each other

In a **mesh topology**, as illustrated in Figure 1-5, all networking devices are directly connected to each other. This provides for full redundancy in the network data paths—but at a cost. The additional data paths increase the costs related to cabling and networking hardware (for example, multiple network ports for each device connected to the network). In addition, the mesh design adds complexity. This topology can be suitable for high-reliability applications but can be too costly for general networking applications.

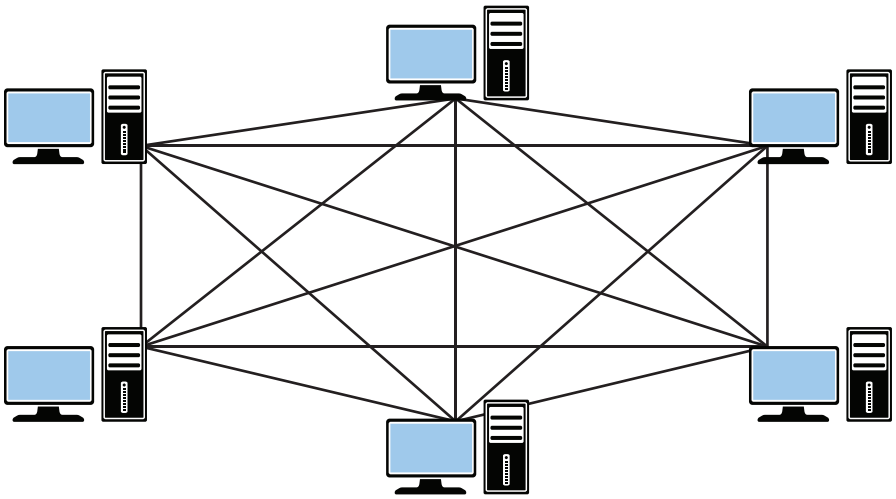


FIGURE 1-5 The mesh topology.

Section 1-2 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.
This section presents the star, ring, bus, and mesh network topologies. You should be able to identify each topology and understand how data travels in each network topology. You should also have a basic understanding of the difference between a topology and a protocol.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
This section introduces some basic networking hardware, such as the hub and switch. Make sure you have a basic understanding of each device. You should also understand that data from a hub is replicated out all ports, which means the information is seen by all networking devices connected to its ports.

Test Your Knowledge

1. What is the most common network topology today?
   a. Star
   b. Hub
   c. Ring
   d. Mesh
2. True or false: A hub is also called a multiport repeater.
   a. True
   b. False

3. In a *deterministic* network, access to the network is provided ____.

   a. at random time intervals

   b. using CSMA/CD

   c. at fixed time intervals

   d. None of these answers are correct.

4. True or false: A protocol defines the network architecture used to interconnect the networking equipment.

   a. True

   b. False

1-3 THE OSI MODEL

This section examines the seven layers of the OSI model. Students should memorize all seven layers and know the function of each layer. Students should refer to Table 1-2 for a summary of the OSI model layers and their functions.

OSI
Open Systems Interconnection

OSI Model
Open Systems Interconnection model, a seven-layer model that describes network functions

The Open Systems Interconnection (**OSI**) reference model was developed by the International Organization for Standardization in 1984 as an open standard for all communication systems to enable different types of networks to be linked together. As illustrated in Figure 1-6, the OSI model contains seven layers that describe networking functions from the physical network interface to the software application interfaces. Different protocols operate at each layer. Each layer performs data encapsulation by putting its own message format or header onto the data as it is being passed down from layer 7 to layer 1 for transmission. When the data is received by an end device, the inverse process, called decapsulation, occurs. Each corresponding layer reads its layer message format or header and takes it off before passing the data to the upper layers. The intent of the **OSI model** is to provide a framework for networking that ensures compatibility in the network hardware and software and to accelerate the development of new networking technologies. A discussion of the OSI model follows, along with a summary of the seven layers outlined in Table 1-2.

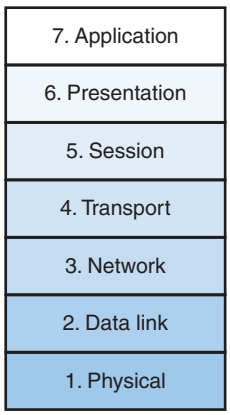


FIGURE 1-6 The seven layers of the OSI reference model.

TABLE 1-2 **Summary of the OSI Layers**

Layer	Function	Examples
7. Application	Provides support for applications	HTTP, FTP, SMTP (email)
6. Presentation	Handles protocol conversion and data translation	ASCII, JPEG
5. Session	Establishes, manages, and terminates sessions	NFS, SQL
4. Transport	Handles end-to-end delivery to ensure error-free packets	TCP, UDP
3. Network	Provides addressing and routing decisions	IP, ICMP
2. Data link	Provides for the flow of data	MAC addresses
1. Physical	Handles signals and media	NICs, twisted-pair cable, fiber, wireless

The OSI model layers are as follows:

1. **Physical layer:** This layer provides electrical and mechanical connection to the network. Examples of technologies working in this layer are Electronic Industries Alliance/Telecommunications Industry Association (EIA/TIA)–related technologies, unshielded twisted-pair (UTP), fiber, and network interface cards (NICs).
2. **Data link layer:** This layer handles error recovery, flow control (synchronization), and sequencing (that is, which terminals are sending and which are receiving). It is considered the media access control (MAC) layer and is where MAC addressing is defined. The Ethernet 802.3 standard relates to this layer, and a MAC address is sometimes called an Ethernet address.
3. **Network layer:** This layer accepts outgoing messages and combines messages or segments into packets, adding a header that includes routing information. It acts as the network controller. An example of a protocol working in this layer is Internet Protocol (IP).
4. **Transport layer:** This layer is responsible for end-to-end delivery between devices. It is concerned with message integrity between source and destination. It also segments/reassembles packets and handles flow control. Examples of protocols working in this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
5. **Session layer:** This layer provides the control functions necessary to establish, manage, and terminate connections, as required, to satisfy user requests. Examples of technologies working in this layer are Network File System (NFS) and Structured Query Language (SQL).
6. **Presentation layer:** This layer accepts and structures messages for an application. It translates the message from one code to another, if necessary. This layer is responsible for data compression and encryption. Examples of

Physical Layer
Layer 1 of the OSI model, which provides the electrical and mechanical connection to the network

Data Link Layer
Layer 2 of the OSI model, which handles error recovery, flow control (synchronization), and sequencing

Network Layer
Layer 3 of the OSI model, which accepts outgoing messages and combines messages or segments into packets, adding a header that includes routing information

Transport Layer
Layer 4 of the OSI model, which is concerned with message integrity between source and destination

Session Layer
Layer 5 of the OSI model, which provides the control functions necessary to establish, manage, and terminate the connections

Presentation Layer
Layer 6 of the OSI model, which accepts and structures the messages for the application

Application Layer
Layer 7 of the OSI model, which interacts with application programs that incorporate a communication component such as an Internet browser and email

technologies working in this layer are American Standard Code for Information Interchange (ASCII) and Joint Photographic Experts Group (JPEG).

7. **Application layer:** This layer interacts with application programs that incorporate a communication component such as an Internet browser and email. This layer is responsible for logging in the message, interpreting the request, and determining what information is needed to support the request. Examples include Hypertext Transfer Protocol (HTTP) for web browsing, File Transfer Protocol (FTP) for transferring files, and Simple Mail Transfer Protocol (SMTP) for email transmission.

Note

Network administrators often refer to layer numbers when describing networking problems. For example, a physical link problem is described as a layer 1 problem, and a router problem is a layer 3 issue.

A network administrator needs to have a good understanding of all seven layers of the OSI model in order to be able to isolate network problems. There are three basic steps in the process of isolating a network problem:

1. Is the connection to the machine down? (This is a layer 1 issue.)
2. Is the network down? (This is a layer 3 issue.)
3. Is a service on a specific machine down? (This is a layer 7 issue.)

A network administrator uses the OSI model to troubleshoot network problems by verifying the functionality of each layer. In many cases, troubleshooting network problems requires the network administrator to isolate at which layer a network problem occurs.

For example, say that a network is having problems accessing an email server that uses SMTP—a layer 7 application. The first troubleshooting step for the network administrator is to ping the IP address of the email server (layer 3 test). A ping to an IP address can be used to quickly check whether there is a network connection. (The **ping** command is discussed in detail in Section 1-7, "Testing and Troubleshooting a LAN.") A "reply from" response for the ping indicates that the connection to the server is up. A "request timed out" response indicates that the network connection is down. This could be due to a cabling problem (layer 1) or a problem with a switch (layer 2) or a router (layer 3), or the email server could be completely down (layer 7). In the event of a "request timed out" response, the network administrator has to go directly to the telecommunications closet or the machine to troubleshoot the problem. In this case, the administrator should first check for layer 1 (physical layer) problems. Many times this just requires verifying that a network cable is connected. Cables sometimes get knocked loose or break.

Section 1-3 Review

This section covers the following Network+ exam objectives.

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

A network administrator needs to have a good understanding of all seven layers of the OSI model in order to be able to isolate a network problem. Remember that there are three basic steps in the process of isolating a network problem:

1. Is the connection to the machine down? (This is a layer 1 issue.)
2. Is the network down? (This is a layer 3 issue.)
3. Is a service on a specific machine down? (This is a layer 7 issue.)

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

A network administrator uses the OSI model to troubleshoot network problems by verifying the functionality of each layer. In many cases, troubleshooting network problems requires a network administrator to isolate at which layer the network problem occurs.

1.7 Explain basic corporate and datacenter network architecture.

A network administrator uses the OSI model to troubleshoot network problems by verifying the functionality of each layer.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section examines the various features of the OSI model that handle flow control.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section examines Layer 1 of the OSI model, which provides the electrical and mechanical connection to the network.

5.3 Given a scenario, use the appropriate network software tools and commands.

*This section introduces the **ping** command, which is a very useful tool for troubleshooting computer networks.*

Test Your Knowledge

1. TCP functions at which layer of the OSI model?
   a. Layer 4
   b. Layer 2
   c. Layer 3
   d. Layer 5
   e. Layer 7

2. HTTP functions at which layer of the OSI model?

    a. Layer 6
    b. Layer 5
    c. Layer 4
    d. Layer 7
    e. All of these answers are correct.

3. IP is an example of a protocol that operates at which layer of the OSI model?

    a. Layer 7
    b. Layer 6
    c. Layer 5
    d. Layer 2
    e. None of these answers are correct.

4. A NIC operates at which layer of the OSI model?

    a. Layer 1
    b. Layer 3
    c. Layer 5
    d. Layer 7
    e. All of these answers are correct.

5. True or false: Network address is another name for a layer 4 address.

    a. True
    b. False

1-4 THE ETHERNET LAN

The key LAN protocol to understand today is Ethernet (CSMA/CD). This section discusses the Token Ring topology and compares deterministic (Token Ring) and nondeterministic (CSMA/CD) networks. Students should be able to use the **ipconfig** command to determine a computer's MAC address. The concept of IP addresses is introduced, and students should understand the concept of Class A–D networks.

CSMA/CD
Carrier-sense multiple access with collision detection, the Ethernet LAN media access method

The networking protocol used in most modern computer networks is Ethernet, a carrier-sense multiple access with collision detection (**CSMA/CD**) protocol for local area networks. It originated in 1972, and the full specification for the protocol was provided in 1980, as a joint effort of Xerox, Digital Equipment Corporation, and Intel. Basically, for a computer to "talk" on an Ethernet network, it first "listens" to see whether there is any data traffic (*carrier-sense*). This means that any computer connected to the LAN can be "listening" for data traffic, and any of the computers

on the LAN can access the network (*multiple access*). There is a chance that two or more computers may attempt to broadcast a message at the same time; therefore, Ethernet systems must have the capability to detect data collisions (*collision detection*).

The information in an Ethernet network is exchanged in a **frame**, which groups the information for a transmission into a header, data, and a trailer. The header consists of the preamble, a start frame delimiter, destination and source addresses, and a length/type field. Next is the actual data being transmitted, followed by the padding used to bring the total number of bytes up to the minimum of 46 if the data field is less than 46 bytes. The last part of the frame is a 4-byte cyclic redundancy check (CRC) value used for error checking. The minimum length of an Ethernet frame is 64 bytes. Figure 1-7 shows the structure of an Ethernet packet frame, and Table 1-3 describes the fields of the Ethernet frame.

Frame
A format that provides grouping of information for transmission

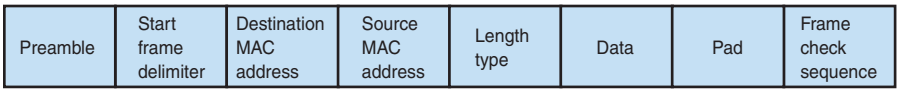


FIGURE 1-7 The data structure for the Ethernet frame. (From *Modern Electronic Communication* 9/e, by G. M. Miller & J. S. Beasley, 2008. Copyright © 2008 Pearson Education, Inc. Upper Saddle River, NJ.)

TABLE 1-3 **Components of the Ethernet Packet Frame (IEEE 802.3 Standard)**

Field	Description
Preamble	An alternating pattern of 1s and 0s that is used for synchronization.
Start frame delimiter	The binary 8-bit sequence 1 0 1 0 1 0 1 1, which indicates the start of the frame.
Destination MAC address and source	The unique media access control address associated with each computer's Ethernet network interface card (NIC) or network adapter.
MAC address	The associated MAC address, which is 6 bytes (12 hex characters) in length.
Length/type	An indication of the number of bytes in the data field if this value is less than 1500. (If this number is greater than 1500, it indicates the type of data format—for example, IP or IPX.)
Data	The variable-length data being transferred from the source to the destination.
Pad	A field used to bring the total number of bytes of the data field up to the minimum of 46 if the data field is less than 46 bytes.
Frame check sequence	A 4-byte CRC value used for error checking. The CRC is performed on the bits from the destination MAC address through pad fields. If an error is detected, the frame is discarded.

Note: The minimum length of an Ethernet frame is 64 bytes from the destination MAC address through the frame check sequence. The maximum Ethernet frame length set by the IEEE 802.3 standard is 1518 bytes: 6 bytes for the destination MAC address, 6 bytes for the source MAC address, 2 bytes for length/type, and 1500 bytes for the data. Ethernet jumbo frames now allow for 9000-byte payload frames with a payload size of 8960 bytes of data.

Source: Adapted from *Modern Electronic Communication* 9/e, by G. M. Miller & J. S. Beasley, 2008. Copyright © 2008 Pearson Education, Inc. Upper Saddle River, NJ.

Network Interface Card (NIC)
The electronic hardware used to interface a computer to a network

How are the destination and source addresses for data determined within a LAN? Each networked device, such as a computer or a network printer, has an electronic hardware interface to the LAN called a **network interface card (NIC)** or an integrated network port. Sometimes more than one NIC is installed on a computer. The NICs are sometimes combined for *NIC teaming*, which involves providing load balancing and fault tolerance (traffic failover). The idea of traffic failover is to keep the computer connected even if there is a failure of the NIC.

MAC Address
A unique 6-byte address assigned by the vendor of a network interface card

Organizationally Unique Identifier (OUI)
The first 3 bytes of the MAC address, which identifies the manufacturer of the network hardware

A NIC contains a unique network address called the **MAC address**. (Recall that MAC stands for media access control.) The MAC address is 6 bytes, or 48 bits, in length. The address is displayed in 12 hexadecimal (base-16) digits. The first 6 digits are used to indicate the vendor of the network interface, also called the **organizationally unique identifier (OUI)**, and the last 6 numbers form a unique value for each NIC assigned by the vendor. IEEE is the worldwide source of registered OUIs. A searchable database of IEEE OUI and company ID assignments is available at http://standards-oui.ieee.org/oui.txt. Large companies may have many OUIs assigned to them. For example, the OUI 00-AA-00 is only one of Intel's many OUIs. Table 1-4 lists a few examples of MAC addresses.

TABLE 1-4 **A Sampling of MAC Addresses**

Company ID-Vendor Serial Number	Manufacturer (Company ID)
00-AA-00-B6-7A-57	Intel Corporation (00-AA-00)
00-00-86-15-9E-7A	Megahertz Corporation (00-00-86)
00-50-73-6C-32-11	Cisco Systems, Inc. (00-50-73)
00-04-76-B6-9D-06	3COM (00-04-76)
00-0A-27-B7-3E-F8	Apple Computer, Inc. (00-0A-27)

Ethernet Address, Physical Address, Hardware Address, or Adapter Address
Other names for the MAC address

ipconfig /all
A command that enables the MAC address information to be displayed from the command prompt

You can find the MAC address, also called the **Ethernet address**, **physical address**, **hardware address**, or **adapter address**, on a computer running Microsoft Windows by typing the **ipconfig /all** command while in the command mode or at the MS-DOS prompt.

In Windows 10, for example, you can search for the command prompt by entering **cmd** in the search field of the Start menu, as shown in Figure 1-8, or by looking under **Start > Windows System**.

At the command prompt, you can enter the **ipconfig /all** command as shown in Figure 1-9. Using the **/all** switch on the command enables the MAC address information to be displayed—in this example, the information for computer 1. Note in this example that the hostname for the computer is COMPUTER-1. This information is typically established when the computer's operating system is installed, but you can change it, as needed. The MAC address is listed under **Ethernet adapter Local Area Connection**, as shown in Figure 1-9. The **Media State: Media disconnected** text indicates that no active Ethernet device, such as a hub or switch, is connected to the computer. **Description** lists the manufacturer and model of the network interface, and the **Physical Address** setting **00-10-A4-13-99-2E** indicates the MAC address for the computer.

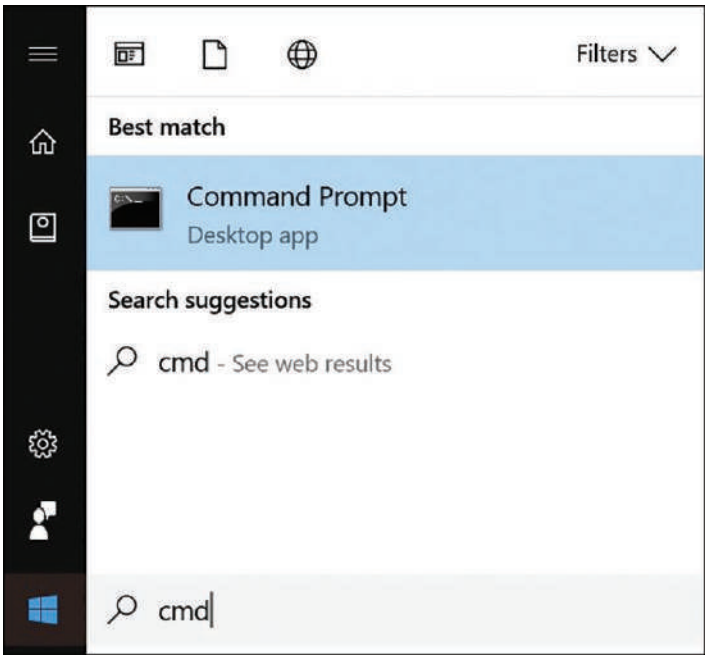


FIGURE 1-8 The command prompt in Windows 10.

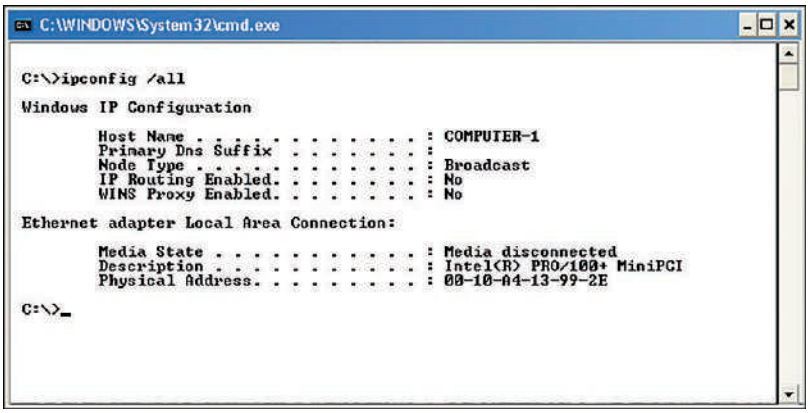


FIGURE 1-9 A typical text screen result when entering the **ipconfig /all** command in the command window.

Table 1-5 describes how to obtain the MAC address in various computer operating systems.

TABLE 1-5 **Commands for Obtaining the MAC Address in Various Operating Systems**

Operating System	Command Sequence	Comments
Windows 10	In Windows 10, enter **cmd** in the search field of the **Start** menu. At the command prompt, type **ipconfig /all** and then press Enter.	The physical address is the MAC address.
Linux	At the command prompt, type **ip addr**.	The HWaddr line contains the MAC address.
macOS	Go to **System Preferences > Network**. Select the network adapter from the left window and click **Advanced > Hardware**.	The hardware address is the MAC address.

In summary, the MAC address provides the information that ultimately enables the data to reach a destination in a LAN. This is also how computer 1 and the printer communicate directly in the star topology example using the switch (refer to Figure 1-4). The switch stores the MAC addresses of all devices connected to its ports and uses that information to forward the data from computer 1 directly to the printer. The switch also uses the MAC address information to forward the data from computer 5 to computer 6 (refer to Figure 1-4).

IP Addressing

IANA
Internet Assigned Numbers Authority, the agency that assigns IP addresses to computer networks

A MAC address provides a physical address for a network interface card but provides no information about its network location or even on what LAN or in which building, city, or country the network resides. Internet Protocol (IP) addressing provides a solution to worldwide addressing by incorporating a unique address that identifies the computer's local network. The Internet Assigned Numbers Authority (**IANA**) is an agency that assigns IP addresses to computer networks and makes sure no two different networks are assigned the same IP network address. The web address for IANA is www.iana.org.

IP Address
A unique 32-bit address that identifies on which network a computer is located and differentiates the computer from all other devices on the same network

IP version 4 (IPv4) is the TCP/IP addressing technique that has been used on the Internet for a number of years. However, the available IPv4 address space has been exhausted due to the rapid growth of the Internet and the development of new Internet-compatible technologies. Version 6 (IPv6) adoption has grown steadily. Both IPv4 and IPv6 are being supported by manufacturers of networking equipment and the latest computer operating systems. Chapter 6, "TCP/IP," provides details on IPv6. Despite the rise in IPv6 addressing, IPv4 addressing is currently the most common method for assigning IP addresses. This text refers to IPv4 addressing as simply "IP addressing." An **IP address** is a 32-bit address that identifies on which network a computer is located and differentiates the computer from all other devices on that network. The address is divided into four 8-bit parts. The format for the IP address is as follows:

A.B.C.D

where the *A.B.C.D* values are written as the decimal equivalent of the 8-bit binary value. The range for each of the decimal values is 0–255. IP addresses can be categorized by class. Table 1-6 provides examples of the classes of IP networks, and Table 1-7 shows the address range for each class.

TABLE 1-6 **The Classes of IPv4 Networks**

Class	Description	Examples of IP Address Numbers	Maximum Number of Hosts
Class A	Governments, very large networks	44.*x*.*x*.*x*	2^{24}=16,777,214
Class B	Midsize companies, universities, and so on	128.123.*x*.*x*	2^{16}=65,534
Class C	Small networks	192.168.1.*x*	2^{8}=254
Class D	Reserved for multicast groups	224.*x*.*x*.*x*	Not applicable
Class E	Reserved for future use and experimentation	240.*x*.*x*.*x*	Not applicable

TABLE 1-7 **The Address Range for Each Class of Network**

Class	Address Range
Class A	0.0.0.0 to 127.255.255.255
Class B	128.0.0.0 to 191.255.255.255
Class C	192.0.0.0 to 223.255.255.255
Class D	224.0.0.0 to 239.255.255.255
Class E	240.0.0.0 to 255.255.255.255

In Table 1-6, the decimal numbers indicate the **network number**, which is the portion of the IP address that defines which network the IP packet is originating from or being delivered to. The *x* entries for each class represent the **host number**, which is the portion of the IP address that defines the address of the networking device connected to the network. The host number is also called the **host address**. The network number provides sufficient information for routing the data to the appropriate destination network. A device on the destination network then uses the remaining information (the *x* portion) to direct the packet to the destination computer or host. The *x* portion of the address is typically assigned by the local network system administrator or is dynamically assigned when users need access outside their local networks. For example, your Internet service provider (**ISP**) may dynamically assign an IP address to your computer when you log on to the Internet. Remember that you can always check the IP address used by or assigned to your computer by using the **ipconfig** command at the command prompt.

The examples in this book use a group of IP addresses called **private addresses**, which are IP addresses set aside for use in private intranets. An **intranet** is an internal internetwork that provides file and resource sharing. Private addresses are not valid addresses for Internet use because they have been reserved for internal use and are not routable on the Internet. However, these addresses can be used within

Network Number
The portion of an IP address that defines which network an IP packet is originating from or being delivered to

Host Number
The portion of an IP address that defines the location of a networking device connected to the network; also called the host address

Host Address
Another term for host number

ISP
Internet service provider, an organization that provides Internet connections and services to individuals and organizations

Private Addresses
IP addresses set aside for use in private intranets

Intranet
An internal network that provides file and resource sharing but that is not accessed from the Internet

IP Internetwork
A network that uses IP addressing for identifying devices connected to the network

TCP/IP
Transmission Control Protocol/Internet Protocol, the protocol suite used for internetworks such as the Internet

a private LAN (intranet) to create an **IP internetwork**. An IP internetwork uses IP addressing to identify devices connected to the network and is also the addressing scheme used in **TCP/IP** networks. TCP/IP stands for Transmission Control Protocol/Internet Protocol and is the protocol suite used for internetworks such as the Internet. The three address blocks for the private IP addresses in this book's examples are as follows:

10.0.0.0–10.255.255.255
172.16.0.0–172.31.255.255
192.168.0.0–192.168.255.255

Notice that the private IP addresses are a reduced subset of the public IP addresses listed in Table 1-7.

The topic of IP addressing is examined in greater detail throughout this book. In this chapter, the objective is to use IP addresses for configuring the addresses of the computers for operation in a TCP/IP network.

Section 1-4 Review

This section covers the following Network+ exam objectives.

1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
This section examines the Ethernet frame and payload.

1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
This section introduces IPv4 and IPv6. It is important to understand the structure of an IPv4 address, including which bits define the network address and which bits are the host bits. Make sure you understand the structure of both a MAC address and an IPv4 address and know how to get this information from many types of computers.

1.8 Summarize cloud concepts and connectivity options.
You should make sure you have an understanding of the concept of private versus public IP addresses.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
This section introduces the concept of NIC teaming, which occurs when more than one NIC is installed on a computer.

2.3 Given a scenario, configure and deploy common Ethernet switching features.
This section introduces CSMA/CD. Make sure you understand how this protocol manages network access from multiple devices.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section examines the CRC check value, which is a 4-byte CRC value used for error detection. The CRC is performed on the bits from the destination MAC address through pad fields. If an error is detected, the frame is discarded.

5.3 Given a scenario, use the appropriate network software tools and commands.

*Remember that you can check the IP address assigned to a computer by using the **ipconfig** command at the command prompt. By issuing the **ipconfig /all** command, you can determine whether the NIC is connected to a network and determine the MAC and IP addresses of a networking device.*

Test Your Knowledge

1. Which of the following statements regarding IP addresses and/or MAC addresses is true?
   a. An IP address is the same as a MAC address.
   b. A MAC address defines a network location.
   c. An IP address is only used as part of an ARP request.
   d. A MAC address provides the physical address of the network interface card, while an IP address provides the network location.
2. True or false: The MAC address on a Windows computer can be accessed by typing **ipconfig /all** at the command prompt.
   a. True
   b. False
3. True or false: The OUI for the MAC address 00-10-A4-13-99-2E is 13992E.
   a. True
   b. False
4. What does NIC stand for?
   a. Network interface card
   b. National integrated communicator
   c. Network integration card
   d. National integration communicator
   e. None of these answers are correct.

1-5 HOME NETWORKING

This section provides an interesting look at networking based on a task with which most students are very familiar: setting up a home network.

Wired Network
A network that uses cables and connectors to establish network connections

Wireless Network
A network that uses radio signals to establish network connections

The process of setting up a home network, as you likely know, can be quite challenging. One of the first issues to determine is whether to set up a wired or wireless home network. A **wired network** uses cabling and connectors to establish network connections. A **wireless network** uses radio signals to establish network connections. A wireless home network is probably the most common home network configuration in use today.

This section covers home networking technologies, and Section 1-6, "Assembling an Office LAN," discusses the setup of wired networks for both office and home networks.

Table 1-8 lists the advantages and disadvantages of wired and wireless networks.

TABLE 1-8 **Wired and Wireless Network Advantages and Disadvantages**

Type of Network	Advantages	Disadvantages
Wired network	Faster network data transfer speeds (within the LAN). Relatively inexpensive setup. Not susceptible to outside interference.	Specialized tools typically required for cable connections. Possibly labor-intensive and expensive cable installation.
Wireless network	User mobility. Simple installation. No cables.	Security issues. Possibly slower data transfer speed than in a wired network.

Wi-Fi Alliance
An organization that tests and certifies wireless equipment for compliance with the 802.11*x* standards

Wireless networks also go by the name Wi-Fi, which stands for *wireless fidelity*. The **Wi-Fi Alliance** is an organization whose function is to test and certify wireless equipment for compliance with the 802.11*x* standards, which is the group of wireless standards developed under IEEE 802.11. These are the most common IEEE wireless standards:

- **802.11a (Wi-Fi 2):** This standard can provide data transfer rates up to 54Mbps and an operating range up to 75 feet. It operates at 5GHz.
- **802.11b (Wi-Fi 1):** This standard can provide data transfer rates up to 11Mbps, with ranges of 100–150 feet. It operates at 2.4GHz.
- **802.11g (Wi-Fi 3):** This standard can provide data transfer rates up to 54Mbps up to 150 feet. It operates at 2.4GHz.
- **802.11n (Wi-Fi 4):** This standard provides data transfer rates up to four times 802.11g speeds (that is, 200Mbps up to 450Mbps). It operates at either 2.4GHz or 5GHz.
- **802.11ac (Wi-Fi 5):** This is the most commonly deployed wireless standard. It provides single-station data transfer rates of 500Mbps up to 1.3Gbps and operates in the 5GHz frequency band.

- **802.11ax (Wi-Fi 6):** This is the latest wireless standard. It was recently ratified, and manufacturers have begun shipping devices with this wireless technology. Theoretically, it could deliver speeds close to 10Gbps.

Figure 1-10 illustrates the placement and type of equipment found in a typical wired or wireless home network. Figure 1-10(a) shows a wired LAN in which cabling interconnects the networking devices and a router is being used to make the connection to the ISP. The router can also contain a switch and a broadband modem. The switch is used to interconnect other networking devices, and the broadband modem is used to make the data connection to the ISP. Its physical ports that interconnect other local network devices may sometimes be labeled as LAN ports, and a physical port that connects to the ISP may be labeled as a WAN port, depending on the manufacturer. The most common broadband connections to the ISP are via a cable modem and DSL. A cable modem connection is sometimes called a cable broadband connection. In some cases the router, switch, and broadband modem are separate devices, but most often they are integrated into one device. One of the computers in a network may also have the configuration settings for managing the router, which can include the settings for connecting to the ISP.

Figure 1-10(b) shows a wireless LAN that is being used to interconnect the networking devices. A **wireless router** makes the data connection to the ISP, which is typically via a cable modem or DSL modem. The wireless router also has a wireless access point and typically has a switch to facilitate wired network connections. Sometimes a broadband modem is integrated into a wireless router. The access point is used to establish the wireless network connection to each of the wireless computers.

Wireless Router
A device used to interconnect wireless networking devices and to give access to wired devices and establish the broadband Internet connection to the ISP

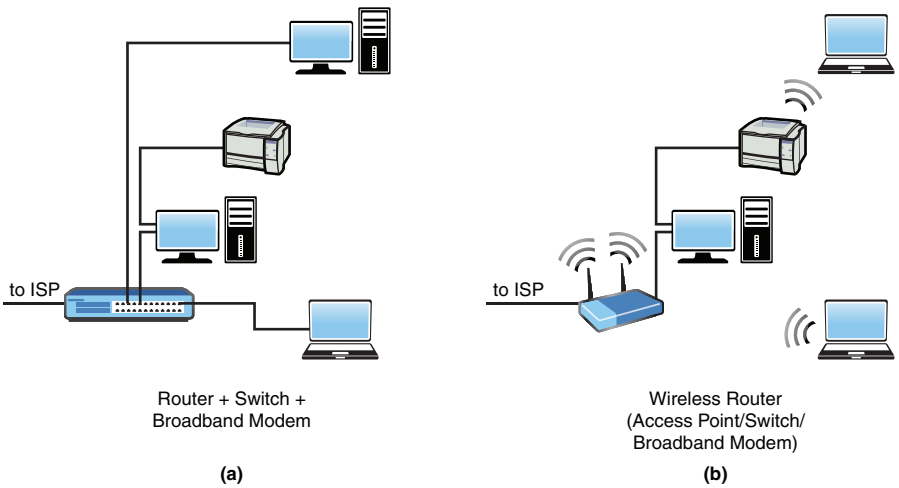


FIGURE 1-10 Examples of (a) wired and (b) wireless Wi-Fi home networks.

A home network can include the following components:

- **Hub:** This type of device is used to interconnect networking devices. A drawback to a hub is that it broadcasts the data it receives to all devices connected to its ports. In most modern networks, hubs have been replaced by network switches.

- **Switch:** This is the best choice for interconnecting networking devices. A switch can establish a direct connection from the sender to the destination without passing the data traffic to other networking devices. Figure 1-11 provides an image of a switch.
- **Network adapter:** Wired and wireless network adapters are available. The type of network adapter used in a desktop computer is a NIC. Figure 1-12 provides an image of a wired network adapter. This type of NIC, which is inserted into an expansion slot on a computer's motherboard, is a wired-only adapter.



FIGURE 1-11 A Cisco 12-port PoE (Power over Ethernet) switch.

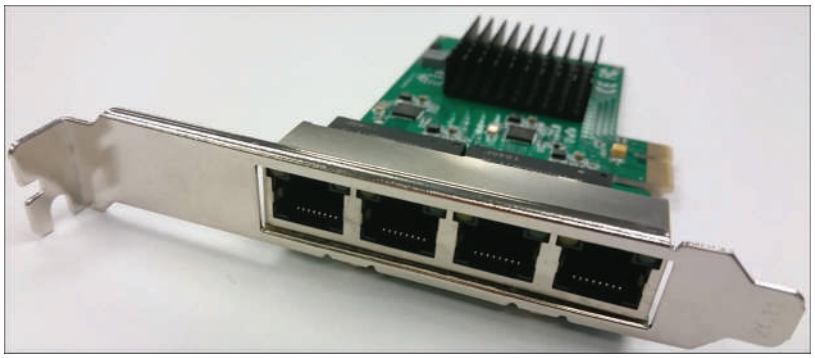


FIGURE 1-12 A four-port PCI Express Gigabit Ethernet card.

Another option for connecting to networks is to use a network adapter that attaches to a USB port on the computer. Such a device has a USB connector (either USB-A or USB-C) on one end and an RJ-45 jack on the other and can support connections up to 1000Mbps (that is, 1Gbps) data networks. Figure 1-13 provides an image of USB and Thunderbolt Ethernet network adapters.

- **Router:** A router is a networking device used to connect two or more networks (for example, a LAN and the Internet) using a single connection to an ISP. As mentioned earlier, a modern home networking router can also contain a switch and a broadband modem. Figure 1-14 provides an image of a router.



FIGURE 1-13 A USB Ethernet adapter and Thunderbolt Ethernet adapter.



FIGURE 1-14 A Netgear wireless router.

- **Access point:** An access point is used to interconnect wireless devices and provide a connection to a wired LAN. The data transfer speeds for access points are dictated by the choice of wireless technology for the clients, but these devices can support up to 802.11ac (or Wireless-ac). Figure 1-15 provides an image of an access point.



FIGURE 1-15 A Linksys 802.11n (Wireless-N) access point.

- **Wireless router:** This device uses RF to connect to the networking devices. A wireless router typically contains a router, switch, and wireless access point and is probably the most common way to interconnect wireless LANs to the ISP's access device. Note that these devices also have wired network connections available on the system. Figure 1-16 provides an image of a wireless router.
- **Broadband modem/gateway:** This type of device is used to provide high-speed data access via your cable connection or via a telephone company's DSL connection. A gateway combines a modem and a router into one network box.
- **Cable modem:** This device is used to make a broadband network connection from your home network to the ISP, using your cable connection. This setup requires a splitter to separate the cable TV from the home network. Access to the Internet is typically provided by the cable TV service provider. Figure 1-17 provides an image of a cable modem.



FIGURE 1-16 A TP-Link wireless router.



FIGURE 1-17 A Surfboard cable modem.

- **DSL modem:** This device is used to make a broadband network connection from your home network to the ISP using the telephone line. Broadband access to the Internet is provided via the phone company or a separate ISP. The

DSL connection requires the placement of filters on all telephone lines except the one going into the modem to prevent interference. Figure 1-18 provides an image of a DSL modem.



FIGURE 1-18 A Zoom DSL wireless router.

Several issues should be considered when planning for a home network, including the following:

- **Data speed:** The data speed is determined by whether you chose to implement a wired or wireless home network. Wired networks offer the best data transfer rate inside the home network, up to 10Gbps. The best data transfer rates for a wireless home network can be obtained using 802.11ax technology. This is the latest generation of high-speed wireless connectivity, providing single-station data transfer rates of 3Gbps.
- **Cost:** Implementing a high-speed wired network can be quite expensive. With the networking hardware, cabling, and related hardware, you can incur unexpected additional costs in implementing a high-speed wired home network. The cost of switching to or implementing a Wireless-ac network is minimal, and such a network is a suitable alternative to a wired network. But remember that the maximum data rate in a Wireless-ac network is still much lower than the possible maximum data rate in a wired LAN.

- **Ease of implementation:** A wireless home network is probably the easiest to implement if the cabling and connectors for a wired network are not already installed. The time required to install a wireless home network is usually minimal as long as unexpected problems do not surface.
- **Appearance:** A wireless home network is the best choice in regard to appearance because cables and networking hardware do not need to be scattered around the house. A wireless home network requires a wireless router and an external wired connection to the ISP (refer to Figure 1-10(b)).
- **Home access:** The choice of wired or wireless technology does not affect home access. However, while a wired network offers the best data transfer speed internal to the network, a wireless network offers the best choice for mobility.
- **Public access:** The choice of wired or wireless technology does not impact public access. The data rate for the connection to/from the ISP is the limiting factor for the data transfer rate for public access.

It is not uncommon for a wired or wireless home network to stop functioning, although the downtime is usually minimal. The steps for troubleshooting wired and wireless home networks include the following:

1. Check the networking device that connects your network to your ISP to ensure that the proper lights are displayed. Incorrect lights can indicate a connection problem with your cable modem, DSL modem, or telephone connection. Your ISP might also be having a problem, and you might need to call the ISP to verify your connection.
2. Reboot the host computer (the computer connected to the router) and reboot the router. This usually fixes the problem, and the correct lights should be displayed. In some cases, you might also have to power down your broadband modem and then power it up again. (Remember that the broadband modem might be integrated with the router.) Once again, check to see whether the correct lights are being displayed.
3. Verify that your hardware cable or phone connection is in place and has not been pulled loose. Make corrections as needed. You should also verify that all wireless units have network connections. Use the following steps to verify wireless connectivity for Windows 10 or macOS:
    - **Windows 10:** Go to **Control Panel > Network and Sharing Center**. The wireless connection appears as enabled if there is a wireless connection.
    - **macOS:** Go to **System Preferences > Network**. Select the network adapter from the left window and click **Advanced > Hardware**. Look for the following indicators:
        - If you are connected, the Wi-Fi status displays **Connected** with a green indicator.

- If the wireless Wi-Fi is on but is not connected to a network, the Wi-Fi status displays **On** with an amber indicator.
- If the Wi-Fi is off, the Wi-Fi status displays **Off** with a red indicator.

Also note that if you are connected to a wireless network, a radio wave icon appears at the top of the screen in the menu bar to indicate that you are connected to a wireless network.

4. Verify your network settings. You may need to do this if your computer has lost the data for the settings. In such a case, follow the steps provided by the manufacturer of your broadband modem or your ISP.

The following are the basic steps for establishing a wireless connection for a wireless notebook computer running Windows 10 or macOS:

- **Windows 10:** Go to **Control Panel > Network and Sharing Center > Set Up a New Connection or Network**. You need to choose the **Connect to the Internet** option and then select **Wireless** to establish a wireless connection.
- **macOS:** Go to **System Preferences > Network**. Select the network adapter from the left window, select the **Wi-Fi** connection, and then click **Turn Wi-Fi On**. The available wireless networks appear under the **Network Name** drop-down menu. Select a desired wireless network and enter the WEP/WPA/WPA2/WPA3 password when prompted. If you are connected, a radio wave should appear at the top of the screen in the menu bar, indicating that the network is connected.

There are many choices of wireless technologies for configuring a wireless network. The 802.11b, g, n, ac, and ax technologies are compatible with one another even though they offer different data speeds. If compatible but different wireless technologies are being used, the data transfer speeds are negotiated at the rate specified by the slowest technology. For example, the 802.11n (that is, Wireless-N) standard offers a faster data rate than 802.11g (that is, Wireless-G), but when devices of both technologies are present, the data transfer rate is negotiated at the Wireless-G data rate.

Range Extender
A device that relays the wireless signal from an access point or wireless router into areas with a weak signal or no signal at all

Hotspot
A limited geographic area that provides wireless access for the public

In some cases, the wireless signal might not be reaching all the areas that need coverage. In such a case, you can use a device called a wireless **range extender**. This device relays the wireless signals from an access point or wireless router into areas with a weak signal or no signal at all. This improves the wireless remote access from all points in the home. This same technology can also be used to improve connectivity in stores and warehouses and can also be used to provide excellent connectivity in public places such as hotspots. A **hotspot** is a limited geographic area that provides wireless access for the public. A captive portal is a web page that the user of a public access network is obliged to view and interact with before being granted network access. Captive portals are typically used in business centers, airports, hotel lobbies, coffee shops, libraries, schools, and other venues that offer free Wi-Fi hotspots for Internet users.

Securing a Home Network

Many potential security issues are associated with wireless networks. Securing a wireless home network is extremely important because if a wireless signal is intercepted by the wrong person, that person can possibly connect to the network. The following are some basic measures you can take to help protect a home network:

- **Change the default factory passwords.** Home network equipment often ships with default passwords that are set at the factory. These default settings are known by the public, including people who would like to gain access to your network and possibly change your settings. It is best to select your own password that is a combination of alphanumeric characters.
- **Enable MAC address filtering (MAC filtering).** Every computer device has a unique MAC address that identifies the device. This address can be used to select which devices can be allowed access to the network. When MAC address filtering (MAC filtering) is turned on, only wireless devices that have specific MAC addresses are allowed access to the network.
- **Change the default SSID.** The **service set identifier (SSID)** is the name used to identify your network that is used by your access point or wireless router to establish an association. Establishing an association means that a wireless client can join the network. The SSID can be up to 32 characters and should be changed often so hackers who have figured out your SSID no longer have access to your home network.
- **Turn on encryption.** It is important to turn on security features such as data encryption. These options include Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and WPA3. WPA2 is a product certification issued by the Wi-Fi Alliance that uses a stronger encryption than WPA and is also backward compatible with adapters using WPA. WPA3, which is the latest Wi-Fi security standard, is interoperable with WPA2 devices. Wi-Fi Protected Setup (WPS) simplifies the configuration process, enabling the user to set up a WPA pre-shared key (PSK) without having to enter a long string of symbols, random numbers, or letters. Although WPS helps protect wireless networks, it is susceptible to brute-force attacks.
- **Turn off the SSID broadcast.** Wireless systems broadcast the SSID so that a network can be easily identified as an available network. Hackers can use this information to possibly gain access to a network, so you should turn off the SSID broadcast. The exception to this is in hotspots where public access is available. Note that hotspots make it easy for the user to gain wireless access, but hackers can also be on the same network, so it is important to have encryption turned on.

Service Set Identifier (SSID)
A name that is used to identify your wireless network and is used by your access point or wireless router to establish an association

Another important security concern is limiting outside access to your home network via your connection to the ISP. The following are some things you can do to protect a home network from outside threats:

- **Network address translation (NAT):** With NAT, an outsider sees only the router's ISP-assigned IP address, and the IP addresses of the internal networking devices are not provided on the Internet. A home network typically uses a private address that is not routable on the Internet. (Private IP addresses are blocked by the ISP.)
- **Firewall protection:** A common practice is to turn on **firewall protection**. The purpose of a firewall is to prevent unauthorized access to a network. Firewall protection is available in both the Windows and macOS operating environments. A type of firewall protection is **stateful packet inspection (SPI)**. This type of protection involves inspecting incoming data packets to make sure they correspond to an outgoing request. For example, if you are exchanging information with a website, data packets that are not requested may be rejected. Firewalls are covered in more detail in Chapter 11, "Network Security."
- **VPN connections for transferring sensitive information:** A **virtual private network (VPN)** establishes a secure network connection and helps protect a LAN's data from being observed by outsiders. The VPN connection capability is available with Windows 10 and macOS. A VPN connection enables a remote or mobile user to access the network as if he or she were actually physically at the network. In addition, the VPN connection is encrypted, providing privacy for the data packets being transmitted.

Firewall Protection
A type of protection used to prevent unauthorized access to a network

Stateful Packet Inspection (SPI)
A type of firewall that inspects incoming data packets to make sure they correspond to an outgoing request

Virtual Private Network (VPN)
A secure network connection that helps protect a LAN's data from being observed by outsiders

IP Addressing in a Home Network

How is IP addressing handled for all the computers connected to the Internet? A home network typically has only one connection to the ISP, but multiple computers can be connected to the Internet at the same time. IP addressing for a home network is managed by the router or wireless router that connects to the ISP. (Figure 1-19 provides an example of a wireless router that connects to an ISP.)

The ISP issues an IP address to the router from an available pool of IP addresses managed by the ISP. The computers in the home network are issued private IP addresses via a DHCP program on the home router (applicable ranges are 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, and 192.168.0.0–192.168.255.255). These private IP addresses are translated into the ISP's assigned IP address using **network address translation (NAT)**.

The routable public IP address that the ISP issues for the wireless router enables all computers in the home network to access the Internet. The wireless router issues private addresses to all computers connected to the network.

Network Address Translation (NAT)
A technique that involves translating a private IP address to a public address for routing over the Internet



FIGURE 1-19 A home network using a wireless router connected to the ISP.

You can use NAT to translate a private IP address to a public address for routing over the Internet. For example, computer 1 in the home network shown in Figure 1-20 might establish a connection to an Internet website. The wireless router uses NAT to translate computer 1's private IP address (192.168.0.64) to the public IP address (128.123.246.55) assigned to the router. The router uses a technique called **overloading**, in which NAT translates the home network's private IP addresses to the single public IP address assigned by the ISP. In addition, the NAT process tracks a port number for the connection; this technique is called **port address translation (PAT)**. The router stores the home network's IP address and port number in a NAT lookup table. The port number differentiates the computer that is establishing a connection to the Internet because the router uses the same address for all computers. This port number is used when a data packet is returned to the home network. The port number identifies the computer that established the Internet connection, and the router can deliver the data packet to the correct computer. Another application of NAT is **port forwarding** (also called **port mapping**), in which packets from one IP address/port number are redirected to another. This process is often used to make services on one part of a network available to hosts on the opposite side of the network.

For example, if computer 1 in Figure 1-20 establishes a connection to a website on the Internet, the data packets from the website are sent back to computer 1 using the home network's routable public IP address. First, the network enables the data packet to be routed back to the home network. Next, the router uses the

Overloading
A process that involves translating a home network's private IP addresses to a single public IP address

Port Address Translation (PAT)
A technique that involves tracking a port number with the client computer's private address when translating to a public address

Port Forwarding (or Port Mapping)
An application of NAT in which packets from one IP address/port number are redirected to another

NAT lookup table and port number to translate the destination for the data packet back to the computer 1 private IP address and original port number, which might be different.

Figure 1-20 shows an example of the NAT process for a home network. The home network has been assigned Class C private IP addresses (192.168.0.*x*) by the router. The *x* is a unique number (from 1 to 254) assigned to each computer. The router translates the private IP addresses to the public routable IP address assigned by the ISP. In addition, the router tracks a port number with the public IP address to identify the computer. For example, the computer with the private IP address 192.168.0.64 is assigned the public IP address 128.123.246.55:1962, where 1962 is the port number tracked by the router.

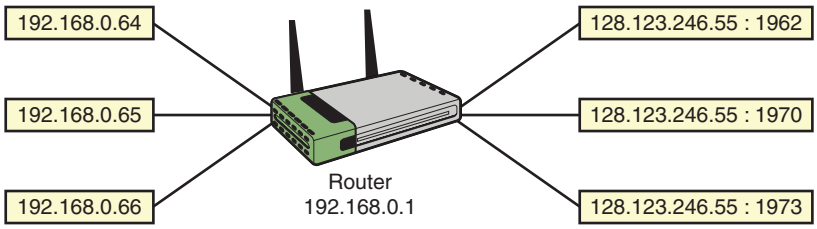


FIGURE 1-20 NAT using PAT.

Section 1-5 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.
The most common broadband connections to an ISP are via cable modem and DSL. In some cases, the router, switch, and broadband modem are separate devices, but most often they are integrated into one device.

1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
This section presents an overview of both NAT (network address translation) and PAT (port address translation). It also presents the concept of port forwarding.

1.6 Explain the use and purpose of network services.
*An important step in verifying connectivity between two networking devices is to issue the **ping** command, using the destination IP address for the other device. The **ping** command is available from the command prompt in Windows. Make sure you know how to issue the command and the options available with the command, such as implementing continuous pinging and setting the buffer size.*

1.8 Summarize cloud concepts and connectivity options.
This section introduces the concept of a VPN, which is a secure network connection that helps protect a LAN's data from being observed by outsiders.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

A cable modem is used to make a broadband network (also called cable broadband) connection from a home network to an ISP by using a cable connection.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

This section introduces NAT, which translates a private IP address to a public address for routing over the Internet.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section shows a Power over Ethernet switch.

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

This section discusses the various wireless standards available today. There are many choices of wireless technologies for configuring a wireless network. It is very important that you understand the advantages and limitations of each wireless standard.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section examines the various data transfer speeds for wireless networks.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section discusses hubs, switches, wireless access points, and range extenders. Make sure you understand the purpose of each.

4.3 Given a scenario, apply network hardening techniques

This section introduces MAC address filtering. When MAC address filtering is turned on, only wireless devices that have specific MAC addresses are allowed to access the network.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section discusses the various wireless standards available today. There are many choices of wireless technologies for configuring a wireless network. It is very important that you understand the advantages and limitations of each wireless standard.

5.3 Given a scenario, use the appropriate network software tools and commands.

*After you have verified that networking devices are physically connected, you can use the **ping** command to verify that the networking devices are communicating.*

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

A captive portal is a web page that the user of a public access network is obliged to view and interact with before being granted network access.

Test Your Knowledge

1. Which of the following issues should be considered when planning for a home network?
    a. Data speed
    b. Public access
    c. Cost
    d. All of these answers are correct.
2. How does MAC address filtering help to secure a wireless network?
    a. It helps prevent the theft of network interface cards.
    b. It requires an additional login step in which the user enters a MAC address.
    c. MAC address filtering is seldom used anymore because of NIC restrictions.
    d. It can be used to select which networking devices can be allowed access to the network.
3. Which of the following is an example of a wireless technology?
    a. 802.11a
    b. 802.11g
    c. 802.11n
    d. All of these answers are correct.
4. What does NAT stand for?
    a. Network asynchronous transfer
    b. Network address translation
    c. Network address transfer
    d. None of these answers are correct.

1-6 ASSEMBLING AN OFFICE LAN

This section guides students through the process of assembling, configuring, and testing a simple office LAN. It helps students understand basic networking concepts prior to bringing more complex networking hardware and architectures into the picture. The concept of twisted-pair cable is introduced in this section and fully explored in Chapter 2. This section also covers many of the networking numerics used in computer networking, such as CAT6, RJ-45, and Mbps (megabits per second). Students should understand the purpose of the link light and, if possible, check the link light regularly. This section also discusses how to configure a computer's IP address and provides an example.

This section presents an example of assembling an office-type LAN. In this example, the Ethernet protocol is used for managing the exchange of data in the

network, and the networking devices are interconnected in a star (also called hub-and-spoke) topology. There are many options for assembling and configuring a LAN; this example presents a networking approach that is simple and consistent with modern computer networking. It also provides a good introduction to the networking topics presented throughout this book.

For this example, three computers and one printer are configured in a star topology. Each device in the network should be assigned an IP address from the private address space. The following steps guide you through the process of assembling, configuring, and testing an office LAN:

Diagram the Network

The first step in assembling an office-type LAN is to document the devices to be connected in the network and prepare a simple sketch of the proposed network. Each device's MAC and IP addresses should be included in the network drawing documentation.

Figure 1-21 provides an example of a small office LAN. It lists the desired IP addresses and the actual MAC addresses for each computer and printer. Remember that each NIC has a unique MAC address, and IP addresses are locally assigned by the network administrator. You can view the MAC addresses by entering the **ipconfig /all** command at the command prompt in Windows 10 (see Table 1-9). Repeat this step for all computing devices connected to the LAN. Each networking device should be assigned an IP address, and Table 1-9 also lists the IP addresses planned for the devices in this office LAN.

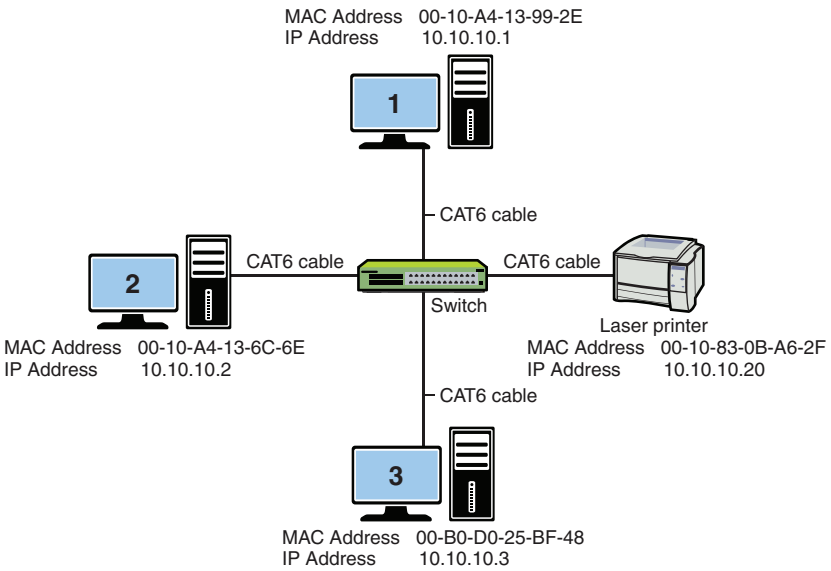


FIGURE 1-21 An example of a LAN star topology for a small office network.

TABLE 1-9 **The MAC Addresses and Assigned IP Addresses for the Devices in an Office LAN**

Device (Hostname)	MAC Address	IP Address
Computer 1	00-10-A4-13-99-2E	10.10.10.1
Computer 2	00-10-A4-13-6C-6E	10.10.10.2
Computer 3	00-B0-D0-25-BF-48	10.10.10.3
Laser printer	00-10-83-0B-A6-2F	10.10.10.20

Note

In this example, you function as the network administrator. You must therefore know how to obtain all IP and MAC address information for devices connected to the network. To do so, it helps to keep good documentation on the network.

Connect the Network Devices

The next step in assembling an office-type LAN is to connect all the networking devices by using the star topology shown in Figure 1-21. At the center of this star topology network is a switch or hub. Recall that either a switch or a hub can be used to connect the networking devices. The switch is the best choice in this case because a hub broadcasts data it receives to all devices connected to its ports, and a switch enables the devices to communicate directly. Although hubs are not as sophisticated as switches and are not used often in modern computer networking, they are still suitable for use in small networks.

CAT6 (Category 6)
Twisted-pair cable, capable of carrying up to 1000Mbps (1Gbps) of data up to a distance of 100 meters

RJ-45
The 8-pin modular connector used with CAT6/5e/5 cable

Mbps
Megabits per second

The connections from the switch to the computers and the printer are achieved using premade twisted-pair patch cables. The cable type used here is **CAT6 (Category 6)** twisted-pair cable. CAT6 twisted-pair cables have **RJ-45** modular connectors on each end, as shown in Figure 1-22, and are capable of carrying 1000**Mbps** (that is, 1Gbps) or more data up to a distance of 100 meters. If the network hardware and software are properly set up, all computers can access the printer and other computers.

Note

Chapter 2 covers twisted-pair cable and its various category specifications (CAT5E, CAT6, CAT6A, CAT7), as well as issues associated with the proper cabling.

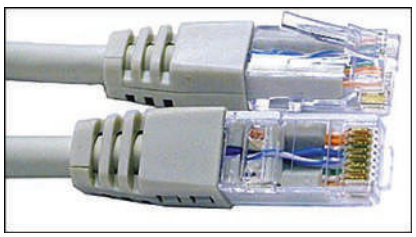


FIGURE 1-22 RJ-45 twisted-pair patch cables (courtesy of StarTech.com).

The media used for transporting data in a modern computer network are either wireless, twisted-pair, or fiber-optic cables. The principles involved in selecting, installing, and testing twisted-pair cabling are presented in Chapter 2. Table 1-10 lists the **numerics** commonly used to describe the data rates for the twisted-pair media and the older-style copper coaxial cable used in a LAN. This table also lists common physical media types for fiber-optic LANs. The names of each of these physical media types provides an alphanumeric description of a technology. For example, 100BASE-T refers to 100Mbps baseband, twisted-pair technology.

Numerics
Numerical representations

TABLE 1-10 **Common Numerics for Ethernet LAN Cabling and Ethernet Deployment Standards**

Numeric	Description
10BASE2	10Mbps over coaxial cable up to 185 m, also called thinnet (seldom used today)
10BASE5	10Mbps over coaxial cable up to 500 m, also called thicknet (seldom used today)
10BASE-T	10Mbps over twisted-pair
10BASE-FL	10Mbps over 850 nm multimode fiber-optic cable
100BASE-TX	100Mbps over twisted-pair (also called Fast Ethernet)
100BASE-SX	10/100Mbps over multimode fiber-optic cable
100BASE-FX	100Mbps over multimode fiber-optic cable
1000BASE-T	1000Mbps over twisted-pair
1000BASE-SX	1000Mbps over multimode fiber-optic cable
1000BASE-LX	1000Mbps over single-mode fiber-optic cable
10GBASE-T	10Gbps over twisted-pair
10GBASE-SR	10Gbps over multimode fiber-optic cable
10GBASE-LR	10Gbps over single-mode fiber-optic cable
40GBASE-T	40Gbps over twisted-pair

The RJ-45 plugs connect to the switch inputs via RJ-45 jacks. Figure 1-23(a) shows a simple eight-port switch. The inputs to the switch, which are also called *input ports*, are the interfaces for the networking devices. The switch inputs marked with an X, as shown in Figure 1-23(b), indicate that these devices are cross-connected, meaning the transmit and receive pairs on the twisted-pair cable are crossed to properly align each for data communication. The term for a cable that has cross-connected TX/RX data lines is **crossover**. Some switches might have the port labeled "uplink," which indicates the cross-connect capability. Furthermore, some newer switches are equipped with automatic crossover detection, so you don't have to worry about whether to use a straight-through cable or a crossover cable. Chapter 2 provides examples of straight-through and crossover cables.

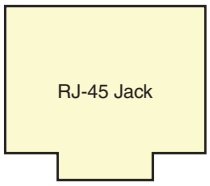
Crossover
A cable in which the transmit and receive signal pairs are crossed to properly align the transmit signal on one device with the receive signal on the other device

Straight-through
An input in which the transmit and receive signal pairs are aligned end-to-end

Uplink Port
A port that allows the connection of a switch to another switch without requiring a crossover cable



The switch used to connect the networking devices
(a)



(cross-connected input)
(b)

FIGURE 1-23 (a) The switch used to connect the networking devices (Jiri Pavlik/Shutterstock); (b) close-up view of X input, indicating an uplink port.

Figure 1-24(a) provides an example of cross-connection. A switch usually has at least one port that can be switched or selected for use as either a cross-connected or **straight-through** input. A straight-through port, also called an **uplink port**, allows for the connection of a switch to a switch or hub without the use of a special cable. Computers, printers, and routers are examples of devices requiring cross-connected input ports. Uplink connections to other switches or hubs, on the other hand, require straight-through connections. Figure 1-24(b) provides a block diagram illustrating the concept of straight-through input.

Link Light
An indicator on a switch or hub that shows whether the transmit and receive pairs are properly aligned

Link Integrity Test
A test used to verify that a communication link has been established between two Ethernet devices

Link Pulses
Pulses sent by two connected devices via twisted-pair cables when data is not being transmitted to indicate that the link is still up

Client
A computer connected to a network that accesses services from the server

Peer
A computer that uses and provides resources to a network

Peer-to-Peer Network
A network in which all the computers provide similar services, including server functions

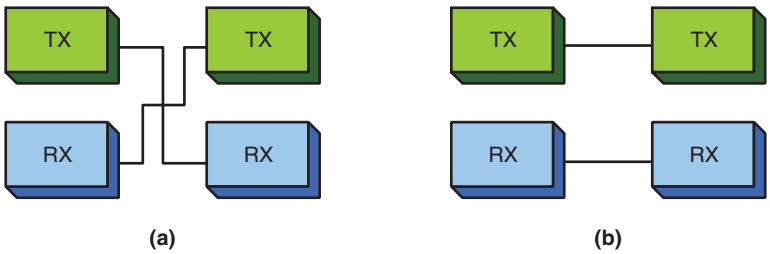


FIGURE 1-24 (a) An example of the wiring on a cross-connect input on a switch; (b) an example of straight-through wiring.

You can verify a networking connection by examining the link light on the switch or hub. The presence of a **link light** indicates that the transmit and receive pairs are properly aligned and the connected devices are communicating. Absence of the light indicates a possible cabling or hardware problem. The Ethernet protocol uses a **link integrity test** to verify that a communication link between two Ethernet devices has been established. The link light remains lit when communication is established, and it remains lit as long as there is a periodic exchange of link pulses from the attached devices. Link pulses are sent by each of the connected devices via the twisted-pair cables to indicate that the link is up, but the **link pulses** are not part of the Ethernet packet and are sent at regular intervals when data is not being transmitted.

When the connection to the network is made, a client/server network or a peer-to-peer network is created. The two network types have advantages and disadvantages. A **client** is a computer connected to a network that uses services from the server. A **peer** is a computer that uses and provides resources to the network. In a **peer-to-peer network**, all computers connected in the network use and provide similar services. The client computer can also function as a server for the network. The small office LAN shown in Figure 1-25 is an example of a peer-to-peer network.

In a **client/server network**, the server handles multiple requests from multiple clients for multiple services. In addition to being a peer-to-peer network, the LAN in Figure 1-25 is an example of a client/server network.

Client/Server Network
A network in which the server handles multiple requests from multiple clients for multiple services

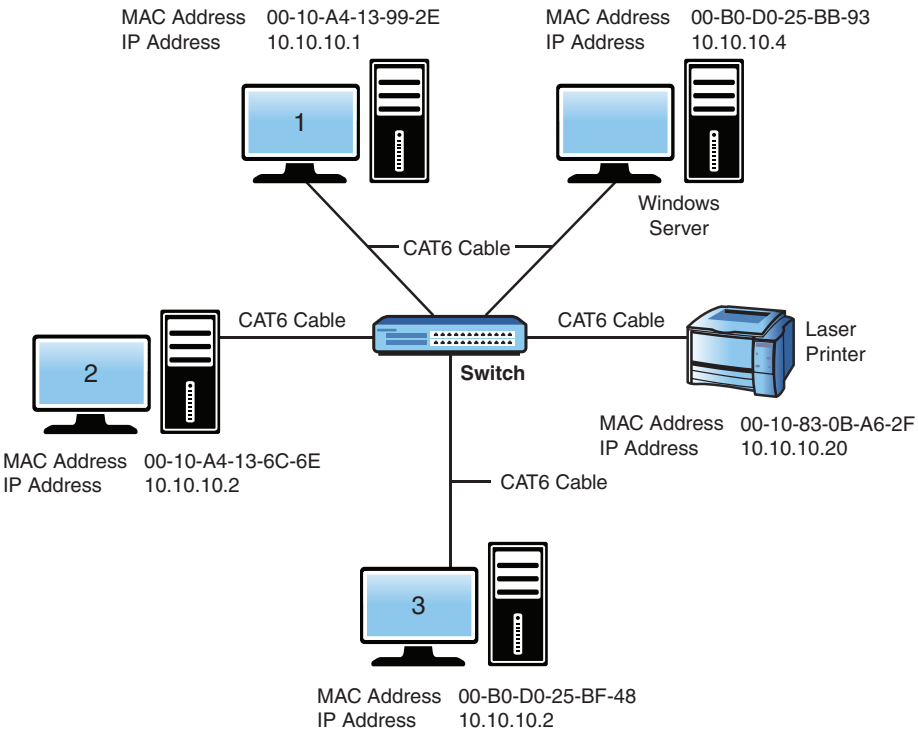


FIGURE 1-25 An example of a client/server or peer-to-peer network.

It isn't practical to say which network choice—peer-to-peer or client/server—is best for all applications. Both types are used, and it is up to the users and the LAN administrator to make the choice. Each has definite advantages and disadvantages, as outlined in Table 1-11.

TABLE 1-11 **Advantages and Disadvantages of Peer-to-Peer and Client/Server Networks**

Type of Network	Advantages	Disadvantages
Peer-to-peer network	Easy network setup	Resource sharing can affect the performance of the computers
	No centralized network administration	Poor security
	Low cost	Users must administer their own computers
	Users control the resource sharing	No central file server
		No centralized administration of the computer's resources
Client/server network	Centralized file storage	Client/server software and licenses can be expensive
	Centralized network security	Server hardware can be expensive
	Easy sharing of the network resources	Requires a network administrator
		Network bandwidth/resource requirements

Configure the Computers to Operate on the LAN

The next step in assembling an office-type LAN is to configure the IP address settings on each computer. In order to configure the computers to operate on the LAN, you need to ensure that each computing device is assigned an IP address. To configure the computers in the office LAN using Windows 10 or macOS, you use the IP addresses from Table 1-9 and the following procedures:

- **Windows 10:** Go to **Control Panel > Network and Internet—Network and Sharing Center**. Click **Local Area Connection** and select **Properties** and then click **Continue**. In the Local Area Connection Properties menu, double-click **Internet Protocol Version 4 (TCP/IPv4)**. From the Properties menu, select **Use the Following IP Address**, enter the IP address and subnet mask, and click **OK**.
- **macOS:** Go to **System Preferences > Network**. Select the network adapter from the left window and select the **Ethernet** or **USB Ethernet** connection. From the Configure IPv4 drop-down menu, select **Manually**. (This option lets you manually set the IP address and subnet mask.) Enter the desired IP address and subnet mask in the fields that now appear and click **Apply**.

As shown in Table 1-9, the IP address for computer 1 is 10.10.10.1, and in this example, the subnet mask 255.255.0.0 is being used. Chapter 6 examines subnet masking in detail. For now, leave the remaining fields empty; you'll learn more about them in later chapters. Your network configuration for computer 1 should now be complete, and you can repeat these steps for computers 2 and 3 in this LAN example.

Section 1-6 Review

This section covers the following Network+ exam objectives.

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

CAT6 UTP cable, 100BASE-T, and RJ-45 plugs and jacks are introduced in this section. The RJ-45 type of connector is used on all computer networks. Table 1-10 provides a good description of the common networking cable types.

1.8 Summarize cloud concepts and connectivity options

Examples in this section show private IP addressing.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

Network connections to hubs, switches, and routers are discussed in this section.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

The typical speeds for CAT6 UTP cable are discussed in this section.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

Each NIC contains a unique MAC address, and IP addresses are locally assigned by a network administrator.

4.5 Explain the importance of physical security.

While not a security issue, some newer switches are equipped with automatic crossover detection, so you don't have to worry about whether to use a straight-through cable or a crossover cable.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

A cable that has cross-connected TX/RX data lines is called a ***crossover cable****.*

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

The typical speed and distance requirements for CAT6 are presented in this section.

Test Your Knowledge

1. True or false: The "X" on the input to a switch represents a router-only port.
   a. True
   b. False
2. A cross-connected input port ____.
   a. has the transmit and receive pairs crossed
   b. is used only on connections to routers
   c. indicates that the cable is wired incorrectly
   d. must be avoided on hub and switch port inputs
3. What does a lit link light indicate?
   a. The link integrity test is operational.
   b. Link pulses are being shared by all devices in the LAN.
   c. A 10Mbps data link has been established.
   d. A 100Mbps data link has been established.

1-7 TESTING AND TROUBLESHOOTING A LAN

A critical step in computer networking is to verify that the network has connectivity. Students should learn to do the following after initial network setup:

- Check the link lights at each end (if possible).
- Use the **ping** command to verify that a link has been established.

The office network used as an example in this section is small, and it should be easy for students to verify connectivity. It is important that students develop the habit of always confirming network connections, and doing so becomes critical when network connections become more complex. The command structure of the **ping** command is presented in this section, along with examples of replies and "request timed out" messages.

When the network configurations on the computers are completed and the cable connections are in place, you need to test and possibly troubleshoot the network.

First, you need to verify that the computers are properly connected on the network. You do this by verifying that you have link lights on the switch ports connected to a computer or other networking device. Figure 1-26 shows an example of a switch with link lights activated.

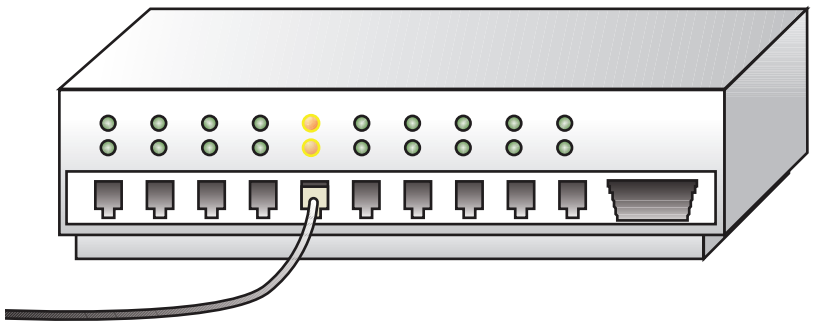


FIGURE 1-26 An example of the link lights on a switch.

ping
A command that is used to test that a device on a network is reachable

ICMP
Internet Control Message Protocol, a protocol which verifies that messages are being delivered

After you have verified that the networking devices are physically connected, you can use the **ping** command in the Windows command window to verify that the devices are communicating. **ping** uses Internet Control Message Protocol (**ICMP**) echo requests and replies to test that a device on the network is reachable. The ICMP protocol verifies that messages are being delivered. The command structure for the **ping** command is as follows:

```
Usage ping[-t][-a][-n count)[-1 size][-f -i TTL][-v TOS]  [-r count]
 [-s  count]
[[-j host-list]:[-k host-list][-w timeout] destination-list
Options
-t Ping the specified host until stopped
 To see statistics and continue, type Control-Break
 To stop, type Control-C
-a Resolve addresses to host-names
-n count Number of echo requests to send
-1 size Send buffer size
-f Set Don't Fragment flag in packet
-I
TTL Time To Live v
TOS Type Of Service
r count Record route for count hops
s count Timestamp for count hops
j host-list Loose source route along host-list
k host-list Strict source route along host-list
w timeout in milliseconds to wait for each reply
```

For example, to ping the IP address for computer 1, you use the command **ping 10.10.10.1** (because 10.10.10.1 is the IP address of computer 1). To ping computer 3, you use **ping 10.10.10.3**. (Refer to Table 1-9 and Figure 1-25 for the IP addresses of the computers in the sample network.)

The following is an example of pinging another computer on the network to verify that the computers are communicating:

```
ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Reply from 10.10.10.2: bytes 32 time<1ms TTL 128
Reply from 10.10.10.2: bytes 32 time<1ms TTL 128
Reply from 10.10.10.2: bytes 32 time<1ms TTL 128
Reply from 10.10.10.2: bytes 32 time<1ms TTL 128
Ping statistics for 10.10.10.2:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Note

Remember that the **ping** command is executed from the command window.

In this example, computer 1 pings computer 2. The text of this example shows 32 bytes of data being sent to the computer with the IP address 10.10.10.2. "Reply from 10.10.10.2" indicates that computer 2 received the message. However, if the computer at IP address 10.10.10.2 does not respond, the message "Request timed out." is displayed:

```
ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.10.10.2:
 Packets: Sent = 4, Received = 0, Lost= 4
(100% loss),
```

You might at some point want to verify the IP address of the computer you are working on. You can obtain the IP address by entering the command **ipconfig** at the command prompt. You don't need to include the **/all** switch after the **ipconfig** command unless you also want to see the MAC address information. Figure 1-27 shows an example of displaying the IP address for computer 1.

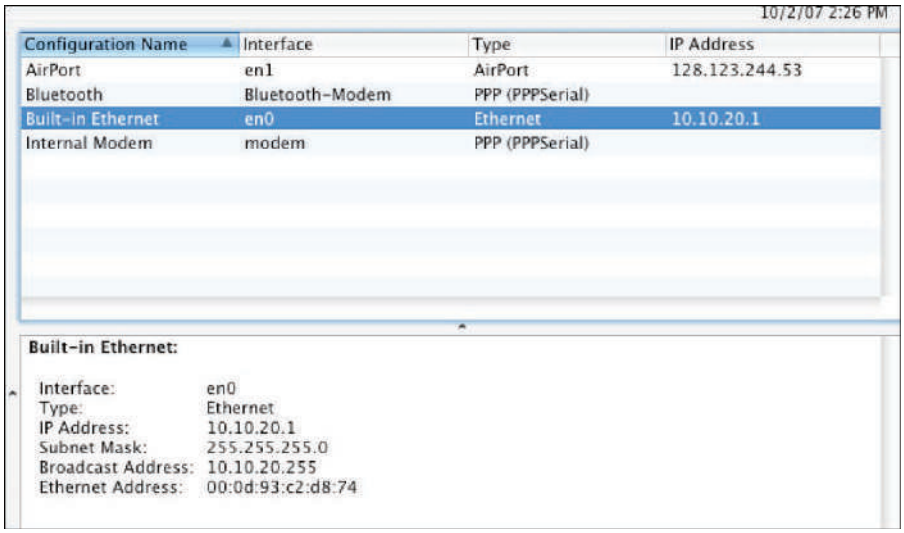
ipconfig
A command used to display a computer's address

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix .:
IP Address.....: 10.10.10.1
Subnet Mask.....: 255.255.0.0
Default Gateway .....:

(a)



(b)

FIGURE 1-27 (a) An example of displaying the IP address for computer 1 by using the **ipconfig** command in Windows; (b) an example of the displayed IP address in macOS for the built-in Ethernet connection.

Section 1-7 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.

This section demonstrates the steps for verifying connectivity in a network.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

*After you have verified that the networking devices are physically connected, you can use the **ping** command to verify that the networking devices are communicating. **ping** uses Internet Control Message Protocol (**ICMP**) echo requests and replies to test whether a device on the network is reachable.*

1.6 Explain the use and purpose of network services.

*This section shows the use of the **ping** command and the TTL messages generated.*

5.3 Given a scenario, use the appropriate network software tools and commands.

*An important step in verifying connectivity between two networking devices is to issue the **ping** command, using the destination IP address for the other device. The **ping** command is available from the command window in Windows. Make sure you know how to issue the command and the options available with the command, such as implementing continuous pinging and setting the buffer size.*

Test Your Knowledge

1. A network administrator needs to verify a network connection. Which of the following steps should be taken? (Select two.)
   a. Verify the link lights.
   b. Use the **ping** command to verify network connectivity.
   c. Perform an ARP request.
   d. Ping the MAC address.
2. What does the **ping -t ip address** command do?
   a. It pings the host at the specified IP address until the command is canceled.
   b. It pings the MAC address of the host at the specified IP address.
   c. It allows the **ping** command to pass through routers.
   d. It allows the **ping** command to be executed from the command prompt.

SUMMARY

This chapter introduces the basic concepts of computer networking. It presents the technologies and techniques for assembling a computer network using the Ethernet protocol. You should now understand the following major topics:

- The various LAN topologies
- The concept of CSMA/CD in the Ethernet protocol
- The structure of an Ethernet frame
- The purpose of a network interface card
- The purpose of a MAC address
- How to determine the MAC address for a computer
- The purpose and structure of an IP address
- The concept of private IP addresses
- The OSI model
- The network topologies and technologies used to implement twisted-pair computer networks
- How to configure and verify a computer's IP address
- How to configure a home network and an office LAN
- The purpose of the link light
- The purpose of using **ping** to test a network connection

QUESTIONS AND PROBLEMS

Section 1-1

1. State whether each of the following network descriptions describes a MAN, a WAN, or a LAN:
   a. A network of users who share computer resources in a limited area

      LAN
   b. A network of users who share computer resources across a metropolitan area

      MAN
   c. A network that connects local area networks across a large geographic area

      WAN

2. Expand the acronym *NIC*.

   Network interface card

3. Expand the acronym *MAC*.

   Media access control

4. Expand the acronym *LAN*.

   Local area network

5. Expand the acronym *WAN*.

   Wide area network

Section 1-2

6. Define the term *protocol*.

   A protocol is a set of rules established for users to gain control of the network to exchange information.

7. Define the term *topology*.

   Topology is the architecture of a network.

8. Define the term *deterministic*.

   Deterministic refers to a way of providing access to a network by giving each network device a fixed time interval to access the network.

9. A disadvantage of Token Ring is that if an error changes the token pattern, it can cause the token to stop circulating. This issue can be eliminated by adding which of the following?

   a. Router
   b. Multiport repeater
   c. Token passer
   d. Token Ring hub

10. Name each network topology shown in Figure 1-28 (bus, star, ring, or mesh).

    a. Mesh
    b. Bus
    c. Ring
    d. Star/hub-and-spoke

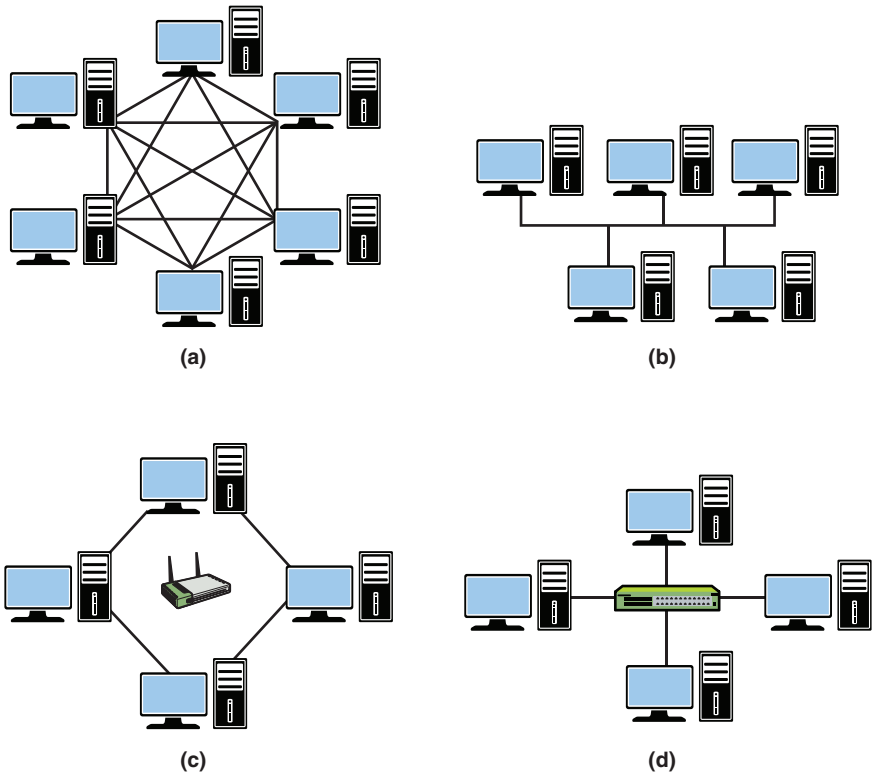


FIGURE 1-28 The networks for question 10.

11. What is the difference between a hub and a switch?

    A hub broadcasts the data it receives to all devices connected to its ports. A switch forwards the data it receives directly to its destination address when the associated port is known.

Section 1-3

12. What are the seven layers of the OSI model?

    1. Physical
    2. Data link
    3. Network
    4. Transport
    5. Session
    6. Presentation
    7. Application

13. Which OSI model layer is responsible for adding a header that includes routing information?

    Layer 3: Network layer

14. Which OSI model layer is considered the media access control layer?

    Layer 2: Data link layer

15. Which OSI model layer combines messages or segments into packets?

    Layer 3: Network layer

16. At what layer does a router work?

    Layer 3: Network layer

17. Which OSI model layer is responsible for the mechanical connection to the network?

    Layer 1: Physical layer

18. Which OSI model layer is responsible for data compression and encryption?

    Layer 6: Presentation layer

19. TCP functions at what layer of the OSI model?

    Layer 4: Transport layer

20. HTTP functions at what layer of the OSI model?

    Layer 7: Application layer

21. IP and IPX are examples of protocols that operate at what layer of the OSI model?

    Layer 3: Network layer

22. A network interface card operates at what layer of the OSI model?

    Layer 1: Physical layer

23. Why are the layers of the OSI model important to a network administrator?

    Knowledge of the OSI model layers can help isolate network problems.

Section 1-4

24. What does *CSMA/CD* stand for, and what protocol uses CSMA/CD?

    CSMA/CD stands for carrier-sense multiple access with collision detection, and Ethernet uses CSMA/CD.

25. What information is not included in an Ethernet frame?

    a. Frame size
    b. Source MAC address
    c. Pad
    d. Frame check sequence

26. What is the minimum size of the data payload in an Ethernet frame?

    46 bytes

27. An Ethernet packet size greater than 1500 bytes is called ____.

    a. a bad frame
    b. a jumbo frame
    c. an MTU
    d. All of the above
    e. None of the above

28. What does *OUI* stand for, and where is an OUI used?

    OUI stands for organizationally unique identifier. The OUI is found in the first 3 bytes of a MAC address.

29. What does an OUI represent?

    The OUI identifies the manufacturer of a network device.

30. In Windows 10, how can you find the Ethernet (MAC) address?

    At the command line, type **ipconfig /all**.

31. INTERNET SEARCH: Find the device manufacturer for each of the following Ethernet devices.

    a. 00-C0-4F-49-68-AB

       Dell Computer Corporation

    b. 00-0A-27-B7-3E-F8

       Apple Computer, Inc.

    c. 00-04-76-B6-9D-06

       3Com Corporation

    d. 00-00-36-69-42-27

       Atari Corporation

32. Indicate the class of address (A, B, or C) for each of the following IP addresses:

    a. 46.39.42.05 ____ A
    b. 220.244.38.168 ____ C
    c. 198.1.0.4 ____ C
    d. 126.87.12.34 ____ A
    e. 99.150.200.251 ____ A
    f. 128.64.32.16 ____ B

33. Expand the acronym *TCP/IP*

    TCP/IP stands for Transmission Control Protocol/Internet Protocol.

Section 1-5

34. What are three advantages of a wireless network?

    User mobility, ease of installation, no cables

35. What does it mean for a wireless networking device to be Wi-Fi compliant?

    It means the wireless equipment is compliant with the 802.11x standards.

36. What are the most common types of equipment that are used to establish broadband connections to ISPs?

    Cable and DSL modems

37. Name six issues that should be considered when planning a home network.

    Data speed, cost, ease of implementation, appearance, home access, public access

38. Why is checking the lights of a networking device that connects to an ISP important?

    Incorrect lights can indicate a connection problem with the cable modem, the DSL modem, or the phone connection, or they might indicate that the ISP is experiencing technical difficulties.

39. What is the purpose of a range extender?

    This device relays the wireless signal from an access point or a wireless router into areas with a weak signal or no signal at all.

40. What is a hotspot?

    A hotspot is a limited geographic area in which wireless access is provided for the public.

41. List five steps that can be used to protect a home network.

    1. Change the default factory passwords.
    2. Change the default SSID.
    3. Turn on encryption.
    4. Turn off SSID broadcast.
    5. Enable MAC address filtering.

42. You have the choice of selecting a networking device with WEP or a device with WPA. Which offers better security and why?

    WPA offers stronger encryption and is supported with most new Wi-Fi systems.

43. What are the potential problems related to using the default factory passwords?

    Wireless equipment is shipped with default passwords that are set at the factory. These default settings are known by the public, including people who would like to gain access to your network and possibly change your settings.

44. What is the purpose of the SSID, and what can a network administrator do to protect a network from hackers who might have learned the SSID?

    The SSID is the name used to identify a network and is used by an access point or a wireless router to establish an association so that a wireless client can join the network. The SSID can be up to 32 characters and should be changed often so hackers who have figured out the SSID lose access to the network.

45. What is the purpose of MAC filtering on a wireless network?

    MAC filtering can be used to select what devices can be allowed access to the network. When MAC address filtering is turned on, only wireless devices that have allowed MAC addresses are granted access to the network.

46. How does NAT (network address translation) help protect outsider access to computers in a home network?

    The bad guy sees only the router because the IP addresses of the internal networking devices are not provided on the Internet; only the IP address of the router is provided. A home network typically uses private address space that is not routable on the Internet. (Private IP addresses are blocked by the ISP.)

47. What is stateful packet inspection?

    Stateful packet inspection is a type of firewall protection that involves inspecting incoming data packets to make sure they correspond to an outgoing request. Data packets that are not requested are rejected.

48. What is a VPN, and how does it protect the data transferred over a wireless network?

    VPN stands for virtual private network, and a VPN connection enables a remote or mobile user to access a network as if he or she were actually physically at the network. In addition, the VPN connection is encrypted, providing privacy for the data packets being transmitted.

49. How is IP addressing typically handled in a home network?

    IP addressing for a home network is managed by a router or wireless router that connects to the ISP. The ISP issues an IP address to the router from an available pool of IP addresses managed by the ISP. The computers in the home network are issued private IP addresses by the router.

50. What is port address translation (PAT)?

    With PAT, a port number is attached to the network connection. This port number identifies the device that is establishing a connection to the Internet. This number is used when a data packet is returned to the home network. The port number identifies the device that established the Internet connection so the router can deliver the data packet to the correct device.

51. A router on a home network is assigned the IP address 128.123.45.67. A computer in the home network is assigned the private IP address 192.168.10.62. This computer is assigned the public IP address 128.123.45.67:1922. Which IP address is used for routing data packets on the Internet? Is overloading being used?

    The IP address 128.123.45.67:1922 is used for routing the data packets on the Internet. Yes, overloading is being used because one routable IP address is being shared by the home network.

Section 1-6

52. Which of the following is not a step in building an office LAN?

    a. Obtaining proper government permits
    b. Configuring the network settings
    c. Connecting the devices together
    d. Creating network documentation

53. What is RJ-45?

    a. A 45-pin connector for CAT6
    b. An IEEE standard for data speed
    c. An 8-pin modular connector for twisted-pair Ethernet
    d. A protocol used to verify a communications link

54. What is an *uplink port*?

    An uplink port is a port on a hub or switch that can be used as either a cross-connected or straight-through input. It is used to connect multiple hubs/switches together.

55. What are the maximum speed and length for Category 6 cabling?

    CAT6 cable is capable of supporting a data rate of 1000Mbps (or greater) over a distance of 100 meters.

56. What do the link lights on a hub indicate?

    The link lights indicate whether the transmit and receive pairs of the cable are properly aligned.

57. What does *cross-connected* mean?

    When the transmit and receive pairs on CAT5 or greater cable are crossed to properly align each for data communication, they are said to be cross-connected.

58. DOCUMENTATION: Draw a network diagram similar to Figure 1-29, consisting of three computers, a switch, and a printer. Use the MAC addresses given in Table 1-9. Assign each network device an IP address from the private address space 192.168.5.*x*. Assume that you are the network administrator and may choose the host address for each device.

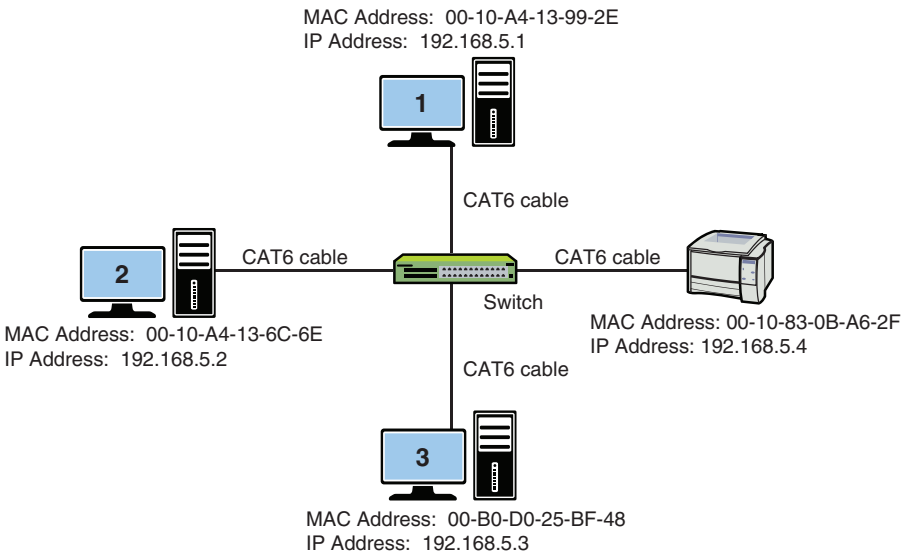


FIGURE 1-29 The sample network diagram for question 58.

Section 1-7

59. What command would you use to ping 10.3.9.42 indefinitely?

    ping -t 10.3.9.42

60. What command would you use to ping 192.168.5.36 20 times with 1024 bytes of data?

    ping -n 20 –l 1024 192.168.5.36

61. Expand the acronym *TTL*.

    TTL stands for time to live.

Certification Questions

62. In terms of computer security, a switch offers better security than a hub. Why is this the case?

    a. A hub requires a special pin to activate the connection.

    b. A hub forwards the data it receives to every device connected to the hub. It is possible for network devices to pick up data intended for a different device. A switch eliminates this by only forwarding data packets to the correct device whenever possible.

    c. A switch forwards the data it receives to every device connected to the switch. It is possible for network devices to pick up data intended for a different device. A hub eliminates this by only forwarding data packets to the correct device whenever possible.

    d. The use of the switch guarantees that all devices connected to it share link integrity pulses. This sharing of the pulses strengthens the security of the connection.

63. What networking protocol does Ethernet use?

    a. Ethernet uses a Token Ring passing scheme. The computer devices must possess the ring to be able to pass a token.

    b. Ethernet uses carrier-access multiple sensing with collision detection.

    c. Ethernet uses carrier-sense multiple access with collision detection.

    d. Ethernet uses collision-sense carrier access with multiple pairing.

64. A network interface card has the MAC address 00-00-86-15-7A. Based on this information, what is the OUI?

    a. There is not sufficient information to specify the OUI.

    b. The OUI is 86-15-7A.

    c. The OUI is 86-00-00.

    d. The OUI is 00-00-86.

65. An IP address for a computer is assigned by which of the following?

    a. Internet Assigned Numbers Authority

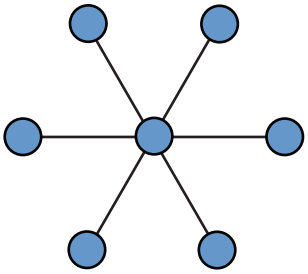
    b. The local network administrator

    c. The user of the computer

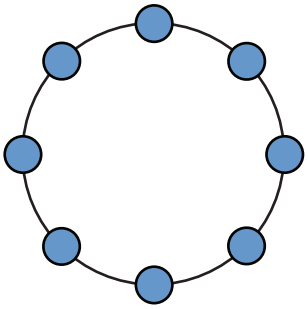
    d. Internet Address Numbers Authority

66. Which network topology is shown in the following diagram?

a. Star
b. Token Ring
c. Bus
d. Mesh
e. None of these answers are correct.

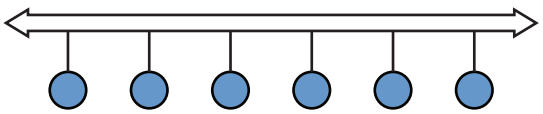


67. Which network topology is shown in the following diagram?



a. Star
b. Token Ring
c. Bus
d. Mesh
e. None of these answers are correct.

68. Which network topology is shown in the following diagram?



a. Star
b. Token Ring
c. Bus
d. Mesh
e. None of these answers are correct.

69. The pad field in an Ethernet packet ____.

    a. is used to bring the total number of bytes up to 46 if the data file is less than 46 bytes
    b. is used to bring the total number of bytes up to 64 if the data file is less than 64 bytes
    c. is not required with CSMA/CD
    d. provides grouping of the information for transmission

70. The IP address 10.10.20.250 is an example of which of the following? (Select all that apply.)

    a. A Class A address
    b. A Class B address
    c. A private IP address
    d. A routable IP address
    e. A non-routable Internet IP address

71. Which of the following are true of an intranet? (Select all that apply.)

    a. It uses class E addressing.
    b. It is used in high-speed (Gigabit) Ethernet.
    c. It is an internal network that provides file and resource sharing.
    d. It enables Fast Ethernet connections.
    e. It is not accessed from the Internet.

2
CHAPTER

Physical Layer Cabling: Twisted-Pair

Chapter Outline

2-1 Introduction
2-2 Structured Cabling
2-3 Twisted-Pair Cable
2-4 Terminating Twisted-Pair Cables
2-5 Cable Testing and Certification
2-6 10 Gigabit Ethernet over Copper
2-7 Troubleshooting Cabling Systems
Summary
Questions and Problems

Objectives

- Describe the six subsystems of a structured cabling system
- Define horizontal cabling
- Define UTP and STP
- Define the categories of UTP cable
- Describe the difference in the T568A and T568B wire color orders
- Describe the procedure for placing RJ-45 plugs and jacks on twisted-pair cable
- Describe how to terminate twisted-pair cable for computer networks
- Define the basic concepts of planning a cable installation for an office LAN
- Describe the procedure for certifying a twisted-pair cable for CAT6 and CAT5e
- Describe the issues related to running 10 Gigabit Ethernet over copper
- Describe the basic steps for troubleshooting cable problems

Key Terms

physical layer cabling
angled physical contact (APC)
ultra-physical contact (UPC)
EIA
TIA
campus network
TIA/EIA 568-B
Gigabit Ethernet
full-duplex
CAT6a
10GBASE-T
coaxial
BIX
RJ-45
RJ-11
F-type
building entrance
entrance facilities (EF)
equipment room (ER)
telecommunications closet
telecommunications room (TR)
backbone cabling
horizontal cabling
TCO
work area
main cross-connect (MC)
intermediate cross-connect (IC)
cross-connect
horizontal cross-connect (HC)
work area outlet (WO)
terminated
8P8C
patch cable
UTP
CAT6/6a
CAT5e
balanced mode
Fast Ethernet
network congestion
bottlenecking
Gigabit Ethernet
full-duplex
CAT7/7a and CAT6a
10GBASE-T
STP
EMI
T568A
T568B
color map
TX
RX
straight-through cable
wiremap
crossover cable

Key Terms continued

link
full channel
attenuation
near-end crosstalk (NEXT)
crosstalk
10GBASE-T
IEEE 802.3an-2006 10GBASE-T
Alien crosstalk (AXT)
PSANEXT
PSAACRF
F/UTP
TCL
ELTCTL
LCL
TCTL
multilevel encoding
hybrid echo cancellation circuit

Physical Layer Cabling
The media interconnecting networking devices

This chapter examines the twisted-pair media used to link computers together to form a local area network (LAN). This media is called **physical layer cabling**. The term *physical layer* describes the media interconnecting networking devices. In this chapter you will gain an introductory understanding of the cable media, including the category types, the steps for terminating cables, cable testing, certification, and troubleshooting. The main focus is on the use of UTP cable in computer networks, although an overview of shielded twisted-pair (STP) is presented as well. (Fiber-optic cable, which also plays an important role in modern computer networks, is thoroughly examined in Chapter 3, "Physical Layer Cabling: Fiber Optics.") A network technician or engineer needs to have a good understanding of how physical layer cable is being used and its specific application.

Other types of cabling you might encounter in computer networking are RG-6 and possibly RG-59. These types of cables, called *coaxial cables*, are primarily used to connect satellite systems or cable television and modems. Cable terminations for these types of cable include F-type and BNC connector types. Another type of coax cable is called twinaxial. This is a type of coaxial cable that contains two inner conductors rather than one.

The following are some of the connector types used with physical layer cabling:

- **UTP coupler:** This small device, which is used to connect two UTP cables, is also called an *inline coupler*. UTP couplers can be used to couple twisted-pair cabling and RJ-11 phone lines but can introduce signal degradation.
- **BNC connectors:** BNC stands for Bayonet Neill–Concelman. This type of connector is a quick-connect connector for coaxial cable that was commonly used with thinnet Ethernet cabling.
- **Fiber coupler:** These couplers come in a variety of styles that support single-mode and multimode fibers. These devices allow a single fiber to be split into two outputs, and multiple input fibers can be combined into one output fiber.
- **APC and UPC:** The difference between these two types of connectors is the fiber endface. An **angled physical contact (APC)** endface is polished and has an 8-degree angle. An **ultra-physical contact (UPC)** endface is polished and has no angle. APC and UPC connectors are easily identified by their color: APC adapters are green, and UPC adapters are blue.

Angled Physical Contact (APC)
A green fiber connector whose endface is polished and has an 8-degree angle

Ultra-Physical Contact (UPC)
A blue fiber connector whose endface is polished and has no angle

- **Fiber-to-coaxial connector:** This device is used to convert an optical signal carried over fiber to an electrical signal carried over coaxial cable. A typical application for this type of connector is coupling cabling that carries digital optical signal to a digital coaxial cable.

2-1 INTRODUCTION

This chapter begins with an overview of structured cabling. This section defines the six subsystems of a structured cabling system and focuses on the basic issues associated with horizontal cabling or wiring a LAN. Next, the basic operational characteristics of UTP cable are examined. The discussion includes an examination of the various categories of UTP cable currently available. Following that is an overview of constructing twisted-pair patch and horizontal link cabling. This chapter discusses the tools and techniques for properly terminating UTP cabling for twisted-pair Ethernet such as CAT5e, CAT6, CAT6a, CAT7, and CAT8. It also provides an introduction to testing and certifying Ethernet cables. This chapter includes several examples of cable test data and how to interpret the test results. The chapter concludes with a section on troubleshooting computer networks, with a focus on cable or physical failures.

Table 2-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 2-1 **Chapter 2 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.2	Explain the characteristics of network topologies and network types.	2-2
1.3	Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	2-2, 2-3, 2-4, 2-6
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes.	2-2
1.6	Explain the use and purpose of network services.	2-2
1.7	Explain basic corporate and datacenter network architecture.	2-2, 2-4
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	2-4
2.3	Given a scenario, configure and deploy common Ethernet switching features.	2-3, 2-5, 2-6

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	2-3, 2-5, 2-6
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	2-4
5.0	**Network Troubleshooting**	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	2-3, 2-4, 2-5, 2-6, 2-7
5.3	Given a scenario, use the appropriate network software tools and commands.	2-4

EIA
Electronic Industries Alliance, a trade organization that represents the interests of manufacturers of electronics-related equipment.

TIA
Telecommunications Industry Association, a trade organization that represents the interests of the telecommunications industry

Campus Network
Interconnected LANs within a limited geographic area

TIA/EIA 568-B
The standard that defines the six subsystems of a structured cabling system

Building Entrance
The point where the external cabling and wireless services interconnect with the internal building cabling

2-2 STRUCTURED CABLING

This section defines the six subsystems of a structured cabling system. Students should be able to identify the purpose of each subsystem. The focus of this section is on issues associated with horizontal cabling.

The first major standard describing a structured cabling system for computer networks was TIA/EIA 568-A, implemented in 1995. **EIA** is the Electronic Industries Alliance, a trade organization that lobbies for the interests of manufacturers of electronics-related equipment. **TIA** is the Telecommunications Industry Association, a trade organization that represents the interests of the telecommunications industry. The wiring standards for modern computer networks are defined by the TIA/EIA 568 standard. The most important addendum to the TIA/EIA 568-A standard is Addendum 5, published in 1999, which defines the transmission performance specifications for four-pair 100-ohm Category 5e twisted-pair cabling. TIA/EIA adopted Category 6 (CAT6) cable specifications in June 2002 as part of TIA/EIA 568-B. This is the type of cabling recommended for use in today's computer networks. CAT6a was adopted in 2018 for 10Gbps speed. CAT7 and CAT8 twisted-pair cables are the latest additions but are not in wide use. The latest TIA/EIA standard is TIA/EIA 568-D.

The TIA/EIA 568-A standard defines the minimum requirements for the internal telecommunications wiring in buildings and between structures in a **campus network**. A campus network consists of interconnected LANs within a limited geographic area such as a college campus, military base, or group of commercial buildings. As mentioned earlier, TIA/EIA 568-A has been revised and updated many times, and in 2000 the standard **TIA/EIA 568-B** was published. TIA/EIA 568-B has three parts:

- **TIA/EIA 568-B.1:** Commercial Cabling Standard, Master Document
- **TIA/EIA 568-B.2:** Twisted-Pair Media
- **TIA/EIA 568-B.3:** Optical Fiber Cabling Standard

Within the TIA/EIA 568-B Commercial Standard for Telecommunication Pathways and Spaces are guidelines defining the six subsystems of a structured cabling system:

- **Building entrance:** The building entrance is the point where the external cabling and wireless services interconnect with the internal building cabling

in the equipment room. It is used for both public and private access (for example, telco, satellite, cable TV, security). The building entrance is also called the **entrance facilities (EF)**. Both public and private network cables enter the building at this point, and typically there are separate facilities for the different access providers.

- **Equipment room (ER):** The ER is a room that contains complex electronic equipment such as network servers and telephone equipment.
- **Telecommunications closet:** The telecommunications closet is the location of the cabling termination points that includes the mechanical terminations and the distribution frames. The connection of the horizontal cabling to the backbone wiring is made at this point. This is also called the **telecommunications room (TR)**, or telecommunications enclosure (TE). In some older systems, the network administrator might encounter two types of punchdown blocks in the telecommunications closet: a 66 block and a 110 block. These types of terminations use insulation-displacement connectors (IDCs) to terminate twisted-pair cables and are commonly used in telephone systems but not computer networks. The wire termination on IDCs requires the use of a punchdown tool. Other tools that can be used are the Krone tool, which is a punchdown tool used for inserting wire into punchdown blocks and insulation displacement connectors. Another tool is the BIX tool, which is used to terminate various wires on BIX blocks and connection products.

Entrance Facilities (EF)
Another name for the building entrance

Equipment Room (ER)
A room that contains complex electronic equipment such as network servers and telephone equipment

Telecommunications Closet
The location of the cabling termination points that includes the mechanical terminations and the distribution frames

Telecommunications Room (TR)
Another name for the telecommunications closet

Note

One room can serve as the entrance facility, the equipment room, and the telecommunications closet.

- **Backbone cabling:** Backbone cabling is cabling that interconnects telecommunications closets, equipment rooms, and cabling entrances in the same building and between buildings.
- **Horizontal cabling:** Horizontal cabling is cabling that extends out from the telecommunications closet into the LAN work area. Typically, the horizontal wiring is structured in a star configuration running to each area's telecommunications outlet (**TCO**), which is the wall plate where the fiber or twisted-pair cable terminates in the room. In some cases, the TCO terminates telephone, fiber, and video in addition to data into the same wall plate.

Backbone Cabling
Cabling that interconnects telecommunications closets in the same building and between buildings

Horizontal Cabling
Cabling that extends out from the telecommunications closet into the LAN work area

TCO
Telecommunications outlet, the wall plate where the fiber or twisted-pair cable terminates in a room

Note

Cable management—which involves keeping cables in order and tangle free—is important with any type of physical layer cabling. A well-managed cable system helps extend the life of cables and is more reliable.

- **Work area:** The work area is the location of computers and printers, patch cables, jacks, computer adapter cables, and fiber jumpers.

Work Area
The location of computers and printers, patch cables, jacks, computer adapter cables, and fiber jumpers

Main Cross-Connect (MC)
Also called the main distribution frame (MDF) or main equipment room or campus distributor (CD), an area that usually connects two or more buildings and is typically the central telecommunications connection point for a campus or building

Intermediate Cross-Connect (IC)
Also called the building distributor (BD), the building's connection point to the campus backbone, which links the MC to the horizontal cross-connect (HC)

Cross-Connect
A space where one or multiple cables are connected to equipment or other cables

Horizontal Cross-Connect (HC)
Also called the floor distributor (FD), the connection between the building distributors and the horizontal cabling to the work area or workstation outlet

Work Area Outlet (WO)
Also called the telecommunications outlet (TO), the workstation used to connect devices (for example, PCs, printers, servers, phones, televisions, wireless access points) to the cable plant, typically with CAT5, CAT5e, CAT6, CAT6a, CAT7, CAT8, and various coaxial cables

Figure 2-1 shows an example of the structure for a telecommunications cabling system. It shows the connection of the carriers (telco, ISP, and so on) coming into the ER, which is the space set aside for the carrier's equipment contained in the **main cross-connect (MC)** or **intermediate cross-connect (IC)**. The EF consists of the cabling, connector hardware, and protection devices that are used as the interface between any external building cabling and wireless services with the equipment room. This area is used by both public and private access providers (for example, telco, satellite, cable TV, security). The ER and EF space is typically combined with the MC equipment room.

Between the MC and the IC is the campus backbone cabling (listed in Figure 2-1 as the interbuilding backbone cabling), which provides connections between the MC and IC. A **cross-connect** is a space where one or multiple cables are connected to equipment or other cables. For example, you could be bringing in 60 UTP cables, with 50 that are cross-connected to a switch and 10 that are cross-connected to a backbone cable going to another location. Typical connections between the MC and IC are single-mode and multimode fibers and possibly coax for cable TV, although most installations are migrating to fiber. The building backbone cabling (that is, intrabuilding backbone cabling) makes the connection between the IC and the telecommunications closet (TC) and **horizontal cross-connect (HC)**. Today this connection is CAT6 UTP or better, although it might be single- or multimode fiber or some combination. Fiber is the best choice for making these connections, although copper is still commonly used. The horizontal cabling is the cabling between the HC and the work area. It is usually CAT6 UTP or better or fiber. The standard currently specifies CAT6. Fiber is gaining acceptance for connecting to the **work area outlets (WOs)**.

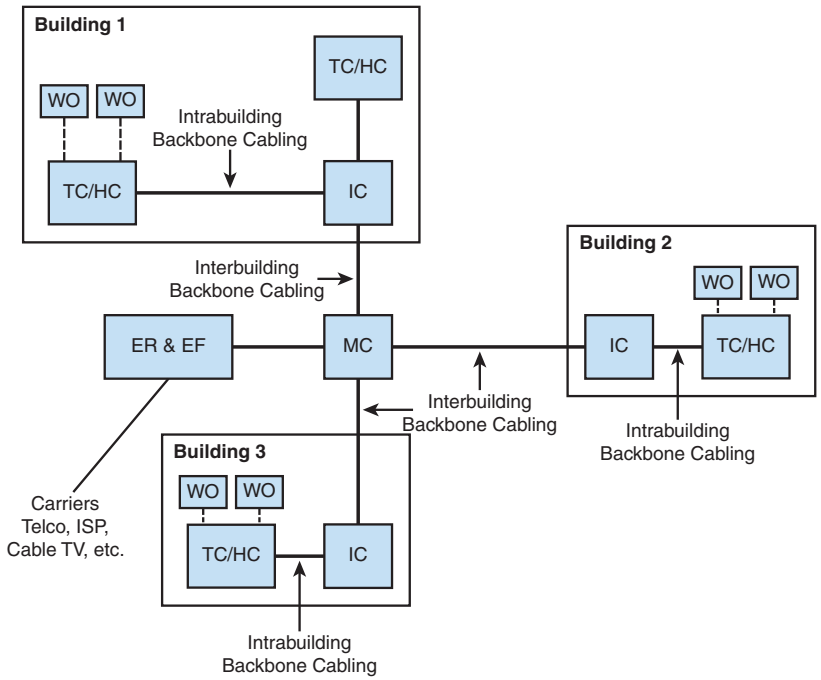


FIGURE 2-1 Telecommunications cabling system architecture.

Figure 2-2 provides a more detailed view of the cabling from the MC to the IC and the HC. This drawing shows the three levels of the recommended backbone hierarchy cabling for a computer network. The first level of the hierarchy is the MC. The MC connects to the second level of the hierarchy, the IC. The backbone cabling connects the MC to the IC and the IC to the TC/HC. The HC connects the horizontal cabling to the work area and to the WO.

Note

The focus of this chapter is on issues associated with the horizontal cabling and the work area (LAN) subsystems. This chapter addresses all six subsystems of a structured cabling system at the point where the networking concepts and related hardware are introduced. Many of the concepts covered in each structured cabling subsystem require that you have a firm grasp of basic networking to gain a full appreciation of how each network piece fits into a structured cabled system.

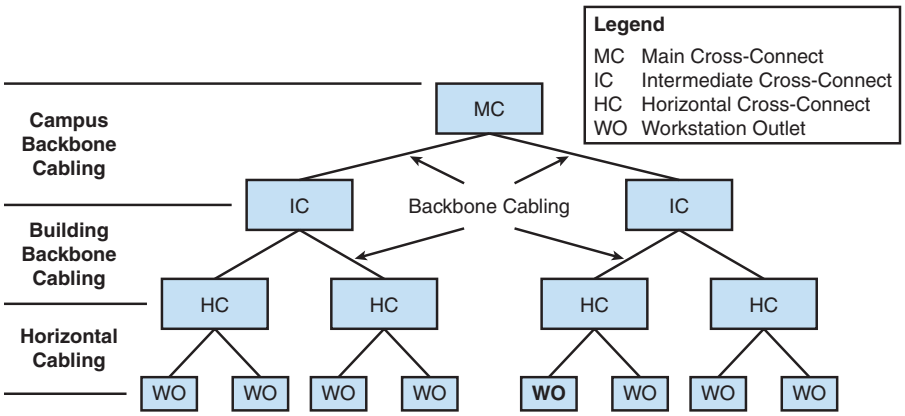


FIGURE 2-2 Campus network hierarchical topology.

Horizontal Cabling

Permanent network cabling within a building is considered *horizontal cabling,* defined as cabling that extends out from the telecommunications closet into the LAN work area. It is important to take time to plan for a horizontal cabling installation because this is where users interface with the network. There is always a substantial installation cost associated with horizontal cabling, and there is even greater cost in having to replace or upgrade a cable installation. You don't want to have to re-cable a system very often. Careful attention should be given to planning for the horizontal cabling of a LAN. It is important to make sure you fully understand your current networking needs and that your proposed plan meets the needs. You should also ensure that your plan addresses the future needs and growth of your network.

Figure 2-3 illustrates the basic blocks of a horizontal cabling system from the telecommunications closet to the computer in the LAN. The figure shows the following components, which are typically found in the telecommunications closet:

A. Backbone cabling interconnecting this closet with other closets

B. Switch or hub

C. Patch panels/patch bay

D. Patch cables

E. Cabling to the LAN (horizontal cabling)

F. Wall plate

G. Patch cable connecting the computer to the wall plate

Item E in Figure 2-3 shows the cabling leaving the telecommunications closet. The cable extends to where it is terminated at the wall plate (item F) in the LAN or work area. The term *terminated* describes where the cable connects to a jack in a wall plate, a patch panel, or an RJ-45 modular plug. In this case, the cable terminates into an RJ-45 jack in the wall plate. Figure 2-4 shows an example of an RJ-45 wall plate and patch panel.

A technique for troubleshooting cable termination is to use a toner probe. A toner probe injects a tone on a cable in a process called tone generation. You can use a speaker/sensor to verify that a tone is present at the other cable end. This technique is also very useful when you need to locate a cable end: The cable you are searching for transmits the tone.

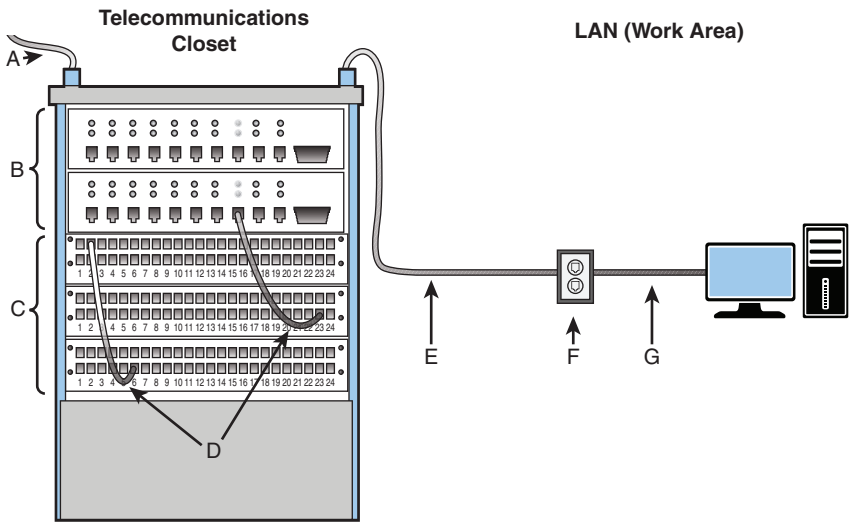


FIGURE 2-3 Block diagram of a horizontal cabling system.

Note

8P8C
The proper term for an RJ-45 modular plug

The proper term for the RJ-45 modular plug used in computer systems is actually **8P8C** for both male and female connectors. 8P8C, which stands for 8 position 8 conductor, is defined in ANSI/TIA-968-A and B. However, both professionals and end users typically use the term RJ-45 instead.

An individual cable is used to connect each connector in an outlet to the patch panel in the telecommunications closet (item F to item E in Figure 2-3). (Section 2-4, "Terminating Twisted-Pair Cables," provides more information on RJ-45 plugs and jacks.) Another 8-pin connector that uses an 8P8C modular connector is the RJ-48. This type of connector, which is commonly used with T1 data lines, typically works with shielded twisted-pair cabling. Although the RJ-45 and RJ-48 connectors look similar, they do not use the same wiring scheme, and they are intended for different data transmission applications.

In a star topology, there is an individual cable run for each outlet in the wall plate. This means that you assign one computer to each terminated outlet. A **patch cable** (item G) is used to make the physical connection from the computer to the wall plate, as shown in Figure 2-3. There is a 100-meter overall length limitation on the cable run from the telecommunications closet to a networking device in the work area. This includes the length of the patch cables at each end (items D and G) plus the cable run (item E). A general rule of thumb is to allow 90 meters for the cable run from the telecommunications closet to the work area (item E). This allows 5 meters of cable length for the work area and 5 meters for the patch cables in the telecommunications closet (item D) and the work area (item G). Figure 2-5 shows an example of the inside of a telecommunications closet.

Patch Cable
A cable used to make a physical connection from a computer to a wall plate



FIGURE 2-4 The Ortronics clarity twisted-pair system (Vlad Nordwing/Shutterstock).

Labeling is extremely important for all aspects of a computer network and data center. Each rack should be labeled to identify the purpose of the equipment installed in the rack (for example, telecommunication equipment that interfaces with the WAN connection). In addition, it is important to label each server to identify the purpose and possibly its name. Cabling should also be labeled. Both cable ends or wall plates should be labeled with some identifying marks that correspond to your building drawings. This type of labeling makes it possible for a technician to easily identify a cable and its path.



FIGURE 2-5 Inside a telecommunications closet.

Two types of labeling are commonly used in networks:

- **Port labeling:** When labeling your equipment and cabling, it is important to develop a standardized format that contains all the information you will need at a later time. Remember that your facility will eventually have a lot of equipment and cables, and being able to easily identify them will be of great benefit to the technical staff. Also make sure the labels correspond to your drawings.
- **System labeling:** System labels are important because they ensure that the technical staff are referencing the same system. A large facility will eventually have many systems doing similar tasks, and being able to identify the correct system will simplify your work.

Creating proper *rack diagrams* is also an extremely important part of documentation and rack management for a system. Racks are used in a multitude of places in network systems. Racks could be installed in closets, or there could be many racks in a data center. You can also expect to have server rack frames with air blowing over the devices for cooling. Racks must be securely installed and grounded. Rack types vary for sites, but the most common are 19-inch rack frames. There also two-post racks used for smaller telecommunication equipment. Four-post racks are typically used for servers.

A data center typically has locks on some racks for security reasons, and these racks should be located in a well-monitored area. There are also "hot" and "cold" aisles. The hot air from the equipment in the hot aisles is blown out of the racks and recirculates to the ceiling ducts. In the cold aisles, the air is pulled through the equipment by fans within that equipment.

Section 2-2 Review

This section covers the following Network+ exam objectives.

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

This section introduces some of the categories of UTP (unshielded twisted-pair) cabling.

1.7 Explain basic corporate and datacenter network architecture.

This section introduces concepts related to infrastructure and the network backbone.

Test Your Knowledge

1. What is the overall length limitation of a UTP cable run from a telecommunications closet to a networking device in a work area?

   a. 10 meters

   b. 100 meters

   c. 10,000 meters

   d. 100,000 meters

2. True or false: The six subsystems of a structured cabling system are as follows:

   - Building entrance
   - Equipment room
   - Backbone cabling
   - Telecommunications closet
   - Vertical cabling
   - Work area

   False

3. Horizontal cabling consists of which of the following basic blocks? (Select two.)

   a. Switch or hub

   b. Routers

   c. Backbone cabling

   d. Patch panel

2-3 TWISTED-PAIR CABLE

UTP cable is an important physical layer component in modern computer networks. Many networks incorporate CAT6 in their installations. The section lists the CAT6 specifications, but the fundamental issues of CAT6 are the same as for CAT5e. Many networks are already wired with CAT5/5e, and some new network connections are now installing CAT6 and higher. CAT6 provides improved network performance, and students should understand this.

The main difference between CAT5e and CAT6 has to do with transmission performance. The bandwidth increases from 100MHz with CAT5e to 200MHz with CAT6, and the CAT6 specifications provide for better noise performance to enable increased data rates. Most new installations specify CAT6 cable; it is important to use the best cable available for an installation, as long as the additional cost is justified. CAT6 specifications require that patch cables be precisely manufactured to maintain CAT6 performance. Also, CAT6 connectors look the same as CAT5e connectors, but these connectors have significantly different performance specifications. This section describes the steps for terminating both CAT6 and CAT5e.

A good task would be for students to prepare a report on CAT6/6a/7/8 cable, connectors, hardware, and testing. This would be a way for students to become aware of the latest developments related to twisted-pair cable.

Unshielded Twisted-Pair Cable

UTP
Unshielded twisted-pair

Unshielded twisted-pair (**UTP**) cable plays an important role in computer networking. The most common twisted-pair standards used for computer networking today are Category 6 (CAT6), Category 6a (CAT6a), and Category 5e (CAT5e). CAT6 cable provides data rates up to 1000Mbps over a maximum distance of 100 meters. CAT6a is an improved version of CAT6 that supports 10Gbps (10GBASE-T) Ethernet.

CAT5e cable is an enhanced version of CAT5 that provides improved performance. CAT6 provides even better performance and bandwidth of 250MHz. CAT5/5e twisted-pair cable contains four color-coded pairs of 24-gauge wires terminated with an RJ-45 connector. Figure 2-6 shows an example of a CAT5e cable terminated with an RJ-45 modular plug. CAT6 twisted-pair cable also contains four color-coded wires, but the wire gauge is 23AWG. CAT6 cable has a stiffer feel than CAT5e.

The precise manner in which the twist of CAT6/5e/5 cable is maintained, even at the terminations, provides a significant increase in signal transmission performance. CAT5/5e standards allow 0.5 inch of untwisted cable pair at the termination. CAT6 has an even tighter requirement and allows for only 0.375 inch of untwisted cable at the termination. The termination is the point where the cable is connected to terminals in a modular plug, jack, or patch panel.

CAT8/7/6/5e/5 twisted-pair cable contains four twisted wire pairs, for a total of eight wires. In twisted-pair cable, none of the wires in the wire pairs are connected to ground. The signals on the wires are set up for a high (+) and low (–) signal line. The (+) indicates that the phase relationship of the signal on the wire is positive,

and the (–) indicates that the phase of the signal on the wire is negative; both signals are relative to a virtual ground. This is called a **balanced mode** of operation, and the balance of the two wire pairs helps maintain the required level of performance in terms of crosstalk and noise rejection.

Balanced Mode
A mode in which neither wire in a wire pair connects to ground

Table 2-2 lists the various categories of twisted-pair cable defined by the TIA/EIA 568-B standard. The table includes an application description and minimum bandwidth for each category.

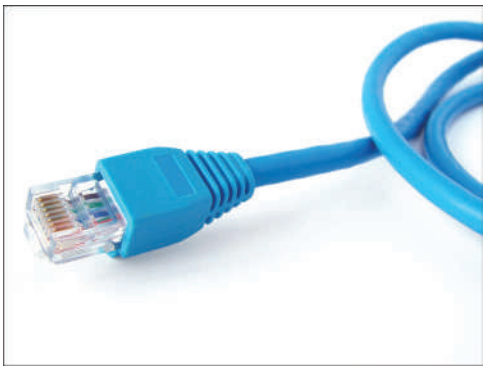


FIGURE 2-6 An example of an RJ-45 modular plug (Denis and Yulia Pogostins/Shutterstock).

TABLE 2-2 **Categories for Twisted-Pair Cable, Based on TIA/EIA 568-B**

Category	Description	Bandwidth/Data Rate
Category 3 (CAT3)	Telephone installations, Class C networks	Up to 16Mbps
Category 5 (CAT5)	Computer networks, Class D networks	Up to 100MHz/100Mbps, 100 meter length
Enhanced CAT5 (CAT5e)	Computer networks	100MHz/1000Mbps applications with improved noise performance in full-duplex mode
Category 6 (CAT6)	Higher-speed computers	Over 250MHz networks, Class E/1000Mbps networks CAT6 supports 10Gbps but at distances shorter than 100 meters
Category 6a (CAT6a)	Increased bandwidth	Over 500MHz networks, Class EA/10Gbps networks
Category 7 (CAT7)	International Organization for Standardization (ISO) standard, not an TIA/EIA standard	Up to 600MHz speed, computer networks, Class F/10Gbps networks
Category 7a (CAT7a)	ISO standard, not an TIA/EIA standard	Up to 1000MHz speed, computer networks, Class FA/10Gbps networks
Category 8 (CAT8)	Shielded UTP capable of competing with fiber optics	2000MHz /40Gbps

CAT1 and CAT2 cable specifications are not defined in the TIA/EIA 568-B standard. The first category specification is for CAT3, although CAT3 has been replaced with CAT5e or better. CAT4 is not listed in the table because the category was removed from the TIA/EIA 568-B standard as its data capacity specification is outdated. The Category 5 cable standard was established in 1991, and many computer networks are still using older CAT5 cables. Certified CAT5 cabling works well in both Ethernet and Fast Ethernet networking environments that run 10Mbps Ethernet and 100Mbps Fast Ethernet data rates. Note that the term **Fast Ethernet** is used to describe the 100Mbps data rate for Ethernet networks.

Fast Ethernet
An Ethernet system operating at 100Mbps

In some cases, users on networks experience **network congestion**, or **bottlenecking**, of data due to increased file transfer sizes and limited network bandwidth. These terms describe excessive data traffic that is slowing down computer communications even in Fast Ethernet networks. Basically, the demands on the network exceed the performance capabilities of the CAT5 cable. In fact, CAT 5 cabling is no longer recommended. The slowdown of data is of major concern in computer networks. Slowdowns mean file access time is delayed, productivity is affected, and the time required to complete a task is increased. A slowdown in a network could cost a company money. Can you imagine the consequences if a slowdown in your network caused a delay in the company's billing?

Network Congestion
A slowdown in network data traffic movement

Bottlenecking
Another term for network congestion

TIA/EIA ratified the CAT5e cabling specification in 1999 to address the continuing need for greater data-handling capacity in computer networks. The enhanced CAT5 cable (CAT5e) provides an improvement in cable performance, and if all components of a cable installation are done according to specification, CAT5e supports full-duplex **Gigabit Ethernet** (1000Mbps Ethernet) using all four wire pairs. **Full-duplex** means that the computer system can transmit and receive at the same time. TIA/EIA ratified the CAT6 cabling specification in June 2002. CAT6 cable provides even better performance and 250MHz of bandwidth, and it maintains backward compatibility with CAT5/5e. CAT6 can support 10Gbps data rates over a distance of less than 100 meters. **CAT6a** supports 10Gbps data rates up to 100 meters. The 10Gbps standard over copper is called **10GBASE-T**.

Gigabit Ethernet
1000Mbps Ethernet

Full-duplex
Refers to the capability to transmit and receive at the same time

CAT6a
A UTP cable standard that supports 10Gbps data rates over a distance of up to 100 meters

10GBASE-T
Twisted-pair copper capable of 10Gbps

Shielded Twisted-Pair Cable

In some applications, a wire screen or metal foil shield is placed around twisted-pair cable. Cable with the addition of a shield is called **STP** (shielded twisted-pair) cable. The addition of this shield reduces the potential for electromagnetic interference (**EMI**) as long as the shield is grounded. EMI originates from devices such as motors and power lines and from some lighting devices, such as fluorescent lights.

The shield on the twisted-pair cable does not eliminate all potentially interfering noise (EMI), but it does greatly reduce noise interference. There is an active debate in the networking community about whether UTP or STP is superior. It is important to note that the objective of both types of cables is to successfully transport data from the telecommunications closet to the work area. Industry testing on STP cable has shown that the addition of a shield does increase the usable bandwidth of the cable by increasing the noise rejection between each of the wire pairs. However, tests have shown that there is not a significant advantage to placing a shield over a properly installed four-pair 100-ohm UTP cable. In addition, STP is more

STP
Shielded twisted-pair, which has an added shield to reduce the potential for EMI

EMI
Electromagnetic interference, which originates from devices such as motors and power lines and from some lighting devices, such as fluorescent lights

expensive, and the increased cost may not justify the benefits. For now, most manufacturers are recommending the use of UTP cable for cabling computer networks except in very noisy environments.

Category 7 (CAT7) and Category 8 (CAT8) are both shielded twisted-pair cables. Because they are shielded, they are able to operate at higher bandwidth or frequency. CAT7 can operate up to 600MHz, and can operate up to 1000MHz (that is, 1GHz). Both are capable of supporting 10Gbps up to 100 meters. CAT8 can operate over a operate up to 2000Mhz (that is, 2GHz) and is capable of supporting up to 40Gbps over a distance of 30 meters. This is because copper cabling attenuation in twisted-pair significantly increases with higher frequency. Therefore, the effective length of CAT8 has been reduced and optimized to 30 meters to reduce attenuation. The physical characteristics, cost, and speed of CAT7 and CAT8 make these options suitable for data center cabling.

A common question when selecting twisted-pair cabling is whether to use PVC or plenum. PVC (polyvinyl chloride) is commonly used as a cable insulation or jacket that consists of chemical compounds that emit toxic smoke when burned. Plenum-rated cable has special coating that emits less toxic smoke when burned. It is important to check your local regulations to make sure you install the proper cabling.

Section 2-3 Review

This section covers the following Network+ exam objectives.

1.3 Summarize the types of cables and connectors and explain this is the appropriate type for a solution.

This section presents the various types of UTP cabling used in computer networking.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section addresses the concept of duplex operation.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section examines the properties of shielded and unshielded twisted-pair cables.

Test Your Knowledge

1. What is the data rate for Fast Ethernet?
   a. 10Mbps
   b. 100Mbps
   c. 1000Mbps
   d. 10Kbps
   e. None of these answers are correct.

2. What type of cable is currently recommended for LAN work areas?

   a. STP
   b. CAT6 STP
   c. CAT 5e UTP
   d. CAT6 UTP
   e. CAT5 UTP

3. What is the benefit of shielded twisted-pair cable?

   a. Ease of installation
   b. Excellent EMI protection
   c. Comparatively inexpensive
   d. Preferred by the industry for all installations
   e. None of these answers are correct.

2-4 TERMINATING TWISTED-PAIR CABLES

This section introduces techniques for terminating high-performance UTP cables. It presents important concepts such as the wiring schemes for T568A and T568B. It also discusses straight-through and crossover cables. Students should understand the importance of properly aligning the TX and RX pairs and the link light. The section concludes with the steps for terminating twisted-pair cable with RJ-45 connectors.

This section introduces techniques for terminating high-performance UTP cables. The standards TIA/EIA 568-B.2 and 568-B.2-1 define the specifications for the copper cabling hardware and copper termination. These standards specify cabling components, transmission media, system models, and the measurement procedures needed for verification of balanced twisted-pair cabling.

T568A
Wire color guidelines specified in the TIA/EIA 568-A standard

T568B
Wire color guidelines specified in the TIA/EIA 568-B standard

Color Map
The specification of which wire color connects to each pin on a connector

Within the TIA/EIA 568-B standard are the wiring guidelines **T568A** and **T568B**, which specify the color of wire that connects to each pin on a connector. The specification of the wire color that connects to each pin is called a **color map**. Table 2-3 shows the color maps specified by the T568A and T568B wiring guidelines.

TABLE 2-3 **The Wiring Color Schemes for T568A and T568B**

Pin Number	T568A Wire Color	T568B Wire Color
1	White–green	White–orange
2	Green	Orange
3	White–orange	White–green
4	Blue	Blue

Pin Number	T568A Wire Color	T568B Wire Color
5	White–blue	White–blue
6	Orange	Green
7	White–brown	White–brown
8	Brown	Brown

Figure 2-7(a) shows the placement of the wire pairs in an RJ-45 modular plug for the T568A standard; Figure 2-7(b) shows the placement of the wire pairs in an RJ-45 modular plug for the T568B standard. The pin numbers for the RJ-45 modular plug are shown at the top of the figure, and a wire color table is provided for reference. In the T568A wire color scheme, as shown in Figure 2-7(a), a white–green wire connects to pin 1, the wire color green connects to pin 2, the wire color connected to pin 3 is white–orange, and so on. Similar information is provided in Figure 2-7(b) for the T568B wiring standard. The color of the wire connected to pin 1 is white–orange, pin 2 is orange, pin 3 is white–green, and so on. This information is also shown in Table 2-3.

What is the difference between T568A and T568B? Basically, these are just two different manufacturer standards used to wire modular connector hardware. There is not a performance improvement with either one; each just specifies a particular color order. The industry tends to favor the T568A wiring order; however, either order can be used, as long as it is maintained throughout the network.

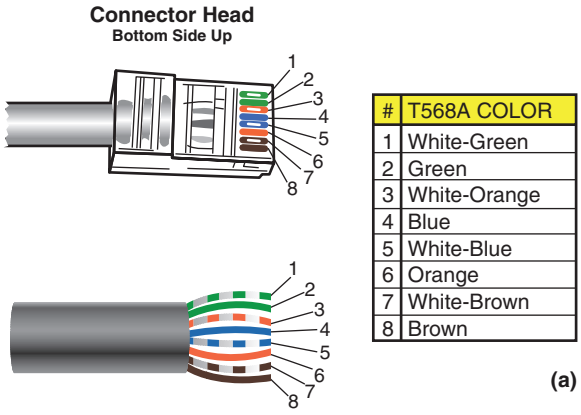
Note

For the Network+ exam, you should be able to describe the difference between the T568A and T568B wire color order. Also make sure you know what wire color configuration you are using in a network (T568A or T568B) and be sure you can specify hardware that is compatible with your selected color scheme.

Any incorrect pinout in either T568A or T568B can lead to a nonfunctioning cable.

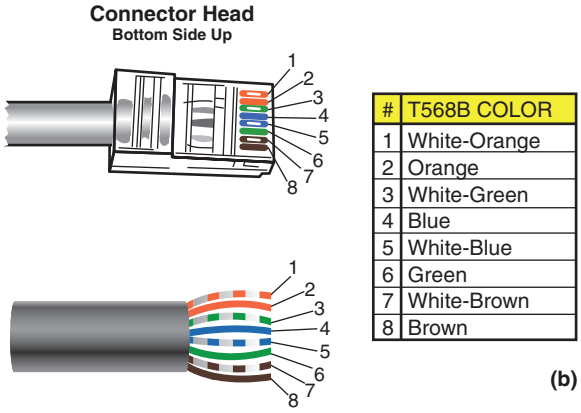
Computer Communication

As mentioned in Section 2-2, "Structured Cabling," CAT8/7/6/5e cable contains four twisted wire pairs. Figure 2-8 provides a picture of the four wire pairs. Figure 2-9 shows the signals and pin number assignments for an RJ-45 plug for CAT5e. Notice in Figure 2-9 that the transmit signals are marked with (+) and (–). The receive (+) and (–) signals are also marked in the same way. The (+) and (–) diagram symbols are typically used to indicate the positive and negative sides of a balanced wire pair. Recall from Section 2-3, "Twisted-Pair Cable," that in a balanced mode of operation, neither signal line is at ground.



#	T568A COLOR
1	White-Green
2	Green
3	White-Orange
4	Blue
5	White-Blue
6	Orange
7	White-Brown
8	Brown

(a)



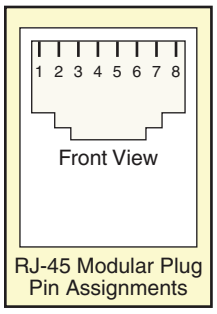
#	T568B COLOR
1	White-Orange
2	Orange
3	White-Green
4	Blue
5	White-Blue
6	Green
7	White-Brown
8	Brown

(b)

FIGURE 2-7 (a) The wiring of an RJ-45 connector and the wire color codes for the T568A standard; (b) the wiring of an RJ-45 connector and the wire color codes for the T568B standard (courtesy of StarTech.com).



FIGURE 2-8 The four wire pairs of CAT6/CAT5e.



Pin No.	Function
Pin 1	Transmit Out +
Pin 2	Transmit Out –
Pin 3	Receive In +
Pin 4	No Connection
Pin 5	No Connection
Pin 6	Receive In –
Pin 7	No Connection
Pin 8	No Connection

FIGURE 2-9 The pin assignments and signal names for an RJ-45 modular plug with CAT5e.

For computers to communicate in a LAN, the transmit and receive pairs must be properly aligned. This means the transmit (**TX**) (+) and (–) pins must connect to the receive (**RX**) (+) and (–) pins, as shown in Figure 2-10. Notice in Figure 2-10 that pins 1–2 of device A connect to pins 3–6 of device B. Pins 1–2 of device B connect to pins 3–6 of device A. This configuration is always valid when the data rates are 10Mbps or 100Mbps.

TX
Abbreviation for transmit

RX
Abbreviation for receive

In a LAN, the proper alignment of the transmit and receive pairs is managed by a switch or hub; it is not typically managed in the cable. Remember that in a star topology, all network communication travels through a switch or hub. An "X" or "uplink" on a switch or hub input port indicates a cross-connected input. This means that transmit and receive pairs are internally swapped to maintain proper signal alignment of the TX and RX pairs. Even if "X" or "uplink" is missing, the switch or hub still properly aligns the TX and RX wire pairs. There is an exception to this on many switches and hubs: Some switches and hubs have an input port that can be selected to be "straight" or "crossed." These ports are typically used in uplink applications when connecting a switch or hub to another switch or hub. If a device has a cross-connected port, a straight-through cable is used because the device is providing the alignment. Just remember that proper alignment of the transmit and receive pair must be maintained in order for the computers to communicate. Also keep in mind that if there is a TX/RX reversal of the wires, you will not see a link light.

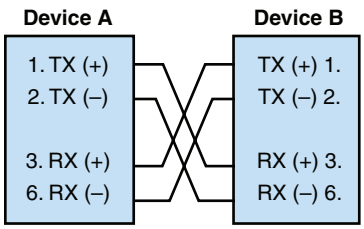


FIGURE 2-10 The proper alignment of the transmit and receive pairs in a CAT6/5e data link operating at 10Mbps or 100Mbps.

There is a difference with the signal names for the UTP cable when operating at 1Gbps and 10Gbps. At these higher data rates, the use of all four wire pairs is required, and the data is bidirectional, which means the same wire pairs are used for both transmitting and receiving data. Figure 2-11 shows the pin assignments and signal names.

Pin	1000Mbps and 10Gbps Color (T568A)	10/100 Mbps	1000Mbps and 10Gbps
1	green/white	TX+	BI_DA+
2	green	TX–	BI_DA–
3	orange/white	RX+	
4	blue	–	BI_DC+
5	blue/white	–	BI_DC–
6	orange	RX–	BI_DB–
7	brown/white	–	BI_DD+
8	brown	–	BI_DD–

(a) The pin assignments and signal names for 1Gbps and 10Gbps (T568A).

Pin	1000Mbps and 10Gbps Color (T568B)	10/100 Mbps Signal	1000Mbps Signal
1	orange/white	TX+	BI_DA+
2	orange	TX–	BI_DA–
3	green/white	RX+	BI_DB+
4	blue	–	BI_DC+
5	blue/white	–	BI_DC–
6	green	RX–	BI_DB–
7	brown/white	–	BI_DD+
8	brown	–	BI_DD–

(b) The pin assignments and signal names for 1Gbps and 10Gbps (T568B).

FIGURE 2-11 The pin assignments and signal names for 1Gbps and 10Gbps (T568A and T568B).

Straight-Through and Crossover Patch Cables

Category 8/7/6/5e twisted-pair cables are used to connect networking components to each other in a network. These cables are commonly called *patch cables.* This section demonstrates a technique for terminating CAT 8/7/6/5e cables with RJ-45 modular plugs for two different configurations of patch cables: a straight-through cable and a crossover cable. In a **straight-through cable**, the four wire pairs connect to the same pin numbers on each end of the cable. For example, pin 1 on one end connects to pin 1 on the other end. Figure 2-12 shows an example of the **wiremap** for a straight-through cable. A wiremap is a graphical or text description of the wire connections from pin to pin for a cable under test. Notice in Figure 2-12 that the transmit and receive pairs connect to the same connector pin numbers at each end of the cable—hence the name *straight,* or *straight-through,* cable.

Straight-Through Cable
A cable in which the wire pairs in the cable connect to the same pin numbers on each end

Wiremap
A graphical or text description of the wire connections from pin to pin

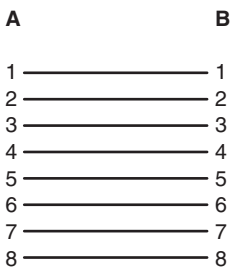


FIGURE 2-12 A wiremap for a straight-through cable.

In some applications in 10/100Mbps data links, it is necessary to construct a cable where the transmit and receive wire pairs are reversed in the cable rather than reversed by a switch or a hub. This cable configuration is called a **crossover cable**, which means the transmit pair of device A connects to the receive pair of device B, and the transmit pair of B connects to the receive pair of A. Figure 2-13 shows the wiremap for a crossover cable.

Crossover Cable
A cable in which the transmit and receive wire pairs are crossed

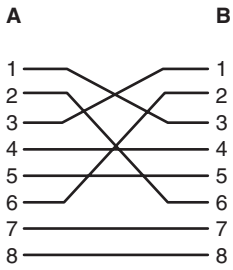


FIGURE 2-13 The wiremap for crossover cable 10/100Mbps links.

Note

The crossover cable diagram shown in Figure 2-13 is for 10/100Mbps. A Gigabit Ethernet crossover cable requires that all four wire pairs be crossed. Although this is possible, it is not practical to make a Gigabit Ethernet crossover cable because of the distance limit on untwisted wire.

Terminating CAT6 Horizontal Link Cable This section presents the steps required for terminating a CAT6 cable using the AMP SL series termination procedure, AMP SL tool, CAT6 cable, and AMP SL Series AMP-TWIST-6S Category 6 modular jacks. In this example, an RJ-45 jack is used to terminate each end of the cable. One end connects to a wall plate in the network work area. The other end terminates into a CAT6 RJ-45 patch panel, which is typically located in a LAN network closet. It is important to document your cable patching using some form of patch management. It is much easier to look up your documentation than to physically go to the site to verify the configuration.

The technical specifications and assembly requirements are more stringent with CAT6 than with earlier cable categories. Therefore, you must take more care when terminating a CAT6 cable. However, advancements in the tools and connectors have actually made it easier to terminate CAT6 compared to using the old punchdown tools.

The steps for terminating the CAT6 horizontal link cables are as follows:

1. Inspect the cable for any damage that might have occurred during installation. Examples of damage to look for include nicked or cut wires and possible stretching of the cable.
2. At the work area outlet end, add about 1 foot extra and cut the wire. (It is good to leave a little extra in case you make an error in installation and have to redo the termination. Remember that you can't splice a CAT6 cable.) Then

coil the extra cable and insert it in the receptacle box. At the distribution end, route the cable and create a *slack loop*—extra cable looped at the distribution end that is used if the equipment must be moved. In cases where you are having the cable pulled through ductwork or conduit by an installer, make sure to specify that extra cable length will be run. The amount will vary for each installation. In general, allow 5 meters extra in the telecommunications closet and 5 meters extra in the work area.

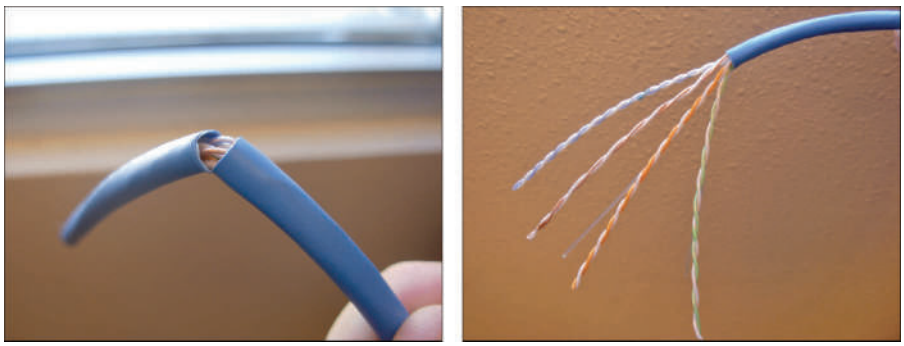
3. Place a bend-limiting strain-relief boot on the cable, as shown in Figure 2-14(a). (This boot is used in the last step to secure the RJ-45 jack.) Then strip approximately 3 inches of cable jacket from the UTP cable, as shown in Figure 2-14(b). Be careful not to nick or cut the wires as you do this.



(a) (b)

FIGURE 2-14 (a) Placing a bend-limiting strain-relief boot on the cable and (b) stripping off 3 inches of jacket from the UTP cable.

4. Remove the jacket from the UTP cable. Bend the cable at the cut, as shown in Figure 2-15(a), and remove the jacket to expose the four wire pairs, as shown in Figure 2-15(b).



(a) (b)

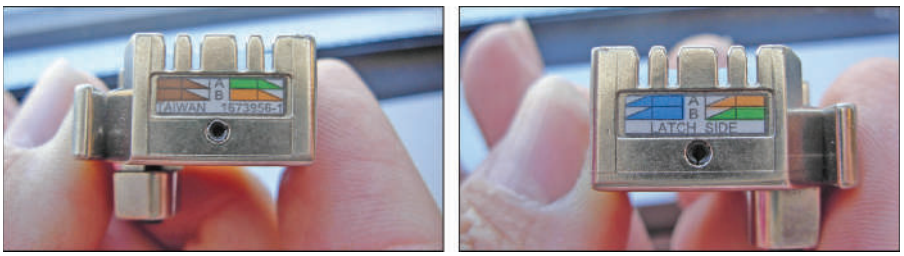
FIGURE 2-15 (a) Separating the cut jacket from the wire pairs and (b) removing the jacket and exposing the four wire pairs.

5. Cut the plastic pull line and the string as shown in Figure 2-16(a). The plastic line adds strength to the cable for pulling, and the string is used to remove extra cable jacket, as needed. Place a lacing fixture on the cable, as shown in Figure 2-16(b), and sort the wires in the correct color order (according to either T568A or T668B) so that you can match up the sorted wire pairs with colors provided on the lacing fixture for T568A and T568B, as shown in Figure 2-17.



(a) (b)

FIGURE 2-16 (a) Removing the plastic pull line and (b) placing the lacing tool on the cable with the color-sorted cable pairs.



(a) (b)

FIGURE 2-17 The sides of the lacing tool, showing the T568A and T568B wire color connections.

6. Place the wires in the slots of the lacing tool, as shown in Figure 2-18, ensuring that the wire colors are in the order (T568A/T568B) displayed on the sides of the lacing tool.

7. Align an RJ-45 jack with the lacing fixture, as shown in Figure 2-19(a). The RJ-45 jack must be properly aligned with the wires on the lacing fixture to maintain proper color order. Figure 2-19(b) provides a close-up picture of the AMP SL series AMP-TWIST-6S modular jack. This picture shows the locations of the displacement connectors on the modulator jack.

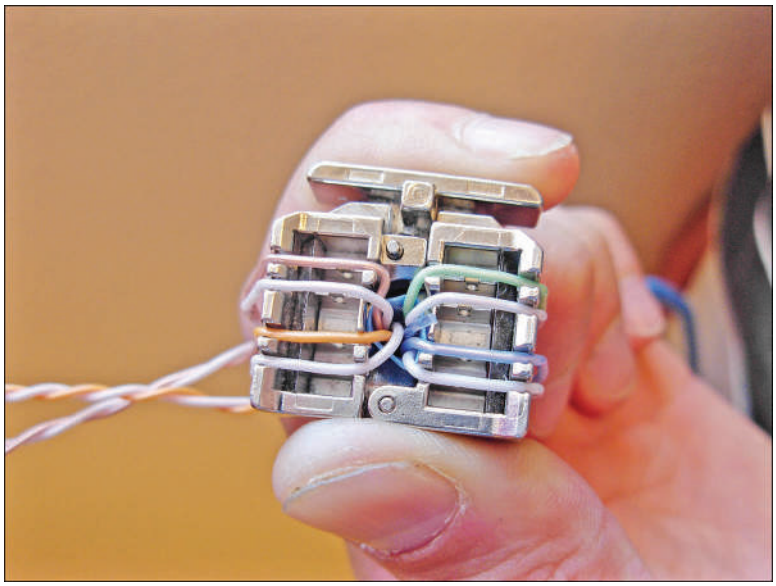


FIGURE 2-18 The routed cable wires on the lacing tool. The wire order shown here is T568B.

8. Insert the RJ-45 modular jack into the AMP SL tool as shown in Figure 2-20(a) and then insert the RJ-45 jack into the AMP SL tool as shown in Figure 2-20(b). Press the wires into the eight displacement connectors on the RJ-45 jack using the AMP SL tool, as shown in Figure 2-20(c). This technique enables you to maintain the pair twist right up to the point of termination. In fact, the untwisted-pair length is less than or equal to 0.25 inch.

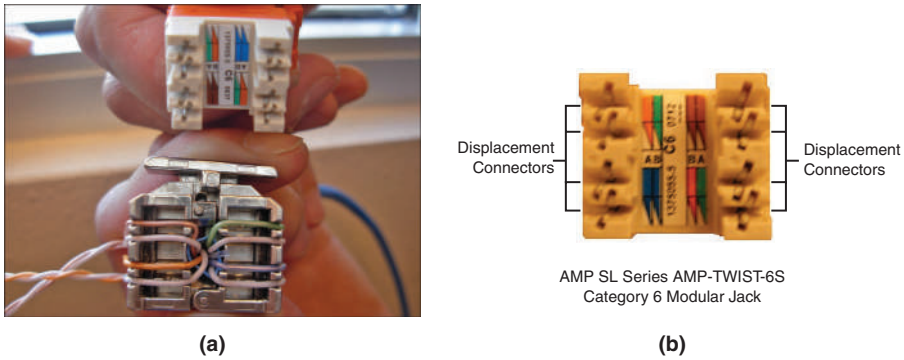
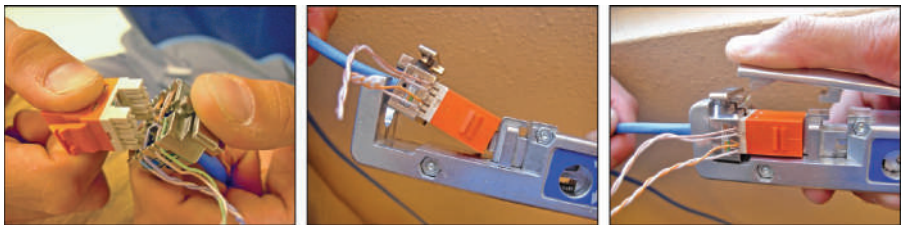


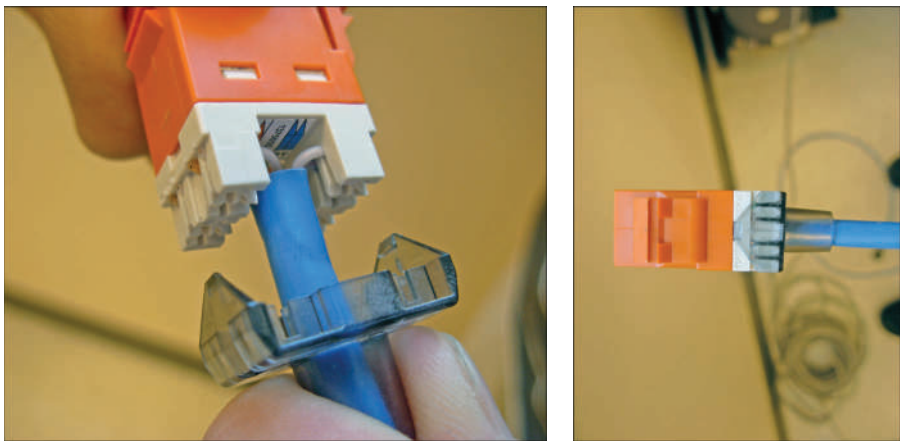
FIGURE 2-19 (a) Aligning the RJ-45 jack and the lacing fixture and (b) a close-up view of the AMP-TWIST-6S CAT6 modular jack.



(a) (b) (c)

FIGURE 2-20 (a) Aligning the RJ-45 jack with the lacing tool, (b) inserting the RJ-45 jack and the lacing tool into the AMP SL tool, and (c) using the AMP SL tool to crimp the RJ-45 jack onto the eight displacement connectors and cut the wires.

9. Connect the bend-limiting strain-relief boot to the RJ-45 jack as shown in Figure 2-21(a). Figure 2-21(b) shows the completed termination.



(a) Connecting the bend-limiting strain relief boot to the RJ-45 jack. (b) The finished RJ-45 jack termination.

FIGURE 2-21 (a) Connecting the bend-limiting strain-relief boot to the RJ-45 jack and (b) the finished RJ-45 termination.

Assembling the Straight-Through CAT5e/5 Patch Cable This section presents a technique for assembling a straight-through CAT5e/5 patch cable. In a straight-through patch cable, the wire pairs in the cable connect to the same pin numbers on each end of the CAT5e/5 patch cable. Figure 2-22 shows a CAT5e patch cable with RJ-45 modular plugs.

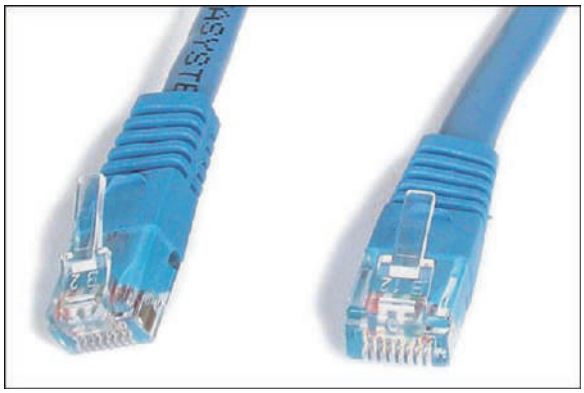


FIGURE 2-22 CAT5e patch cable with RJ-45 modular plugs (courtesy of StarTech.com).

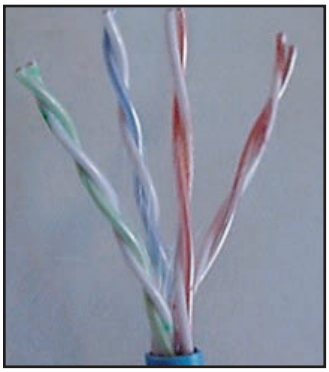
The steps for making a straight-through patch cable are as follows:

1. Inspect the cable for any damage that might have occurred during installation, such as nicked or cut wires or stretching of the cable.
2. Measure the cable to length, add about 6 inches extra, and cut the wire. (It is good to have a little extra in case you make an error in installation and have to redo the termination. Remember that you can't splice CAT5e/5 twisted-pair cable.)
3. Use a cable stripper to strip approximately 0.75 inch of the cable jacket from the end of the cable. (Figure 2-23 illustrates how to use a cable stripper.) Remove the cable insulation by rotating the insulation stripper around the wire until the wire jacket is loose and easily removable. (Note that these cable strippers must be periodically adjusted so that the blade cuts through the outer insulation only. If the blades are set too deep, they will nick the wires, and the process must be repeated after the damaged portion of the cable is cut away. You need to be careful to not nick the insulation.)

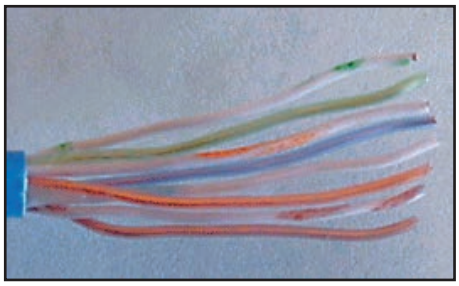


FIGURE 2-23 An example of using the cable jacket stripper to remove the insulation.

4. Sort the wire pairs so that they fit into the connector and orient the wire in the proper order for either T568A or T568B, as shown in Figures 2-24(a) and 2-24(b). Be careful to avoid creating a split pair connection (that is, using a wire from one pair and a wire from another pair to make a connection). A split pair connection may create interference and crosstalk problems, thus preventing the cable from passing a certification test. This problem is discussed in Section 2-5, "Cable Testing and Certification."



(a)



(b)

FIGURE 2-24 (a) Separating wire pairs and (b) orienting the wires.

5. Clip the wires so that they are even and insert the wires onto the RJ-45 modular plug, as shown in Figure 2-25.



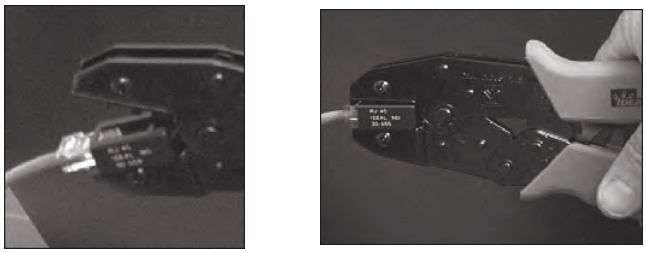
FIGURE 2-25 The clipped wires, ready for insertion into the RJ-45 plug.

6. Push the wires into the connector until you can see the end of each wire through the clear end of the connector. The wires are visible through the plastic connector, as shown in Figure 2-26. Verify that the wire order is correct.
7. Use a crimping tool (also called a crimper) to crimp the wires onto the RJ-45 plug. Insert the RJ-45 plug into the crimping tool until it stops, as shown in Figure 2-27(a). Squeeze the handle on the crimping tool all the way until it clicks and releases, as shown in Figure 2-27(b), to crimp the wire onto the insulation displacement connector pins on the RJ-45 jack.
8. Repeat steps 1–7 for the other end of the twisted-pair cable.

The next step is to test the cable, as discussed in the next section.



FIGURE 2-26 Wires pushed into the RJ-45 plug.



(a) (b)

FIGURE 2-27 (a) Inserting the connector and (b) crimping the connector.

Section 2-4 Review

This section covers the following Network+ exam objectives.

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

The termination standards for UTP cable are presented in this section.

1.7 Explain basic corporate and datacenter network architecture.

Remember that you can't splice a CAT6 cable. At the distribution end, you must route the cable and create a slack loop—extra cable looped at the distribution end that is used if the equipment must be moved.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

In some applications in 10/100Mbps data links, it is necessary to construct a cable in which the transmit and receive wire pairs are reversed in the cable rather than by the switch or the hub. This cable configuration is called a crossover cable, which means the transmit pair of device A connects to the

receive pair of device B, and the transmit pair of B connects to the receive pair of A.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section presents the pin assignments and the signal names for wiring twisted-pair cables. Figure 2-10 shows the proper alignment of the transmit and receive pairs. This is an important concept when configuring cable. This section also covers the concept of a split pair.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

The concept of a crossover cable is presented.

5.3 Given a scenario, use the appropriate network software tools and commands.

At the distribution end, you must route the cable and create a slack loop—extra cable looped at the distribution end that is used if the equipment must be moved.

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

This section discusses a split-pair connection that can create interference and crosstalk problems, thus preventing the cable from passing a certification test.

Test Your Knowledge

1. True or false: The following table shows a color map and pin numbers for T568A.

Pin Number	Wire Color
1	White–green
2	Blue
3	White–orange
4	Green
5	White–blue
6	Orange
7	White–brown
8	Brown

False

2. True or false: The following table shows a color map and pin numbers for T568B.

Pin Number	Wire Color
1	White–orange
2	Orange
3	White–green

Pin Number	Wire Color
4	Blue
5	White–blue
6	Green
7	White–brown
8	Brown

True

3. How many wires are in a CAT5e/6 twisted-pair cable?

   a. 12 wires

   b. 8 wires

   c. 4 wires

   d. 6 wires

2-5 CABLE TESTING AND CERTIFICATION

Link
The point from one cable termination to another

Full Channel
All the link elements from a wall plate to a hub or switch

Attenuation
Also called insertion loss, the amount of loss in signal strength as it propagates down a wire or fiber strand

Near-End Crosstalk (NEXT)
A measure of the level of crosstalk or signal coupling within a cable, with a high NEXT (dB) value being desirable

This section discusses issues and specifications for certifying CAT6 cable. It also examines the parameters that are defined by the TIA/EIA 568-B channel specifications. The specifications presented define the basis for most twisted-pair certification. CAT7 and CAT8 promise improved performance capability, and a good task would be to ask students what is unique about certifying CAT7 or CAT8 cable. Students are likely to say that the cable and the connectors have improved performance specifications—and this is correct. This section concludes with examples of conducting CAT6 cable tests.

The need for increased data rates is pushing the technology of twisted-pair cable to even greater performance requirements and placing greater demands on accurate testing of the cable infrastructure. Twisted-pair copper cable now allows data speeds up to 40Gbps. The TIA/EIA 568-B standard defines the minimum cable specifications for twisted-pair categories.

The CAT8/7/6/5e designations are minimum performance measurements of the cables and the attached terminating hardware, such as RJ-45 plugs, jacks, and patch panels. The **link** (the point from one cable termination to another) and the **full channel** (which consists of all the link elements from the hub or switch to the wall plate) must satisfy minimum **attenuation** loss and **near-end crosstalk (NEXT)** for a minimum frequency of 100MHz. Figure 2-28 provides a graphical representation of the link and the full channel. Table 2-4 lists the CAT5e, CAT6, CAT6a, CAT7, CAT7a, and CAT8 TIA/EIA 568-B channel specifications for UTP cables.

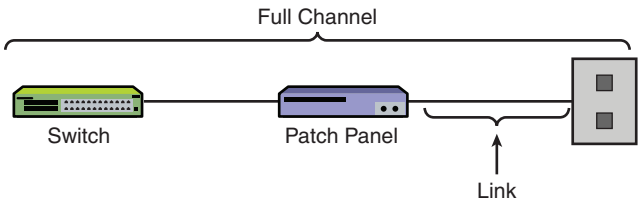


FIGURE 2-28 The link and channel areas for cable testing.

TABLE 2-4 **TIA/EIA 568-B CAT5e, CAT6, CAT6a, CAT7, CAT7a, and CAT8 Channel Specifications at 100 MHz**

Parameter	Category 5e	Category 6	Category 6a	Category 7/7a	Category 8
Class	Class D	Class E	Class EA	Class F/FA	Class I/II
Bandwidth	100MHz	250MHz	500MHz	600MHz/1000MHz	2000MHz
Insertion loss (dB)	24.0	21.3	20.9	20.8/20.3	6.5
NEXT loss (dB)	30.1	39.9	39.9	62.9/65.0	40.5
PSNEXT loss (dB)	27.1	37.1	37.1	59.9/62.0	37.1
ACR (dB)	6.1	18.6	18.6	42.1/46.1	39.74
PSACR (dB)	3.1	15.8	15.8	39.1/41.7	36.74
ACRF1 (ELFEXT) (dB)	17.4	23.3	23.3	44.4/47.4	32
PSELFEXT (dB)	14.4	20.3	20.3	41.1/44.4	32.0
Return loss (dB)	10.0	12.0	12.0	12.0/12.0	16.0
PANEXT loss (dB)*	n/s	n/s	60.0	n/s / 67.0	75
PSAACRF (dB)*	n/s	n/s	37.0	n/s / 52.0	61
TCL (dB)*	n/s	n/s	20.3	20.3/20.3	20
ELTCTL (dB)*	n/s	n/s	0.5	0/0	5
Propagation delay (ns)	548	548	548	548/548	176.8
Delay skew (ns)	50	50	50	30/30	50

*These parameters are discussed in Section 2-6, "10 Gigabit Ethernet over Copper."

The list that follows describes some of the parameters listed in Table 2-4:

- **Attenuation (insertion loss):** This parameter defines the amount of loss in signal strength as the signal propagates down the wire. It is caused by the resistance of the twisted-pair cable, the connectors, and leakage of the electrical signal through the cable insulation. Attenuation also increases with an increase in frequencies due to the inductance and capacitance of the cable. The cable test results will report a margin. Margin for attenuation (insertion loss) is defined as the difference between the measured value and the limit for the test. If the margin shows a negative value, the test has failed. A negative value is produced when the measured value is less than the limit. The limit for attenuation (insertion loss) at 100 MHz for CAT6 is 21.3 dB, for CAT6a is 20.9dB, for CAT7 is 20.8dB, for CAT7a is 20.3dB, and for CAT8 is 6.5dB.

It is also important to note that for UTP cables, there is a limit on how much the cable can be bent. This limit, called the *bend radius*, is four times the outer jacket diameter. Bends exceeding this limit can introduce attenuation loss.

- **NEXT:** When current travels in a wire, an electromagnetic field is created. This field can induce voltage in adjacent wires, resulting in crosstalk. **Crosstalk** is signal coupling within a cable. On analog land-line telephones, users could sometimes faintly hear another conversation; this is where the term crosstalk originated. Near-end crosstalk, or NEXT, is a measure of the level of crosstalk. The measurement of NEXT is called *near-end testing* because the receiver is more likely to pick up the crosstalk from the transmit to the receive wire pairs at the ends. The transmit signal levels at each end are strong, and the cable is more susceptible to crosstalk at this point. In addition, the receive signal levels have been attenuated due to normal cable path loss and are significantly weaker than the transmit signal. A high NEXT (dB) value is desirable.

Crosstalk
Signal coupling in a cable

- Figure 2-29 graphically depicts NEXT. The shaded areas show where the near-end crosstalk occurs. The margin is the difference between the measured value and the limit. A negative number means the measured value is less than the limit, and therefore the measurement fails. Crosstalk is more problematic at higher data rates (for example, 1Gbps, 10Gbps) than at lower rates. Figure 2-30 shows that CAT6 cable has a built-in separator to help minimize crosstalk among wire pairs. This separator is used to keep each wire pair a minimum distance from other wire pairs. This separator reduces crosstalk at higher frequencies and helps provide improved signal bandwidth; the cable therefore supports faster data rates. This separator also helps improve the far-end crosstalk. Note, however, that not all cable manufacturers use separators.

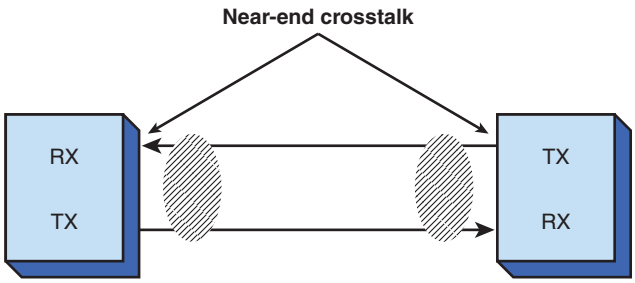


FIGURE 2-29 A graphical depiction of near-end crosstalk.

- **Power-sum NEXT (PSNEXT):** Enhanced twisted-pair cable must meet four-pair NEXT requirements, called PSNEXT testing. Basically, power-sum testing measures the total crosstalk of all cable pairs. This testing ensures that the cable can carry data traffic on all four pairs at the same time with minimal interference. A higher PSNEXT value is desirable because it indicates better cable performance.

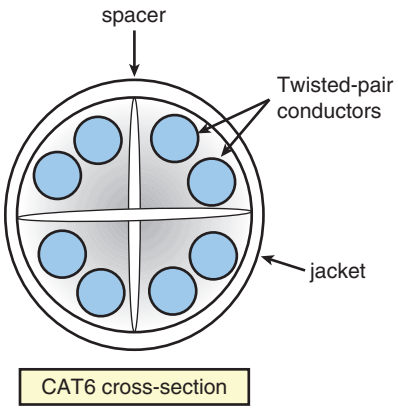


FIGURE 2-30 A cross-section of a CAT6 cable, showing the separator used to minimize crosstalk problems.

- **Equal-level FEXT (ELFEXT):** This measurement differs from NEXT in that it is for the far end of the cable. In addition, the ELFEXT measurement does not depend on the length of the cable. This is because ELFEXT is obtained by subtracting the attenuation value from the far-end crosstalk (FEXT) loss. Higher ELFEXT values (dB) indicate that the signals at the far end of the cable are larger than the crosstalk measured at the far end. A larger ELFEXT (dB) value is desirable. A poor ELFEXT value can result in data loss. Data loss prevention begins with properly terminating your cabling.
- **Power-sum ELFEXT (PSELFEXT):** PSELFEXT uses all four wire pairs to obtain a combined ELFEXT performance measurement. This value is the difference between the test signal level and the crosstalk measured at the far end of the cable. A higher PSELFEXT value indicates better cable performance.
- **Attenaution to Crosstalk Ratio (ACR):** This measurement compares the signal level from a transmitter at the far end to the crosstalk measured at the near end. A larger ACR value indicates that the cable has a greater data capacity and also indicates the cable's ability to handle a greater bandwidth. Essentially, it is a combined measurement of the quality of the cable. A higher ACR value (dB) is desirable.
- **Power-sum ACR (PSACR):** PSACR uses all four wire pairs to obtain the measure of the attenuation/crosstalk ratio. This is a measurement of the difference between PSNEXT and attenuation (insertion loss). The difference is measured in dB, and higher PSACR dB values indicate better cable performance.
- **Return loss:** An important twisted-pair cable measurement is return loss. This measurement provides a measure of the ratio of power transmitted into a cable to the amount of power returned or reflected. The signal reflection is due to impedance changes in the cable link and the impedance changes contributing to cable loss. Cables are not perfect, and there will always be some

reflection. Examples of the causes of impedance changes are non-uniformity in impedance throughout the cable, the diameter of the copper, cable handling, and dielectric differences. A low return loss value (dB) is desirable.

- **Propagation delay:** This is a measure of the amount of time it takes for a signal to propagate from one end of the cable to the other. The delay of the signal is affected by the nominal velocity of propagation (NVP) of the cable. NVP is some percentage of the velocity of light and is dependent on the type of cable being tested. The typical delay value for CAT5/5e UTP cable is about 5.7 ns per meter. The TIA/EIA specification allows for 548 ns for the maximum 100 meter run for CAT5e, CAT6, CAT6a, CAT7, and CAT7a.
- **Delay skew:** This is a measure of the difference in arrival time between the fastest signal and the slowest signal in a UTP wire pair. It is critical in high-speed data transmission that the data on the wire pair arrives at the other end at the same time. If the wire lengths of different wire pairs are significantly different, the data on one wire will take longer to propagate along the wire and arrive at the receiver at a different time and potentially create distortion of the data and data packet loss. The wire pair with the shortest length typically has the least delay skew.

Note

The power-sum measurements are critical for high-speed data communication over UTP. It has also been shown that twisted-pair cable can handle Gigabit data rates over a distance up to 100 meters. However, the Gigabit data rate capability of twisted-pair requires the use of all four wire pairs in the cable, with each pair handling 250Mbps of data. The total bit rate is 4×250Mbps, or 1Gbps—hence the need to obtain the combined performance measurements of all four wire pairs.

Section 2-5 Review

This section covers the following Network+ exam objectives.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

As discussed in this section, a larger ACR indicates that the cable has a greater data capacity and also indicates the cable's ability to handle greater bandwidth.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section introduces some very important cable concepts. Make sure you have a good understanding of near-end crosstalk, far-end crosstalk, attenuation, and distance limitations.

Test Your Knowledge

1. True or false: A full-channel test involves testing all the link elements from the computer through the patch panel to the wall plate.

   False

2. True or false: NEXT stands for near-end crosstalk, and a low NEXT (dB) value is desirable.

   False

3. True or false: Signals travel in a cable at some percentage of the velocity of light. The term for this is *nominal velocity of propagation*.

   True

2-6 10 GIGABIT ETHERNET OVER COPPER

Even though CAT8 can deliver 40Gbps (40 Gigabit Ethernet), it is not widely adopted in the industry because network equipment is not available to deliver 40Gbps. 10Gbps is the maximum speed over twisted-pair that network equipment can deliver. 40Gbps is more typically available over fiber-ready interfaces. This section focuses on the widely used 10Gbps Ethernet over copper. The increase in the required bandwidth for transporting a Gigabit data transfer rate is placing increased demands on the copper cable as well as the hardware used for terminating the cable ends and for connecting to the networking equipment. Three improvements are required for transmitting the higher data bit rates over copper cabling:

- Improve the cable so it can carry greater bandwidth.
- Improve the electronics used to transmit and receive (recover) the data.
- Utilize improvements in both the cable and electronics to facilitate greater bandwidths and distances

Alien crosstalk (AXT), which is an important issue at higher data rates such as with 10GBASE-T, is unwanted signal coupling from one permanent link to another. Basically, it is the coupling of a signal from one four-pair cable to another four-pair cable. Cable manufacturers are starting to offer CAT6 and higher grades of twisted-pair cable with foil over each of the four wire pairs. The designation for this type of cable is foil twisted-pair (F/UTP). Students should investigate the latest UTP cabling improvements.

Ethernet over copper is available for 10Mbps (Ethernet), 100Mbps (Fast Ethernet), 1000Mbps (Gigabit Ethernet), 10Gbps (10 Gigabit Ethernet), and now 40Gbps (40 Gigabit Ethernet). The increase in the required bandwidth for transporting a 40Gbps data transfer rate is placing greater demands on copper cable as well as the

hardware used for terminating the cable ends and for connecting to the networking equipment. Three improvements are required for transmitting the higher data bit rates over copper cabling:

- Improve the cable so it can carry greater bandwidth
- Improve the electronics used to transmit and receive (recover) the data
- Utilize improvements in both the cable and electronics to facilitate greater bandwidths and distance

This section examines the changes in technology that are required to enable 10 Gigabit (10GBASE-T) data transmission over copper. It first presents an overview of 10 Gigabit Ethernet over copper. Then it examines the modifications required to the technical specs (CAT6a and CAT7/7a) for testing and certifying twisted-pair copper cable transporting 10 Gigabit data rates. Finally, this section examines how 10 Gigabit data is actually transmitted.

Overview

IEEE 802.3an-2006 10GBASE-T
The standard for 10Gbps

The standard for 10Gbps is **IEEE 802.3an-2006 10GBASE-T**. This standard was developed to support running 10Gbps data over twisted-pair cabling. It requires the bandwidth to be increased from 250MHz to 500MHz. In addition, this standard supports distances up to 100 meters. At one time, most people assumed that higher data rates would be limited to fiber optics. While that is still true for lengthy runs (over 100 meters), twisted-pair copper is finding a place in the horizontal runs from telecommunications closets to work areas.

Alien Crosstalk

Alien Crosstalk (AXT)
Unwanted signal coupling from one permanent link to another

PSANEXT
Power-sum alien near-end crosstalk

PSAACRF
Power-sum alien attenuation to crosstalk ratio

Alien crosstalk (AXT) is unwanted signal coupling from one permanent link to another; it is an important issue at higher data rates, such as with 10GBASE-T. Basically, AXT is the coupling of a signal from one four-pair cable to another four-pair cable. Figure 2-31 depicts the AXT from one four-pair cable to another four-pair cable. The other key measurements for 10GBASE-T are NEXT (PSANEXT), FEXT (PSAACRF), and return loss. **PSANEXT** (power-sum alien near-end crosstalk) and **PSAACRF** (power-sum alien attenuation to crosstalk ratio) are new measurements for NEXT and FEXT that incorporate measures for AXT. AXT is considered to be the main electrical limiting parameter for 10 Gigabit Ethernet. AXT causes disturbances in the neighboring cable. It is difficult for the electronics to cancel the AXT noise created; therefore, new cables have been developed to support 10Gbps data rates. The newer cables have improved cable separation, and new connector types have also been developed to help meet the required specifications to support 10 Gigabit Ethernet.

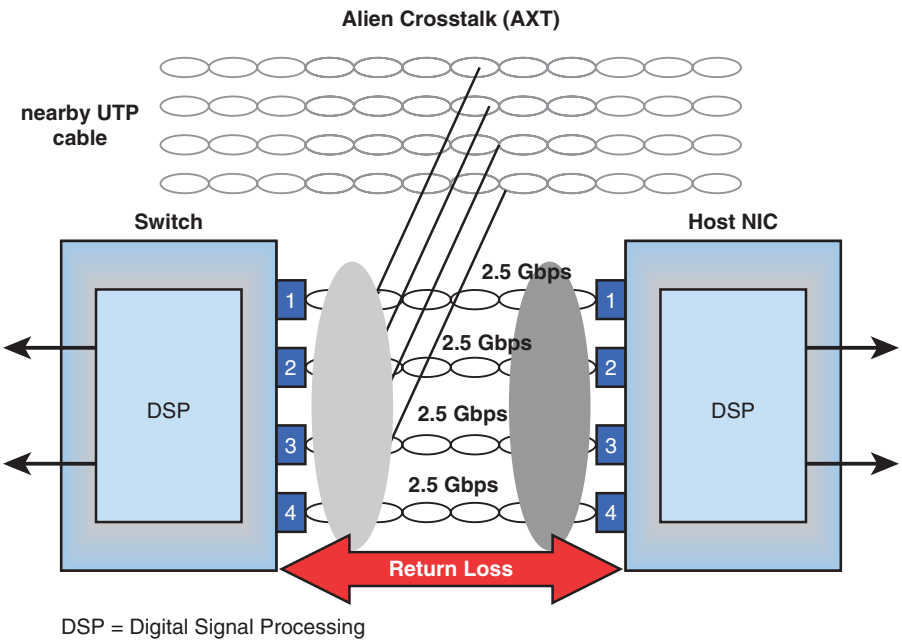


FIGURE 2-31 Alien crosstalk from a neighboring four-pair cable.

Cable manufacturers offer CAT6 and higher grades of twisted-pair cable with foil over each of the four wire pairs. The designation for this type of cable is **F/UTP**. There are two main advantages to using a shielded cable:

- A shielded cable offers better security because there is less chance that the data will radiate outside the cable.
- The foil shield helps improve immunity from EMI, radio frequency interference (RFI), and (most importantly) AXT.

F/UTP
Foil over twisted-pair cabling, a higher grade of twisted-pair cable with foil over each of the four wire pairs

Transmission of data over twisted-pair cabling relies on the signals being "balanced" over the wire pairs. The balance, or symmetry, of the signal over the wire pairs helps minimize unwanted leakage of the signal. Two parameters are defined for CAT6 and better cabling that address the issue of balanced data: **TCL** (transverse conversion loss) and **ELTCTL** (equal-level transverse conversion transfer loss). The TCL measurement is obtained by applying a common-mode signal to the input and measuring the differential signal level on the output. TCL is sometimes called **LCL** (longitudinal conversion loss). The ELTCTL value (expressed in dB) is the difference between the **TCTL** (transverse conversion transfer loss) and the differential mode insertion loss of the pair being measured. TCTL is the loss from a balanced signal at the near end to the unbalanced signal at the far end.

TCL
Transverse conversion loss

ELTCTL
Equal-level transverse conversion transfer loss

LCL
Longitudinal conversion loss

TCTL
Transverse conversion transfer loss

Newer tests include additional power-sum tests, as described earlier in this chapter: PSANEXT (power-sum alien near-end crosstalk) and PSAACRF (power-sum alien attenuation crosstalk ratio far-end). These tests have been developed to help ensure cable compatibility with data transmission and reception that require the use of all four wire pairs. Both Gigabit and 10 Gigabit Ethernet require the use of all four wire pairs.

Signal Transmission

10GBASE-T requires the use of all four wire pairs, as shown in Figure 2-32. This system splits the 10Gbps of data into four 2.5Gbps (that is, 250Mbps) data channels. This same technique is also used for 1000Mbps (that is, 1Gbps) data rates, except that the 1000Mbps signal is split into four 250Mbps data channels. The system requires the use of signal conditioners and digital signal processing (DSP) circuits for both transmission and reception. The data transmission for 10 Gigabit uses a **multilevel encoding** technique, as illustrated in Figure 2-33. The advantage of this type of encoding is that it reduces the bandwidth required to transport data.

Multilevel Encoding
A technique used to reduce the bandwidth required to transport data

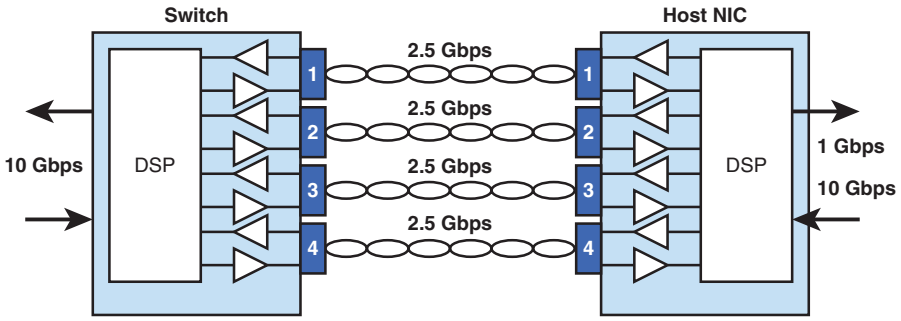


FIGURE 2-32 The four wire pairs in UTP cabling required for transporting 10GBASE-T data. This same technique is used for 1000Mbps, except the data rate for each of the four channels is 250Mbps.

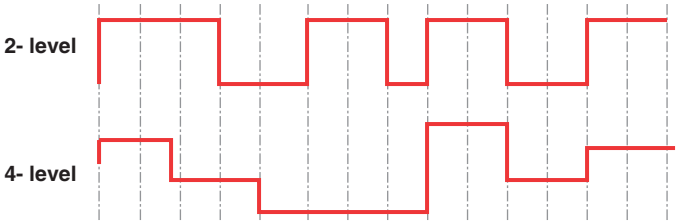


FIGURE 2-33 An example of multilevel encoding of the data streams to reduce the required bandwidth.

10GBASE-T data transmission also requires the use of DSP compensation techniques. The DSP circuitry provides many functions, such as signal conditioning and echo cancellation. Any time a signal is transmitted down a cable, part of the signal is reflected. This reflection adds to overall signal degradation and limits the performance of the system. In 10GBASE-T, the transmit and receive signals share the same wire pair. This is called *full-duplex transmission* and requires the use of a device called a **hybrid echo cancellation circuit**. The hybrid circuit removes the transmitted signal from the receive signal.

Hybrid Echo Cancellation Circuit
A circuit that removes the transmitted signal from the received signal

The final issue with 10GBASE-T signal transmission is the performance of the cable. As mentioned previously, return loss, insertion loss, and crosstalk are all key limiting issues for 10GBASE-T. Crosstalk is the most important factor. The types of

crosstalk observed are AXT, NEXT, FEXT, and ELFEXT. The cabling systems that support 10GBASE-T operation with links up to 100 meters are CAT6 with the foil screen, augmented CAT6 (CAT6a), CAT7, and CAT7a.

Section 2-6 Review

This section covers the following Network+ exam objectives.

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

This section looks at running data over UTP cable at 10Gbps, based on the 10GBASE-T Ethernet standard. Probably one of the most important concepts associated with 10Gbps over twisted-pair is alien crosstalk (AXT), which is unwanted signal coupling from one permanent link to another.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

In 10GBASE-T, the transmit and receive signals share the same wire pair. This is called full-duplex transmission.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section introduces multilevel encoding, which is a technique used to reduce the bandwidth required to transport data.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section looks at running data over UTP cable at 10Gbps, based on the 10GBASE-T Ethernet standard. One of the most important concepts associated with 10Gbps over twisted-pair is alien crosstalk (AXT), which is unwanted signal coupling.

Test Your Knowledge

1. The term for unwanted signal coupling from one permanent link to another is ____.
   a. near-end crosstalk
   b. alien crosstalk
   c. far-end crosstalk
   d. None of these answers are correct.
2. 10GBASE-T requires the use of which of the following in the transmission of data over UTP?
   a. High data lines
   b. Pins 4–5 and 7–8 only
   c. All four wire pairs
   d. 10 Gigabit is not possible over UTP.

2-7 TROUBLESHOOTING CABLING SYSTEMS

This section presents some test results taken from several CAT6/5e cable tests. The objective is to acquaint students with possible test results and problems they might encounter on the job.

This section examines some of the cable considerations and common issues that a network administrator may face with both CAT6 and CAT5e cable tests. It is important that a network administrator monitor all parts of a cable installation, from pulling to terminating the cable ends. A cable may fail a certification test due to multiple types of problems, such as problems with installation, cable stretching, and the cable failing to meet manufacturer specifications. This section discusses these types of problems and describes how to use certification reports to understand failures of CAT6 and CAT5e cabling.

If you obtain bad power-sum measurements or NEXT or FEXT measurements during network testing, there might be a problem with the installation. The certification report provided in Figure 2-34 indicates that this cable does not pass CAT6 certification, as shown by the X in the upper-right corner of the report. This test indicates a NEXT failure, which is most likely due to a problem at the terminations. This error is commonly due to the installer allowing too much untwisted cable at the termination point. Remember that the twist in UTP cable must be maintained to less than 0.375 inch. This certification test result should prompt you to inspect the terminations to see whether any terminations have too much untwisted cable and verify whether there is a procedure problem with the installation.

Cable Stretching

It is important to avoid stretching UTP cable because doing so changes the electrical characteristics of the cable, increasing the attenuation and crosstalk. The maximum pulling tension (expressed in lb-ft) is specified in the manufacturer's data sheets.

Cable Failing to Meet Manufacturer Specifications

Occasionally, manufacturers experience problems with cable failing to meet specifications. For example, a bad production run may cause the cable to fail to meet minimum specifications. Repeated test failures with no apparent cause could indicate that the problem is with the cable. This rarely happens, but a bad cable production run could be the culprit. As a network manager, you need to isolate the source of the problem.

Figure 2-35 shows a CAT6 certification report which indicates that the cable failed due to excessive insertion loss. The certification report shows that the cable length for pair 7–8 is 311 feet. The maximum cable length for a permanent link is 295 feet. Therefore, this cable run is too long to be certifiable.

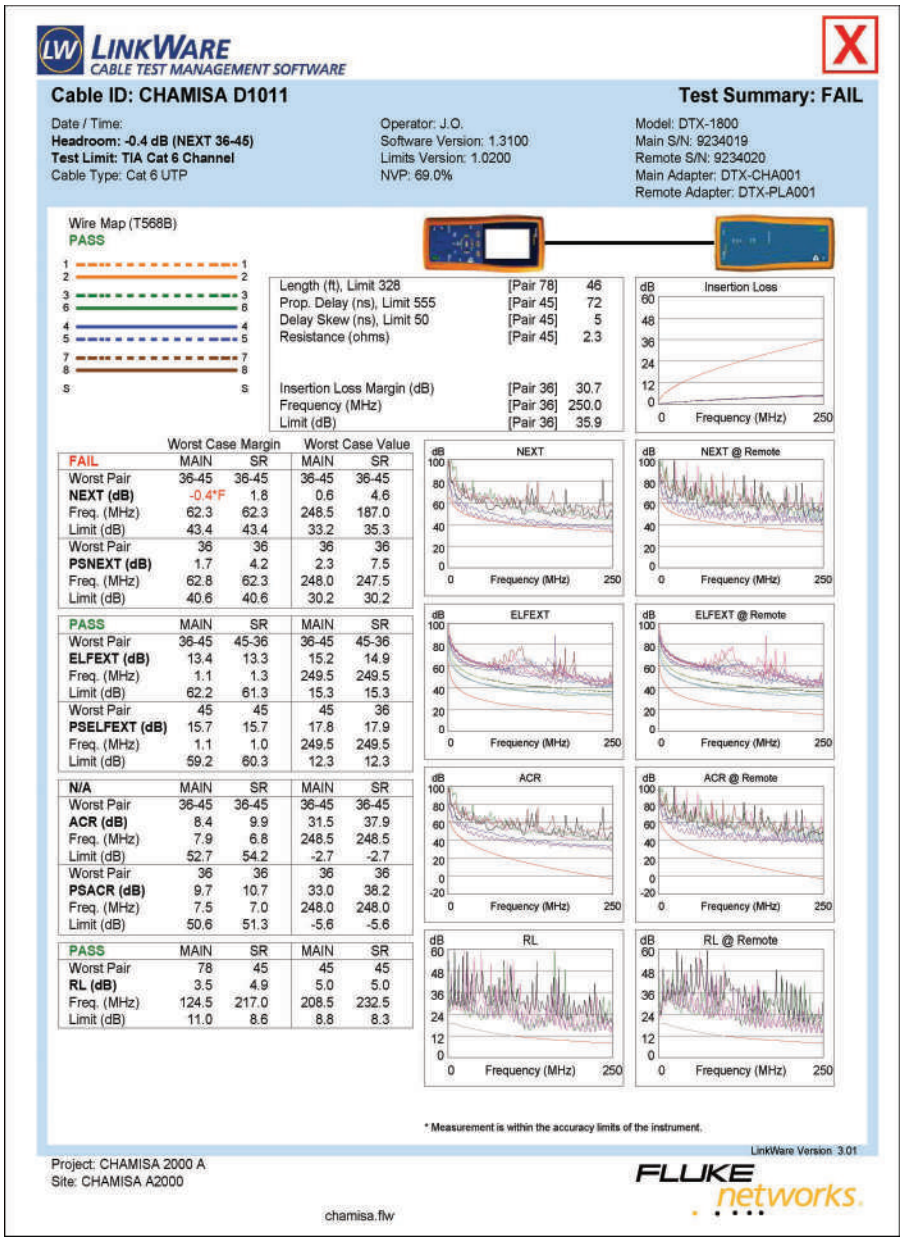


FIGURE 2-34 DTX-1800 certification report: Failure due to a termination problem.

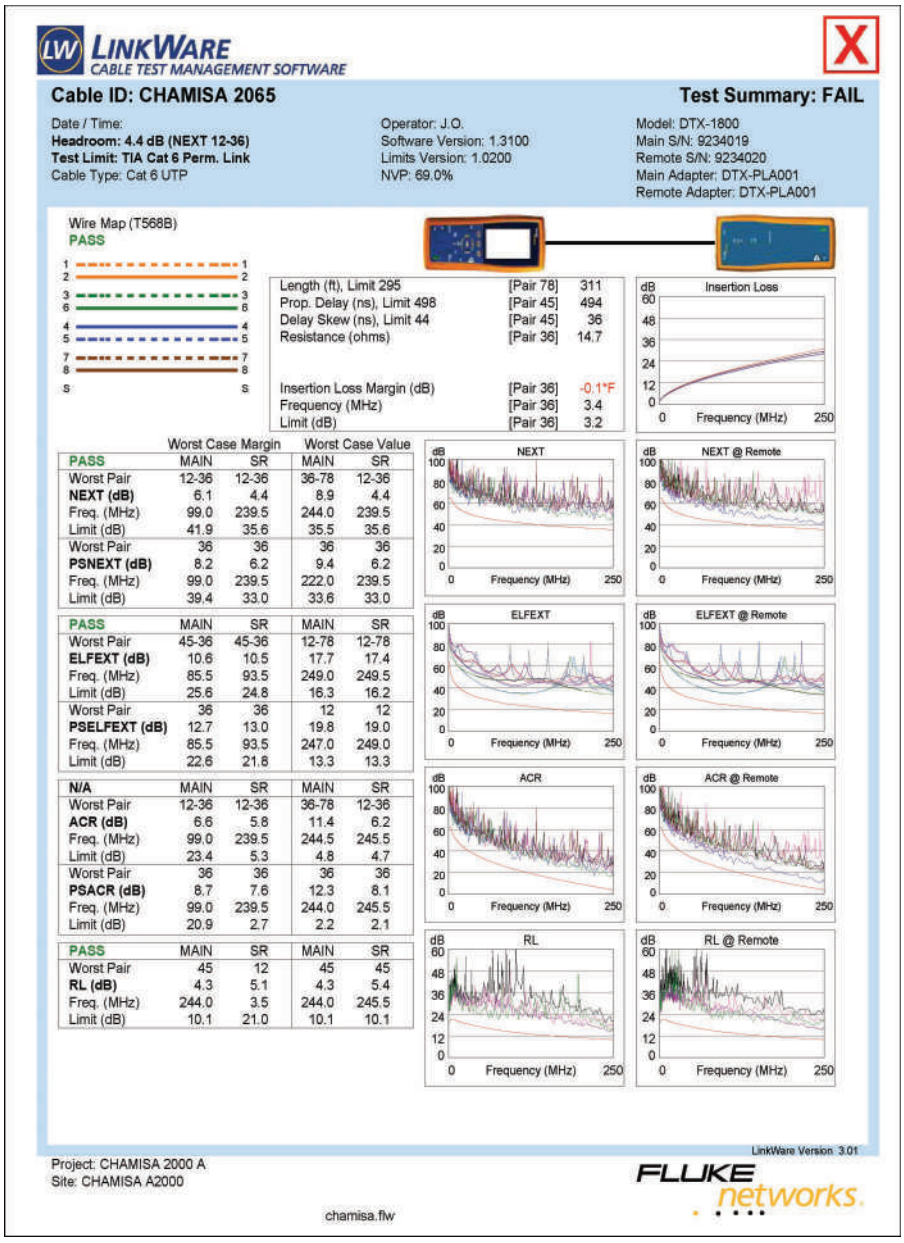


FIGURE 2-35 DTX-1800 certification report: Failure due to excessive insertion loss.

CAT5e Cable Test Examples

This section presents test results for several CAT5e cable tests. There are many CAT5e horizontal cable runs already in place, and these runs support 100Mbps data rates. Therefore, it is important for a network administrator to have a good understanding of how to certify CAT5e links. The goal of this section is to acquaint you with possible CAT5e test results and problems you might encounter on the job. The procedures presented are the same for CAT6 except that the test mode of the cable analyzer must be set to CAT5e performance specifications. The testers used

for conducting the CAT5e certification reports in this section are the Fluke OMNIScanner and OMNIRemote.

Test 1 UTP cable testing is not restricted to long cables. Short patch cables (around 3 feet) can and should also be tested. It's a good idea to have a record of even short patch cables meeting CAT5e requirements.

Figure 2-36 shows an OMNIScanner certification report which verifies that the cable passes the CAT5e link test. This report shows that the length of the cable tested is 3 feet.

OMNI Scanner™

PASS

OMNIScanner2 Certification Report

Circuit ID:	Pre-cut
Project:	TIA Project
Owner:	OMNISCANNER 2
Autotest:	*Cat 5E Link*
Cable:	Cat 5E UTP
NVP:	72
Site:	Las Cruces
Building:	Manufacturing
Floor:	3rd
Closet:	315A

OMNIScanner
50D99L00377 SW: V06.00
Adapter
CHAN 5/5E/6

OMNIRemote
50E99L00037
Adapter
CHAN 5/5E/6



	Limit	12	36	45	78
Length ft	(308)	3	3	3	3
Delay (ns):	(518)	4	4	4	4
Resistance (Ohms):	(—)	—	—	—	—

Wiremap	Expected	Actual		
OMNI:	12345678	12345678	Skew (ns):	(45) 0
Remote:	12345678	12345678	Bandwidth (MHz):	—

Attenuation Overall Margin (dB)* 19.9

Pairs	dB	Margin	MHz
12	0.3	21.0	97.4
36	0.4	20.1	90.7
45	0.4	21.0	97.4
78	0.3	19.9	88.4

Return Loss Overall Margin (dB)* —

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	23.8	11.4	90.7	23.4	11.2	99.0
36	23.2	10.4	80.8	22.5	10.0	88.9
45	23.1	10.1	74.7	24.2	11.0	70.7
78	23.9	11.5	91.3	24.1	12.0	99.0

NEXT Overall Margin (dB)* 3.0

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12/36	62.5	18.7	19.6	61.7	14.0	11.3
12/45	59.2	21.8	48.6	46.6	14.3	99.9
12/78	93.1	33.1	1.2	52.4	20.0	99.2
36/45	50.5	8.6	25.9	45.9	3.0	22.6
36/78	56.0	13.3	23.2	53.5	9.0	18.1
45/78	51.6	14.6	51.6	47.3	14.9	99.0

ACR Overall Margin (dB)* —

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12/36	—	—	—	—	—	—
12/45	—	—	—	—	—	—
12/78	—	—	—	—	—	—
36/45	—	—	—	—	—	—
36/78	—	—	—	—	—	—
45/78	—	—	—	—	—	—

ELFEXT Overall Margin (dB)* 15.3

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12/36	60.0	22.0	12.7	60.1	22.1	12.7
12/45	55.3	16.9	12.0	74.6	16.9	1.4
12/78	69.8	30.6	10.9	85.3	30.4	1.9
36/12	60.1	22.1	12.7	60.0	22.0	12.7
36/45	46.1	20.0	49.5	76.8	20.4	1.6
36/78	64.2	28.2	16.0	48.9	28.6	97.4
45/12	74.6	16.8	1.4	73.3	16.9	1.6
45/36	76.7	20.3	1.6	45.9	20.0	51.1
45/78	71.9	15.5	1.6	73.0	15.3	1.4
78/12	85.3	30.4	1.9	69.9	30.6	10.9
78/36	48.8	28.6	97.4	64.2	28.2	16.0
78/45	73.0	15.3	1.4	53.7	15.5	12.4

PSNEXT Overall Margin (dB)* 4.9

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	65.7	20.4	10.4	44.8	15.5	99.9
36	49.1	10.3	25.9	44.7	4.9	22.6
45	49.8	11.0	25.9	46.1	6.0	21.9
78	50.4	14.6	39.6	50.6	11.8	26.2

PSELFEXT Overall Margin (dB)* 15.5

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	73.6	18.8	1.4	54.2	18.7	12.0
36	75.9	21.2	1.4	75.8	21.1	1.4
45	68.9	15.5	1.6	69.0	15.6	1.6
78	71.7	18.2	1.6	72.8	18.0	1.4

PSACR Overall Margin (dB)* —

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	—	—	—	—	—	—
36	—	—	—	—	—	—
45	—	—	—	—	—	—
78	—	—	—	—	—	—

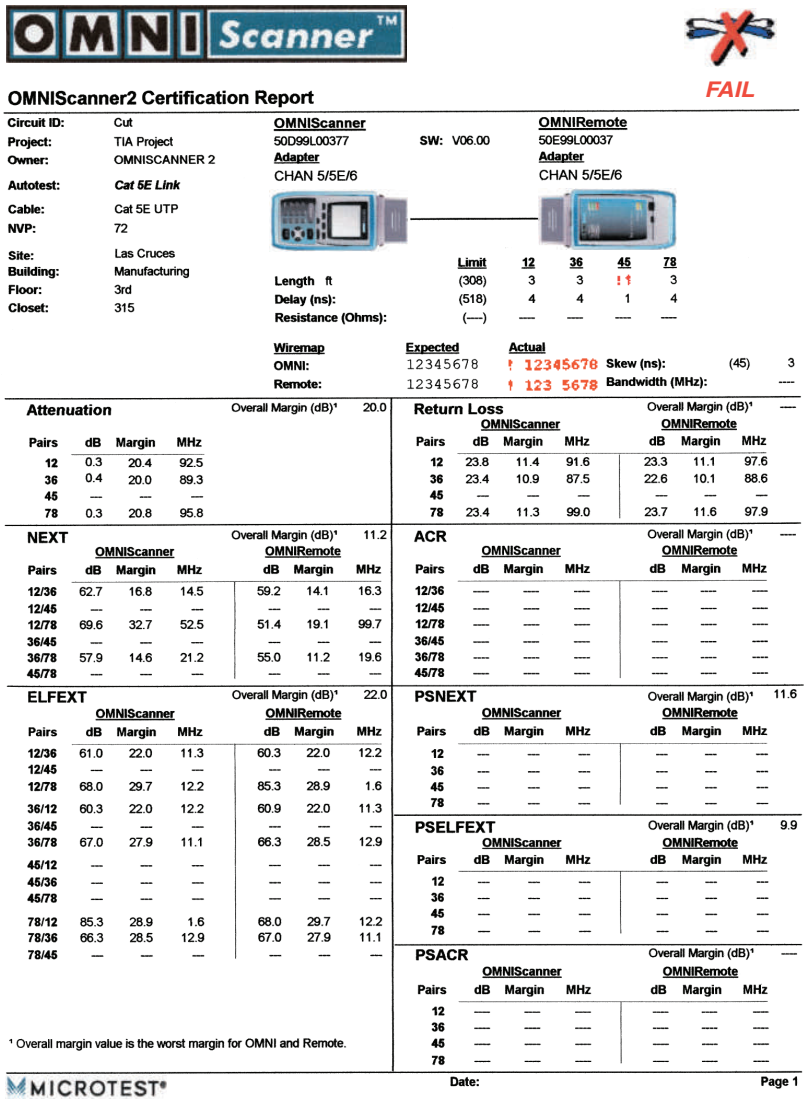
* Overall margin value is the worst margin for OMNI and Remote.

MICROTEST® Date: Page 1

FIGURE 2-36 The certification report for Test 1, showing that a short jumper cable passes the CAT5e link test.

Test 2 A second test on the same 3-foot cable used in Test 1 shows that the cable no longer meets CAT5e requirements (see Figure 2-37). The test results indicate FAIL. In this case, careful inspection of the cable shows that it has been cut or nicked. This underscores the importance of documenting the network installation and having a record of the cable link having been certified. Test 1 showed that the cable met specifications, but the cable has since been damaged and no longer meets the CAT5e link specifications.

In this example, the cable has failed a wiremap test. Not only is the text highlighted, but there is an exclamation point preceding the text that indicates a failure. A quick check of the wiremap test shows that the number 4 wire was not detected at the remote.



OMNI Scanner™

FAIL

OMNIScanner2 Certification Report

Circuit ID:	Cut
Project:	TIA Project
Owner:	OMNISCANNER 2
Autotest:	*Cat 5E Link*
Cable:	Cat 5E UTP
NVP:	72
Site:	Las Cruces
Building:	Manufacturing
Floor:	3rd
Closet:	315

OMNIScanner		**OMNIRemote**
50D99L00377	**SW:** V06.00	50E99L00037
Adapter		**Adapter**
CHAN 5/5E/6		CHAN 5/5E/6

	Limit	12	36	45	78
Length ft	(308)	3	3	! 4	3
Delay (ns):	(518)	4	4	1	4
Resistance (Ohms):	(---)	---	---	---	---

Wiremap	**Expected**	**Actual**			
OMNI:	12345678	! 12345678	**Skew (ns):**	(45)	3
Remote:	12345678	! 123 5678	**Bandwidth (MHz):**		---

Attenuation — Overall Margin (dB)[1]: 20.0

Pairs	dB	Margin	MHz
12	0.3	20.4	92.5
36	0.4	20.0	89.3
45	---	---	---
78	0.3	20.8	95.8

Return Loss — Overall Margin (dB)[1]: ---

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	23.8	11.4	91.6	23.3	11.1	97.6
36	23.4	10.9	87.5	22.6	10.1	88.6
45	---	---	---	---	---	---
78	23.4	11.3	99.0	23.7	11.6	97.9

NEXT — Overall Margin (dB)[1]: 11.2

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12/36	62.7	16.8	14.5	59.2	14.1	16.3
12/45	---	---	---	---	---	---
12/78	69.6	32.7	52.5	51.4	19.1	99.7
36/45	---	---	---	---	---	---
36/78	57.9	14.6	21.2	55.0	11.2	19.6
45/78	---	---	---	---	---	---

ACR — Overall Margin (dB)[1]: ---

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	---	---	---	---	---	---
36/45	---	---	---	---	---	---
36/78	---	---	---	---	---	---
45/78	---	---	---	---	---	---

ELFEXT — Overall Margin (dB)[1]: 22.0

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12/36	61.0	22.0	11.3	60.3	22.0	12.2
12/45	---	---	---	---	---	---
12/78	68.0	29.7	12.2	85.3	28.9	1.6
36/12	60.3	22.0	12.2	60.9	22.0	11.3
36/45	---	---	---	---	---	---
36/78	67.0	27.9	11.1	66.3	28.5	12.9
45/12	---	---	---	---	---	---
45/36	---	---	---	---	---	---
45/78	---	---	---	---	---	---
78/12	85.3	28.9	1.6	68.0	29.7	12.2
78/36	66.3	28.5	12.9	67.0	27.9	11.1
78/45	---	---	---	---	---	---

PSNEXT — Overall Margin (dB)[1]: 11.6

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

PSELFEXT — Overall Margin (dB)[1]: 9.9

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

PSACR — Overall Margin (dB)[1]: ---

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

[1] Overall margin value is the worst margin for OMNI and Remote.

MICROTEST®

Date:

Page 1

FIGURE 2-37 The results for Test 2, showing that the cable failed the CAT5e link test.

Test 3 A third cable test, as shown in Figure 2-38, also generates the test result FAIL. Examination of the attenuation and return loss menu shows that the cable failed to meet CAT5e attenuation and return loss specifications. The permitted attenuation in CAT5e cable is 24 dB. However, the 1–2 and 3–6 pairs have attenuation losses of 38.0 dB and 41.1 dB. Both cases greatly exceed the permitted maximum. An arrow points to these attenuation loss scores.

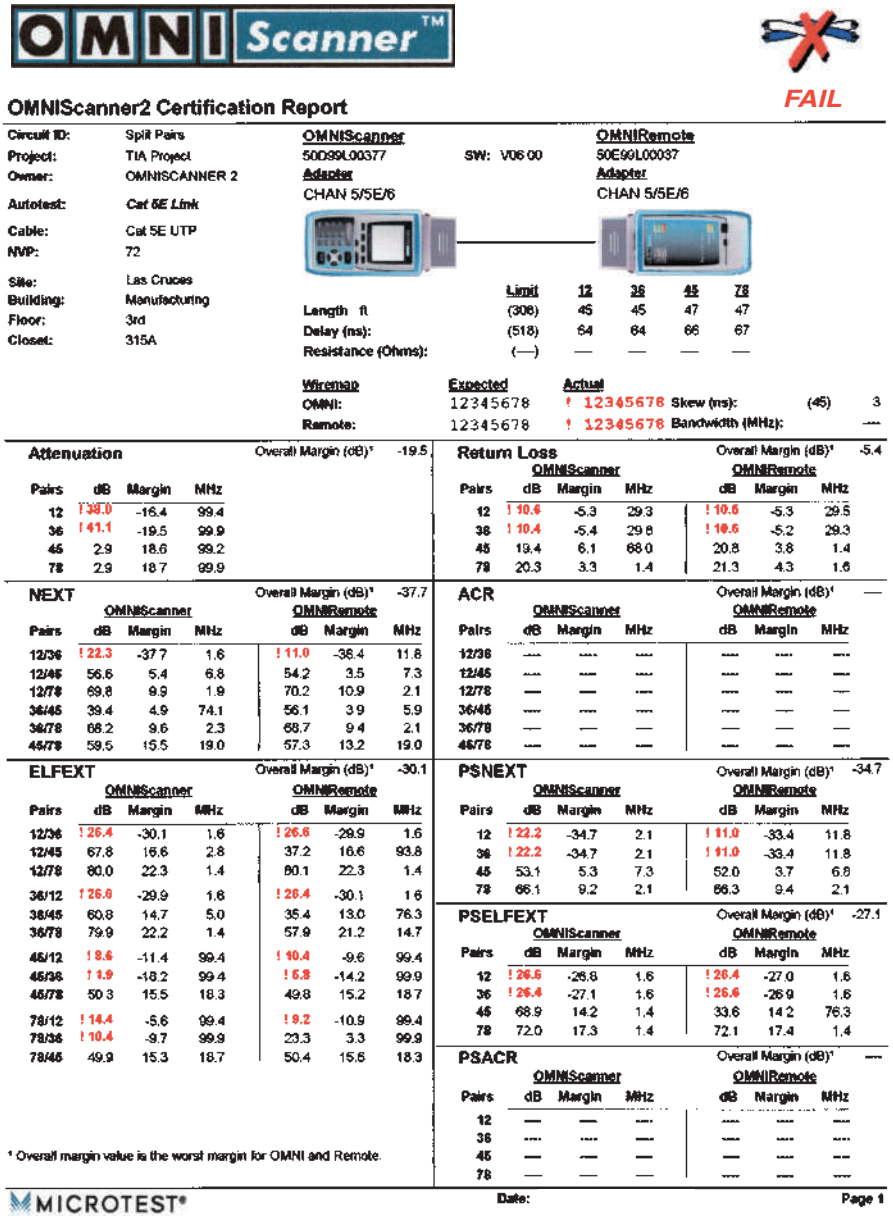
This cable also fails return loss testing for pairs 1–2 and 3–6. CAT5e cable permits 10 dB of return loss. The report shows that the pairs failed the return loss test at both the OMNIScanner and the OMNIRemote test unit. This cable fails CAT5e certification based on its attenuation or return loss. In fact, this cable also fails the NEXT, ELFEXT, and PSELFEXT tests. Any of these failures is sufficient to prevent this cable from being certified.

Test 4 Figure 2-39 shows the certification report for the cable tested in Test 4. Examination of the certification report shows that the cable failed the delay skew test. This cable exceeds the maximum skew allowed by TIA/EIA 568-B. In addition, this cable fails attenuation, ELFEXT, and PSELFEXT tests. The cable is not certified.

The measured delay skew of 47 ns exceeds the tester setting of 45 ns. However, the TIA/EIA 568-B standard permits a delay skew of 50 ns, so actually this cable meets delay skew requirements for CAT5e cable. Should the cable have been certified? Look at the length measurement for the 3–6 pair length. The cable is 1040 feet (317 meters) long. Remember that the maximum cable length for a CAT5e cable run is 100 meters.

Summary of CAT5e Cable Test Examples You have just seen a few examples of CAT5e link tests that provide actual test data for various cable problems that you might encounter on the job. In the tests where a failure was detected, the tester displays a FAIL screen, and the certification report identifies the problem. The following is a summary of the test results:

- **Test 1:** The certification report shows the test result PASS.
- **Test 2:** The certification report shows the test result FAIL. The report shows that the cable failed the wiremap test.
- **Test 3:** This cable test generated the test result FAIL. Examination of the attenuation and return loss shows that the cable failed to meet CAT5e attenuation and return loss specifications. The cable also failed NEXT, ELFEXT, PSNEXT, and PSELFEXT tests.
- **Test 4:** The certification report shows the cable failing the CAT5e link test. Examination of the report shows that the cable failed the delay skew measurement because the cable length exceeded the 100 meter maximum. The cable also failed the attenuation, ELFEXT, and PSELFEXT tests.



OMNI Scanner™

FAIL

OMNIScanner2 Certification Report

Circuit ID:	Split Pairs
Project:	TIA Project
Owner:	OMNISCANNER 2
Autotest:	*Cat 5E Link*
Cable:	Cat 5E UTP
NVP:	72
Site:	Las Cruces
Building:	Manufacturing
Floor:	3rd
Closet:	315A

OMNIScanner 50D99L00377 SW: V06.00
Adapter: CHAN 5/5E/6

OMNIRemote S0E99L00037
Adapter: CHAN 5/5E/6

	Limit	12	36	45	78
Length ft	(308)	45	45	47	47
Delay (ns):	(518)	64	64	66	67
Resistance (Ohms):	(—)	—	—	—	—

Wiremap	Expected	Actual		
OMNI:	12345678	! 12345678	Skew (ns):	(45) 3
Remote:	12345678	! 12345678	Bandwidth (MHz):	---

Attenuation — Overall Margin (dB)[1] -19.5

Pairs	dB	Margin	MHz
12	! 39.0	-16.4	99.4
36	! 41.1	-19.5	99.9
45	2.9	18.6	99.2
78	2.9	18.7	99.9

Return Loss — Overall Margin (dB)[1] -5.4

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12	! 10.6	-5.3	29.3	! 10.6	-5.3	29.5
36	! 10.4	-5.4	29.8	! 10.6	-5.2	29.3
45	19.4	6.1	68.0	20.8	3.8	1.4
78	20.3	3.3	1.4	21.3	4.3	1.6

NEXT — Overall Margin (dB)[1] -37.7

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12/36	! 22.3	-37.7	1.6	! 11.0	-36.4	11.8
12/45	56.6	5.4	6.8	54.2	3.5	7.3
12/78	69.8	9.9	1.9	70.2	10.9	2.1
36/45	39.4	4.9	74.1	56.1	3.9	5.9
36/78	68.2	9.6	2.3	68.7	9.4	2.1
45/78	59.5	15.5	19.0	57.3	13.2	19.0

ACR — Overall Margin (dB)[1] —

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	—	—	---	---	---	---
36/45	---	---	---	---	---	---
36/78	—	—	—	—	—	—
45/78	---	---	---	---	---	---

ELFEXT — Overall Margin (dB)[1] -30.1

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12/36	! 26.4	-30.1	1.6	! 26.6	-29.9	1.6
12/45	67.8	16.6	2.8	37.2	16.6	93.8
12/78	80.0	22.3	1.4	80.1	22.3	1.4
36/12	! 26.6	-29.9	1.6	! 26.4	-30.1	1.6
36/45	60.8	14.7	5.0	35.4	13.0	76.3
36/78	79.9	22.2	1.4	57.9	21.2	14.7
45/12	! 8.6	-11.4	99.4	! 10.4	-9.6	99.4
45/36	! 1.9	-18.2	99.4	! 5.8	-14.2	99.9
45/78	50.3	15.5	18.3	49.8	15.2	18.7
78/12	! 14.4	-5.6	99.4	! 9.2	-10.9	99.4
78/36	! 10.4	-9.7	99.9	23.3	3.3	99.9
78/45	49.9	15.3	18.7	50.4	15.6	18.3

PSNEXT — Overall Margin (dB)[1] -34.7

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12	! 22.2	-34.7	2.1	! 11.0	-33.4	11.8
36	! 22.2	-34.7	2.1	! 11.0	-33.4	11.8
45	53.1	5.3	7.3	52.0	3.7	6.8
78	66.1	9.2	2.1	66.3	9.4	2.1

PSELFEXT — Overall Margin (dB)[1] -27.1

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12	! 26.6	-26.8	1.6	! 26.4	-27.0	1.6
36	! 26.4	-27.1	1.6	! 26.6	-26.9	1.6
45	68.9	14.2	1.4	33.6	14.2	76.3
78	72.0	17.3	1.4	72.1	17.4	1.4

PSACR — Overall Margin (dB)[1] ---

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12	—	—	---	---	---	---
36	---	---	---	---	---	---
45	—	—	—	—	—	—
78	—	—	—	---	---	---

[1] Overall margin value is the worst margin for OMNI and Remote.

MICROTEST® Date: Page 1

FIGURE 2-38 The Test 3 CAT5e link test, showing failures with attenuation.

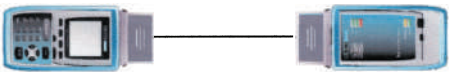
You need to examine test results to find out why a cable has failed a test. You need to know whether the problem is with the terminations, the cable layout, or the way the cable is installed. Keeping a record of the cable tests will help you isolate recurring problems.

OMNI Scanner™

FAIL

OMNIScanner2 Certification Report

Circuit ID:	Long Box	**OMNIScanner**		**OMNIRemote**			
Project:	TIA Project	50D99L00377	**SW:** V06.00	50E99L00037			
Owner:	OMNISCANNER 2	**Adapter**		**Adapter**			
Autotest:	*Cat 5E Link*	CHAN 5/5E/6		CHAN 5/5E/6			
Cable:	Cat 5E UTP						
NVP:	72						
Site:	Las Cruces						
Building:	Manufacturing						
Floor:	3rd						
Closet:	315						



	Limit	12	36	45	78
Length ft	(308)	1068	! 1640	1050	1074
Delay (ns):	(518)	1508	! 1469	1482	1516
Resistance (Ohms):	(—)	---	---	---	---

	Wiremap	**Expected**	**Actual**			
OMNI:		12345678	12345678	**Skew (ns):**	(45)	! 47
Remote:		12345678	12345678	**Bandwidth (MHz):**		---

Attenuation

Overall Margin (dB)[1] -62.1

Pairs	dB	Margin	MHz
12	! 72.7	-52.8	86.4
36	! 74.5	-54.1	89.8
45	! 80.4	-61.5	78.3
78	! 82.4	-62.1	89.1

Return Loss

Overall Margin (dB)[1] 4.9

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12	23.2	7.0	26.4	27.4	10.4	2.1
36	25.2	8.2	1.4	23.3	9.1	50.7
45	20.9	4.9	27.5	24.6	7.6	12.9
78	25.4	8.4	2.3	24.6	8.6	28.0

NEXT

Overall Margin (dB)[1] 7.6

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12/36	60.3	13.8	13.6	63.6	13.8	8.4
12/45	44.1	10.1	78.5	53.8	15.7	44.1
12/78	48.4	8.6	34.9	59.6	8.2	6.6
36/45	66.1	8.1	2.5	62.6	7.6	3.9
36/78	45.4	13.0	99.2	69.3	12.4	3.0
45/78	63.8	13.0	7.3	69.4	16.9	5.7

ACR

Overall Margin (dB)[1] ----

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12/36	---	---	---	---	---	---
12/45	---	---	---	---	---	---
12/78	---	---	---	---	---	---
36/45	---	---	---	---	---	---
36/78	---	---	---	---	---	---
45/78	---	---	---	---	---	---

ELFEXT

Overall Margin (dB)[1] -21.1

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12/36	! 6.1	-15.7	91.6	! 7.6	-13.5	89.8
12/45	! 9.6	-11.1	92.5	! 4.4	-17.8	78.3
12/78	! 3.0	-18.0	89.1	! 0.6	-20.4	89.1
36/12	! 13.0	-8.7	83.0	! 11.2	-9.1	96.1
36/45	! 1.4	-20.8	78.3	! 5.5	-16.1	82.8
36/78	! 5.3	-12.6	90.4	! 1.7	-19.4	89.1
45/12	! 7.7	-13.6	86.4	! 8.3	-13.0	86.4
45/36	! 5.4	-16.3	82.8	! 8.1	-13.5	82.8
45/78	! 1.3	-19.0	96.7	! 1.3	-19.7	89.1
78/12	! 8.6	-13.1	83.0	! 6.7	-14.9	83.0
78/36	! 4.7	-16.2	89.8	! 7.6	-13.4	89.8
78/45	! 1.1	-21.1	78.3	! 4.9	-17.2	78.3

PSNEXT

Overall Margin (dB)[1] 9.4

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12	47.9	11.1	34.9	59.3	10.8	6.6
36	64.3	10.2	3.0	62.2	10.0	3.9
45	64.7	9.4	2.5	62.1	9.9	3.9
78	58.5	10.7	7.3	59.5	11.0	6.6

PSELFEXT

Overall Margin (dB)[1] -18.4

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12	! 5.0	-13.3	86.4	! 6.2	-12.4	83.0
36	! 1.3	-16.5	91.6	! 3.4	-14.6	89.8
45	! 4.3	-14.9	78.3	! 0.7	-18.4	78.3
78	! 0.3	-17.7	89.1	! 0.2	-17.2	90.4

PSACR

Overall Margin (dB)[1] ----

	OMNIScanner			OMNIRemote		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12	---	---	---	---	---	---
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

[1] Overall margin value is the worst margin for OMNI and Remote.

MICROTEST®

Date:

Page 1

FIGURE 2-39 A CAT5e link test, showing failures with delay skew (Test 4).

Tests 1 and 2 demonstrate the importance of keeping a record of tests. In this case, the cable was certified but later failed. The documentation provided by the certification report provides evidence that the cable was functioning properly and did meet CAT5e specifications.

Wired Connectivity and Performance Issues Summary There are many other issues associated with troubleshooting wired connectivity and performance issues, including the following:

- **Open/short:** A cable may have a wire connection that is open or shorted. This issue is most often associated with patch cables and wall plates.
- **Incorrect pin-out:** This error should be easily detected when conducting a wiremap test on a terminated cable. A cable tester provides a visual indicator of the wiremap.
- **Incorrect cable type:** This problem usually occurs when data speeds increase and a cable is not designed to support the higher data rate. In addition, an application might require a shielded twisted-pair cable or a plenum-rated cable. It is important to make sure the proper cable has been used.
- **Bad port:** When troubleshooting, it might be discovered that a port is not "hot," meaning that it is not connecting to the network. You have to make sure the cable to the switch port is connected and the cable link is good. Next, you need to verify that the switch port or wall port is functional. If it isn't, it needs to be replaced.
- **Damaged cables:** This problem is usually associated with cable installation, but it can be associated with patch cables. In either case, a cable tester can be used to identify the problem.
- **Bent pins:** This condition can be associated with connectors on a computer motherboard and with a connector cable such as a DTE V.35 cable or other types of serial cables. If this condition occurs, you can carefully straighten the cable pins with needle-nose pliers.
- **Bad ports:** A poorly terminated UTP plug can be susceptible to RFI that could degrade data transfers and result in poor signal integrity. A bad or broken UTP jack can cause an intermittent network connection.

A useful tool for verifying continuity with cable wiring is a multimeter. This device is used to measure voltage, current, and resistance. A basic multimeter function related to cabling is conducting a continuity check to verify that two ends are connected.

Section 2-7 Review

This section covers the following Network+ exam objectives.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section presents several examples of tests and possible problems that might be encountered. Problems may result from poor installation, bad connectors, or bad cable, and a network administrator needs to have good documentation that each cable has been certified, if possible.

Test Your Knowledge

1. True or false: Patch cables are too short to be tested.

   False

2. A UTP certification report lists the following.

Pairs	12	36	45	78
Length	285	288	284	283

   What do these results indicate?

   a. The test must be repeated.
   b. There is not enough information to obtain an answer.
   c. The cable length is too long.
   d. The cable passes the length test.

3. A data problem is reported to the network administrator. The problem is found to be with the UTP network connection. Which steps could the network administrator have taken to isolate the problem? (Select two.)

   a. Visually inspect all UTP terminations.
   b. Run a cable test, using a cable tester.
   c. Use the **ping** command to verify network connectivity.
   d. Use pairs 4–5 and 7–8 to repair the connection.
   e. Contact the installer of the UTP cable to obtain a certification report.

SUMMARY

This chapter introduces the basics of horizontal cabling and unshielded twisted-pair cable. The major topics you should now understand include the following:

- The six subsystems of a structured cabling system
- The purpose of the telecommunications closet and the LAN work area
- The performance capabilities of CAT6/5e UTP
- The wiring color schemes for T568A and T568B
- The pin assignments for an RJ-45 modular plug
- The technical issues of copper over 10 Gigabit Ethernet
- The procedures for testing a CAT6/5e link
- The procedures for troubleshooting a CAT6/5e link
- How to examine and use the test results provided by a CAT6/5e link certification report

QUESTIONS AND PROBLEMS

Section 2-2

1. What is an 8P8C connector?

    a. An RJ-11 connector
    b. An RJ-6 connector
    c. An RJ-45 connector
    d. An RS-232

2. What do EIA and TIA stand for?

    EIA: Electronics Industries Alliance

    TIA: Telecommunication Industry Association

3. What are the three parts of the TIA/EIA 568-B standard?

    TIA/EIA-568-B.1 Commercial Cabling Standard

    TIA/EIA-568-B.2 Twisted-Pair Media

    TIA/EIA-568-B.3 Optical Fiber Cabling Standard

4. Identify the six subsystems of a structured cabling system.

    1. Building entrance
    2. Equipment room
    3. Backbone cabling
    4. Telecommunications closet

5. Horizontal cabling
6. Work area

5. Which subsystem does permanent networking cabling within a building belong to?

   Horizontal cabling

6. What is a cross-connect?

   A cross-connect is a space where one or multiple cables are connected to equipment or other cables.

7. What is the main cross-connect?

   The main cross-connect is the point that usually connects two or more buildings.

8. A telco and an ISP usually connect to what room in the campus network hierarchy?

   Main cross-connect (MC)

9. What is a WO, and what is its purpose?

   A WO is a work area outlet. It is the termination for a horizontal cross-connect.

10. The patch cable from a computer typically terminates into which of the following?

    a. Jack in a wall plate
    b. BNC connector
    c. Thinnet
    d. RJ-11 modular plug
    e. RG-59

11. What is the overall length limitation of an individual cable run from the telecommunications closet to a networking device in the work area?

    100 meters

12. A general rule of thumb is to allow how many meters for the cable run from the telecommunications closet to the work area?

    90 meters

Section 2-3

13. How many pins does an RJ-45 modular plug have?

    8 pins

14. What is the difference between CAT5 and CAT5e?

    CAT5e is an enhanced cable capable of carrying data at a rate of 1000Mbps. CAT5 can carry data at a rate of 100Mbps.

15. What is the data rate for Ethernet?

    10Mbps

16. What is the data rate for Fast Ethernet?

    100Mbps

17. What improvements do CAT6, CAT7, and CAT8 cable provide?

    They provide improved bandwidth, which leads to improved data rates.

18. What is the data rate for Gigabit Ethernet?

    1000Mbps

19. What is a benefit of using shielded twisted-pair cabling?

    The shield reduces the potential for electromagnetic interference (EMI).

20. Which cable type—UTP or STP—is preferred by the industry?

    Testing shows little performance improvement using STP. The additional cable and installation cost do not justify its use in all cases. Therefore, the industry usually recommends the use of UTP cable. However, this can change with higher data rates such as 10Gbps or 40Gbps.

Section 2-4

21. What are the color maps and pin number assignments for T568A and T568B?

Pin Number	T568A Wire Color	T568B Wire Color
1	White–green	White–orange
2	Green	Orange
3	White–orange	White–green
4	Blue	Blue
5	White–blue	White–blue
6	Orange	Green
7	White–brown	White–brown
8	Brown	Brown

22. What is the difference between T568A and T568B?

    T568A and T568B are two different standards for wiring modular connectors.

23. How many wires are in a CAT6 twisted-pair cable?

    8 wires

24. How many wire pairs are in a CAT6 twisted-pair cable?

    4 pairs

25. In regard to a CAT6 cable, what pins in an RJ-45 connecter are used to carry data in a Fast Ethernet network?

    TX (+)

    TX (–)

    RX (+)

    RX (–)

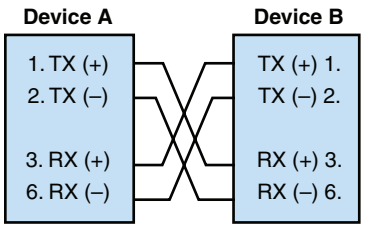
26. What does an "X" on the input to a hub or switch represent?

    It indicates a cross-connected input.

27. Define the term *cross-connected input*.

    A cross-connected input is an input in which the transmit and receive pairs are internally swapped to maintain proper alignment of the TX and RX pairs.

28. Draw a picture of properly aligned transmit and receive signals for a computer's data link that is running Ethernet data rates.

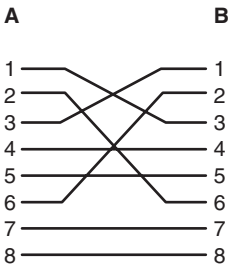


29. What is the difference between straight and cross-connected input ports?

    Straight =Tx–Tx Rx–Rx

    Crossed = Tx–Rx Rx–Tx

30. Draw the wiremap for a crossover CAT6 UTP cable running Fast Ethernet.



31. What is a UTP link test?

    It is a test that evaluates a cable from one cable termination to another.

32. What is a UTP full channel test?

    It is a test that evaluates all the link elements from a hub or switch through the path panel to the wall plate.

33. What does NEXT stand for, and what does it measure?

    NEXT stands for near-end crosstalk and is a measure of the level of crosstalk within a cable.

34. A NEXT measurement of 59.5 dB is made on wire pairs 1–2 and 3–6. A NEXT measurement of 51.8 dB is made on wire pairs 3–6 and 7–8. Which cable pairs have the best measured NEXT performance?

    1–2 and 3–6 have the best measured NEXT performance because a high NEXT (dB) value is desirable.

35. Define power-sum measurements.

    With power-sum measurements, all four-wire pairs are used to obtain a combined performance measurement.

36. Define propagation delay.

    Propagation delay is the amount of time it takes a signal to propagate from one end of a cable to the other.

37. Signals travel in a cable at some percentage of the velocity of light. What is the term for this?

    Nominal velocity of propagation (NVP)

38. Why is delay skew critical?

    If the wire lengths of different wire pairs are significantly different, then the data on different wires will arrive at the receiver at different times, potentially creating distortion of the data.

39. Why are power-sum measurements critical for high-speed data communication over UTP?

    High-speed data communications (such as Gigabit) require the use of all four-wire pairs, hence the need to obtain the combined performance measurement of all four-wire pairs.

40. Should the expected + loss of a 20-meter UTP cable be greater than or less than that of a 90-meter UTP cable?

    The expected + loss of a 20-meter UTP cable should be less than that of a 90-meter UTP cable.

41. What is 8P8C, and what connector type is most associated with it?

    8P8C is an 8-pin connector. The RJ-45 plug and jack are the most common 8P8C connectors.

42. What are the pin assignments for 1Gbps and 10Gbps?

    Refer to Figure 2-11.

43. What is the purpose of a lacing tool?

    A lacing tool is used to properly align the wires to make sure the untwisted wire is minimized.

Section 2-5

44. What is the limit on the bend radius for a UTP cable, and why is this limit important?

    The limit is four times the diameter of the cable. Bends exceeding this limit can introduce attenuation loss.

45. Is a high PSNEXT measurement desirable?

    Yes. It indicates better cable performance.

46. Define margin (dB) relative to cable measurements. What does it mean if the margin lists a negative value?

    The margin indicates the number of decibels by which the measured value exceeds the limit. A negative value indicates a measurement lower than the limit.

Section 2-6

47. Define alien crosstalk and draw a picture of how it can happen.

    Basically, alien crosstalk (AXT) is an unwanted signal coupling from one four-pair cable to another. See Figure 2-31 for an example of AXT.

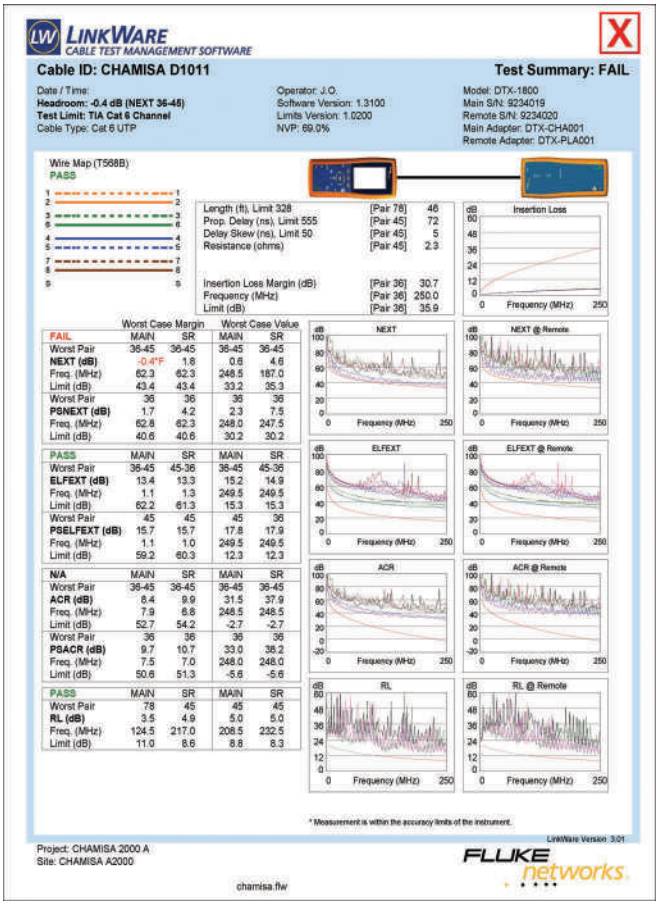
48. What is F/UTP, and what is its purpose?

    F/UTP is foil over twisted-pair cabling, and it provides improved security and noise immunity.

49. Why is balance an issue in UTP cables, and what is TCL?

    The balance or symmetry of the signal over wire pairs helps minimize unwanted leakage of the signal when transmitting Gigabit data rates. TCL, which stands for transverse conversion loss, measures the differential output signal, given a common-mode signal on the input.

50. Answer the following questions related to the certification report shown here.



a. What is the length of pair 7–8?

46 feet

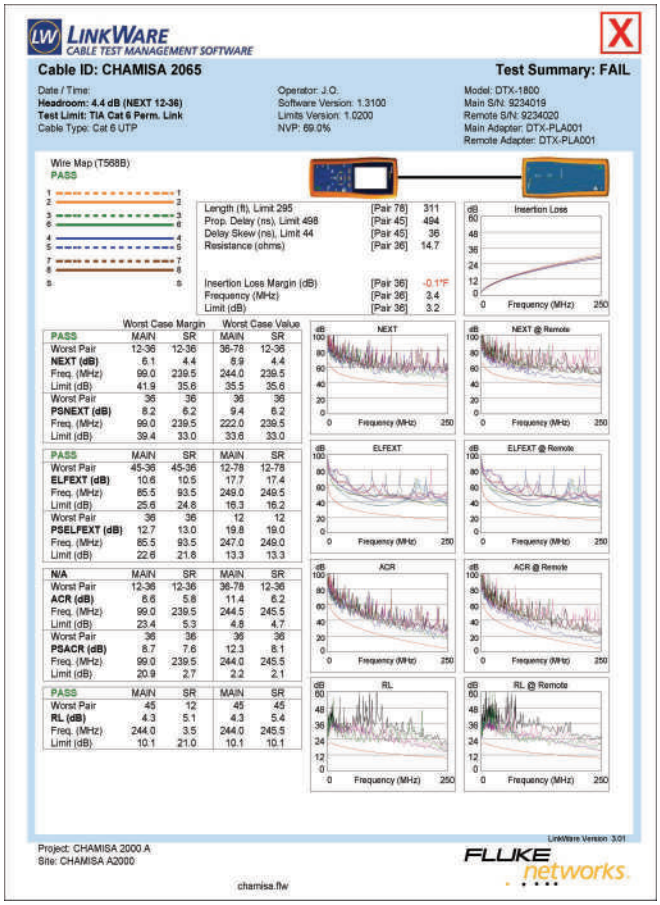
b. What is the length of pair 4–5?

72 feet

c. Why did this cable fail the test?

It failed the NEXT measurement.

51. Answer the following questions related to the certification report shown here.



a. What is the length of wire pair 7–8?

311 feet (which exceeds the maximum length for a permanent link)

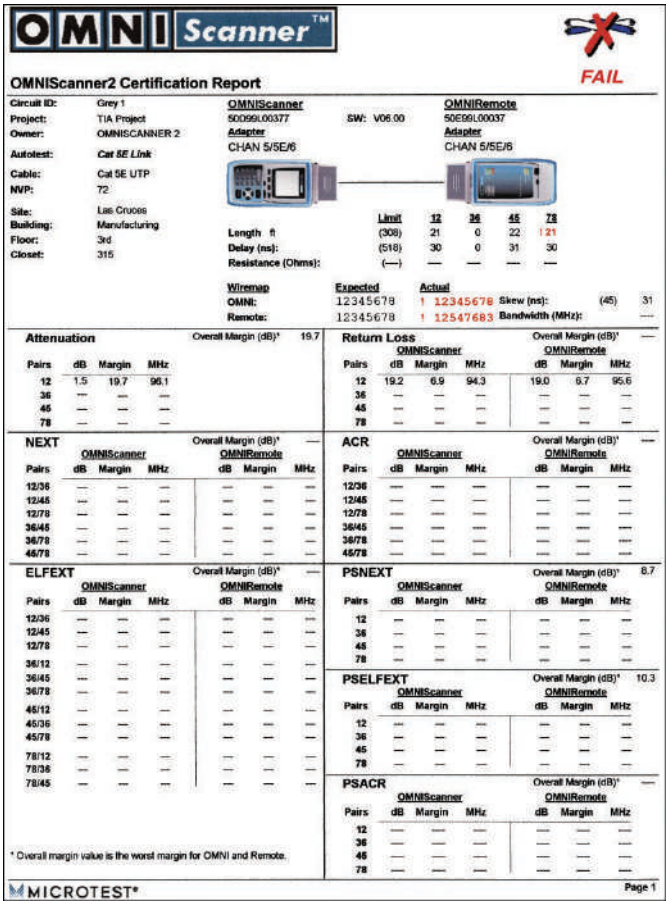
b. What is the delay skew for pair 4–5?

36 ns

c. Why did this cable fail the wiremap test?

The cable is too long.

52. Answer the following questions related to the certification report shown here.



OMNI Scanner™

FAIL

OMNIScanner2 Certification Report

Circuit ID:	Grey 1		
Project:	TIA Project		
Owner:	OMNISCANNER 2		
Autotest:	*Cat 5E Link*		
Cable:	Cat 5E UTP		
NVP:	72		
Site:	Las Cruces		
Building:	Manufacturing		
Floor:	3rd		
Closet:	315		

OMNIScanner		OMNIRemote	
SO090L00377	SW: V06.00	SO090L00037	
Adapter		Adapter	
CHAN 5/5E/6		CHAN 5/5E/6	

	Limit	12	36	45	78
Length ft	(308)	21	0	22	!21
Delay (ns):	(518)	30	0	31	30
Resistance (Ohms):	(—)	—	—	—	—

	Wiremap	Expected	Actual			
	OMNI:	12345678	! 12345678	Skew (ns):	(45)	31
	Remote:	12345678	! 12547683	Bandwidth (MHz):		—

Attenuation — Overall Margin (dB)* 19.7

Pairs	dB	Margin	MHz
12	1.5	19.7	96.1
36	—	—	—
45	—	—	—
78	—	—	—

Return Loss — Overall Margin (dB)* —

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	19.2	6.9	94.3	19.0	6.7	95.6
36	—	—	—	—	—	—
45	—	—	—	—	—	—
78	—	—	—	—	—	—

NEXT — Overall Margin (dB)* —

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12/36	—	—	—	—	—	—
12/45	—	—	—	—	—	—
12/78	—	—	—	—	—	—
36/45	—	—	—	—	—	—
36/78	—	—	—	—	—	—
45/78	—	—	—	—	—	—

ACR — Overall Margin (dB)* —

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12/36	—	—	—	—	—	—
12/45	—	—	—	—	—	—
12/78	—	—	—	—	—	—
36/45	—	—	—	—	—	—
36/78	—	—	—	—	—	—
45/78	—	—	—	—	—	—

ELFEXT — Overall Margin (dB)* —

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12/36	—	—	—	—	—	—
12/45	—	—	—	—	—	—
12/78	—	—	—	—	—	—
36/12	—	—	—	—	—	—
36/45	—	—	—	—	—	—
36/78	—	—	—	—	—	—
45/12	—	—	—	—	—	—
45/36	—	—	—	—	—	—
45/78	—	—	—	—	—	—
78/12	—	—	—	—	—	—
78/36	—	—	—	—	—	—
78/45	—	—	—	—	—	—

PSNEXT — Overall Margin (dB)* 8.7

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	—	—	—	—	—	—
36	—	—	—	—	—	—
45	—	—	—	—	—	—
78	—	—	—	—	—	—

PSELFEXT — Overall Margin (dB)* 10.3

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	—	—	—	—	—	—
36	—	—	—	—	—	—
45	—	—	—	—	—	—
78	—	—	—	—	—	—

PSACR — Overall Margin (dB)* —

Pairs	OMNIScanner dB	OMNIScanner Margin	OMNIScanner MHz	OMNIRemote dB	OMNIRemote Margin	OMNIRemote MHz
12	—	—	—	—	—	—
36	—	—	—	—	—	—
45	—	—	—	—	—	—
78	—	—	—	—	—	—

* Overall margin value is the worst margin for OMNI and Remote.

MICROTEST®

Page 1

a. Why did the cable fail the test?

There are multiple errors with cable wiring.

b. Draw the wiremap diagram for this cable.

1–1 5–7

2–2 6–6

3–5 7–8

4–4 8–3

Section 2-7

53. A data problem is reported to the network administrator. The problem is found to be with the UTP network connection. What steps could the network administrator have taken to isolate the problem? (Select two.)

    a. Visually inspect all UTP terminations.
    b. Run a cable test using a cable tester.
    c. Use the **ping** command to verify network connectivity.
    d. Use pairs 4–5 and 7–8 to repair the connection.
    e. Contact the installer of the UTP cable to obtain a certification report.

Certification Questions

54. A NEXT measurement of 59.5 dB is made on wire pairs 1–2 and 3–6. A NEXT measurement of 51.8 dB is made on wire pairs 3–6 and 7–8. True or false: Pairs 3–6 and 7–8 have the best NEXT performance measurement.

    a. True
    b. False

55. True or false: In regard to CAT5e/CAT6 cable operating in half-duplex mode for Ethernet or Fast Ethernet, pins 1–2 and 3–6 are used to carry the data.

    a. True
    b. False

56. True or false: A CAT5e/6 link test tests from one termination to another.

    a. True
    b. False

57. True or false: Only two wire pairs are used to obtain a proper power-sum measurement.

    a. True
    b. False

58. True or false: Delay skew is critical because if the wire lengths of different wire pairs are significantly different, the data will arrive at the receiver at different times, potentially creating distortion of the data.

    a. True
    b. False

59. Permanent networking cabling within a building ____.

    a. is vertical cabling
    b. belongs to the work area
    c. belongs to the equipment room
    d. None of these answers are correct.

60. How many pins does an RJ-45 modular plug have?

    a. 4
    b. 6
    c. 8
    d. 16
    e. None of these answers are correct.

61. Which of the following best defines horizontal cabling?

    a. Cabling that extends out from the telecommunications closet into the LAN work area
    b. Cabling that extends out from the work area into the LAN
    c. Cabling that extends out from the backbone into the LAN work area
    d. Cabling that extends out from the equipment room into the LAN work area
    e. None of these answers are correct.

62. A UTP certification report lists the following.

Pair	12	36	45	78
Length	! 310	308	! 311	307

    What do these results indicate?

    a. The cable fails the certification test.
    b. Pairs 3–6 and 7–8 will be certified.
    c. Pairs 1–2 and 4–5 will be certified.
    d. The cable passes the certification test.
    e. The ! sign indicates that the cable pair meets or exceeds power-sum test criteria.

63. The length difference in wire pairs for UTP ____.

    a. indicates that the cable should not be certified
    b. indicates that the cable should be certified
    c. is due to the difference in the cable twists for each wire pair
    d. is due to poorly manufactured cable

This page intentionally left blank

3
CHAPTER

Physical Layer Cabling: Fiber Optics

Chapter Outline

3-1 Introduction
3-2 The Nature of Light
3-3 Fiber Attenuation and Dispersion
3-4 Optical Components
3-5 Optical Networking
3-6 Safety
3-7 Troubleshooting Fiber Optics: The OTDR
Summary
Questions and Problems

Objectives

- Describe the advantages of glass fiber over copper conductors
- Describe the differences in how light travels in single-mode fiber and multimode fiber
- Define the terms *attenuation* and *dispersion* as they relate to fiber-optic cabling
- Describe the components of a fiber-optic system
- Describe the issues involved in 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 involved in working with fiber optics

Key Terms

refractive index
infrared light
optical spectrum
cladding
numerical aperture
multimode fiber
pulse dispersion
graded-index fiber
single-mode fiber
long haul
mode field diameter
scattering
absorption
macrobending
microbending
dispersion
zero-dispersion wavelength
dispersion compensating fiber
fiber Bragg grating
DL
LED
distributed feedback (DFB) laser
dense wavelength division multiplexing (DWDM)
vertical cavity surface emitting laser (VCSEL)
tunable laser
fiber, light pipe, or glass
isolator
received signal level (RSL)
fusion splicing
mechanical splice
index-matching gel
SC, ST, FC, LC, MT-RJ
SONET/SDH
STS
FTTC
FTTH
FTTB
FTTD
optical Ethernet
fiber cross-connect
IDC
IC fibers
GBIC
SFP
XENPAK, XPAK, X2, XFP, SFP+
logical fiber map
physical fiber map
mm
sm
backbone
optical link budget
visual fault locator (VFL)
optical time-domain reflectometer (OTDR)
event

Recent advances in the development and manufacture of fiber-optic systems have made them the latest frontier in the field of optical networking. These systems 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 developments in optical networking are Gigabit Ethernet and 10 Gigabit Ethernet.

3-1 INTRODUCTION

This chapter presents a thorough introductory examination of fiber optics and optical networking. The material presented examines the fundamentals of fiber optics through system design. You might choose to focus on Section 3-5, "Optical Networking," if the students have already had an introduction to fiber optics.

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

- 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.
- A source of invisible infrared (IR) radiation—usually a light-emitting diode (LED) or a solid-state laser—light beam can be modulated by digital data or an analog signal.
- A photosensitive detector converts the optical signal back into an electrical signal at the receiver.
- Efficient optical connectors are at the light-source-to-cable interface and at the cable-to-photo detector interface. These connectors are critical when splicing the optical cable due to the fact that excessive loss can occur at connections.

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

- **Extremely wide system bandwidth:** The intelligence is impressed on the light by varying the light's amplitude. The best LEDs have a 5 ns response time and provide a maximum bandwidth of about 100MHz. With laser light sources, however, data rates over 10Gbps are possible with single-mode fiber. The amount of information multiplexed on such a system—in the hundreds of gigabits per second—is indeed staggering.
- **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 and not the metallic cable components or connecting electronics.

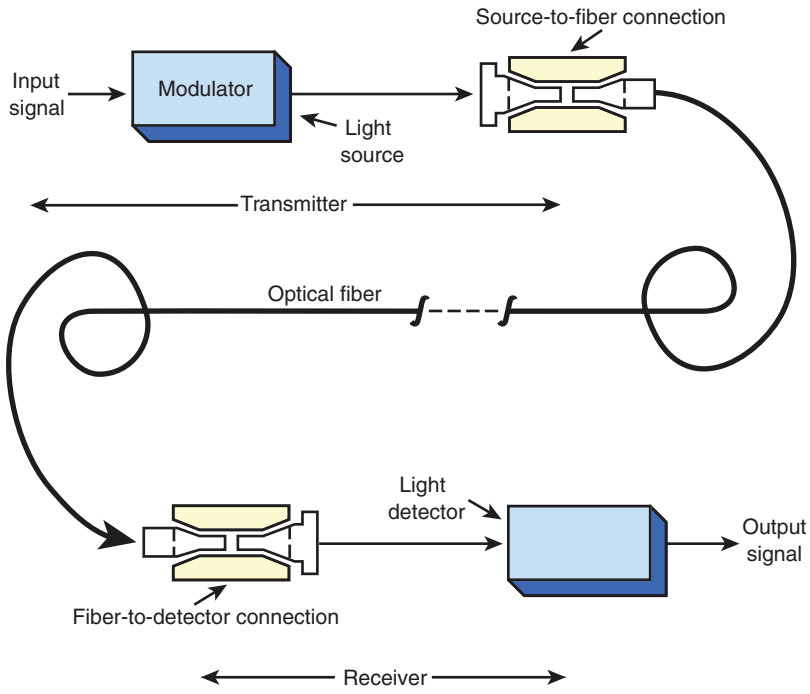


FIGURE 3-1 Fiber-optic communication system. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 781. Copyright © 2002 Pearson Education, Inc. Upper Saddle River, NJ.)

- **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.
- **Lower signal attenuation than with other propagation systems:** Typical attenuation of a 1GHz bandwidth signal for optical fibers is 0.03 dB per 100 feet, compared to 4.0 dB for RG-58U coaxial.
- **Lower costs:** Optical fiber costs are continuing to decline, and the costs of many optical systems are decreasing as fiber is used more and more.
- **Safety:** In many wired systems, the potential hazard of short circuits requires precautionary designs. In addition, the dielectric nature of fiber optics eliminates the spark hazard.
- **Corrosion:** Given that glass is basically inert, the corrosive effects of certain environments are not a problem.
- **Security:** Due to its immunity to electromagnetic coupling and radiation, optical fiber can be used in most secure environments. Although interception and tapping are possible, they are very difficult to do.

This chapter examines optical networking. Section 3-2, "The Nature of Light," presents an overview of optical fiber fundamentals, including a discussion on wavelengths and types of optical fibers. Section 3-3, "Fiber Attenuation and Dispersion," examines the two distance-limiting parameters in fiber-optic transmission: attenuation and dispersion. Optical components are presented in Section 3-4, "Optical Components," including the various types of connectors currently used on fiber. Section 3-5, "Optical Networking," provides an overview of SONET and FDDI, as well as optical Ethernet. It also includes a discussion on setting up a 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, "Safety." Section 3-7 "Troubleshooting Fiber Optics" examines traces obtained from OTDR tests.

Table 3-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 3-1 **Chapter 3 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.2	Explain the characteristics of network topologies and network types.	3-5
1.3	Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	3-2, 3-4, 3-5
1.6	Explain the use and purpose of network services.	3-5
1.7	Explain basic corporate and datacenter network architecture.	3-5
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	3-2, 3-5
2.2	Compare and contrast routing technologies and bandwidth management concepts.	3-4
2.3	Given a scenario, configure and deploy common Ethernet switching features.	3-2, 3-5
2.4	Given a scenario, install and configure the appropriate wireless standards and technologies.	3-4

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	3-2, 3-3, 3-4, 3-5
3.2	Explain the purpose of organizational documents and policies.	3-5
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	3-4, 3-5
4.0	**Network Security**	
4.3	Given a scenario, apply network hardening techniques.	3-4
4.5	Explain the importance of physical security.	3-5
5.0	**Network Troubleshooting**	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	3-2, 3-3, 3-4, 3-5, 3-6
5.4	Given a scenario, troubleshoot common wireless connectivity issues.	3-3
5.5	Given a scenario, troubleshoot general networking issues.	3-6

3-2 THE NATURE OF LIGHT

This section provides an introduction to the basics of light refraction and reflection. The concepts presented in this section are important because many of them are used when fiber is described in the literature or data sheets. Key concepts are multimode fiber, single-mode fiber, and pulse dispersion.

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 meters per second 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(a). The speed reduction and subsequent refraction are different for each wavelength, as shown in Figure 3-2(b). The visible light striking the prism in this figure 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 (that is, the various frequencies).

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.

Refractive Index
The ratio of the speed of light in free space to its speed in a given material

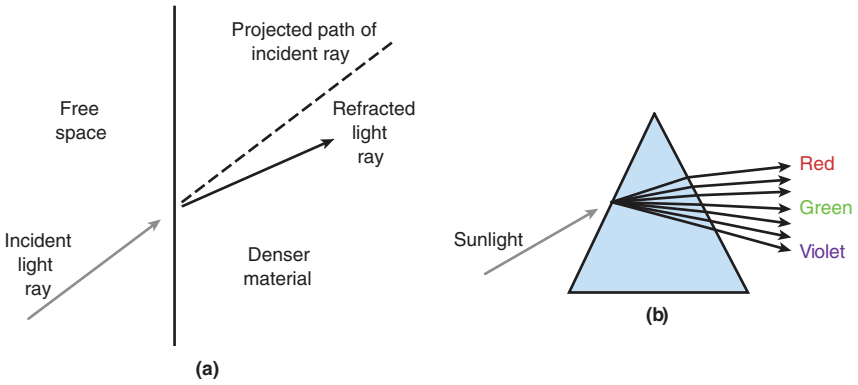


FIGURE 3-2 Refraction of light. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 782. Copyright ©2002 Pearson Education, Inc. Upper Saddle River, NJ.)

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 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**.

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

Optical Spectrum
Light frequencies from the infrared on up

These are the commonly used wavelengths in today's fiber-optic systems:

- **Multimode fiber:** 850 and 1310 nm
- **Single-mode fiber:** 1310 and 1550 nm
- **Fiber-to-the-home/fiber-to-the-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; plastic cladding of a glass fiber is available but rarely used. In any event, the refraction indexes 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 of optical fiber, which must have a lower index of refraction to keep the light in the core

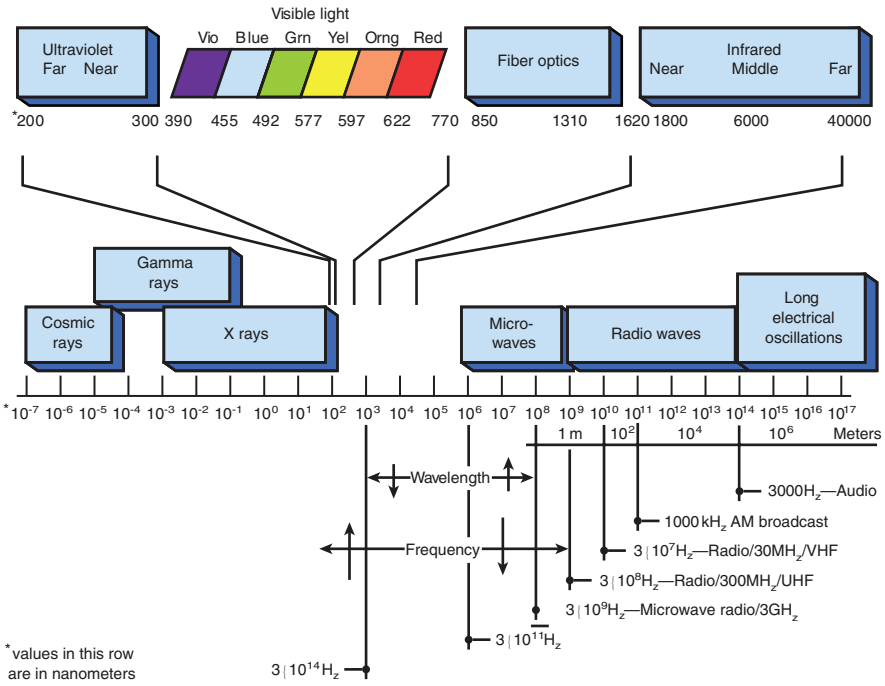


FIGURE 3-3 The electromagnetic wavelength spectrum. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 784. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

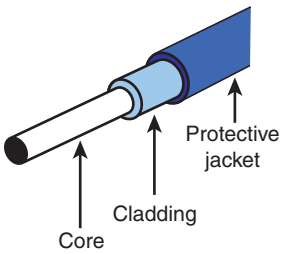


FIGURE 3-4 Single-fiber construction. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 785. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

Another measure of a fiber's light acceptance is **numerical aperture**, which 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.

Numerical Aperture
A measure of a fiber's ability to accept light

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



FIGURE 3-5 Fiber strands (focal point/Shutterstock).

Multimode Fiber
A fiber that supports many optical waveguide modes

The difficulty of coupling significant light into such a small fiber led to the 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 multimode fiber, termed *graded-index fiber*, was subsequently developed and 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 led to their use at 1300 nm, 1550 nm, and 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:

- Signal losses
- Ease of light coupling and interconnection
- Bandwidth

Figure 3-6 illustrates a fiber with three modes (that is, multimode) of propagation:

- The lowest-order mode is 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.

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, termed **pulse dispersion**, limits the maximum distance and rate at which data (pulses of light) can be practically transmitted. In addition, the output pulse has reduced amplitude as well as increased width. The greater the fiber length, the more pronounced this effect. As a result, manufacturers rate their fiber in bandwidth per length. For example, the rating 400MHz/km means the fiber can successfully transmit pulses at the rate of 400MHz for 1 kilometers, 200MHz for 2 kilometers, and so on. In fact, current networking standards limit multimode fiber distances to 2 kilometers. 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.

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

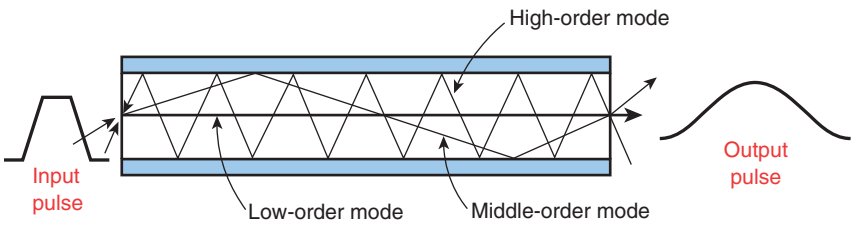


FIGURE 3-6 Modes of propagation for step-index fiber. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 787. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

Graded-Index Fiber

In an effort to overcome the pulse-dispersion problem, **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 transmission distances before pulse dispersion effects destroy intelligibility and introduce bit errors.

Graded-Index Fiber
Fiber in which the index of refraction is gradually varied with a parabolic profile

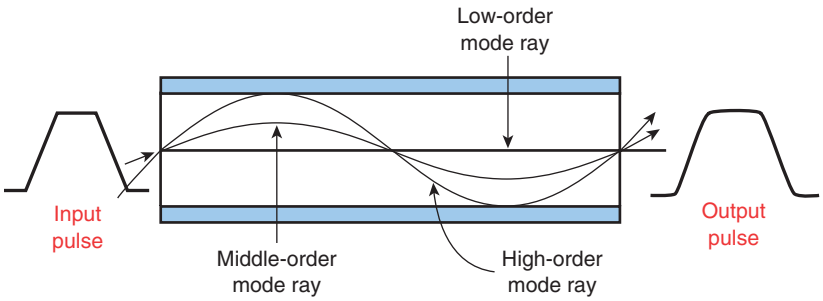


FIGURE 3-7 Modes of propagation for graded-index fiber. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 788. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

Graded-index multimode fibers with 50 µm-diameter cores and 125 µm cladding are used in many telecommunication systems at up to 300Mbps 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: 50 µm and 62.5 µm. Both have 125 µm cladding. The large core diameter and the high numerical aperture (NA) of these fibers simplify input cabling and make it possible to use 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, in which 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 of fiber 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 lasers. Fibers of this variety are called **single-mode** (or monomode) **fibers**. Core diameters of only 7–10 µm are typical. Figure 3-8 provides a graphical summary of the three types of fiber discussed in this section, including typical dimensions, refractive index profiles, and pulse-dispersion effects.

Long Haul
Refers to 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 repeater spacing of up to 80 km. These bandwidth and repeater spacing capabilities are constantly being upgraded with new developments.

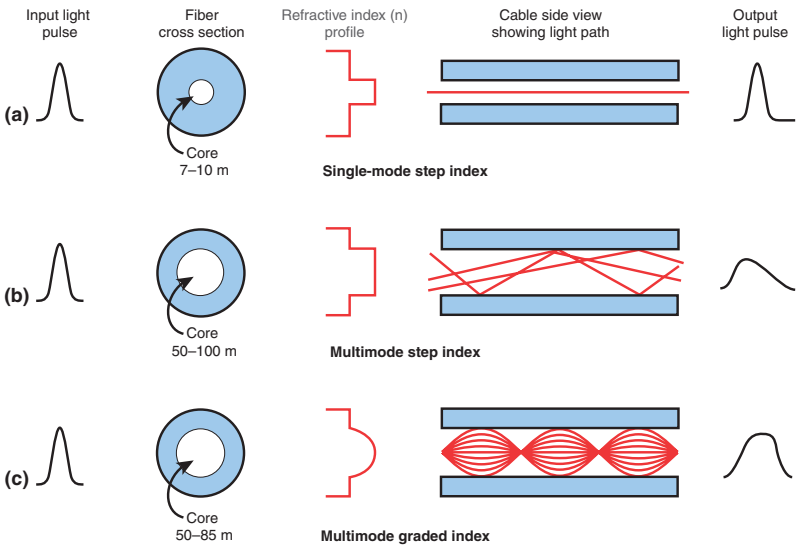


FIGURE 3-8 Types of optical fiber. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 789. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

When describing the core size of single-mode fibers, the term **mode field diameter** is commonly used. Mode field diameter is the actual guided optical power distribution diameter. In a typical single-mode fiber, the mode field diameter is approximately 1 μm 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.

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 covers the following Network+ exam objectives.

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

This section introduces the concept of multimode fiber and examines the three modes of operation.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section examines single-mode fibers, which are widely used in long-haul and WAN applications. They permit transmission of about 10Gbps and repeater spacing of up to 80 kilometers. These bandwidth and repeater spacing capabilities are constantly being upgraded with new developments.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section examines the concept of refractive index, which is the ratio of the speed of light in free space to its speed in a given material.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

The concept of bandwidth of the various fiber cables are examined in this section.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section examines the various limitations on distance for various types of fiber.

Test Your Knowledge

1. What light waves are just below the frequencies in the visible spectrum?
   a. Sub-light waves
   b. Infrared light waves
   c. Refractive waves
   d. Multimode waves
   e. Polar waves

2. What is the name for the material surrounding the core of an optical waveguide?

   a. Cladding
   b. Aperture
   c. Mode field
   d. Step-index
   e. Graded-index

3. True or false: Single-mode fiber cables have a core diameter of about 7–10 micrometers.

   True

3-3 FIBER ATTENUATION AND DISPERSION

The two distance-limiting parameters in fiber-optic transmission, attenuation and dispersion, are presented in this section. Students need to become familiar with these concepts. A good understanding of these topics will make it easier for students to work with system design issues (covered in Section 3-6).

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

Attenuation

Attenuation is the loss of power introduced by 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 attenuation, or loss, of the signal is due to the combination of four factors: scattering, absorption, macrobending, and microbending. There are also two types of attenuation: intrinsic and extrinsic.

Scattering
An attenuation factor caused by refractive index fluctuations, which accounts for 96% 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

Scattering is the primary loss factor over the three wavelength ranges. Scattering in telecommunication systems accounts for 96% 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. Scattering known as Rayleigh scattering is caused by refractive index fluctuations. Rayleigh scattering decreases as wavelength increases, as shown in Figure 3-9.

The second loss factor, **absorption**, is 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 hydroxoyl ions dissolved in the glass during manufacture. They cause the water attenuation or OH peaks, shown in Figure 3-9, and other attenuation curves.

Macrobending is 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 a 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 contribute to this loss. This loss is noted in fractions of a decibel.

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

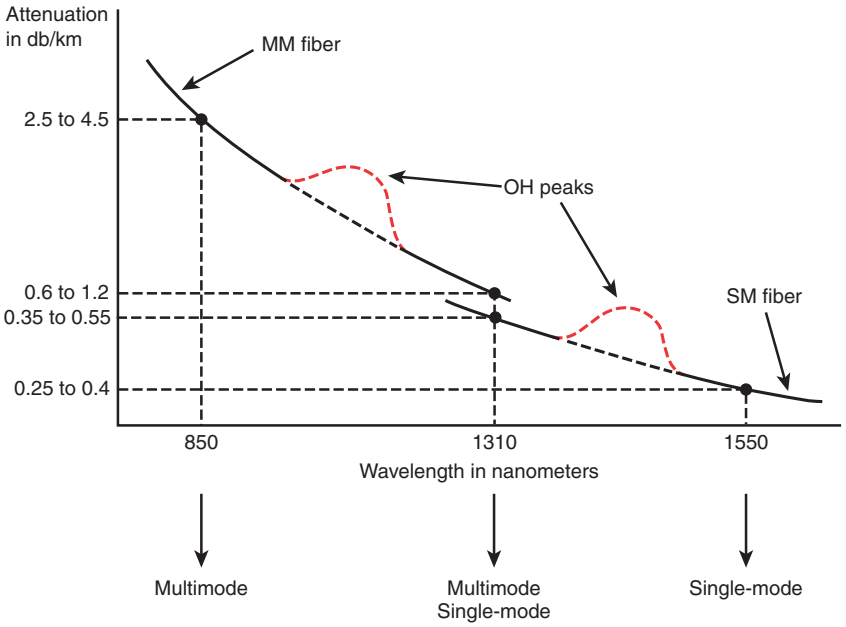


FIGURE 3-9 Typical attenuation of cabled fiber strands. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 792. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

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

There are three types of dispersion:

- **Modal dispersion:** The broadening of a pulse due to different path lengths being 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.

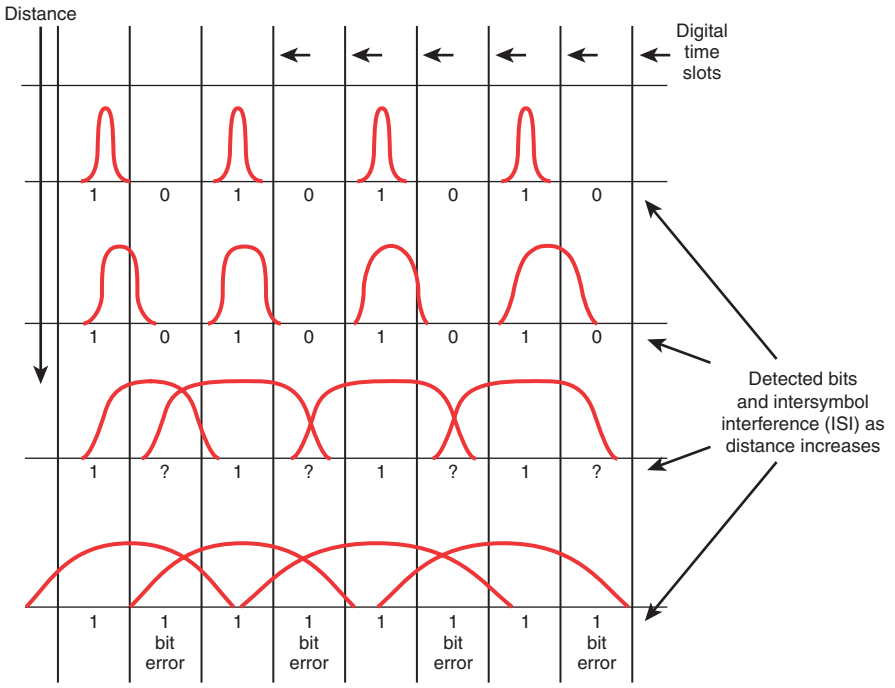


FIGURE 3-10 Pulse broadening or dispersion in optical fibers. (Adapted from *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 793. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

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 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 (refer to 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 (whether laser or LED) produces several different wavelength light rays when generating the light pulse. The light rays travel at different velocities, and as a result, these rays arrive at the receiver detector at different times, causing the broadening of the pulse.

Zero-Dispersion Wavelength
The point at which dispersion is zero

There is a point at which dispersion is actually at zero, and it is determined by the refractive index profile. It 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 occurs 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 it becomes a 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.

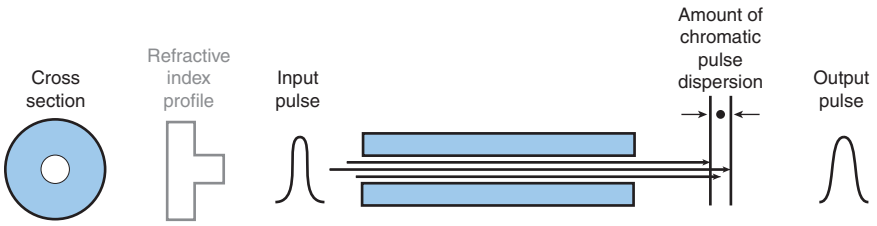


FIGURE 3-11 Polarization mode dispersion in single-mode fiber. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 794. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

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 as an equalizer, with 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 introduces some insertion loss (3–10 dB) and may require the addition of an optical-line amplifier.

A relatively 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
Fiber that acts as 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 covers the following Network+ exam objectives.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section examines the issues of increasing bandwidth in certain fiber-optic cables.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

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

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

This section examines 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.*

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 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 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

The basic components used in optical networking are presented in this section. Students should know what an attenuator does, the basic issues related to a tunable laser, and how wave division multiplexing works. In addition, they need to understand at least the basic connectors used in optical networking.

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 an optimum system, the special qualities of each light source should be considered. Diode lasers and LEDs bring different characteristics to systems:

- Power levels
- Temperature sensitivities
- Response times
- Lifetimes
- 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 μW). 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 DLs 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, in the range 0.01–0.1 nm. This allows the use of more channels in **dense wavelength division multiplexing (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 face some of the operational and stability problems that plague conventional lasers, however.

VCSELs offer the simplicity of LEDs and the performance of lasers. Their primary wavelengths of operation are in the 750–850 nm region and the 1310 nm region.

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

DL
Diode laser, the preferred light source for moderate-band to wideband fiber-optic communication systems

LED
Light-emitting diode, a light source used in fiber-optic communication systems that operate at a slower bit rate and require more modest levels of fiber-coupled optical power

Distributed Feedback (DFB) Laser
A relatively stable laser that is suitable for use in DWDM systems

Dense Wavelength Division Multiplexing (DWDM)
A system that incorporates the propagation of several wavelengths in the 1550 nm range for a single fiber

Vertical Cavity Surface Emitting Laser (VCSEL)
A laser that offers the simplicity of an LED and the performance of a laser

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

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 network operations environments that involve DWDM. 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.

A technique that is now being used to combine multiple channels with different wavelengths for transmission over fiber-optic cables is coarse wavelength division multiplexing (CWDM). CWDM channels have 20 nm separation and use low-cost lasers that don't require cooling. This technology is useful for up to 70 kilometers. The wavelengths used in this technology are 1620 nm, 1590 nm, 1570 nm, 1550 nm, 1530 nm, 1510 nm, 1490 nm, and 1470 nm.

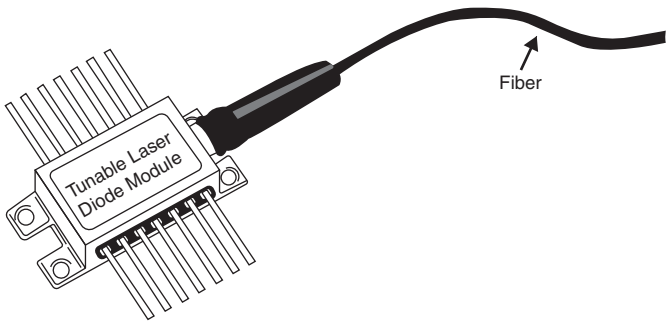


FIGURE 3-12 A tunable laser diode module.

Intermediate Components

Fiber, Light Pipe, or Glass
Terms used to describe a fiber-optic strand

A typical fiber-optic telecommunication link (refer to 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:

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

- **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.

Fiber termination kits provide many common tools for terminating and joining optical fibers. They are typically joined either in a permanent fusion splice or with a mechanical splice (for example, connectors and camsplices). 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 are 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% displacement. Figure 3-13 illustrates this condition as well as other loss sources.

Angular misalignment, illustrated in 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 because 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 with polishing or by using prepolished 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. Four other situations can cause additional connector or splice loss, although in smaller values, as shown in Figure 3-13(e), (f), (g), and (h). These situations 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 through the use of a rotary mechanical splice, which by the joint rotation will get a better core alignment.

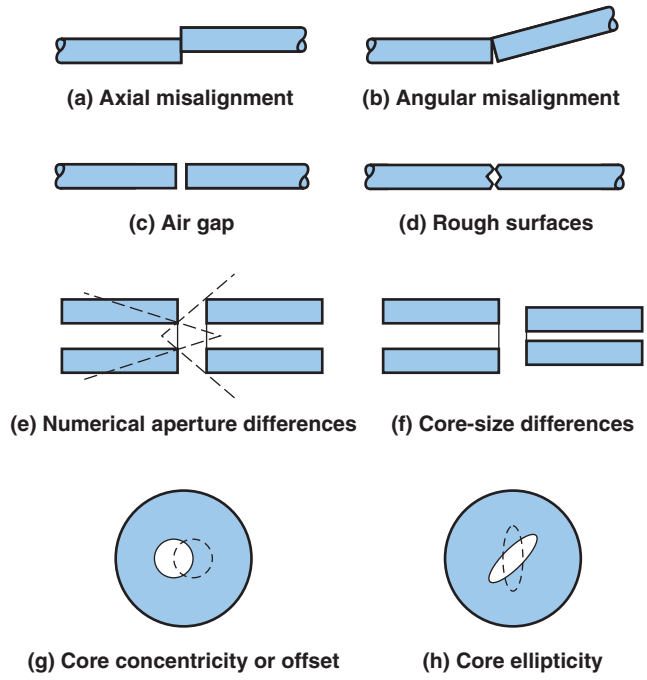


FIGURE 3-13 Sources of connection loss. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 806. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

Fusion Splicing
A long-term splicing method in which two fibers are fused or welded together

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, budget. Typical insertion losses of less than 0.1 dB—frequently in the 0.05 dB range—can be consistently achieved.

Mechanical Splice
A splice in which two fibers are joined together with an air gap, 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 that of glass than to that of air

Mechanical splices can be permanent and an economical choice for certain fiber-splicing applications. Mechanical splices 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 that of glass than to that of 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.

Considering that the core diameter of a single-mode fiber is only 9 μm, it is easy to understand that dirty optical cables can easily degrade data performance. Problems can result from a dirty fiber cable endface or loose contamination preventing good physical glass-to-glass contact.

The best method for splicing depends on the application, including the expected future bandwidth (for example, Gigabit), traffic, the job size, and economics. The loss in a mechanical splice can be minimized by using an optical time-domain reflectometer (OTDR) to properly align the fiber while making the splice.

Fiber Connectorization

There are several choices on the market for fiber connectorization, including **SC, ST, FC, LC,** and **MT-RJ**. The choice of the connector is typically dictated by the hardware being used and the fiber application. Figure 3-14 provides examples of SC, ST, FC, LC, and MT-RJ connectors

SC, ST, FC, LC, MT-RJ
Typical optical fiber connectors

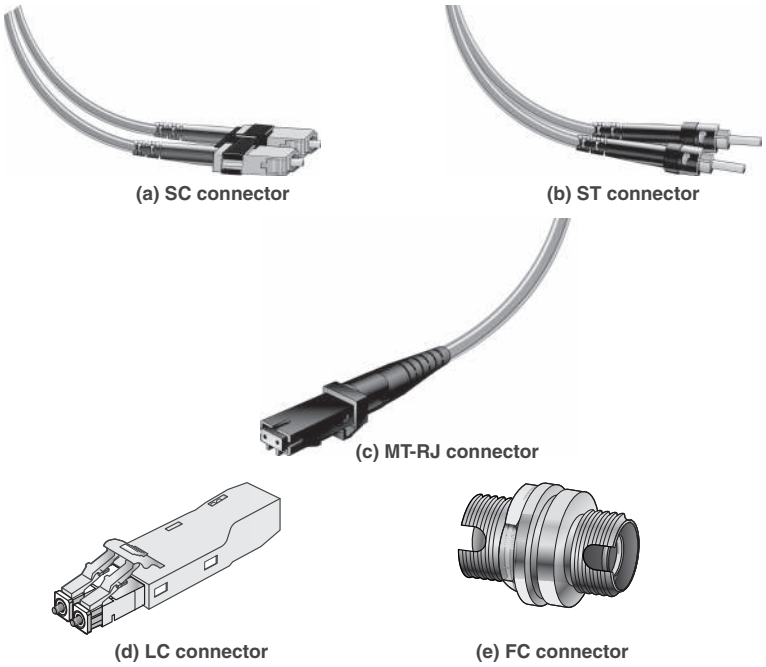


FIGURE 3-14 Typical fiber connections. [(a), (b), and (c) from *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 808. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ. (d) and (e) from Black Box Corporation.]

Some general features of fiber connectors are as follows:

- They are easy and quick to install.
- They offer low insertion loss. A properly installed connector has as little as 0.25 dB insertion loss.
- They provide a high return loss (greater than 50 dB). This is increasingly important in Gigabit networks, DWDM systems, high-bandwidth video, and so on.
- They offer repeatability.
- They are economical.

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

Is it not advisable to splice 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 a result of tests with 50 µm and 62.5 µm multimode fiber for a local area network.

Two additional concepts associated with fiber are APC and UPC. The difference between these two types of connectors is the fiber endface. An angled physical contact (APC) endface is polished and has an 8-degree angle. An ultra-physical contact (UPC) endface is polished and has no angle. APC and UPC connectors are easily identified by their color: APC adapters are green, and UPC adapters are blue.

Sometimes it may be necessary to verify that light is passing through an unconnected fiber. To do so, the fiber must not be connected to anything at either end. A light meter is sometimes used for this purpose. The function of a light meter is to shine light down a fiber, providing a safe way to visually verify that light is propagating down a fiber.

Section 3-4 Review

This section covers the following Network+ exam objectives.

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

This section examines the various fiber terminations, including LC, ST, SC, and MT-RJ. Figure 3-13 shows issues with connection loss, and Figure 3-14 shows different types of connectors.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

This section introduces tunable lasers, which are used along with either passive or tunable wavelength division multiplexing (WDM) filters to accommodate dynamic routing or networking, bandwidth on demand, seamless restoration (serviceability), optical packet switching, and so on.

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

One technique being used to combine multiple channels with different wavelengths for transmission over fiber-optic cables is coarse wavelength division multiplexing (CWDM).

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

Diode lasers and LEDs bring different characteristics to systems, including power levels, temperature sensitivities, response times, lifetimes, and characteristics of failure.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section introduces the concept of attenuators, which are used to reduce the received signal level (RSL). They are available in fixed and variable configurations.

4.3 Given a scenario, apply network hardening techniques.

Diode lasers and LEDs bring different characteristics, such as power levels, to systems.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section discusses using an OTDR to properly align the fiber while making a splice. The concept of fusion splicing is also examined.

Test Your Knowledge

1. What is fusion splicing?
   a. A temporary method for splicing fiber
   b. An inexpensive alternative to mechanical splicing
   c. A type of splicing that requires index-matching gel
   d. A long-term method in which two fibers are fused or welded together
2. True or false: The function of an attenuator is to reduce the received signal level.

   True

3-5 OPTICAL NETWORKING

This section provides an overview of optical networking, including concepts such as fiber-to-the-home and fiber-to-the-business. This section also introduces optical Ethernet, which provides high-speed data delivery with fiber-optic links. This section also includes discussions on some important issues encountered when designing a fiber-optic network.

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 as the cost of fiber infrastructure decreases, fiber is more and more being chosen to carry data. Of course, the copper infrastructure is already in place, and new developments are providing increases in data speed over copper (for example, CAT6, CAT6a, CAT7, and CAT8). However, optical fiber is smaller and easier to install in already crowded ducts and conduits. In addition, 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 in order 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. DWDM 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 1022 wavelengths over a single fiber. This transport of multiple wavelengths opens up possibilities for 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 Synchronous Digital Hierarchy (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:

SONET/SDH
Synchronous Optical Network/Synchronous Digital Hierarchy; protocol standards for optical transmission in long-haul communication

- 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 specifies the various optical carrier (OC) levels and the equivalent electrical Synchronous Transport Signal (**STS**) used for transporting data in a fiber-optic transmission system. Optical network data rates are typically specified in terms of the SONET hierarchy. When a digital signal is carried over SONET, the signal is essentially enveloped or encapsulated within the optical carrier. Table 3-2 lists the most common data rates. The table shows the capacity, not equivalence. It merely states that OC-1 is capable of carrying 28 DS-1s or 1 DS-3. With the conversion overhead, it yields a bit rate of 51.84Mbps when carrying one DS-3 signal.

STS
Synchronous Transport Signal, an electrical signal used for transporting data in a fiber-optic transmission system

TABLE 3-2 **SONET Hierarchy Data Rates***

Signal	Bit Rate	Capacity
OC-1 (STS-1)	51.840Mbps	28 DS-1s or 1 DS-3
OC-3 (STS-3)	155.52Mbps	84 DS-1s 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-1s 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, which is being deployed today, 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-speed digital subscriber line). This is a cost-effective way to provide large bandwidth capabilities to a home. Currently, the Google Fiber project is at the forefront of FTTH. It has deployed FTTH in several cities, including Kansas City, Austin, Provo, Salt Lake City, Charlotte, Atlanta, Durham, and Nashville.

FTTC
Fiber-to-the-curb, an optical architecture that provides high bandwidth to a location with proximity to the home and provides a high-speed data link, via twisted-pair, using VDSL

FTTH
Fiber-to-the-home, an optical architecture that connects directly to the home

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

FTTB
Fiber-to-the-business, an optical architecture in which a fiber connection to a business provides for the delivery of all current communication technologies

FTTD
Fiber-to-the-desktop, an optical architecture that requires a computer to have a fiber NIC

Conventional high-speed Ethernet networks are operating over fiber. This configuration, called **optical Ethernet**, uses the numerics listed in Table 3-3 for describing the types of network configuration. Fiber helps eliminate the 100 meter distance limit associated with unshielded twisted-pair (UTP) copper cable. This is possible because fiber has lower attenuation loss. In a star network, the computer and the switch are directly connected. If 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 each end, as shown in Figure 3-15. The media converter is typically built in to the NIC.

Optical Ethernet
Ethernet data running over a fiber link

A technology associated with fiber-to-premises is a smart jack, which is a network interface device (NID) that provides the connection point and also has built-in diagnostic capabilities.

TABLE 3-3 **802.3 Physical Media Types for Optical Ethernet**

Name	Description
10BASE-F	10Mbps Ethernet over fiber; a generic specification for fiber
10BASE-FB	10Mbps Ethernet over fiber; part of the IEEE 10BASE-F 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; replaces the FOIRL specification
10BASE-FP	A passive fiber star network; segments can be up to 500 m in length
100BASE-FX	A 100Mbps multimode fiber technology; uses a 1300 nm wavelength; transmission distances can be up to 2 km
100BASE-SX	A lower-cost alternative to 100BASE-FX; uses LEDs instead of lasers and can be used for shorter distances (up to 300 meters)
1000BASE-LX	Gigabit Ethernet standard that uses fiber strands using long-wavelength transmitters
1000BASE-SX	Gigabit Ethernet standard that uses short-wavelength transmitters
10GBASE-R	10 Gigabit (10.325Gbps) Ethernet for LANs
10GBASE-SR	10 Gigabit Ethernet; physical layer standard for use with multimode fibers for a short range of 300 to 400 m
10GBASE-LR	10 Gigabit Ethernet; physical layer standard for use with single-mode fibers for a long range of 10 km
10GBASE-ER	10 Gigabit Ethernet; physical layer standard for use with single-mode fibers for extended range or reach up to 40 km
10GBASE-W	10 Gigabit (9.95328Gbps) Ethernet for WANs using OC-192 and SONET framing
10GBASE-SW	10 Gigabit Ethernet; physical layer standard for WAN connection; designed for longer-distance connections, like SONET, with extra encapsulation support; maximum distance of 80 km

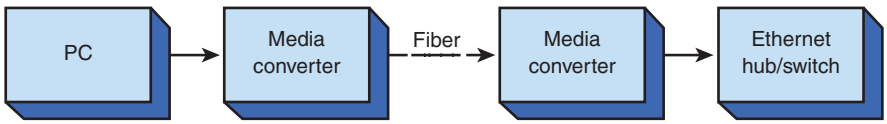


FIGURE 3-15 An example of connecting a PC to an Ethernet hub or switch via fiber. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 820. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

Two important issues must be considered when designing a fiber network:

- 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, and the second is 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 full-duplex mode, which means the links must be able to simultaneously transmit and receive—hence the need for two fibers on each link. This is also referred to as *duplex operation*.

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 an optical patch panel used to connect fiber cables to the next link at the fiber distribution panel. A fiber cross-connect typically uses mechanical splices to make the fiber connections.

Fiber Cross-Connect
An optical patch panel used to interconnect fiber cables

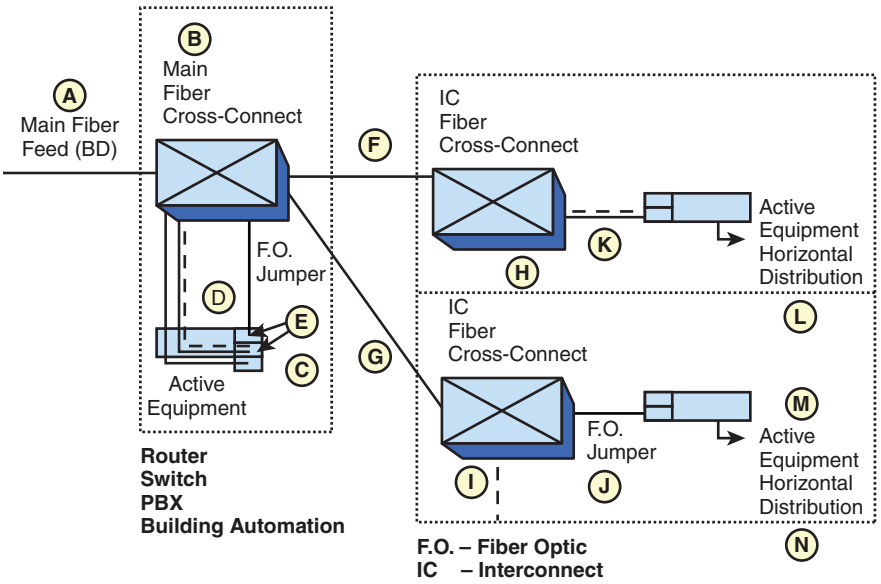


FIGURE 3-16 A simple fiber distribution panel for a building.

Figure 3-17 shows an example of a fiber patch panel.

In Figure 3-16, 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).

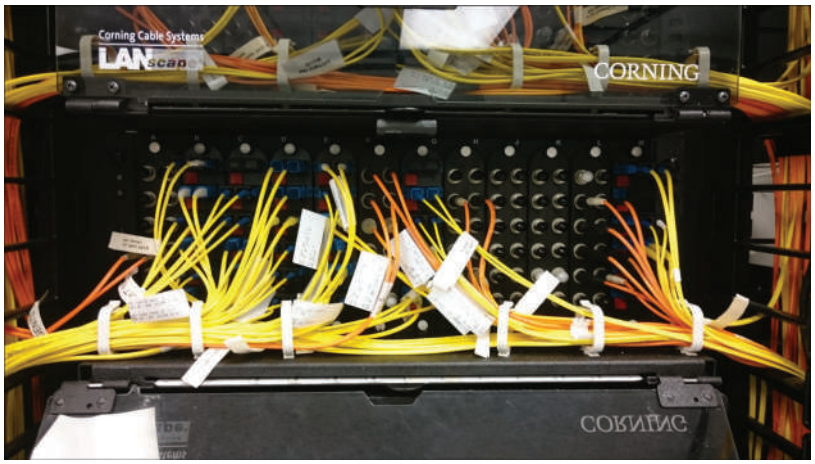


FIGURE 3-17 An example of a fiber patch panel.

IDC
Intermediate distribution closet

IC Fibers
Interconnect fibers

In 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. 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 "two 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. These distributions are also known as IDF/MDF (intermediate distribution frame/main distribution frame).

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

GBIC
Gigabit Interface Converter, a hot-swappable fiber-optic transceiver

The active equipment needs some type of fiber-optic transceiver for transmitting and receiving higher-speed signals over fiber-optic lines. There are transceiver types to use for each media type such as Ethernet transceivers and wireless transceivers. A Gigabit interface converter (**GBIC**; pronounced "gee-bick") shown in Figure 3-19(a), is a hot-swappable fiber-optic transceiver. It is very important to not select or install incorrect transceivers.

SFP
Small form-factor pluggable

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). The SFP shown in Figure 3-19(b) is less than half the size of the GBIC shown in Figure 3-19(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.

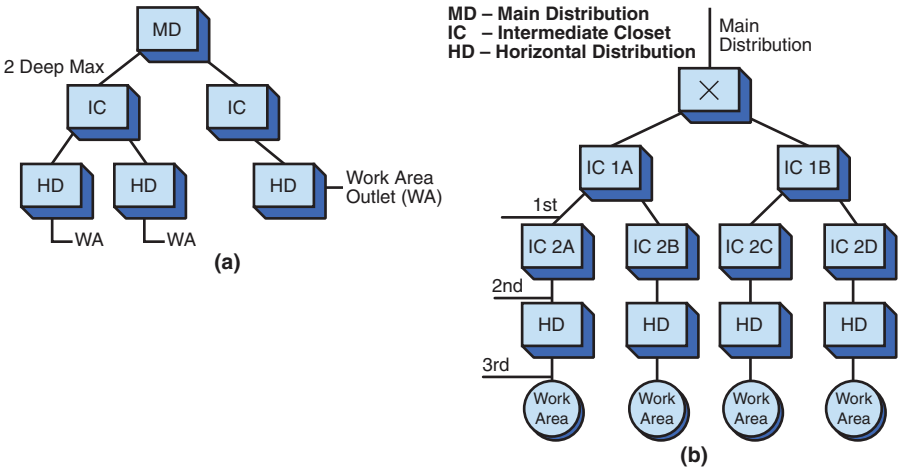


FIGURE 3-18 Examples of the "two deep" rule: (a) the distribution meeting the requirement; (b) the distribution not meeting the requirement.

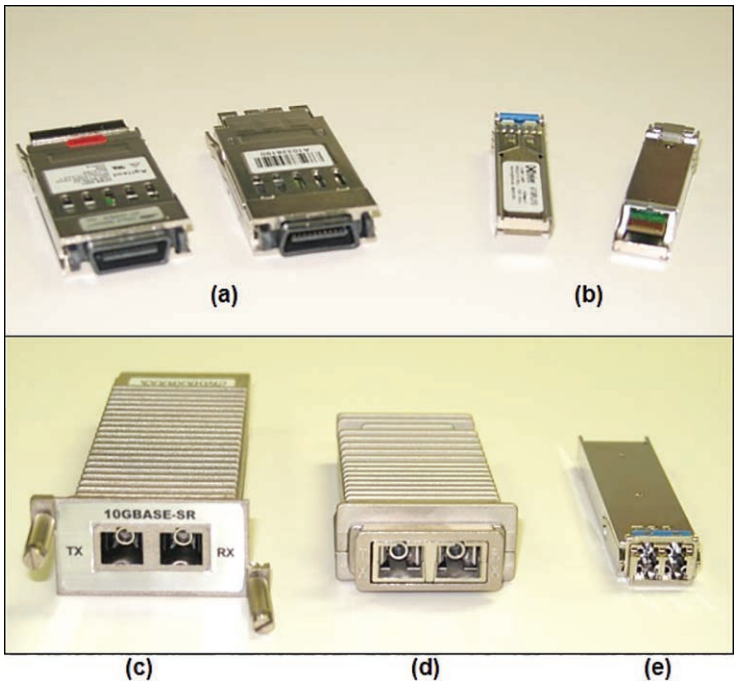


FIGURE 3-19 The Cisco (a) GBIC, (b) SFP, (c) XENPAK, (d) X2, and (e) XFP optical-to-fiber transceivers (courtesy of Cisco).

In the 10 Gigabit (10Gbps) Ethernet world, several versions of optical-to-fiber transceivers have been developed. It all started with the **XENPAK**, shown in Figure 3-19(c), transceivers, which were followed by the **XPAK** and the **X2**, shown in Figure 3-19(d). These later transceiver modules are smaller than the XENPAK. Then, an even smaller module called XFP was developed. The **XFP**, shown in

XENPAK, XPAK, X2, XFP, SFP+
10 Gigabit interface adapters

Figure 3-19(e), has lower power consumption than the XENPAK, XPAK, and X2, but it still can deliver up to 80 kilometers 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 10 Gigabit transceiver. Recently, a new type of 10G transceiver has emerged, however: the **SFP+**. Its looks just like a 1000BASE SFP transceiver and is the same size. To be able to deliver 10 Gigabit speed in its small form factor, the working distance that the SFP+ can deliver is reduced to 40 kilometers. So, if distance is not of concern, SFP+ might be the 10 Gigabit transceiver of choice. These modules support 850, 1310, and 1550 fiber wavelengths. Figure 3-19 shows examples of all these 1000BASE and 10GBASE transceivers. A quad small form-factor plus (QSFP+) is a new compact, hot-pluggable transceiver that has four SFP+ interfaces—that is 4 channels of 10Gbps date rate, so it can transfer up to 40Gbps.

In regard to characteristics of fiber transceivers, an optical transceiver chip is an integrated circuit (IC) that transmits and receives data using optical fiber rather than electrical wire. Almost all modern optical transceivers provide bidirectional data transmission by using two fibers to transmit data between switches, firewalls, servers, routers, and so on. The first fiber is dedicated to receiving data from networking equipment, and the second fiber is dedicated to transmitting data to the networking equipment.

A new optical transceiver technology is now available that allows transceivers to both transmit and receive data to/from interconnected equipment through a single optical fiber. This technology first emerged in 2012 and has led to the development of bidirectional (BiDi) transceivers. The primary difference between BiDi transceivers and traditional two-fiber fiber-optic transceivers is that BiDi transceivers are fitted with WDM couplers, also known as *diplexers*, which combine and separate data transmitted over a single fiber based on the wavelengths of the light. For this reason, BiDi transceivers are also referred to as WDM transceivers.

Note

It is very important to avoid transceiver mismatch. Incorrectly selected transceivers can create communication losses.

Campus Distribution

Logical Fiber Map
A map that shows how fiber is interconnected and data is distributed throughout a campus

Physical Fiber Map
A map that shows the routing of fiber and also shows detail about the terrain, underground conduit, and entries into buildings

Figure 3-20 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. Figure 3-21 shows another style of map often used to show the fiber distribution: a **physical fiber map**. This map shows the routing of the fiber and also shows detail about the terrain, underground conduit, and entries into buildings. Both logical and physical maps (diagrams) are important and necessary for documentation and planning of a fiber network. This section focuses on the documentation provided in the logical fiber map.

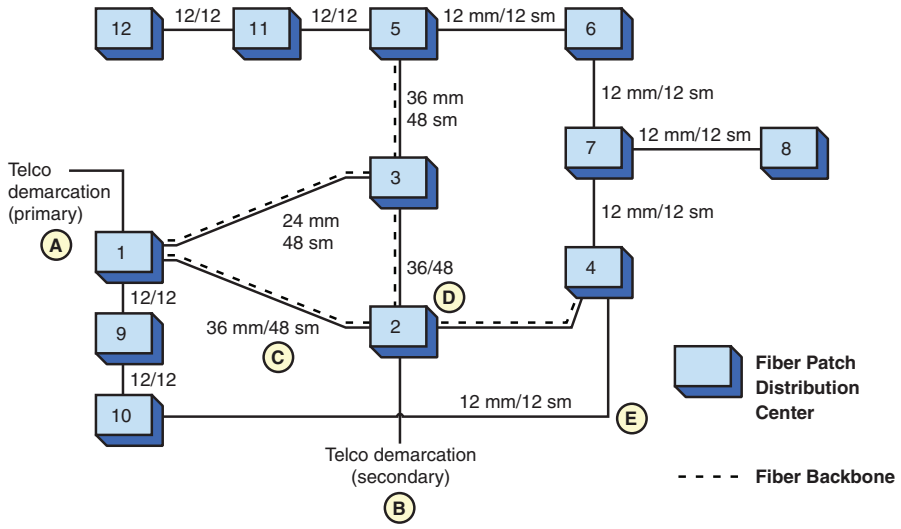


FIGURE 3-20 A logical fiber map.

The campus network in Figure 3-20 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 WAN 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 bottlenecking. 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 (the dotted line) also extends from building 2 to building 4 and from building 3 to building 5.

mm
Multimode

sm
Single-mode

Backbone
The main fiber distribution for a network

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, 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 3-21 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 has two bundles: one bundle of multimode and one bundle of single-mode fiber. A 36/48 cable has three bundles of multimode and four 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 three 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-Coding for the 12 Fibers in a Bundle**

Bundle	Color
1/2	Blue/orange
3/4	Green/brown
5/6	Slate/white
7/8	Red/black
9/10	Yellow/violet
11/12	Rose/aquamarine

In the Figure 3-20 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 lower, 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 that 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, it is important to 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 great capacity, enabling fast transfer of data, minimizing congestion problems, and providing 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 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 3-3, earlier in this chapter, to describe the network configuration.

Optical Link Budget

Now that you have learned how to design optical networks and interconnect the optical links, you need to know how to ensure that the signals will arrive at the destination with the desired received signal level (RSL). This section demonstrates the steps required for calculating an **optical link budget**. Basically, an optical link budget begins with the transmitter output power and then subtracts the losses. Losses can be from fiber splices or from patch panels, pig-tails, or multiplexers.

Optical Link Budget
A set of calculations used to verify that the proper received signal level (RSL) is received

You need to use the manufacturer specifications to determine the transmit power and subtract losses due to cable losses, splice losses, connector losses, and extra losses from any mechanical or WDM devices. Figure 3-22 provides an example of a link budget calculation.

Link Budget calculation
+ Transceiver Output Power
  - Cable losses
  - Splice losses
  - Connector losses
  - Extra losses

= Total Link Budget

FIGURE 3-22 An optical link budget calculation.

A positive result for the total link budget indicates that the proper signal level will be received at the receiver. A negative result indicates that the signal level is not sufficient to properly drive the receiver.

To practice calculating a link budget, try this example. Provide a link budget calculation given the following:

Transceiver output power of –15 dBm
6 splices at 0.1 dB each
2 connectors at 0.3 dB each
Total link budget = –15 dBm – (6 × 0.1) – (2 × 0.3)
= –15 dBm – 0.6 dB – 0.6 dB = –16.2 dBm

Next, compare the total link budget to the desired RSL, which is the minimum signal level required to meet the desired bit error rate (BER) for the receiver. In this case, the desired RSL is –18 dBm; therefore, the system has 1.8 dB of extra margin.

Note

dBm is a unit of level used to indicate that a power level is expressed in decibels (dB) with reference to 1 milliwatt (mW).

Section 3-5 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.
This section speculates on whether fiber will replace copper in computer networks. Industry experts expect that, for many years, a hybrid solution of fiber and copper will be used.

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
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).

1.6 Explain the use and purpose of network services.
Almost all modern optical transceivers provide bidirectional data transmission by using two fibers to transmit data between switches, firewalls, servers, routers, and so on.

1.7 Explain basic corporate and datacenter network architecture.
This section addresses the fact that fiber has the capacity to carry more bandwidth, and as the cost of fiber infrastructure decreases, fiber is more and more being chosen to carry data.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
If 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 each end, as shown in Figure 3-15. The media converter is typically built in to the NIC.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section introduces the concept of duplex operation. Fiber lines consist of a minimum of two fibers: one for transmitting and one for receiving. Fiber networks work in the full-duplex mode, which means that the links must be able to simultaneously transmit and receive—hence the need for two fibers on each link. This is also referred to as duplex operation.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section discusses the idea that active equipment must have a GBIC or some other interface for the optical–electrical signal conversion.

3.2 Explain the purpose of organizational documents and policies.

A general rule for fiber is that the distribution in a building should be limited to "two 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. These distributions are also known as IDF/MDF (intermediate distribution frame/main distribution frame).

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section introduces the concept of using two telco connections to provide for redundant Internet and WAN 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.

4.5 Explain the importance of physical security.

This section addresses the fact that security is enhanced with fiber-optic systems because it is difficult to tap optical fiber without detection.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section mentions that fiber helps eliminate the 100 meter distance limit associated with UTP copper cable. This is possible because fiber is subject to lower attenuation loss.

Test Your Knowledge

1. What does a 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 a 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. Which of the following is an optical-to-fiber interface used with 10 Gigabit Ethernet?

   a. GBIC
   b. 10GBIC
   c. XENPAK
   d. ZENPAK

3-6 SAFETY

As the first paragraph of this section states, any discussion of fiber optics or optical networking is not complete unless it addresses safety issues. Students need to understand that they must be careful when working with fiber-optic cable. Have an open discussion with the class about safety, even if you only advise the students not to look into the end of a fiber.

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 further attenuate the light if there is an open circuit:

- A light beam disperses or fans out from an open connector.
- 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, two factors can increase the optical power at an exposed fiber end:

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

There are two factors to be aware of:

- The human 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, which shows the electromagnetic spectrum.)

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

Those working on fiber-optic equipment should keep in mind these warnings:

- *Do not ever* look into the output connector of energized test equipment. Such equipment, particularly OTDRs, can have higher powers than the communication equipment itself.
- 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, consider the following:

- Good work practices are detailed in safety, training, and installation manuals. (Read and heed!)
- Be careful with machinery, cutters, snips, chemical solvents, and epoxies.
- Fiber ends are brittle and can 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.
- Use safety glasses specifically designed to protect the eyes when working with fiber-optic systems.
- Obtain and use an optical safety kit.
- Keep the work area clean and orderly.

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

Section 3-6 Review

This section covers the following Network+ exam objectives.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section mentions that if a fiber is damaged, there will be some attenuation.

5.5 Given a scenario, troubleshoot general networking issues.

This section examines safety considerations to keep in mind when working with fiber.

Test Your Knowledge

1. True or false: The human eye cannot see fiber-optic communication wavelengths, so you should never look into the end of a fiber.

   True

2. True or false: It is important to be very careful when working with fiber ends. These ends are extremely difficult to see and can become lost and/or easily embedded in your finger.

   True

3-7 TROUBLESHOOTING FIBER OPTICS: THE OTDR

This section provides traces obtained from an OTDR from tests conducted on multimode fiber. The traces are well documented with statements explaining the cause or possible cause of an event (disturbance) in the trace.

Several techniques can be used to measure and troubleshoot fiber links. A common technique is to use an optical power meter to determine power loss. Another tool used is a **visual fault locator (VFL)**, which shines light down the fiber to help locate broken glass. Figure 3-23 shows traces obtained from an **optical time-domain reflectometer (OTDR)** for two different sets of multimode fibers; this is called *shooting* the fiber. The OTDR sends a light pulse down the fiber and measures the reflected light. The OTDR enables an installer or a maintenance crew to verify the quality of each fiber span and obtain some measure of performance. The *X* axis on the traces indicates the distance, and the *Y* axis indicates the measured optical power value in decibels. Both OTDR traces are for 850 nm multimode fiber.

Visual Fault Locator (VFL)
A device that shines light down fiber to help locate broken glass

Optical Time-Domain Reflectometer (OTDR)
A device that sends a light pulse down fiber and measures the reflected light, providing a measure of performance for the fiber

In Figure 3-23(a), point A is a "dead" zone, or a point too close to the OTDR for a measurement to be made. The measured value begins at about 25 dB and decreases as the distance traveled increases. An **event**, or a disturbance in the light propagating down the fiber, occurs at point B. This is an example of what a poor-quality splice looks like (in regard to reflection as well as insertion loss). It is most likely a mechanical splice. The same type of event occurs at points C and D, which are also most likely mechanical splices. Points F and G are most likely the jumpers and patch panel connections at the fiber end. The steep drop at point H is actually the end of the fiber. Point I is typical noise that occurs at the end of an unterminated fiber. Notice at point G that the overall value of the trace has dropped to about 17 dB. There has been about 8 dB of optical power loss in the cable in a 1.7 kilometer run.

Event
A disturbance in the light propagating down a fiber span that results in a disturbance on the OTDR trace

An OTDR trace for another multimode fiber is shown in Figure 3-23(b); the hump at point A is basically a dead zone. An OTDR cannot typically return accurate measurement values in this region. This is common for most OTDRs, and the dead zone varies for each OTDR. The useful trace information begins at point B, with a

measured value of 20 dB. Point C shows a different type of event, which is typical of coiled fiber or fiber that has been tightly bound, possibly with a tie-wrap, or that has had some other disturbance affecting the integrity of the fiber. Points D and F are actually the end of the fiber. At point D, the trace level is about 19 dB, for a loss of about 1 dB over the 150 meter run. Point G is just the noise that occurs at the end of a terminated fiber.

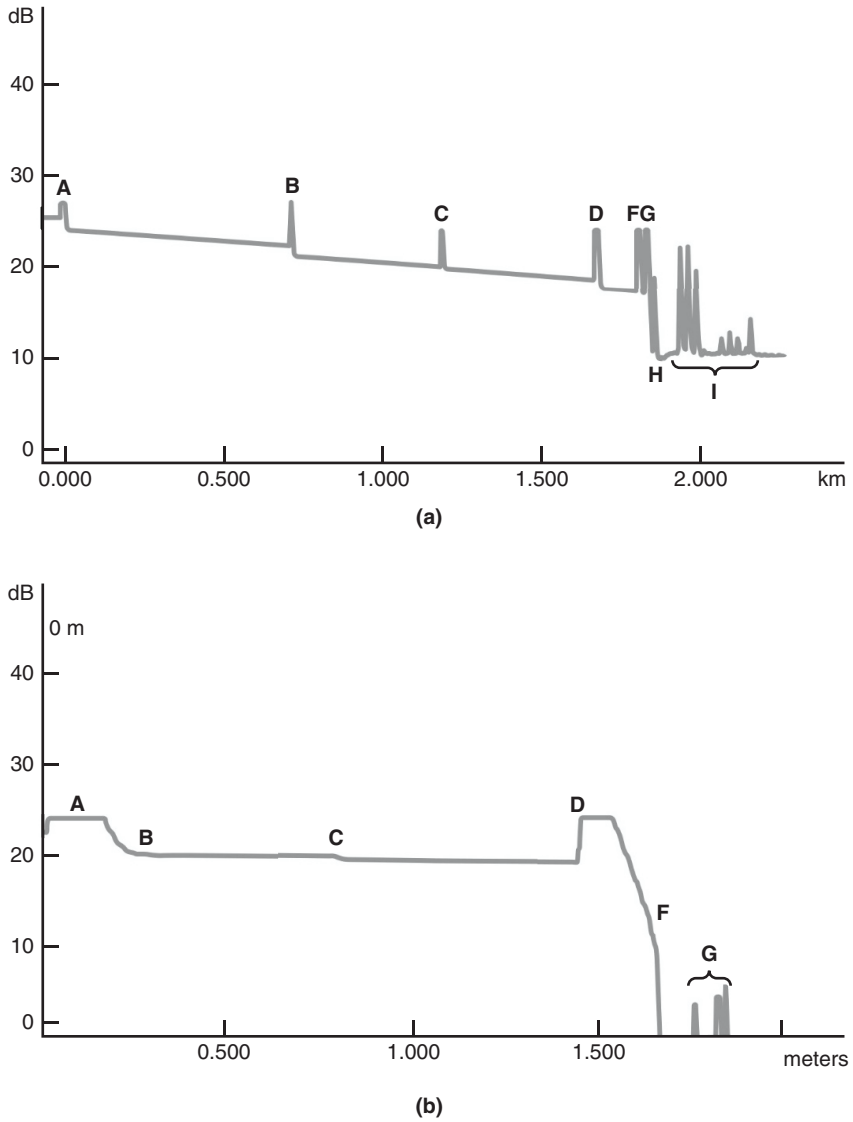


FIGURE 3-23 An OTDR trace of an 850 nm fiber. (From *Modern Electronic Communication* 9/e, by J. S. Beasley & G. M. Miller, 2008, p. 814. Copyright © 2008 Pearson Education, Inc. Upper Saddle River, NJ.)

Section 3-7 Review

Test Your Knowledge

1. What is a dead zone?
    a. A point too far from the OTDR for a measurement to be made
    b. A point too far from the OTDR for a calculation to be made
    c. A point too close to the OTDR for a measurement to be made
    d. The point where an event is likely to occur
2. Signal loss is characterized by which of the following? (Select all that apply.)
    a. It is not expected in fiber.
    b. It is expected as the signal travels down a fiber.
    c. It can result in crosstalk in a fiber.
    d. It is measured in decibels.

SUMMARY

This chapter introduces the field of fiber optics and optical networking. The chapter provides examples using fiber to interconnect LANs in both a building and a campus network. The major topics that you 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 techniques commonly used to connect fiber
- The use 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.

   Fiber

   Optical light source

   Photosensitive detection

   Efficient optical connectors

2. List five advantages of an optical communications link.

   The answers should include five of the following:

   - Bandwidth
   - Immunity to electrostatic interference
   - Elimination of crosstalk
   - Lower signal attenuation
   - Lower costs
   - Safety
   - No corrosion problem
   - Security

Section 3-2

3. Define refractive index.

   The refractive index is the ratio of the speed of light in free space to its speed in a given material.

4. What are the commonly used wavelengths in fiber-optic systems?

   750 to 850 nm, 1310 nm, and 1530 to 1560 nm

5. What part of an optical fiber carries the light?

   The core

6. What is a measure of a fiber's light acceptance?

   Numerical aperture

7. Define pulse dispersion.

   Pulse dispersion is a stretching of the received pulse width because of the multiple paths taken by the light.

8. What are the typical core/cladding sizes (in microns) for multimode fiber?

   50/125 µm, 62.5/125 µm

9. What is the typical core size for single-mode fiber?

   7 to 10 µm

10. Define mode field diameter.

    Mode field diameter is the actual guided optical power distribution.

Section 3-3

11. What are the two key distance-limiting parameters in fiber-optic transmissions?

    Attenuation and dispersion

12. What are the four factors that contribute to attenuation?

    Scattering, absorption, macrobending, and microbending

13. Define dispersion.

    Dispersion is the broadening of an optical pulse as it propagates through a fiber strand.

14. What are three types of dispersion?

    Modal, chromatic, and polarization mode

15. What is meant by the term *zero-dispersion wavelength*?

    The point where the dispersion is actually zero

16. What is a dispersion compensating fiber?

    A dispersion compensating fiber acts like an equalizer, canceling dispersion effects and yielding close to zero dispersion in the 1550 nm region.

Section 3-4

17. What are the two kinds of light sources used in fiber-optic communication systems?

    Diode laser (DL) and the light-emitting diode (LED)

18. Why are narrower spectra advantageous in optical systems?

    Dispersion effects on the pulse width are reduced, and therefore pulse degradation is minimized.

19. Why is a tunable laser important in optical networking?

    Traffic routing can be made by wavelengths.

20. What is the purpose of an optical attenuator?

    It reduces the received signal level (RSL).

21. List two purposes of optical detectors.

    Optical detectors convert transmitted light back into an electrical signal and monitor the output of laser diode sources.

22. What is the advantage of fusion splicing over mechanical splicing?

    Fusion splicing is long term and has low insertion loss.

Section 3-5

23. Expand the following acronyms:

    a. FTTC

       Fiber-to-the-curb

    b. FTTH

       Fiber-to-the-home

    c. FTTB

       Fiber-to-the-business

    d. FTTD

       Fiber-to-the-desktop

24. What is the purpose of a GBIC?

    A GBIC provides an optical interface for the optical–electrical signal conversion for 1Gbps and lower frequencies.

25. What is the "two deep" rule?

    This rule limits the fiber distribution in a building to two 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.

26. What is the purpose of a logical fiber map?

    It shows how fiber is interconnected and data is distributed.

27. What are the typical maximum lengths for multimode fiber and single-mode fiber?

    Multimode fiber: 2 kilometers

    Single-mode fiber: 80 kilometers

28. What is a fiber cross-connect used for?

    A fiber cross-connect is an optical patch panel used to connect fiber cables to the next link. The fiber cross-connect typically uses mechanical splices to make the fiber connections.

29. Provide a link budget calculation, given the following:

    Transceiver output power of –16 dBm

    2 splices at 0.1 dB each

    2 connectors at 0.3 dB each

    Determine the extra margin if the RSL is –20 dB.

    Total link budget = $-16\ \text{dBm} - (2 \times 0.1) - (2 \times 0.3)$

    $= -16\ \text{dBm} - 0.2\ \text{dB} - 0.6\ \text{dB} = -16.8\ \text{dBm}$

    In this case, the desired RSL is –20 dBm; therefore, the system has 3.2 dB of extra margin.

Section 3-6

30. Why is safety an important issue in optical networking?

    The eye can't see fiber-optic communication wavelengths, so there is no awareness of exposure, but the eye's retina can be damaged.

31. A campus network is planning to replace outdated coaxial cables with fiber-optic cables. Should the network use single-mode, multimode, or a combination of single- and multimode fibers in the ground? Why?

    The best choice is to select a combination of multimode and single-mode fibers. This enables maximum flexibility when designing the system and connecting to various equipment.

32. 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.

    At this point, both twisted-pair and fiber should be used. It may not be practical to run fiber to the work area, but fiber should at least be run to the closets (IDCs).

Section 3-7

33. Examine the OTDR trace provided in Figure 3-24. Explain the trace behavior of points A, B, C, D, and E.

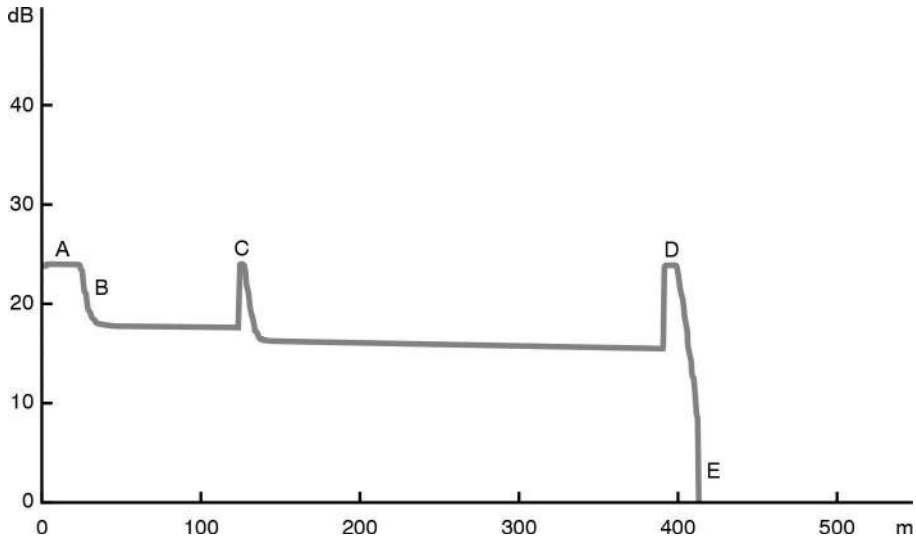


FIGURE 3-24 Figure for problem 33. (From *Modern Electronic Communication* 9/e, by J.S. Beasley & G. M. Miller, 2008, p. 833. Copyright © 2008 Pearson Education, Inc. Upper Saddle River, NJ.)

A. Dead zone
B. Begins useful trace info
C. Splice
D. Termination at the fiber end
E. End of the fiber

Certification Questions

34. 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

35. The stretching of a received pulse is due to which of the following? (Select two.)

    a. Multiple paths taken by the light waves
    b. Misaligned connectors
    c. Pulse dispersion
    d. OTDR testing

36. The broadening of a pulse due to the different path lengths taken through the fiber by different modes is called ____.

    a. chromatic dispersion
    b. polarization mode dispersion
    c. modal dispersion
    d. diffusion

37. The broadening of a pulse due to different propagation of the spectral components of the light pulse is called ____.

    a. chromatic dispersion
    b. modal dispersion
    c. polarization mode dispersion
    d. diffusion

38. 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 ____.

    a. modal dispersion
    b. chromatic dispersion
    c. diffusion
    d. polarization mode dispersion

39. What is the data rate for OC-192?

    a. 1.522Mbps
    b. 155.52Mbps
    c. 9.95Gbps
    d. 2.488Gbps

40. Which of the following is an optical-to-fiber interface used with 1 Gigabit Ethernet?

    a. XENPAK
    b. GBIC
    c. 10GBIC
    d. ZENPAK

41. What is the “two deep” rule relative to optical networking?

    a. The horizontal distribution to the work floor can have only two 8P8C connections.
    b. The horizontal distribution to the work floor can have only two ST connections to the fiber patch panel.
    c. This is no longer an issue with high-speed single-mode fiber and wave division multiplexing equipment.
    d. A building should have only the main distribution and the intermediate distribution that feeds the horizontal distribution to the work area.

42. Which type of fiber is preferred for use in modern computer networks?

    a. Multimode
    b. Polarized mode
    c. Single-mode
    d. All of these answers are correct.

43. What is the material surrounding the core of an optical waveguide called?

    a. Aperture
    b. Mode field
    c. Step-index
    d. Cladding
    e. Graded-index

4
CHAPTER

Wireless Networking

Chapter Outline

4-1 Introduction
4-2 The IEEE 802.11 Wireless LAN Standard
4-3 802.11 Wireless Networking
4-4 Bluetooth, WiMAX, RFID, and Mobile Communications
4-5 Configuring a Point-to-Multipoint Wireless LAN: A Case Study
4-6 Troubleshooting Wireless Networks
Summary
Questions and Problems

Objectives

- Define the features of the 802.11 wireless LAN standard
- Understand the components of a wireless LAN
- Explore how wireless LANs are configured
- Examine how site surveys are done for wireless LANs
- Investigate the issues of securing a wireless LAN
- Explore how to configure a point-to-multipoint wireless LAN

Key Terms

WLAN
basic service set (BSS)
ad hoc network
access point
transceiver
extended service set (ESS)
hand-off
roaming
CSMA/CA
DSSS
ISM band
FHSS
pseudorandom
hopping sequence
OFDM
OFDMA
U-NII
MIMO
MU-MIMO
beamforming
Wi-Fi
SSID
site survey
inquiry procedure
paging procedure
piconet
pairing
passkey
WiMAX
BWA
NLOS
last mile
radio frequency identification (RFID)
backscatter
Slotted Aloha

WLAN
Wireless local area network

This chapter examines the features and technologies used in a wireless local area network (**WLAN**). Wireless networking is an extension of computer networks into the radio frequency (RF) world. A WLAN provides increased flexibility and mobility for connecting to a network. A properly designed WLAN for a building provides mobile access for a user from virtually any location in the building. The user doesn't have to look for a connection to plug into; also, the expense of pulling cables and installing wall plates required for wired networks can be avoided. However, a network administrator must carefully plan a wireless LAN installation and have a good understanding of the issues of using WLAN technologies to ensure the installation of a reliable and secure network.

4-1 INTRODUCTION

The objective of this section is to introduce students to wireless networking. Wireless networks are being used everywhere, and it is a network administrator's job to ensure that the addition of a wireless network meets the connectivity, data throughput, and security requirements for the network.

This chapter addresses the basic issues of incorporating WLAN technologies into a network. Section 4-2, "The IEEE 802.11 Wireless LAN Standard," includes an overview of WLAN concepts and terminology, frequency allocations, and spread spectrum communication. The applications of WLANs are presented in Section 4-3, "802.11 Wireless Networking," which looks at various types of WLAN configurations, such as point-to-point and point-to-multipoint. Section 4-4, "Bluetooth, WiMAX, RFID, and Mobile Communications," looks at wireless networking technologies such as Bluetooth, WiMAX, and RFID. Any time a signal is transmitted over the air or even through a cable, there is some chance that the signal can be intercepted. Transmitting data over a wireless network introduces unique security issues. Section 4-5, "Configuring a Point-to-Multipoint Wireless LAN: A Case Study," presents an example of configuring a WLAN to provide access for users in a metropolitan area. Section 4-6 "Troubleshooting Wireless Networks" provides an overview of common techniques for troubleshooting wireless networks.

Table 4-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 4-1 **Chapter 4 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.2	Explain the characteristics of network topologies and network types.	4-2
1.3	Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	4-4
1.6	Explain the use and purpose of network services.	4-2, 4-3
1.7	Explain basic corporate and datacenter network architecture.	4-4
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	4-2, 4-3, 4-4, 4-5
2.3	Given a scenario, configure and deploy common Ethernet switching features.	4-2, 4-4
2.4	Given a scenario, install and configure the appropriate wireless standards and technologies.	4-2, 4-3, 4-4, 4-5
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	4-2, 4-3, 4-4
3.2	Explain the purpose of organizational documents and policies.	4-3, 4-5
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	4-2, 4-5
4.0	**Network Security**	
4.3	Given a scenario, apply network hardening techniques.	4-2, 4-4, 4-5
4.4	Compare and contrast remote access methods and security implications.	4-2
5.0	**Network Troubleshooting**	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	4-2, 4-3, 4-4
5.4	Given a scenario, troubleshoot common wireless connectivity issues.	4-2, 4-3, 4-5, 4-6
5.5	Given a scenario, troubleshoot general networking issues.	4-4

4-2 THE IEEE 802.11 WIRELESS LAN STANDARD

The anatomy of 802.11 wireless networking is presented in this section. This section introduces the basic service set wireless network, the extended service set, the independent basic service set (ad hoc), the frequencies used for wireless networks, the power output, and spread spectrum communications. Many topics are presented, including the 802.11 wireless (Wi-Fi) standards. Students need to be aware of these topics to fully comprehend how a wireless network functions.

A typical computer network uses twisted-pair and fiber-optic cable to interconnect LANs. Another media option competing for use in higher-data-rate LANs is

wireless, based on the IEEE 802.11 wireless standard. The advantages of wireless include the following:

- It is cost-effective for use in areas that are difficult or too costly to wire.
- It enables user mobility in the workplace.

Wireless networks have become the network of choice in environments such as homes, small offices, and public places. Being able to connect to a network without a wire is convenient for users, and the cost is relatively low. In the age of laptops and mobile devices, wireless opens the door to user mobility in the workplace, and user mobility provides flexibility. Workers can potentially access the network or wireless data services from virtually any location within the workplace. Accessing information from the network is as easy as if the information were on a USB drive.

The benefits of wireless networks in the workplace are numerous. To provide wireless connectivity, a network administrator must be sure the network services are reliable and secure. In order to provide reliable network services, an administrator must have a good understanding of WLAN configurations and technologies. This and the following sections examine the fundamentals of wireless networking, the 802.11 standard and its family (802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax), and how WLANs are configured.

The IEEE 802.11 WLAN standard defines the physical (PHY) layer, the media access control (MAC) layer, and the MAC management protocols and services.

The PHY layer defines the following:

- The method of transmitting the data, which can be either RF or infrared (although infrared is rarely used)
- How it interfaces with the MAC layer
- The reliability of the data service
- Access control to the shared wireless medium
- Privacy protection for transmitted data

The wireless management protocols and services are authentication, association, data delivery, and privacy.

Basic Service Set (BSS)
An independent network

Ad hoc network
An independent network

The fundamental topology of a WLAN is the **basic service set (BSS)**. This is also called the independent basic service set, or **ad hoc network**. Figure 4-1 provides an example of an ad hoc network. In this network, the wireless clients (stations) communicate directly with each other. This means the clients have recognized the other stations in the WLAN and have established a wireless data link.

A related concept is a wireless mesh network (WMN), which is a communications network made up of Wi-Fi radios connected in a mesh topology (that is, a heavily interconnected network). A WMN is basically a wireless ad hoc network.

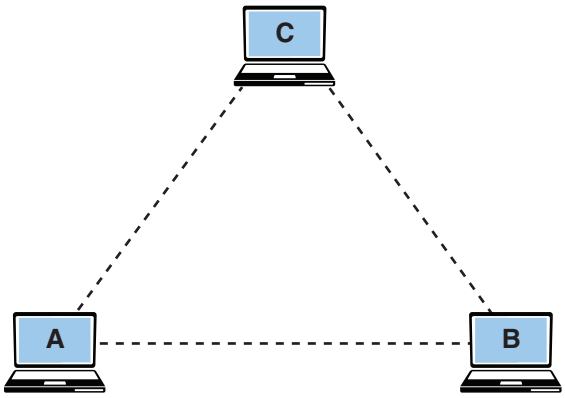


FIGURE 4-1 An example of an independent basic service set, or ad hoc, network.

The performance of the basic service set can be improved by including an **access point**, which is a transmit/receive unit (**transceiver**) that interconnects data from the wireless LAN to the wired network. In addition, the access point provides 802.11 MAC layer functions and supports bridge protocols. The access point typically uses an RJ-45 jack for connecting to the wired network. If an access point is being used, users establish a wireless communications link through it to communicate with other users in the WLAN or the wired network, as shown in Figure 4-2.

Access Point
A transceiver used to interconnect a wireless LAN and a wired LAN

Transceiver
A transmit/receive unit

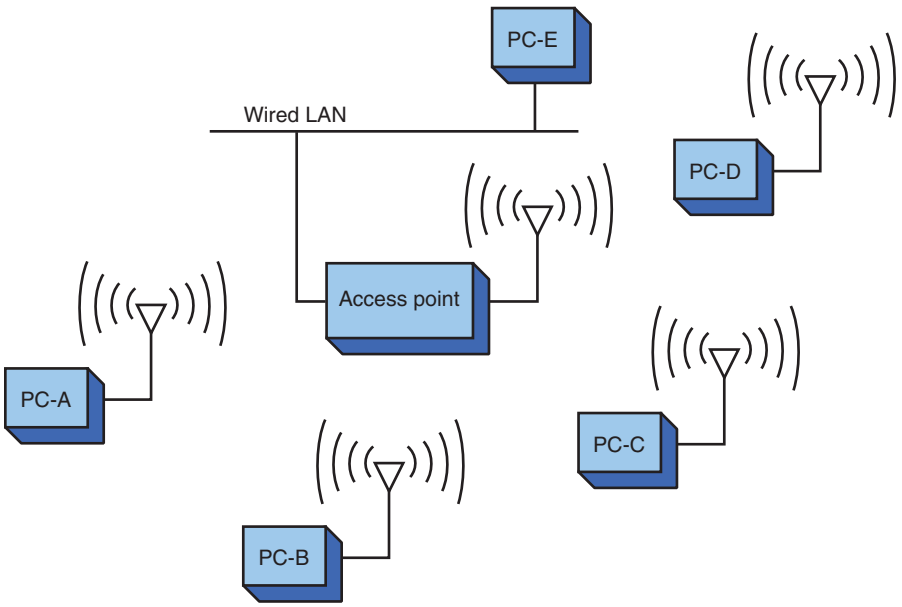


FIGURE 4-2 Adding an access point to a basic service set.

If data is being sent from PC-A to PC-D in the network shown in Figure 4-2, the data is first sent to the access point and then relayed to PC-D. Data sent from a wireless client to a client in the wired LAN also passes through the access point.

Extended Service Set (ESS)
A network with multiple access points to extend user mobility

Hand-off
The process in which a user's computer establishes an association with another access point

Roaming
The term used to describe a user's ability to maintain network connectivity while moving through the workplace

CSMA/CA
Carrier sense multiple access with collision avoidance

The users (clients) in the wireless LAN can communicate with other members of the network as long as a link is established with the access point. For example, data traffic from PC-A to PC-E first passes through the access point and then to PC-E in the wired LAN.

The problem with a basic service set is that mobile users can travel outside the radio range of a station's wireless link if there is only one access point. One solution is to add multiple access points to the network. Multiple access points extend the range of mobility of a wireless client in the LAN. This arrangement is called an **extended service set (ESS)**. In the example of an ESS in Figure 4-3, the mobile computer establishes an authorized connection with the access point that has the strongest signal level (for example, AP-1). As the user moves, the strength of the signal from AP-1 decreases. At some point, the signal strength from AP-2 exceeds that from AP-1, and the wireless bridge establishes a new connection with AP-2. This is called a **hand-off**. The hand-off is an automatic process for the wireless client adapter in 802.11, and the term used to describe this is **roaming**.

Network access in 802.11 uses a technique called carrier sense multiple access with collision avoidance (CSMA/CA). In **CSMA/CA**, the client station listens for other users of the wireless network. If the channel is quiet (that is, no data transmission is occurring), the client station can transmit. If the channel is busy, the station(s) must wait until transmission stops. Each client station uses a unique random back-off time. This technique prevents client stations from trying to gain access to the wireless channel as soon as it becomes quiet. Currently four physical layer technologies are being used in 802.11 wireless networking: direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), infrared, and orthogonal frequency-division multiplexing (OFDM). DSSS is used in 802.11b/g/n wireless networks, and OFDM is used in 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax.

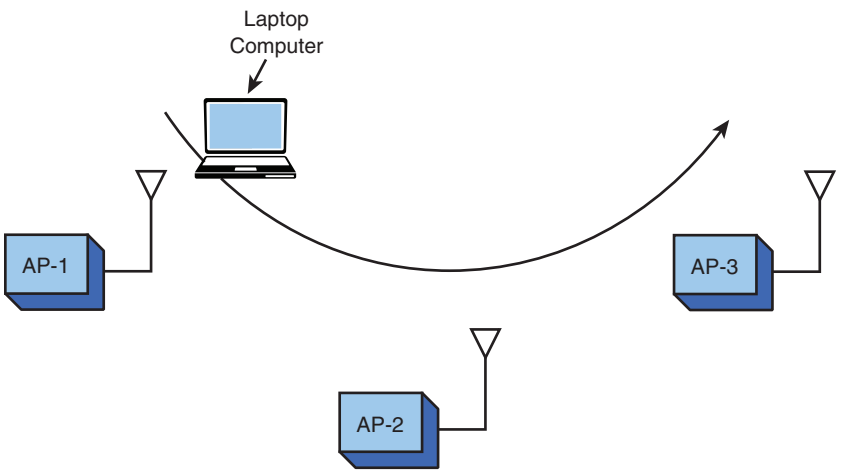


FIGURE 4-3 An example of an extended service set used for increased user mobility.

802.11 **DSSS** implements 14 channels (each consuming 22MHz) over approximately 90MHz of RF spectrum in the 2.4GHz **ISM** (industrial, scientific, and medical) **band**. DSSS is a technique used to spread the transmitted data over a wide bandwidth; in this case, it is a 22MHz bandwidth channel. A channel is a medium through which information is transmitted between transmitter and receiver. The bandwidth is a measure of the upper to lower frequencies of the channel required to transmit the information.

DSSS
Direct-sequence spread spectrum

ISM band
Industrial, scientific, and medical band

A related concept is *channel bonding*, in which two adjacent channels are combined to facilitate an increase in throughput between wireless devices. This is also called *Ethernet bonding* and is used in Wi-Fi applications.

Table 4-2 lists the frequency channels used in North America. Note that only 11 out of 14 channels are made available in North America due to regulatory requirements of the Federal Communication Commission (FCC). Figure 4-4 shows an example of the frequency spectrum for three-channel DSSS. Note that the three channels listed in Figure 4-4 (1, 6, and 11) do not overlap, while Table 4-2 shows that the other channels do have channel overlap. Remember that each channel is 22MHz in bandwidth. For example, channel 2 extends from 2.406GHz to 2.429GHz, with a center frequency of 2.417GHz, which clearly overlaps a portion of channel 1 and channel 3. Channels 1, 6, and 11 are the only channels that do not have overlap.

TABLE 4-2 **North American DSSS Channels**

Channel Number	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

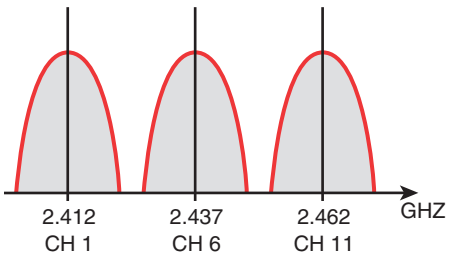


FIGURE 4-4 An example of the three channels in the DSSS spectrum.

FHSS
Frequency-hopping spread spectrum, a technique in which the transmit signal frequency changes based on a pseudorandom sequence

Pseudorandom
A number sequence that appears random but actually repeats

Hopping Sequence
The order of frequency changes

In frequency-hopping spread spectrum (**FHSS**), the transmit signal frequency changes based on a pseudorandom sequence. **Pseudorandom** means the sequence appears to be random but in fact does repeat, typically after some lengthy period of time. FHSS uses 79 channels (each 1MHz wide) in the ISM 2.4GHz band. FHSS requires that the transmitting and receiving units know the **hopping sequence** (the order of frequency changes) so that a communication link can be established and synchronized. FHSS data rates are typically 1Mbps and 2Mbps. FHSS is not commonly used anymore for wireless LANs. It's still part of the standard, but very few (if any) FHSS wireless LAN products are sold.

The maximum transmit power of 802.11b wireless devices is 1000 mW; however, the nominal transmit power level is 100 mW. The 2.4GHz frequency range used by 802.11b/g is shared by many technologies, including Bluetooth, cordless telephones, and microwave ovens.

LANs emit significant RF noise in the 2.4GHz range that can affect wireless data. A significant improvement in wireless performance is available with the IEEE 802.11a standards. The 802.11a equipment operates in the 5GHz range and provides significant improvement over 802.11b with respect to RF interference. An important concept related to noise is signal-to-noise ratio, which is a measure of the signal level relative to the noise level. The value is usually expressed in decibels (dB), and a high dB value is desirable.

OFDM
Orthogonal frequency-division multiplexing, a technique that involves dividing the signal bandwidth into smaller subchannels and transmitting the data over these subchannels in parallel

Another technique used in the 802.11 standard is **orthogonal frequency-division multiplexing (OFDM)**. The basic idea with this technique is to divide the signal bandwidth into smaller subchannels and to transmit the data over these subchannels in parallel. These subchannels can be overlapping, but they do not interfere with each other. The subchannels are mathematically orthogonal, and this setup yields uncorrelated or independent signals.

U-NII
Unlicensed National Information Infrastructure

The 802.11a standard transports data over 12 possible channels in the Unlicensed National Information Infrastructure (**U-NII**). The FCC set aside U-NII to support short-range, high-speed wireless data communications. The 802.11 channels and frequencies are governed by FCC regulations, which are periodically revised. A wireless manufacturer must keep its products up to date due to the regulatory impacts. Table 4-3 lists the operating frequencies for 802.11a, and Table 4-4 lists the transmit power levels for 802.11a.

TABLE 4-3 **IEEE 802.11a Channels and Operating Frequencies**

Channel	Center Frequency (GHz)	
36	5.180	
40	5.20	Lower band
44	5.22	
48	5.24	
52	5.26	
56	5.28	Middle band
60	5.30	
64	5.32	

Channel	Center Frequency (GHz)	
149	5.745	
153	5.765	Upper band
157	5.785	
161	5.805	

TABLE 4-4 **Maximum Transmit Power Levels for 802.11a with a 6 dBi Antenna Gain**

Band	Power Level
Lower	40 mW
Middle	200 mW
Upper	800 mW

IEEE 802.11a equipment is not compatible with 802.11b or 802.11g. The upside of this is that 802.11a equipment does not interfere with 802.11b or g; therefore, 802.11a and 802.11b/g links can run next to each other without causing interference. 802.11n can operate either in the 2.4GHz range or the 5GHz range. Cheaper 802.11n wireless cards tend to be manufactured with only 2.4GHz antennas, so users have to check the frequency specifications as not all 802.11n equipment has both 2.4GHz and 5GHz frequencies. Figure 4-5 shows an example of the two links operating together. Along the same lines, frequency mismatch is an issue if the two ends of the communications link are operating on different channels or if you are trying to make 802.11a communicate with 802.11b, as the frequencies are not compatible.

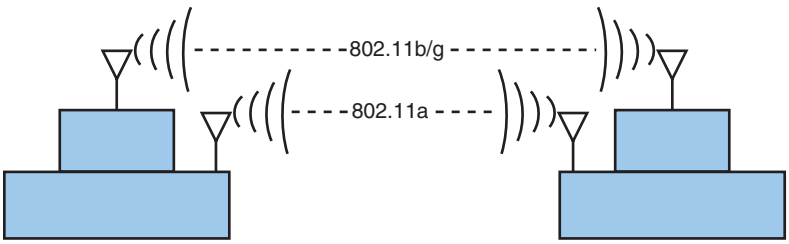


FIGURE 4-5 An example of an 802.11a installation and an 802.11b link running alongside each other.

The downsides of 802.11a are the increased cost of the equipment and increased power consumption because of the OFDM technology. This is of particular concern with mobile users because of the effect it can have on battery life. However, the maximum usable distance (RF range) for 802.11a is about the same as or even greater than that of 802.11b/g/n/ac/ax. It is important to note that any RF signal has distance limitations either due to limited output transmitted power, antenna pattern, or terrain issues.

Another IEEE 802.11 wireless standard is IEEE 802.11g. The 802.11g standard supports the higher data transmission rates of 54Mbps but operates in the same 2.4GHz range as 802.11b. The 802.11g equipment is also backward compatible with 802.11b equipment. This means that 802.11b wireless clients can communicate with the 802.11g access points, and the 802.11g wireless client equipment can communicate with the 802.11b access points. The obvious advantage of this is that a company with an existing 802.11b wireless network can migrate to the higher data rates provided by 802.11g without having to sacrifice network compatibility. In fact, new wireless equipment supports both the 2.4GHz and 5GHz standards, and it therefore has the flexibility of high speed, compatibility, and noninterference.

Another entry into wireless networks is 802.11n. This wireless technology operates in the same ISM frequency as 802.11b/g (2.4GHz) and can also operate in the 5GHz band. A significant improvement with 802.11n is multiple-input multiple-output (**MIMO**). MIMO uses a technique called space-division multiplexing, in which the data stream is split into multiple parts called spatial streams. The different spatial streams are transmitted using separate antennas. With MIMO, doubling the spatial streams doubles the effective data rate. The downside of this is the possibility of increased power consumption. The 802.11n specification includes a MIMO power-save mode. With this mode, 802.11n uses multiple data paths only when faster data transmission is required—thus saving power.

MIMO
Multiple-input multiple-output

The 802.11ac technology operates in the 5GHz band. It uses a newer version of MIMO technology with eight spatial streams and has channels up to 80MHz wide. It also introduces multiuser MIMO (**MU-MIMO**), which can send MIMO spatial streams to multiple clients at the same time. 802.11ac incorporates standardized **beamforming**, a technique that is used to direct transmission of the radio signal to a specific device. Beamforming increases data throughput and reduces power consumption. 802.11n used beamforming, but it was not standardized. The transmit range for 802.11ac is similar to or better than that of 802.11n.

MU-MIMO
Multiuser Multiple-input Multiple-output

Beamforming
A technique used to direct transmission of a radio signal to a specific device

The latest addition to the 802.11 family is 802.11ax, also known as Wi-Fi 6. Whereas 802.11ac operates in the 5GHz band only, 802.11ax operates in both 2.4GHz and 5GHz bands. 802.11ax uses OFDMA (orthogonal frequency-division multiple access) rather than OFDM. OFDMA allows multiple users or clients to share the same channel simultaneously. Wireless devices can optionally support WPA3 (Wi-Fi Protected Access 3), but 802.11ax increases security requirements by mandating the use of WPA3 as its encryption and authentication standard. WPA3 is discussed in more detail in Chapter 11, "Network Security."

Table 4-5 provides a comparison of 802.11n, 802.11ac, and 802.11ax in terms of their compatibility with other Wi-Fi technologies and the frequencies supported.

TABLE 4-5 **A Comparison of 802.11ac, 802.11n, and 802.11ax**

	802.11n	802.11ac	802.11ax
Backward-compatible with	802.11g, 802.11b, and 802.11a	802.11n	802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac
Frequencies supported	2.4GHz and 5GHz	5GHz	2.4GHz and 5GHz

Wireless networks also go by the name **Wi-Fi**, which is not an acronym, but a term created and is a trademark of Wi-Fi Alliance to represent the standards for wireless communication. Wi-Fi is sometimes referred to as *wireless fidelity*. The Wi-Fi Alliance is an organization whose function is to test and certify wireless equipment for compliance with the 802.11*x* standards, the group of wireless standards developed under the IEEE 802.11 standard. The following list provides a summary of the most common wireless standards:

Wi-Fi
A term created and is a trademark of the Wi-Fi Alliance to represent the standards for wireless communication.

- **802.11b (Wi-Fi 1):** This standard can provide data transfer rates up to 11Mbps with ranges of 100–150 feet. It operates at 2.4GHz and uses DSSS.
- **802.11a (Wi-Fi 2):** This standard can provide data transfer rates up to 54Mbps and an operating range up to 75 feet. It operates at 5GHz and uses OFDM.
- **802.11g (Wi-Fi 3):** This standard can provide data transfer rates up to 54Mbps and an operating range up to 150 feet. It operates at 2.4GHz and uses DSSS or OFDM.
- **802.11n (Wi-Fi 4):** This high-speed wireless connectivity promises data transfer rates over 200Mbps. It operates at 2.4GHz and 5GHz and uses DSSS or OFDM.
- **802.11i:** This standard for WLANs provides improved data encryption for networks that use the 802.11a, 802.11b, and 802.11g standards.
- **802.11r:** This standard is designed to speed hand-offs between access points or cells in a WLAN. This standard is a critical addition to 802.11 WLANs if voice traffic is to become widely deployed.
- **802.11ac (Wi-Fi 5):** This is currently the most deployed wireless standard. It provides single-station data transfer rates of 500Mbps up to 1.3Gbps and operates in the 5GHz frequency band.
- **802.11ax (Wi-Fi 6):** This is the latest wireless standard, and manufacturers are starting to ship more equipment with this wireless technology. Theoretically, it could deliver close to 10Gbps data rates.

Another wireless technology is Z-Wave. This wireless communications protocol was developed for home automation. Typical applications include sensors for home lighting, security systems, and HVAC systems. The operating frequencies for Z-Wave in the United States are 908.4MHz and 916MHz.

Another entry into the ultra-low-power wireless protocol space is ANT+, which is used for wireless sensor networks (WSNs). This technology operates at 2.4GHz.

Section 4-2 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.
This section introduces the new wireless technologies Z-Wave and ANT+.

1.6 Explain the use and purpose of network services.
This section provides an example of a network in which the wireless clients (stations) communicate directly with each other.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
An access point is a transmit/receive unit (transceiver) that interconnects data from the wireless LAN to the wired network. In addition, an access point provides 802.11 MAC layer functions and supports bridge protocols.

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.
This section introduces the terms basic service set, extended service set, and ad hoc set and the concept of roaming.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.
This section examines the 802.11a/b/g/n/i/r/ac/ax standards as well as issues such as transmit distance, data speed, and frequencies. This section also introduces the concept of MIMO, which is used to increase the effective transmit data rate.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.
To provide reliable network services, an administrator must have a good understanding of WLAN configurations and technologies.

4.3 Given a scenario, apply network hardening techniques.
Table 4-3 lists the operating frequencies for 802.11a, and Table 4-4 lists the transmit power levels for 802.11a.

4.4 Compare and contrast remote access methods and security implications.
This section introduces wireless management protocols and indicates that the services are authentication, association, data delivery, and privacy.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.
Technical issues related to throughput, speed, and distance are examined in this section.

Test Your Knowledge

1. True or false: 802.11ac networking equipment is compatible with 802.11b.

   True

2. True or false: 802.11g networking equipment is compatible with 802.11b.

   True

3. True or false: 802.11a and 802.11b wireless networks can run side-by-side.

   True

4. True or false: 802.11ac networking equipment is compatible with 802.11n.

   True

4-3 802.11 WIRELESS NETWORKING

This section introduces techniques for assembling a wireless network and helps students understand the purpose of the access point and the SSID (service set identifier). The techniques for implementing point-to-point and point-to-multipoint wireless networks are presented, and so is the very important concept of a site survey. Make sure students understand the importance of performing a good site survey to ensure user mobility and connectivity.

A wireless LAN can be configured in many ways to meet the needs of an organization. Figure 4-6 provides an example of a basic 802.11b/g/n/ac/ax WLAN configuration. In this configuration, each PC is outfitted with a wireless LAN adapter card. Today, most computer desktops and especially computer laptops are equipped with wireless adapters. For devices that lack these cards, an external USB wireless adapter can be used. A wireless adapter (or wireless LAN adapter) is a device that connects a client to the wireless medium, which is typically a radio wave channel in the 2.4GHz or 5GHz ISM band. The wireless medium can also be infrared, although that is not used very often. The following services are provided by a wireless LAN adapter:

- Delivery of the data
- Authentication
- Privacy

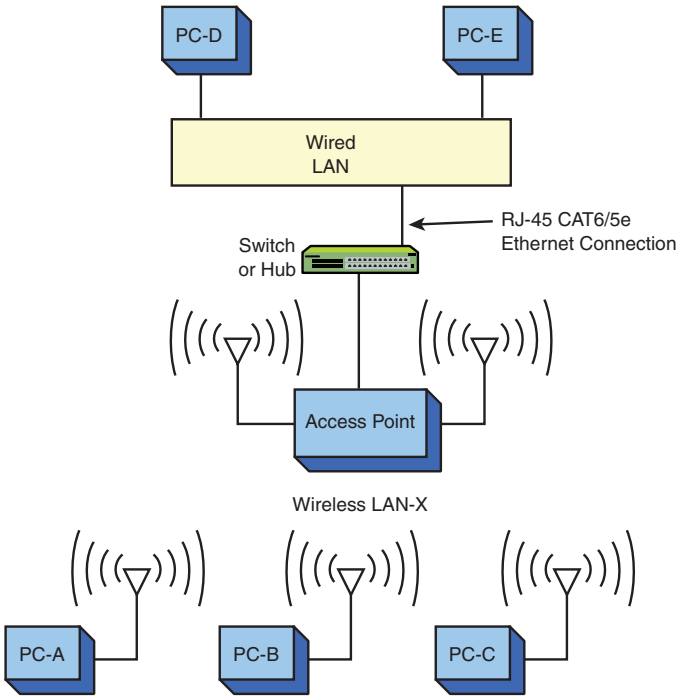


FIGURE 4-6 The setup for a basic WLAN.

One of the biggest misconceptions about wireless is that it does not require a wired connection. This is not quite correct. The connection to a wired LAN is provided by a wireless access point (WAP), which provides a bridge between the wireless LAN and the wired network. A physical cable connection (typically CAT6 or higher) ties the access point to the wired network's switch or hub (typically Ethernet).

For example, computer PC-A in Figure 4-6 sends a data packet to PC-D, a destination in the wired LAN. PC-A first sends a data packet over the wireless link. The access point recognizes the sender of the data packet as a host in wireless LAN-X and allows the wireless data to enter the access point. At this time, the data is sent out the physical Ethernet connection to the wired LAN. The data packet is then delivered to PC-D in the wired LAN.

SSID
Service set identifier, a password that enables the client to join the wireless network

How does the access point know that the wireless data packet is being sent from a client in the wireless LAN? The 802.11 wireless LAN devices use an **SSID** to identify what wireless data traffic is allowed to connect to the network. The SSID is the wireless *service set identifier*, which enables the client to join the wireless network.

The access point uses the SSID to determine whether the client is to become a member of the wireless network. The term *association* is used to describe a wireless connection that is made. The wrong SSID prevents an association, keeping the client from being able to become a member of the wireless network.

People are commonly surprised by the fact that an access point has two antennas. The two antennas implement *spatial diversity*, improving received signal gain and performance.

Figure 4-7 provides an example of the information displayed on the wireless adapter's console port when an association is made. The text indicates that a connection has been made to a parent (access point) whose MAC address is 00-40-96-25-9d-14. The text indicates that this MAC address has been added to the list of associations. This type of information is typically available via the wireless management software that comes with the wireless PC or PCMCIA adapter.

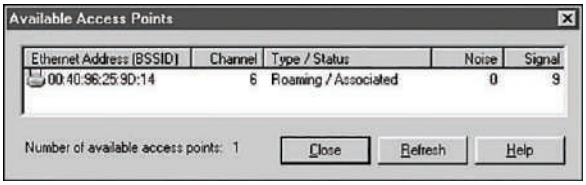


FIGURE 4-7 An example of the information displayed when an association is formed between a client and an access point.

An access point uses an association to build a table of users (clients) on the wireless network; this association table lists the MAC addresses for each networking device connected to the wireless network. Figure 4-8 provides an example of an association table. The access point uses the association table to forward data packets between the access point and the wireless network. As shown in Figure 4-8, the wireless client adapter also notifies the user if the client has lost an association with the access point.

A wireless bridge is a popular choice for connecting LANs that are running similar network protocols, even if the LANs are miles apart. Figure 4-9 provides examples. Figure 4-9(a) shows a point-to-point wireless bridge. Each building shown in Figure 4-9(a) has a connection from the wireless bridge to the building's LAN, as shown in Figure 4-10. The wireless bridge then connects to an antenna placed on the roof. A clear (line-of-sight) transmission path must exist between the two buildings; otherwise, signal *attenuation* (loss) or signal disruption can result. Antenna selection is also critical when configuring the connection. (This issue is addressed in Section 4-5.) The antenna must be selected so that the signal strength at the receiving site is sufficient to meet the required received signal level.

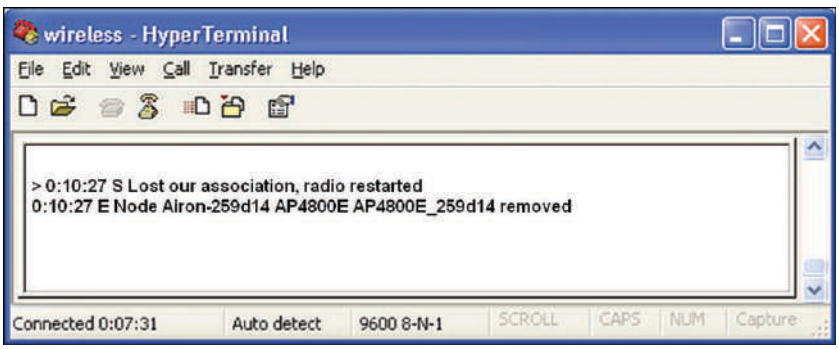


FIGURE 4-8 An example of a lost association.

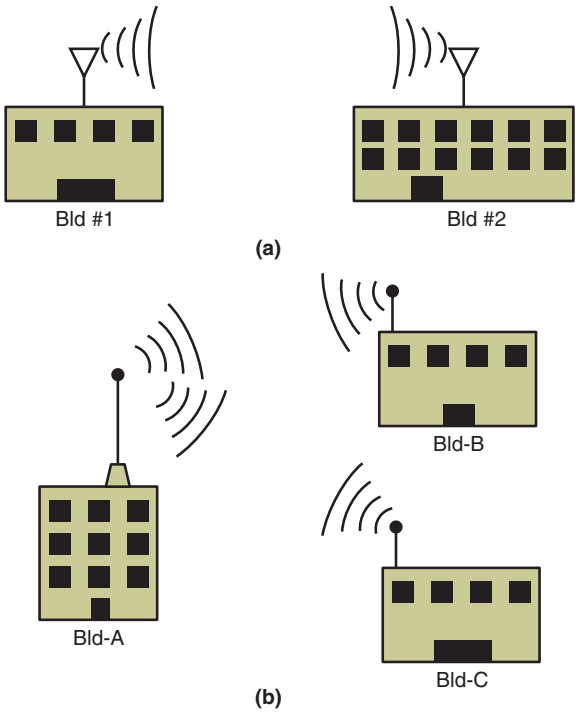


FIGURE 4-9 Examples of (a) point-to-point and (b) point-to-multipoint wireless bridge configurations.

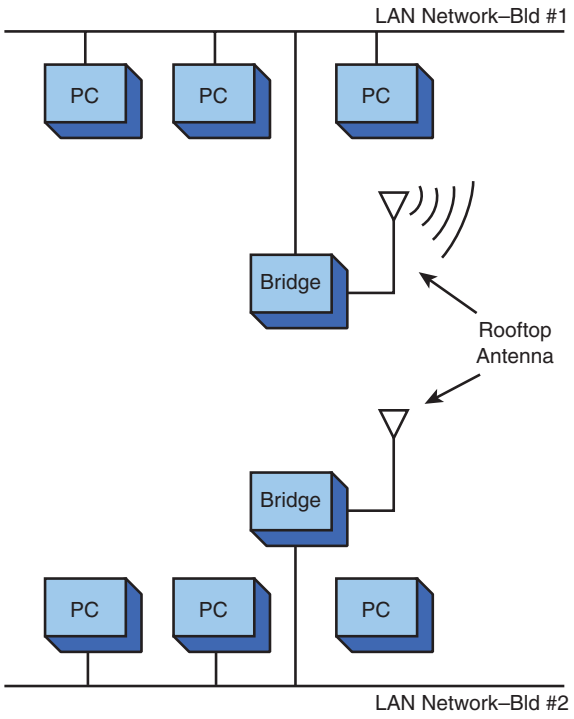


FIGURE 4-10 The wireless bridge connection to the wired network inside the building.

Figure 4-9(b) shows how a wireless bridge can be used to connect multiple remote sites to the main transmitting facility. Each building uses a bridge setup similar to that shown in Figure 4-10. The bridge connects to its respective LAN. In this case, Bld-A uses an antenna that has a wide coverage area (radiation pattern). The key objective with antenna selection is that the antenna must provide coverage for all receiving sites (in this case, Bld-B and Bld-C).

Wireless controllers are commonly used in enterprise wireless environments when managing hundreds of APs or more. In a traditional stand-alone wireless environment, each AP is managed individually. In an enterprise wireless controller environment, an AP communicates with its controller when booting up to download its necessary firmware and software, to register and authenticate itself, to receive its network information settings, and to receive its wireless LAN (WLAN) configuration. The wireless controller becomes the brain and manager of the whole operation. When wireless changes need to be made, they can be made at the controller, which pushes the changes out to all of the APs. CAPWAP (Configuration and Provisioning of Wireless Access Points) is the underlying wireless control protocol that APs use to communicate with wireless controllers. It supersedes LWAPP (Lightweight Access Point Protocol), which is a Cisco-proprietary protocol.

Wireless capacity is an issue today with the ever-increasing number of wireless users. Device density is the number of connecting wireless clients, and it has to be considered. Every wireless access point has a maximum device density that it can handle at one time. From a system design perspective, you have to plan for potential overcapacity with high-density Wi-Fi hotspots that can accommodate video streaming, image downloads, and multiple clients. Make sure you select access points than can handle the bandwidth demand; you don't want your clients to have to sacrifice bandwidth, especially when a cell phone can be set up as a hotspot that a wireless device can use to connect to the Internet via the data plan.

With wireless LANs, there is a maximum distance the signal can be transmitted. The distance limitation is a critical issue inside buildings when user mobility is required. Many obstacles can reflect and attenuate signals, causing reception to suffer. Also, the signal level for mobile users is hampered by increased distance from the access point. Distance is also a critical issue in outdoor point-to-multipoint wireless networks.

A solution is to place multiple wireless access points within the facility, as shown in Figure 4-11. Mobile clients can maintain a connection as they travel through the workplace because the wireless client automatically selects the access point that provides the strongest signal level. The access points can be arranged so that overlapping coverage of the workplace is provided, thus enabling seamless roaming for the client. The signal coverage is shown as circles in Figure 4-11. In actual practice, the radiation patterns are highly irregular due to reflections of the transmitted signal.

To have good wireless coverage in a large environment, it is not unusual to see the number of wireless access points in the range of hundreds or thousands. When dealing with so many wireless access points, it is very difficult and inefficient to program and manage each WAP individually and manually. Typically, a wireless LAN controller (WLC) is used as a central point or controller to deploy and manage all WAPs on a wireless network. When connecting to the network, each WAP connects to its WLC to get its configuration, radio channel, transmission power, and other settings. The WAPs communicate with the WLC and send their operational

wireless information to the WLC. The WLC can then use the collective information from all its WAPs to automatically adjust settings such as user load, radio channels, and radio power to improve the performance of the wireless network.

Site Survey
A process used to determine the best location(s) for placing the access point(s) to provide maximum RF coverage for wireless clients

It is important to verify that sufficient RF signal level is available for the users in a WLAN. This is best accomplished by performing a **site survey**. Inside a building, a site survey is performed to determine the best location(s) for placing the access point(s) for providing maximum RF coverage for wireless clients. Site surveys are also conducted for outside installations to determine the coverage area.

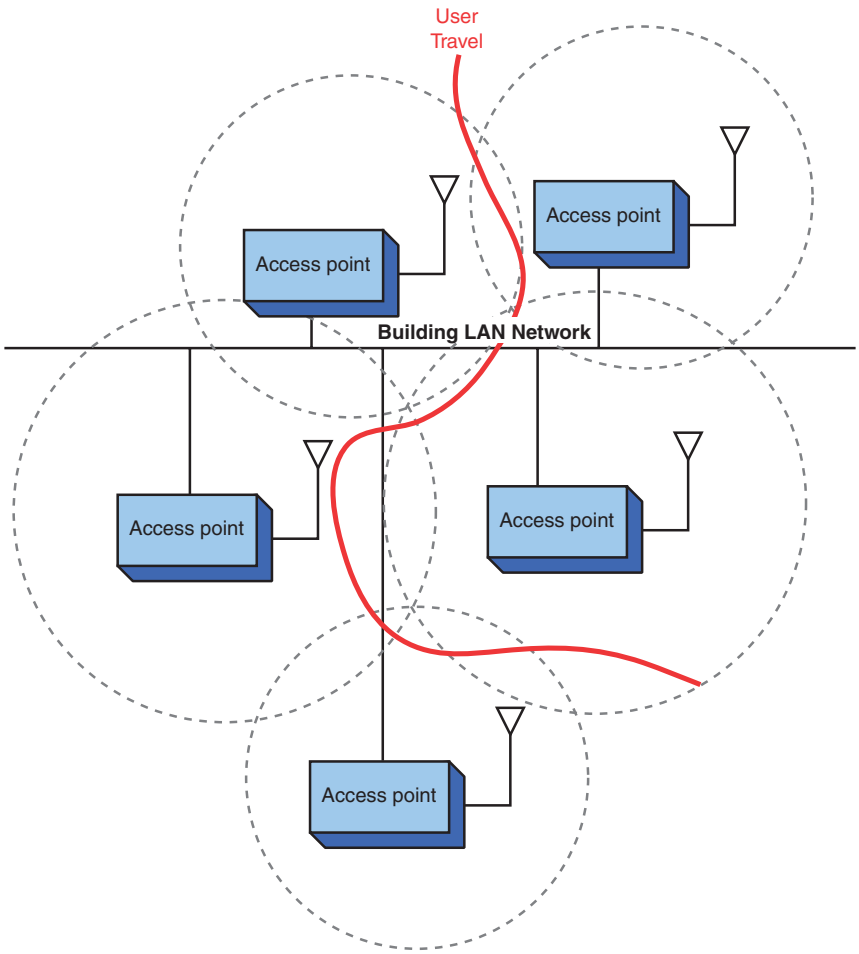


FIGURE 4-11 An example of configuring multiple access points to extend the range for wireless connectivity.

A site survey for indoor and outdoor installations should obtain the following key information:

- Indoor:
  - Electrical power
  - Wired network connection point(s)

- Access point placement
- RF coverage—user mobility
- Bandwidth supported
- Identify any significant RF interference

- Outdoor:
  - Electrical power (base access point)
  - Connection back to the home network
  - Antenna selection
  - Bandwidth supported
  - RF coverage
  - Any significant RF interference

Say that a site survey is conducted to determine access point placement to provide wireless network connectivity for the building whose floor plan is shown in Figure 4-12. The objective is to provide mobile client access throughout the building. The building already has two wired connections available for placing an access point.

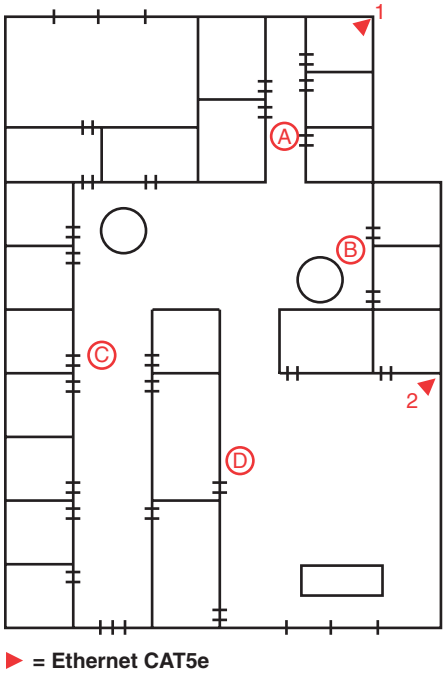


FIGURE 4-12 The floor plan for a building being surveyed for a wireless LAN.

The available wired network connections are indicated in the drawing in Figure 4-12. The site survey begins with placing an access point at position 1. A wireless mobile client is used to check the signal throughout the building. This checking used to be performed by a laptop with a purpose-built WLAN adapter as a Wi-Fi analyzer, but today, many more options are available. Handheld devices, such as tablets and smartphones, can be conveniently used for wireless site surveys. Their form factor and mobility are perfect for this purpose. Most of these devices are already equipped with built-in wireless chips. All they need is one of the many available wireless apps. This example shows test results gathered from an Android tablet with a free Wi-Fi analyzer app installed.

Figure 4-13 shows a snapshot of the wireless environment in the area. The graph shows the signal strength for each wireless SSID found. The signal strength is the wireless signal power level, and it is represented in –dBm format, from 0 to –100. This is the power ratio, in dB, of the measured power referenced to 1 mW. The closer the value is to 0, the stronger the signal, and the stronger the signal, the more reliable the wireless connection. Wireless is everywhere today, so when you conduct a site survey, you should not be too surprised to see more SSIDs than just yours. For this example, the site survey is intended for the wireless SSID ET377. As the graph shows, ET377 has the strongest signal of all the SSIDs. However, the signal strength may not represent the goodput. *Goodput* refers to the actual wireless data throughput, as measured by an application on the end device. It represents the actual transmission rate of a wireless connection, which is not the maximum theoretical transmission rate.

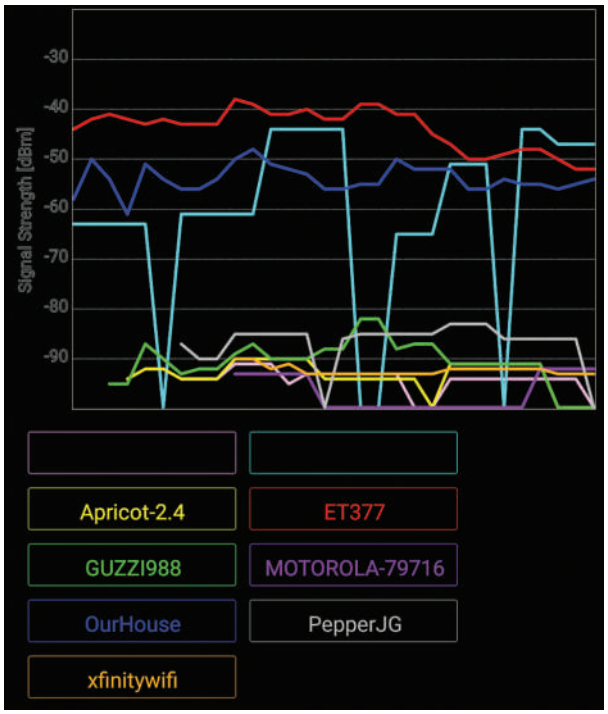


FIGURE 4-13 A snapshot of the RF signal environment.

The first measurement, shown in Figure 4-14, is taken at point A. Notice that the signal strength is at –43 dBm, which is an excellent connection. This will change if the signal level decreases significantly.

The next observation is made at point B, and the signal strength is measured at –52 dBm (see Figure 4-15). The signal has decreased somewhat, but it is still acceptable, which indicates that a connection is still good. The signal level drops to –67 dBm at point C, as shown in Figure 4-16. This connection is fair.

A floor plan showing the locations of wireless access points and wireless signal strength and coverage is a wireless or Wi-Fi heat map. Typically, a wireless/Wi-Fi heat map shows a real map of a room, floor, or even a city overlaid by a graphical representation of a wireless signal.

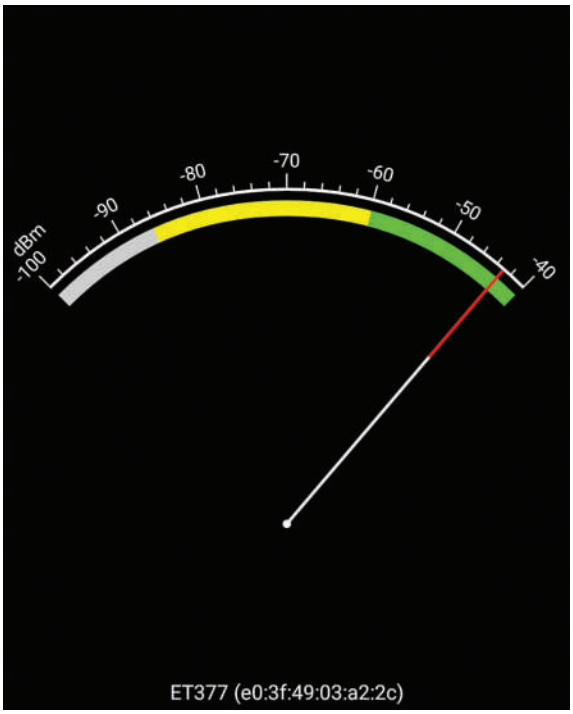


FIGURE 4-14 The RF signal strength observed at point A.

The mobile client is moved to point D in the building, and signal quality "Out of range" is observed (see Figure 4-17). This is also called a *loss of association* with the access point.

The site survey indicates that one access point placed at point 1 in the building is not sufficient to cover the building's floor plan. The survey shows that the additional cost of another access point is easily justified for providing full building wireless LAN coverage. The building has two wired network connections available for placing an access point (points 1 and 2). It is decided to place another access point at point 2. The site survey is repeated, and it shows excellent signal strength obtained throughout the building.

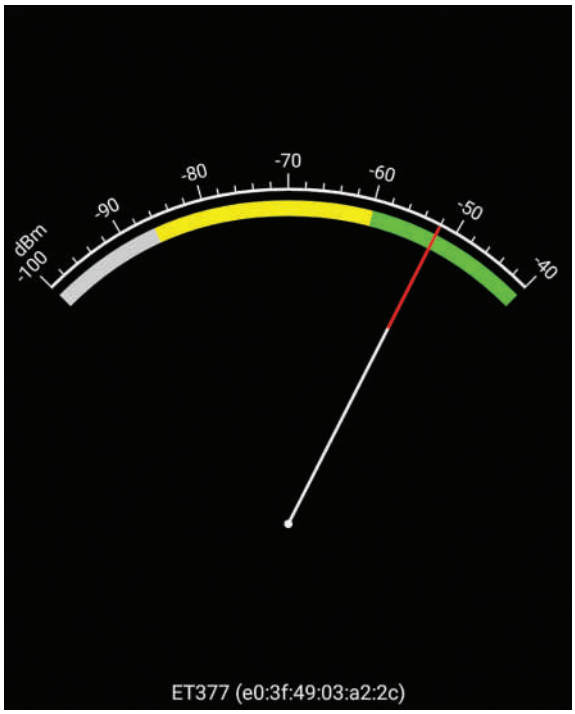


FIGURE 4-15 The RF signal strength at point B.

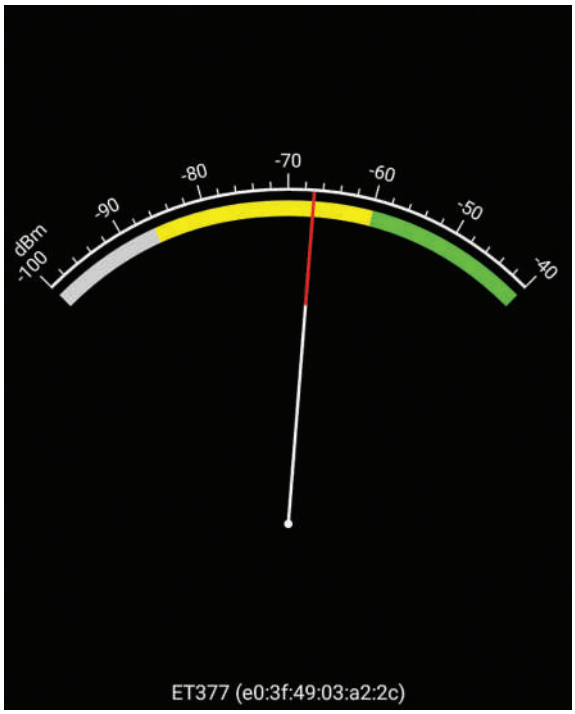


FIGURE 4-16 The drop in the signal quality to fair at point C.

In some cases, a *range extender* can be used to provide additional wireless coverage. This device basically extends the reach of the wireless network.

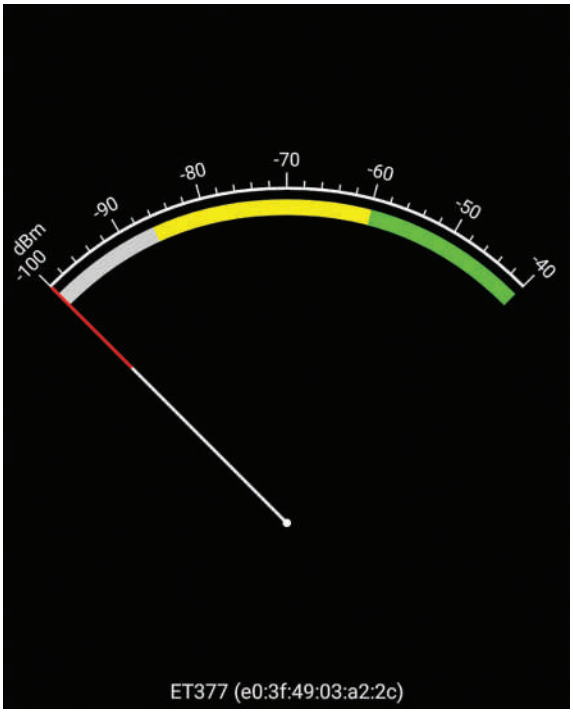


FIGURE 4-17 The "Out of range" measurement for point D.

Section 4-3 Review

This section covers the following Network+ exam objectives.

1.6 Explain the use and purpose of network services.

This section introduces the services provided by a wireless LAN adapter: delivery of the data, authentication, and privacy.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

A physical cable connection (typically CAT6 or greater) ties an access point to a wired network's switch or hub (typically Ethernet).

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

This section introduces the SSID. An 802.11 wireless LAN device uses an SSID to identify what wireless data traffic is allowed to connect to the network. The SSID is the wireless service set identifier, basically a password that enables the client to join the wireless network.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section talks about preparing a site to support access point placement and the changes in signal strength that result from environmental factors.

3.2 Explain the purpose of organizational documents and policies.

The available wired network connections are indicated in a floor plan for a building being surveyed for a wireless LAN.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

A site survey for indoor and outdoor installations should obtain the following key information:

- Electrical power
- Wired network connection point(s)
- Access point placement
- RF coverage—user mobility
- Bandwidth supported
- Identify any significant RF interference

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

The wrong SSID prevents an association, keeping a client from being able to become a member of the wireless network.

Test Your Knowledge

1. What happens when an *association* is made?

   a. A wireless connection is obtained.
   b. The MAC address of the client is obtained.
   c. Unauthorized network access is prevented.
   d. Excessive routing is prevented.

2. True or false: Site surveys help determine the following:

   - The best location for placing access points
   - Power connection
   - RF coverage
   - Antenna selection
   - IP address selection

   True

4-4 BLUETOOTH, WIMAX, RFID, AND MOBILE COMMUNICATIONS

This section looks at four wireless technologies: Bluetooth, WiMAX, RFID, and mobile communications. These technologies all play important roles in wireless networks, and this section looks at each of them. This section also looks at configurations and examples of the hardware being used. A fun exercise is to have students connect their laptops to each other using Bluetooth, as described in the example presented in this section.

This section looks at four wireless technologies: Bluetooth, WiMAX, RFID, and mobile communications. Each of these technologies plays an important role in wireless networks. The sections that follow examine each of these wireless technologies, including a look at configuration and examples of the hardware being used.

Bluetooth

The wireless technology Bluetooth is based on the 802.15 standard. Bluetooth was developed to replace the cable connecting computers, mobile phones, handheld devices, portable computers, and fixed electronic devices. The information normally carried by a cable is transmitted over the 2.4GHz ISM frequency band, which is the same frequency band used by 802.11b/g/n/ax. There are four output power classes for Bluetooth. Table 4-6 lists the maximum output power and the operating distance for each class.

Bluetooth Low Energy (BLE) technology has been developed to provide operation on a small battery for up to five years. This technology is ideal for applications that require the exchange of small amounts of data periodically. BLE operates in the 2.4GHz ISM band and remains in sleep mode except when a connection is initiated. BLE devices have significantly lower power requirements than do traditional Wi-Fi devices. For example, whereas a Wi-Fi device consumes about 500 µW for 10 messages, a BLE device consumes only 50 µW.

TABLE 4-6 **Bluetooth Output Power Classes**

Power Class	Average Output Power	Operating Distance
1	100 mW	~100 meters
2	2.5 mW	~10 meters
3	1 mW	~1 meter
4	0.5 mW	~0.5 meter

When a Bluetooth device is enabled, it uses an **inquiry procedure** to determine whether any other Bluetooth devices are available. The device also uses this procedure to allow itself to be discovered.

If a Bluetooth device is discovered, it sends an inquiry reply back to the Bluetooth device initiating the inquiry. Next, the Bluetooth devices enter the **paging procedure**, which is used to establish and synchronize a connection between

Inquiry Procedure
A process used to determine whether other Bluetooth devices are available

Paging Procedure
A process used to establish and synchronize a connection between two Bluetooth devices

Piconet
An ad hoc network of up to eight Bluetooth devices

two Bluetooth devices. When the procedure for establishing the connection has been completed, the Bluetooth devices will have established a **piconet**, an ad hoc network of up to eight Bluetooth devices, such as a computer, mouse, headset, earpiece, and so on. In a piconet, one Bluetooth device (the primary) is responsible for providing the synchronization clock reference. All other Bluetooth devices are called *secondaries*.

Let's look at an example of setting up a Bluetooth network linking a macOS computer to another Bluetooth-enabled device. To enable Bluetooth on macOS, click **Apple icon > System Preferences > Bluetooth** and then click **Turn Bluetooth On** (see Figure 4-18). The Mac automatically discovers other Bluetooth devices nearby.

Pairing
Setting up a Bluetooth device to connect to another Bluetooth device

Passkey
A passphrase used in Bluetooth security to limit outsider access to pairing

Next, you need to select the device with which you will be establishing a Bluetooth connection. When Bluetooth is turned on, the Mac searches for another Bluetooth device. When a Bluetooth device is found, it appears in the Devices window. To connect the desired Bluetooth device, select the **Pair** button next to the device. (The process of setting up a Bluetooth device to connect to another Bluetooth device is called **pairing**.) You are asked for a passkey or passphrase. The **passkey** is used in Bluetooth security to limit outsider access to the pairing. Only people with the passkey can pair with the Bluetooth device. Anyone who tries to pair units with the wrong passphrase will not be able to pair.

At this point, you can transfer files between the paired devices if the Bluetooth Sharing settings for the device have been set to allow files to come in. Find these settings by clicking **Apple icon > System Preferences > Sharing** and selecting **Bluetooth Sharing**. Figure 4-19 shows an example of the setup for the file transfer.

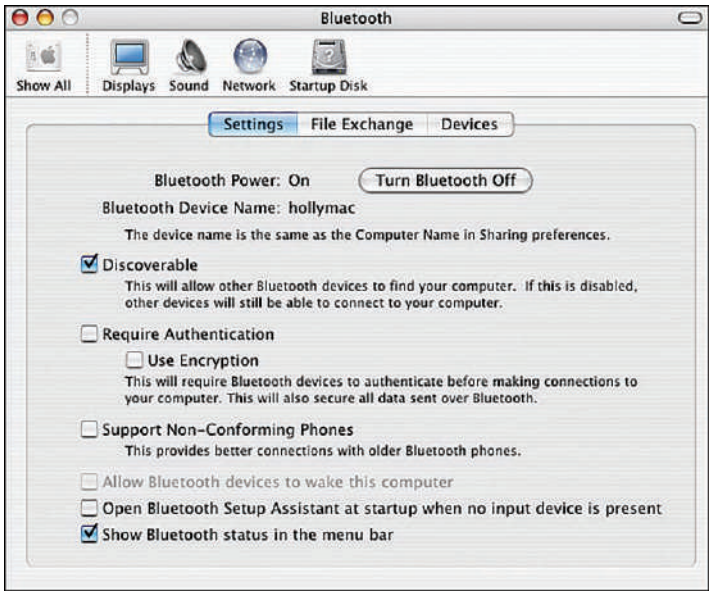


FIGURE 4-18 The window for configuring Bluetooth settings on a Mac.

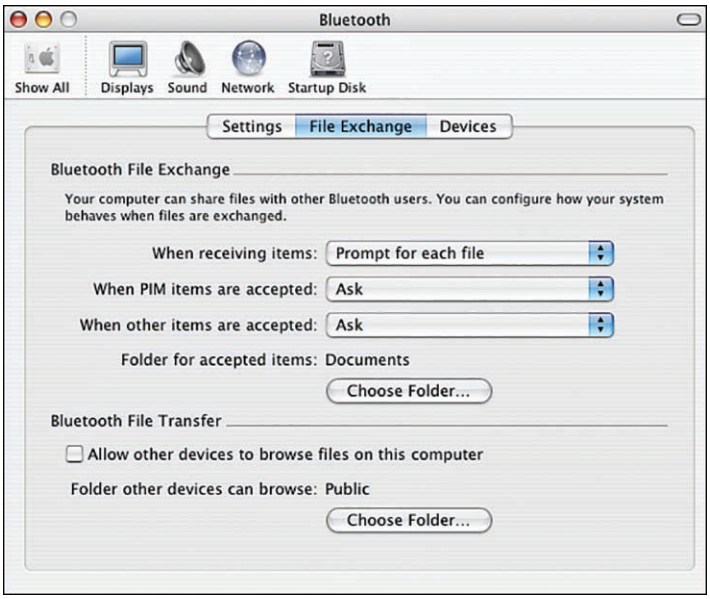


FIGURE 4-19 The Mac window showing the settings for a file transfer.

Figure 4-20 shows an incoming text file. The File Transfer menu enables you to select where received files are saved. In this case, the incoming files are being saved to the desktop.

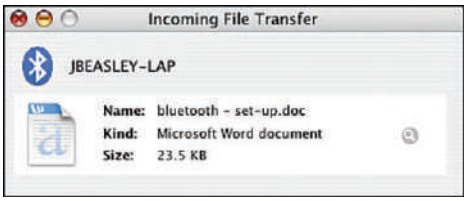


FIGURE 4-20 The Mac window showing that a text file is coming in from another Bluetooth device.

The details for setting up Bluetooth on Windows 10 differ slightly from those for macOS, but the basic steps are the same:

1. Enable the Bluetooth radio.
2. Enable discoverability (to allow other Bluetooth devices to find the device).
3. Select the device for pairing.

WiMAX
Worldwide Interoperability for Microwave Access, a broadband wireless system based on the IEEE 802.16e standard

BWA
Broadband wireless access

WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is a broadband wireless system that has been developed for broadband wireless access (**BWA**) for fixed

and mobile stations and can provide a wireless alternative for last-mile broadband access in the 2GHz–66GHz frequency range. BWA access for fixed stations can be up to 30 miles, whereas mobile BWA access is 3–10 miles. Internationally, the WiMAX frequency standard is 3.5GHz, while the United States uses both the unlicensed 5.8GHz and the licensed 2.5GHz spectra. In addition, WiMAX has been investigationally adapted for use in the 700MHz frequency range. Information transmitted at this frequency is less susceptible to signal blockage due to trees. The disadvantage of the lower frequency range is the reduction in bandwidth.

NLOS
Non-line-of-sight

WiMAX uses OFDM as its signaling format. This signaling format was selected for the WiMAX IEEE 802.16a standard because of its improved **NLOS** (non-line-of-sight) characteristics in the 2GHz–11GHz frequency range. An OFDM system uses multiple frequencies for transporting the data, which helps minimize multipath interference problems. Some frequencies may experience interference problems, but the system can select the best frequencies for transporting the data.

WiMAX also provides flexible channel sizes (for example, 3.5MHz, 5MHz, and 10MHz), which provides adaptability to standards for WiMAX worldwide. This also helps ensure that the maximum data transfer rate is supported. For example, the allocated channel bandwidth could be 6MHz, and the adaptability of the WiMAX channel size enables it to adjust to use the entire allocated bandwidth.

In addition, the WiMAX (IEEE 802.16e) media access control (MAC) layer differs from the IEEE 802.11 Wi-Fi MAC layer in that the WiMAX system has to compete only once to gain entry into the network. When a WiMAX unit has gained access, the base station allocates a time slot to it, thereby providing the WiMAX system scheduled access to the network. The WiMAX system uses time-division multiplexing (TDM) data streams on the downlink and time-division multiple access (TDMA) on the uplink and centralized channel management to ensure that time-sensitive data is delivered on time. In addition, WiMAX operates in a collision-free environment, which improves channel throughput.

Last Mile
The last part of the connection from a telecommunications provider to a customer

WiMAX has a range of up to 30 miles, and it operates in both point-to-point and point-to-multipoint configurations. This can be useful in situations where DSL or cable network connectivity is not available. WiMAX is also useful for providing the last-mile connection. The **last mile** is basically the last part of the connection from a telecommunications provider to a customer. The cost of the last mile connection can be high, which makes a wireless alternative attractive to customers.

The 802.16e WiMAX standard holds a lot of promise for use as a mobile air interface.

Radio Frequency Identification (RFID)
A technique that uses radio waves to track and identify people, animals, objects, and shipments

Backscatter
The reflection of radio waves striking an RFID tag and reflecting back to the transmitter source

Radio Frequency Identification

Radio frequency identification (RFID) uses radio waves to track and identify people, animals, objects, and shipments. It is based on the principle of modulated **backscatter**—the reflection of the radio waves striking an RFID tag back to the transmitter source, with its stored unique identification information.

Figure 4-21 illustrates a basic RFID system, which consists of two elements:

- **RFID tag:** An RFID tag (also called an RF transponder) includes an integrated antenna and radio electronics.

- **Reader:** A reader (also called a transceiver) consists of a transceiver and an antenna. A transceiver is a combination of a transmitter and receiver.

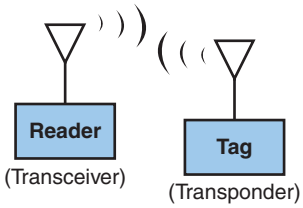


FIGURE 4-21 Basic block diagram of an RFID system.

The reader transmits radio waves, which activates (turns on) an RFID tag. The tag then transmits modulated data, containing its unique identification information stored in the tag, back to the reader. The reader then extracts the data stored on the RFID tag.

The RFID idea dates back to 1948, when the concept of using reflected power as a means of communication was first proposed. The 1970s saw further development in RFID technology—in particular, a UHF scheme that incorporates rectification of the RF signal for providing power to the tag. Development of RFID technology significantly increased in the 1990s. Applications included toll collection that allowed vehicles to pass through tollbooths at highway speeds while still being able to record data from the tag.

Today, RFID technology is being used to track inventory shipments for major commercial retailers, by the transportation industry, and by the Department of Defense. In addition, RFID applications are being used in Homeland Security for tracking container shipments at border crossings. In addition, RFID is being incorporated into WLAN computer networks to keep better track of inventory. RFID technology is being used as a wireless means of asset tracking and is therefore becoming more important in networks. The tracking technology is even being extended to tracking Wi-Fi devices within the WLAN infrastructure.

Three parameters define an RFID system:

- Means of powering the tag
- Frequency of operation
- Communications protocol (also called the air interface protocol)

Powering the Tag

RFID tags are classified in three ways, based on how they obtain their operating power:

- **Passive:** Power is provided to a passive tag by rectifying the RF energy, transmitted from the reader, that strikes the RF tag antenna. The rectified power level is sufficient to power the ICs on the tags and also provides

sufficient power for the tag to transmit a signal back to the reader. Figure 4-22 shows an example of a passive RFID tag (also called an inlay). A tag inlay includes both an RFID chip and an antenna mounted on a substrate.

- **Semi-active:** With semi-active tags, a battery powers the electronics on a tag, but the tag uses backscatter to transmit information back to the reader.
- **Active:** With active tags, a battery powers the tag and transmits a signal back to the reader. Basically, this is a radio transmitter. New active RFID tags are incorporating wireless Ethernet (that is, 802.11 Wi-Fi connectivity). An example is the G2C501 active RFID tag from G2 Microsystems, shown in Figure 4-23. The power consumption of the G2C501 is 10 µA in sleep mode, and the device uses two AA batteries with an expected lifetime of five years. The G2C501 also works in the standard 915MHz range. In addition, the G2C501 has location capability. This is accomplished by making receive signal strength indicator (RSSI) measurements from three separate access points. The three measurements provide sufficient information to make a triangulation measurement for use in locating the object.

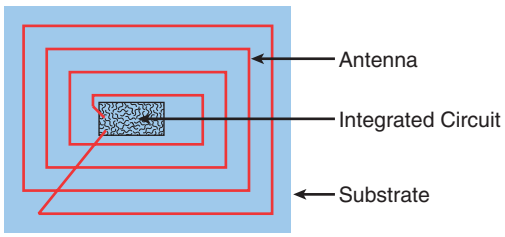


FIGURE 4-22 An example of an RFID inlay.

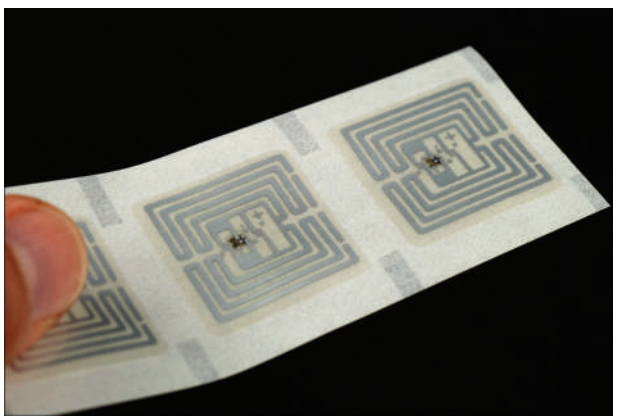


FIGURE 4-23 The G2C501 active RFID tag from G2 Microsystems (Albert Lozano/Shutterstock).

Frequency of Operation RFID tags must be tuned to the reader's transmit frequency in order to turn on. RFID systems typically use three frequency bands for operation (see Figure 4-24):

- **Low frequency (LF):** LF tags typically use frequency-shift keying (FSK) between the 125KHz and 134KHz frequencies. These tags can handle only low data rates (~12Kbps), and they are not appropriate for any applications requiring fast data transfers. However, LF tags are suitable for animal identification, such as with dairy cattle and other livestock. The RFID tag information is typically obtained when the livestock are being fed. The read range for low-frequency tags is approximately 0.33 meter.
- **High frequency (HF):** HF tags operate in the 13.56MHz industrial band. High-frequency tags have been available commercially since 1995. The longer wavelengths of the HF radio signal are less susceptible to absorption by water or other liquids. Therefore, these tags are suitable for tagging liquids. The read range for HF tags is approximately 1 meter. The short read range provides for better-defined read ranges. The applications for tags in this frequency range include access control, smart cards, and shelf inventory. The data rate for HF tags is 26Kbps.
- **Ultra-high frequency (UHF):** UHF tags work at 860–960MHz and at 2.4GHz. The data rates for these tags can be 50–150Kbps and greater. These tags are popular for tracking inventory. The read range for passive UHF tags is 3–6 meters, which makes them a good choice for reading pallet tags. However, if an active tag is used, a read range up to 100 meters is possible.



FIGURE 4-24 The frequency bands used by RFID tags.

Communications (Air Interface) Protocol The air interface protocol adopted for RFID tags is **Slotted Aloha**, a network communications protocol similar to the Ethernet protocol. With Slotted Aloha, the tags are only allowed to transmit at predetermined times after being energized. This technique reduces the likelihood of data collisions between RFID tag transmissions and allows for the reading of up to 1000 tags per second (for high-frequency tags). The operating range for RFID tags can be up to 30 meters. This means that multiple tags can be energized at the same time, and RF data collisions can possibly occur. If a collision occurs, the tag will transmit again after a random back-off time. The readers transmit continuously until there is no tag collision.

Slotted Aloha
A wireless network communications protocol similar to the Ethernet protocol

Mobile (Cellular) Communications

Today, many types of mobile devices, also called cellular devices, can be used to access computer networks. Examples include smartphones, laptops, tablets, and gaming devices. All of these devices are extremely powerful and use wireless technology to connect to the network. This chapter has provided an overview of many of the wireless technologies being used today, including the 802.11 family of Wi-Fi technologies, Bluetooth, WiMAX, and RFID. This section provides a brief summary of some of the other wireless technologies currently available.

CDMA CDMA (code-division multiple access) is a communications technology in which spread-spectrum techniques are used to multiplex more than one signal within a single channel. In this case, each device uses a different binary sequence to modulate the carrier, spreading the spectrum of the waveform (spread spectrum). The signals are separated at the receiver by a correlator that accepts only the signal from the selected binary sequence.

LTE/4G LTE (Long Term Evolution) is a 4G wireless communications standard. It is designed to provide speeds up to 10 times those of 3G networks.

HSPA+ HSPA+ (Evolved High-Speed Packet Access) provides network speeds comparable to those of LTE networks. Theoretical speeds are 168Mbps for download and 22Mbps uplink.

3G/4G/5G 3G (Third Generation) was developed to provide broadband network wireless services. The standard defining 3G wireless is International Mobile Communications, or IMT 2000. 4G (Fourth Generation), which is the successor to 3G technology, provides download speeds of 100Mbps. 5G (Fifth Generation) is the latest wireless network technology provided by the cellular network, with speeds ranging from 40Mbps to 1.5Gbps.

EDGE EDGE (Enhanced Data GSM Evolution) provides download speeds of 384Kbps.

NFC A concept related to mobile communications and smartphones is NFC, which stands for Near Field Communication. NFC is a set of communication protocols that are used to enable two electronic devices to communicate. A typical NFC device is a smartphone. By using NFC, smartphones can establish communication if they are within 4 cm of each other. Applications of NFC include reading electronic tags and making payments.

Geofencing With many type of wireless devices using different type of wireless technologies, it has become more and more difficult for network administrators to keep track of the devices entering and leaving the premises. *Geofencing* is used to create a virtual electronic boundary for mobile and wireless devices to detect their whereabouts as well as control certain functionalities, such as camera or microphone, of the devices through the use of mobile device management (MDM). For example, geofencing may be used in a highly classified area or a restricted area in a corporate building.

Section 4-4 Review

This section covers the following Network+ exam objectives.

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

This section introduces the RFID reader, which consists of a transceiver and an antenna. A transceiver is a combination of a transmitter and receiver.

1.7 Explain basic corporate and datacenter network architecture.

This section introduces Bluetooth, RFID, WiMAX, and mobile can support links up to 30 miles and is a possible alternative for providing last-mile connections.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section introduces geofencing, which is used to create a virtual electronic boundary for mobile and wireless devices to detect their whereabouts as well as control certain functionalities, such as camera or microphone, of the devices through the use of mobile device management (MDM).

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section introduces 5G (Fifth Generation), which is the latest wireless network technology provided by the cellular network, with speeds ranging from 40Mbps to 1.5Gbps.

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

This section introduces Bluetooth, RFID, WiMAX, and mobile technologies.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section examines the download speeds for many different technologies.

4.3 Given a scenario, apply network hardening techniques.

This section introduces the concept of geofencing.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section mentions that WiMAX operates in a collision-free environment, which improves channel throughput.

5.5 Given a scenario, troubleshoot general networking issues.

The air interface protocol adopted for RFID tags is Slotted Aloha, a network communications protocol similar to the Ethernet protocol. With Slotted Aloha, tags are only allowed to transmit at predetermined times after being energized. This technique reduces the likelihood of data collisions between RFID tag transmissions and allows for the reading of up to 1000 tags per second (for high-frequency tags).

Test Your Knowledge

1. WiMAX operates at which frequencies in the United States?
    a. Both the unlicensed 5.2GHz and the licensed 2.4GHz spectra
    b. Both the unlicensed 5.3GHz and the licensed 2.6GHz spectra
    c. Both the unlicensed 13.2GHz and the licensed 5.6GHz spectra
    d. Both the unlicensed 5.8GHz and the licensed 2.5GHz spectra
2. What is the maximum range of WiMAX?
    a. 30 kilometers
    b. 30 miles
    c. 30 meters
    d. None of these answers are correct.
3. At what frequency does Bluetooth operate?
    a. 5GHz
    b. 100MHz
    c. 2.4GHz
    d. None of these answers are correct.

4-5 CONFIGURING A POINT-TO-MULTIPOINT WIRELESS LAN: A CASE STUDY

This section presents an example of preparing a proposal for providing a point-to-multipoint wireless network for a company. It walks through the multiple steps involved in implementing a point-to-multipoint wireless network, including performing an antenna site survey, establishing a link to the home network, configuring the multipoint distribution, and configuring the remote site.

This section presents an example of preparing a proposal for providing a point-to-multipoint wireless network for a company. The administrators for the company have decided that it would be beneficial to provide a wireless network connection for their employees back to the company's network (the home network). This example walks through the following steps:

1. Conducting an initial antenna site survey
2. Establishing a link from the home network to the distribution point
3. Configuring the multipoint distribution
4. Conducting an RF site survey for establishing a baseline signal level for the remote wireless user
5. Configuring the remote user's installation

The objective of this example is to establish a point-to-multipoint wireless network that provides remote users with a wireless network connection. The remote users are to be at fixed locations within the proposed coverage area. Figure 4-25 shows a simple terrain profile of the proposed area. The data rate for the wireless connection to remote users needs to be at least 2Mbps.

Note

Antenna placement is critical when setting up a point-to-multipoint wireless LAN. Incorrect antenna placement can severely affect reception quality.

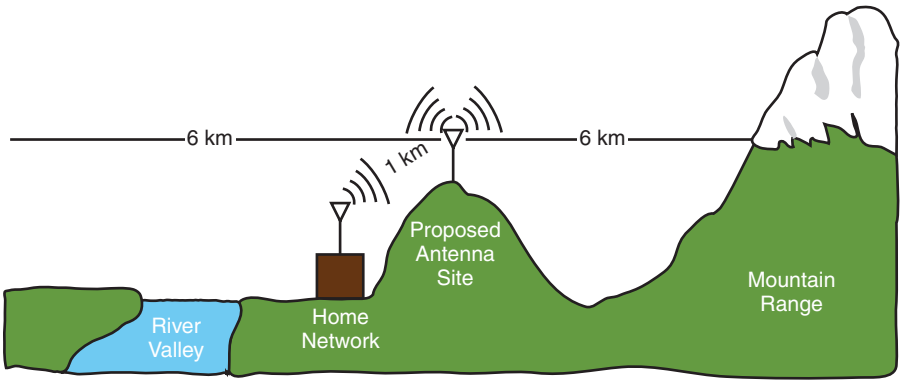


FIGURE 4-25 The terrain profile of the area to be supported by the proposed point-to-multipoint wireless network.

Step 1: Conducting an Antenna Site Survey

The proposed antenna site (refer to Figure 4-25) is on top of a hill approximately 1 kilometer from the home network. A site survey provides the following information:

- The site has a tower that can be used to mount the wireless antenna.
- The site has a small building and available rack space for setting up the wireless networking equipment.
- There is a clear view of the surrounding area for 6 kilometers in every direction.
- There is not an available wired network connection back to the home network. The decision is made to use the proposed antenna site and set up an 11Mbps wireless link back to the home network.

Step 2: Establishing a Point-to-Point Wireless Link to the Home Network

The cost of installing a wired connection back to the home network would be too high, so it is decided to use a point-to-point 802.11 wireless link for the interconnection. This requires that antennas be placed at both the home network and the antenna site. A wireless bridge is used at each end of the point-to-point wireless link to interconnect the networks. The bridge will connect to the wired home network and to the multipoint distribution on the antenna site. Also, each antenna will be outfitted with lightning arrestors to protect the electronics from any possible lightning strikes. Figure 4-26 shows the proposed wireless connection.

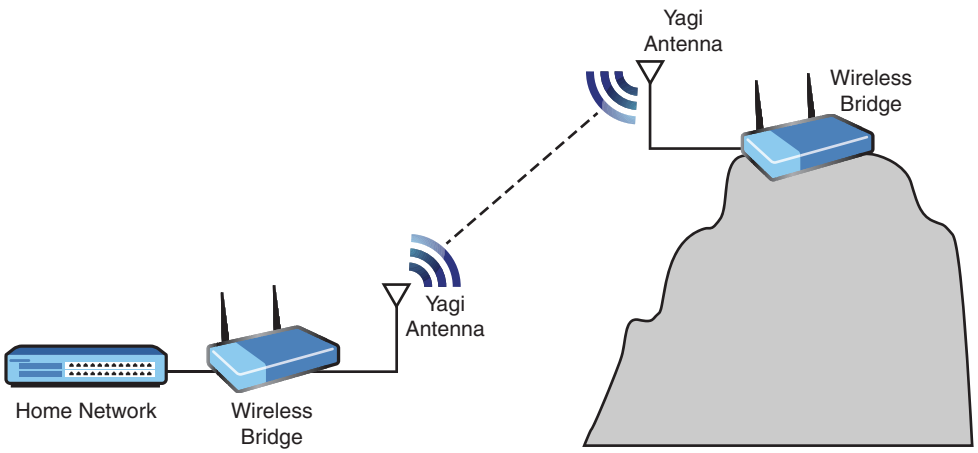


FIGURE 4-26 The proposed point-to-point wireless link between the home network and the antenna site.

Many manufacturers of antennas support wireless networking, and many types of antenna can be used. Antenna types from many manufacturers were investigated for possible use in the interconnection. Three possible antennas were selected for the wireless network, as outlined in Table 4-7.

Note

The selection of the incorrect antenna type can lead to a poorly designed radio link and poor reliability.

TABLE 4-7 **Sample of 802.11 Wireless Antennas**

Antenna	Type	Radiation Pattern	Costs
A	Omni	Omnidirectional	Moderate
B	Yagi	Directional	Moderate
C	Dish	Highly directional	High

Antenna A has an omnidirectional radiation pattern. This means the antenna can receive and transmit signals in a 360-degree pattern. Figure 4-27(a) shows the radiation pattern for an omnidirectional antenna. Antenna A supports all 802.11 types. Table 4-7 also indicates that this antenna has a moderate cost.

Antenna B is a Yagi antenna with a directional or unidirectional radiation pattern, as shown in Figure 4-27(b). The Yagi antenna supports all 802.11 antenna types.

Antenna C is a dish antenna, or parabolic reflector. These antennas provide extremely high directional gain, as illustrated in Figure 4-27(c). The dish antenna supports 802.11 systems. The cost of a dish antenna can be quite high relative to the cost of a Yagi or an omnidirectional antenna.

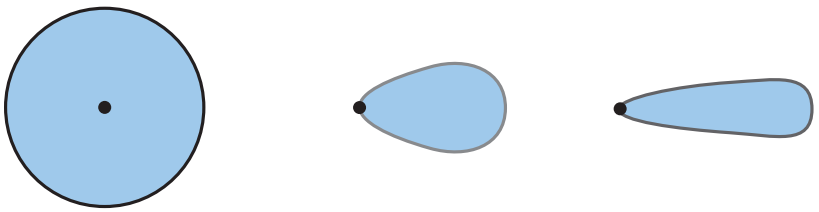


FIGURE 4-27 Antenna radiation patterns for (a) omnidirectional, (b) Yagi, and (c) dish [parabolic reflector] antennas. The cost of the Yagi antenna is comparable to that of the omnidirectional antenna.

Antenna B, the directional Yagi, is selected for the point-to-point link. The antenna meets the distance requirement and also meets the 11Mbps data rate requirement. Antennas A and C were not selected for the following reasons:

- **Antenna A:** The omnidirectional radiation pattern is not appropriate.
- **Antenna C:** The cost of a high-gain dish antenna is not justified for the short distance.

Steps 3 and 4: Configuring the Multipoint Distribution and Conducting an RF Site Survey

At this point, a wireless data link has been established with the home network. The next task is to configure the antenna site for multipoint distribution. It was previously decided that a 300Mbps link would be adequate for the remote users, based on the data rate to be supported for the planned coverage area.

The site survey in step 1 showed that there is a clear view of the surrounding area for 6 kilometers in each direction. Antenna A (see Table 4-7) provides an omnidirectional radiation pattern for 7 kilometers. This satisfies the coverage area. Antenna A is mounted on the antenna site tower, connected to a lightning arrestor,

and then connected to the output of a wireless bridge. Next, an RF site survey of the planned coverage area is conducted to verify the signal quality provided by the antenna selected. Measurements are made from multiple locations in the planned coverage area. All remote sites within 4 kilometers of the distribution show excellent signal strength (see Figure 4-28).

The signal quality drops to good at 6 kilometers at all surveyed remote locations except for one area, which shows a poor quality (see Figure 4-29). The signal is apparently being affected by multipath distortion from a small lake area. A fix to this might be to move the antenna to a different height to minimize reflection problems. An antenna at a different height will receive different reflections and possibly less interference. In some cases, antenna alignment can be changed to decrease the interference. A more costly solution would be to add antenna diversity, which basically means placing multiple antennas on the receiving tower and using the best signal for the connection.

Note

When dealing with antennas, it is important to consider effective isotropic radiated power (EIRP), which is the power that comes off an antenna and is the value the FCC uses to determine and measure power limits in wireless equipment.

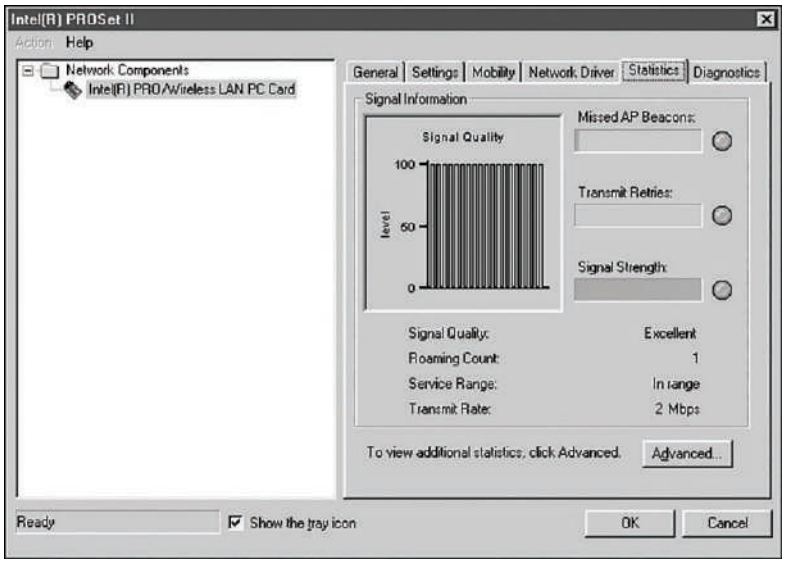


FIGURE 4-28 The excellent signal quality measured for the multipoint distribution.

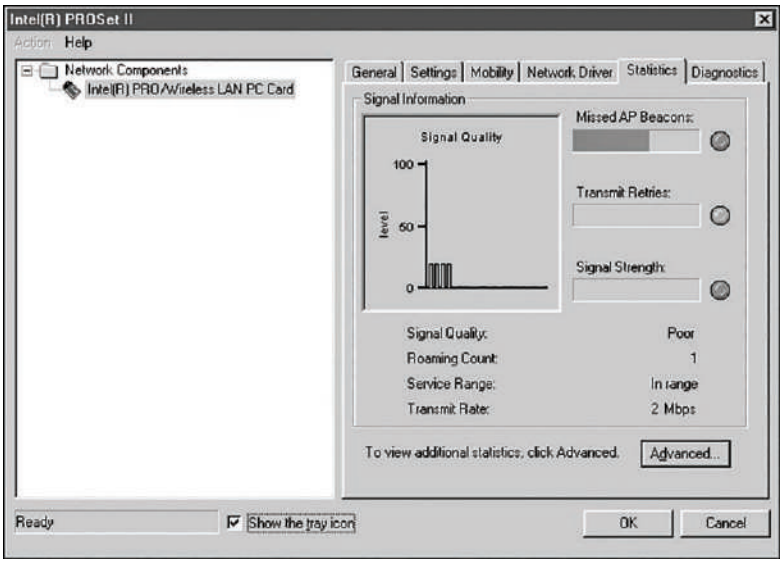


FIGURE 4-29 The poor signal quality measured at the remote site near the lake.

Step 5: Configuring the Remote Installations

The last task is to develop a configuration for the remote users. The antenna for each remote user needs to be able to see only the multipoint distribution antenna site. The requirements for the remote client are as follows:

- 300Mbps data rate connection
- Directional antenna (Yagi) plus mount, lightning arrestor, and wireless bridge

Antenna B (refer to Table 4-7) is selected for the directional antenna. This antenna will provide a sufficient RF signal level for the remote users. Each remote user will need a wireless bridge and a switch to connect multiple users. (Note that the bridge is set for a 2.4Mbps data rate.) Figure 4-30 shows the setup for the remote users.

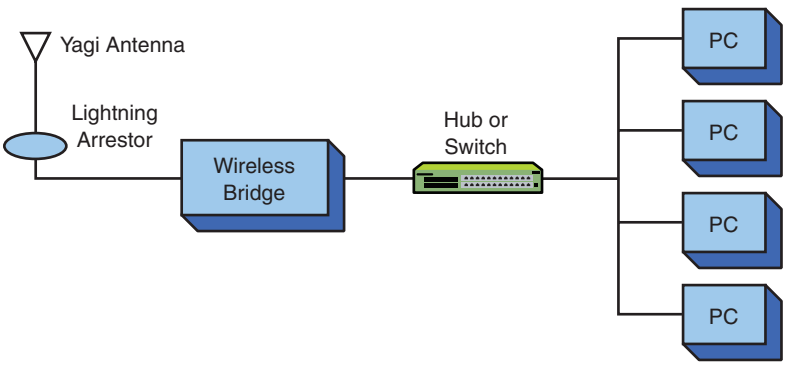


FIGURE 4-30 The setup for the remote users in the proposed point-to-multipoint wireless network.

Section 4-5 Review

This section covers the following Network+ exam objectives.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section examines various networking devices for establishing wireless networks.

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

This section presents various types of antennas that can be used to develop a wireless network.

3.2 Explain the purpose of organizational documents and policies.

This section introduces the steps for completing a wireless antenna site survey.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section discusses a situation in which the signal is being affected by multipath distortion from a small lake area. A fix to this might be to move the antenna to a different height to minimize reflection problems.

4.3 Given a scenario, apply network hardening techniques.

This section discusses the issues related to and planning for antenna placement.

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

This section presents antenna types and placement.

Test Your Knowledge

1. Which types of antennas are typically used at receive sites from a multipoint distribution system? (Select all that apply.)

   a. Yagi
   b. Omnidirectional
   c. Parabolic
   d. Hydroxyl

2. True or false: When configuring remote installations for wireless networks, the receive site needs to be able to see the multipoint distribution antenna site.

   True

4-6 TROUBLESHOOTING WIRELESS NETWORKS

This section provides an overview of common techniques for troubleshooting wireless networks. Students should become familiar with each scenario presented.

This section examines some common techniques for troubleshooting wireless networks. Wireless networks have greatly simplified the steps for connecting to a network, but they do occasionally fail. The following sections describe some scenarios that users might encounter and steps for troubleshooting and resolving the wireless issues.

Access Point Hardware Issues

The primary hardware device in wireless networks is the access point. Some networks have multiple access points. A simple first step is to ping the IP address for an access point in order to verify network connectivity. You should expect a reply to the ping, but if you don't get a reply, you can verify the IP address and repeat the ping. If it still doesn't work, there is a good chance there is a problem with the access point. Try unplugging the access point and plugging it back in to reset the access point. Try the ping again, and if it still doesn't work, the access point might have a problem.

Wireless Router Issues

Make sure the client and wireless router support the same Wi-Fi version. For example, if a client computer's Wi-Fi card supports only 802.11b, the wireless router must also support 802.11b or must be configured to run in a mixed mode, with multiple protocols supported.

Also, in the case where multiple clients are connecting to the wireless router, it is important to understand that when an association is made between the client and the wireless router, the client with the lowest 802.11 system will set the clock speed. For example, say that a client running 802.11b and another running 802.11g connect to the same wireless router. The data transfer rate for 802.11b is 11Mbps, and the rate for 802.11g is 54Mbps. The wireless router will select 802.11b's lower clock rate for all associations. This can be of some concern to clients that have the capability to connect at a higher data transfer rate.

Wireless Compatibility

Not all wireless clients are created equal, and wireless clients depend on their hardware and software, which they must keep up to date. Also, in order to have reliable and good wireless connectivity, the wireless access point and the wireless clients must be compatible and use the same standard.

802.11n is a standard that can offer connectivity in either 2.4GHz or 5GHz or both. This means a wireless client can be 802.11n compatible just by operating in one frequency, not both. Therefore, an 802.11n wireless client with only a 2.4GHz radio will never achieve the high speed of 300Mbps offered by 5GHz. When troubleshooting the RF spectrum associated with a signal such as a Wi-Fi signal, a spectrum analyzer is typically used.

Signal Strength Problems

The purpose of measuring signal strength is to verify that you have good signal level at the receive location. Typically, the signal strength of a wireless connection can be adjusted at the access point to expand or reduce the area of coverage. Things change, and a loss in signal strength might not be a problem with the access point. It is possible that something could have been moved and is physically blocking the signal, thus causing RF attenuation. The RSSI (received signal strength indicator) value of a user should be monitored to identify signal strength issues.

Wireless Coverage

A wireless coverage area, or a cell, is very dependent on the RF transmission radiated from a wireless router or an access point. So, there is a limitation to the size of a cell for each access point. In a large geographic area, multiple wireless access points are deployed to create multiple cells in an attempt to give enough total coverage area. Good coverage depends on cells overlapping. Failure of cells to overlap introduces weak or dead wireless spots, thus creating insufficient wireless coverage. Also, bad coverage negatively affects client roaming. When a wireless client moves from one cell to another, it must establish an association with the new access point. With bad coverage, the AP association time increases, in turn causing delay or interruption.

Extending the Wireless Range

Another way to improve wireless coverage is to extend the wireless range. The following are general tips for extending the wireless range:

- Make sure the antenna is placed high and is not obstructed by any metal. It is important to remember that radio waves reflect off metal surfaces. Also, surfaces such as concrete and brick attenuate the signal.
- In some cases, you might have to use a high-gain antenna to help boost the receive signal strength.

Frequency Interference Problems

An electrical device such as a microwave oven may cause interference. Microwave ovens operate at the 2.4GHz frequency, which is the same band in which 802.11b/g/n devices operate. It is good to have a baseline measurement of the signal strength expected at each location in order to better identify interference. A good indicator of interference is the signal-to-noise RATIO (SNR).

Wireless Channel Utilization

For the 2.4GHz wireless frequency, the default channel for 802.11b, 802.11g, and 802.11n wireless routers is channel 6. If you have interference problems, there may be a wireless router nearby with an SSID using the same channel. In such a case, you can change the channel to 1 or 11 so that the RF spectra on these channels do

not overlap (refer to Figure 4-4). 802.11b, 802.11g, and 802.11n wireless routers have 11 possible channels, and you can select an alternate channel via the wireless router's settings. Changing to a different channel will reduce the SNR, which is likely to solve your problem. Even though 5GHz wireless has more channels, the same concept applies for 802.11a, 802.11n (5GHz), 802.11ac, and 802.11ax.

Load Issues

Wireless users share the same frequency channel to communicate to the same access point. If too many users connect to the same access point at the same time, they start experiencing slowness and packet drops due to overcapacity. For optimum load capacity, consult the documentation of the access point manufacturer.

SSID Issues

Once the SSID has been configured for a computer, it normally does not require reconfiguration. However, while traveling, you might reconfigure the SSID to connect to a different network. Also, when manually configuring an incorrect SSID or settings, human-error mistakes can be made. The simple fix is to reset the SSID when you return to your home network.

Securing Wi-Fi Issues

Any time you are connecting a wireless device to a public hotspot, there is a chance that someone using a packet sniffer will be able to see your data traffic. You can avoid possible problems by enabling WPA to secure your data traffic. Most wireless systems support multiple network security protocols (for example, different versions of WPA3, WPA2, WPA, or WEP). Make sure the client and access point are running the same security mode. Otherwise, an encryption protocol mismatch will occur, resulting in no wireless connection.

Cable Issues

Even when you are focusing on troubleshooting wireless issues, a problem could be due to a simple physical cable connection. A cable could be loose, may have become disconnected, or may be bad. It is always good to have a spare cable just in case. Remember that you can always verify that you have a connection by checking for the presence of a link light. Also, bad cables create attenuation and introduce loss of signal. Attenuation in any type of cable connecting to the access point—such as antenna cable attenuation, fiber cable attenuation, or Ethernet cable attenuation—could introduce signal issues into the wireless connection.

Deauthentication/Disassociation Attacks

Deauthentication and disassociation are legitimate handshakes used by a wireless client when leaving a wireless network. However, a denial of service (DOS) attack that exploits deauthentication and disassociation creates client disassociation issues. By spoofing a disassociate or deauthenticate message while pretending to be a targeted wireless client, the access point disassociates the targeted wireless client from the wireless network.

DHCP Issues

Wireless devices require valid IP addresses. Access points typically assign a 192.168.0.*x* address to the client. You can verify the IP address assigned by entering the command **ipconfig** at the command prompt (refer to Section 1-4, "The Ethernet LAN," in Chapter 1, "Introduction to Computer Networks").

Wireless Printer Issues

If you are experiencing problems with a wireless printer that was recently working, the first step is to restart the printer, your computer, and your wireless router. If this doesn't fix the problem, you can print the network configuration from the printer. Check the IP address for the printer and verify that it is assigned an IP address in your network. You can check the IP address of your computer by issuing the command **ipconfig** from the command prompt (refer to Section 1-4 in Chapter 1).

Section 4-6 Review

This section covers the following Network+ exam objective.

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

This section presents the concept of an RSSI, which provides a signal strength measurement.

Test Your Knowledge

1. You are experiencing problems with a wireless printer that was recently working. How can you verify the IP address?
   a. Set the **ping** command to **auto** and look for a reply.
   b. Verify the IP address assigned by entering the command **ipconfig** at the command prompt.
   c. Remove the cover to the printer to find the MAC address.
   d. Ping the server
2. What issue is likely to happen if one wireless client is running 802.11b and another is running 802.11g, and both connect to the wireless router at the same time?
   a. There will be no issues.
   b. The wireless router will select 802.11g for setting the data transfer rate.
   c. The wireless router will select 802.11b for setting the data transfer rate.
   d. The access point will temporarily shut down until one client goes offline.

SUMMARY

This chapter presents an overview of wireless networking, including fundamental concepts and sample networks. The vendors of wireless networking equipment have made their devices easy to integrate into existing networks, but you must understand that the key objective of a network administrator is to provide a fast, reliable, and secure computer network. Carelessly integrating wireless components into a network can easily compromise this objective.

You should understand the following from reading this chapter:

- The operating characteristics of the 802.11 wireless networks
- The purposes of access points, wireless LAN adapters, and wireless bridges
- How to perform a basic site survey on a building
- How to configure a network for user mobility
- How to plan multipoint wireless distribution

Wireless networking technologies have greatly simplified planning and installation. However, they have also brought some complications. For example, any time you are working with RF, there is a chance of unexpected interference and noise. A well-planned RF installation requires a study of all known interference and a search for any possible interference. An RF study should also include signal path studies that enable the user to prepare a well-thought-out plan and allow an excellent prediction of received signal level. The bottom line is to obtain support for conducting an RF study.

QUESTIONS AND PROBLEMS

Section 4-2

1. List two advantages of wireless networking.

   User mobility and cost-effectiveness for areas where wiring would be too expensive

2. What are the three areas defined for the IEEE 802.11 standard?

   The physical layer, the MAC layer, and wireless management protocols and services

3. What is an ad hoc network?

   An ad hoc network is an independent network.

4. What is the purpose of an extended service set?

   An ESS uses multiple access points to extend user mobility.

5. What are the four physical layer technologies used in 802.11 wireless networking?

   DHSS: direct-sequence spread spectrum

   FHSS: frequency-hopping spread spectrum

   Infrared

   OFDM: orthogonal frequency-division multiplexing

6. Describe the frequency spectrum for the DSSS channels in 802.11b wireless networking.

   802.11 DSSS implements 14 channels (each consuming 22MHz) over approximately 90MHz of RF spectrum in the 2.4GHz ISM (industrial, scientific, and medical) band.

7. Define pseudorandom sequence as it applies to FHSS.

   Pseudorandom sequence means that the frequency-hopping sequence appears to be random, but it does repeat.

8. What must the FHSS transmitting and receiving units know in order to communicate?

   They must know the hopping sequence.

9. What are the frequency range and modulation technique used by 802.11a?

   5GHz, OFDM

10. What is the maximum data rate for each of the following?

    a. 802.11b

       11Mbps

    b. 802.11a

       54Mbps

    c. 802.11g

       54Mbps

    d. 802.11n

       200Mbps+

    e. 802.11ac

       1Gbps+

    f. 802.11ax

       10Gbps

11. Define MIMO as it applies to 802.11n.

    MIMO (multiple-input multiple-output) uses a technique called space-division multiplexing, in which the data stream is split into multiple parts called spatial streams. The different spatial streams are transmitted using separate antennas.

12. What is the purpose of the power save mode in 802.11n?

    With the power save mode, 802.11n uses multiple data paths only when faster data transmission is required, thus saving power.

Section 4-3

13. What is the purpose of an access point?

    An access point provides a bridge between a wireless LAN and a wired network.

14. How does an access point know if a wireless data packet is intended for its network?

    802.11 wireless LAN devices use an SSID to identify what wireless data traffic is allowed to connect to the network.

15. What is an association, and what is its purpose?

    An association is an established wireless connection. An access point uses an association to build a table of users (clients) on the wireless network.

16. Draw a picture of a point-to-point wireless connection.

    Refer to Figure 4-9(a)

17. Draw a picture of a point-to-multipoint wireless network.

    Refer to Figure 4-9(b)

18. What are the key issues to explore when conducting a site survey for each of the following?

    a. Indoor environment

       Electrical power connection points(s)

       Wired network connection point(s)

       Access point placement

       RF coverage area

       Bandwidth supported

    b. Outdoor environment

       Electrical power for the base access point

       Connection back to the home network

       Antenna selection

       Bandwidth supported

       RF coverage

Section 4-4

19. In what frequency band does Bluetooth operate?

    The 2.4GHz ISM band

20. How many output power classes does Bluetooth have? List the power level and the operating range for each class.

    Bluetooth has four operating classes.

Power Class	Average Output Power	Operating Distance
1	100 mW	~100 meters
2	2.5 mW	~10 meters
3	1 mW	~1 meter
4	0.5 mW	~0.5 meter

21. What is a piconet?

    A piconet is an ad hoc network consisting of up to eight Bluetooth devices.

22. What is the purpose of the inquiry procedure in Bluetooth?

    A Bluetooth device uses the inquiry procedure to discover other Bluetooth devices or to allow itself to be discovered.

23. What is the purpose of the paging procedure in Bluetooth?

    A Bluetooth device uses the paging procedure to establish and synchronize a connection between two networking devices.

24. Define the term backscatter.

    Backscatter refers to the reflection of the radio waves striking an RFID tag back to the transmitter source.

25. What are the three parameters that define an RFID system?

    Means of powering the tag, frequency of operation, communication protocol

26. Explain how power is provided to a passive RFID tag.

    Power is provided by rectifying the RF energy transmitted by the reader that strikes the RF tag antenna.

27. What are three advantages of using an active RFID tag?

    Can incorporate wireless Ethernet connectivity, can incorporate location capability, the unit is always turned on

28. What three frequency bands are typically used for RFID tags?

    LF: 125/134KHz

    HF: 13.56MHz

    UHF: 860–960MHZ and 2.4GHz

29. What is the WiMAX frequency standard for the United States?

    5.8GHz and 2.5GHz

30. Why was OFDM selected for WiMAX?

    OFDM was selected for WiMAX because of its improved NLOS characteristics.

31. How does WiMAX differ from Wi-Fi?

    Frequency assignments differ and data rates differ, but the main difference is that the WiMAX unit only has to compete once to gain entry to a network.

Section 4-5

32. What type of wireless connection is used to connect a home network to a multipoint distribution site?

    Point-to-point

33. Use the Internet to find a source of omnidirectional and directional antennas for each of the following standards:

    a. 802.11b
    b. 802.11a
    c. 802.11g
    d. 802.11n
    e. 802.11ac
    f. 802.11ax

34. Prepare a list of three manufacturers for each antenna type. Include cost figures.

    There are many sources for wireless network antennas. Expect the students to come up with many possible solutions.

Section 4-6

35. What command can you issue to verify network connectivity in a wireless LAN?

    ping

36. True or false: When an association is made between a client and a wireless router, the client with the lowest 802.11 system sets the clock speed.

    True

37. True or false: In order to have reliable and good throughput wireless connectivity, the wireless access point and the wireless clients must be compatible and use the same standard.

    True

38. What is the purpose of measuring signal strength at the receive location?

    The purpose of measuring signal strength at the receive location is to verify that you have good signal level.

39. What happens when wireless cell coverage isn't overlapping?

    Weak or dead wireless spots appear, thus creating insufficient wireless coverage.

40. Which of the following are general tips for extending your wireless range? (Select all that apply.)

    a. Make sure the antenna is placed high.
    b. Use a high-gain antenna to help boost the receive signal strength.
    c. Enclose the antenna with brick or concrete.
    d. Place the antenna on the ground.

41. True or false: Microwave ovens can cause interference with Wi-Fi signals.

    True

42. The default channel for 802.11b and 802.11g wireless routers is channel 6. If you have interference problems, there may be a wireless router nearby with an SSID using the same channel. You can change the channel to which of the following? (Select all that apply.)

    a. 1
    b. 3
    c. 7
    d. 8
    e. 11

43. What is meant by the term *load issues* regarding wireless access points?

    Too many users are connecting to the same access point at the same time.

44. True or false: Once the SSID (service set identifier) has been configured for a computer, it normally does not require reconfiguration. However, when you travel, you should use a PSSID (portable service set identifier) to connect to remote access points.

    False

45. What happens when an encryption protocol mismatch occurs?

    a. The SSID has to be reconfigured.
    b. The wireless authentication fails and requires reconfiguration of the client's SSID.
    c. The wireless authentication is not successful, resulting in not being able to connect to the SSID.
    d. The lowest level of encryption is applied.

46. You can avoid security problems when connecting a wireless device to a public hotspot by doing which of the following?

    a. Enabling WPA to secure your data traffic
    b. Enabling WAP to secure your data traffic
    c. Disabling WPA
    d. Disabling WAP

47. Which of the following can introduce signal loss into a wireless connection? (Select all that apply.)

    a. Antenna cable attenuation
    b. Wrong IP address
    c. An object blocking the wireless signal
    d. Radio station broadcast

48. A denial of service (DOS) attack creates client disassociation issues by doing two of the following?

    a. Setting up a continuous ping, thereby taking control of the network
    b. Replacing the SSID with a PSSID and connecting to non-authenticated access points
    c. Spoofing a disassociate or deauthenticate message and pretending to be a targeted wireless client
    d. Downgrading WPA3 to WPA2 encryption

49. An access point typically assigns a 192.168.0.*x* address to a client. How can you verify the IP address assigned?

    a. By entering the command **config-ip** at the command prompt
    b. By entering the command **ipconfig** at the command prompt
    c. By entering the command **configip** at the command prompt
    d. By pushing the reset button on the WAP

50. When you experience problems with a wireless printer that was recently working, what is the first step you should take?

    a. Restart the printer, your computer, and your wireless router.
    b. Replace the access point and router and reconfigure both of them.
    c. Remove the cable connecting the printer and replace it.
    d. Update the firmware on the wireless router.

Critical Thinking

51. A wireless network receiving site is experiencing occasional loss of signal due to interference. Discuss the steps you would take to correct this problem.

    The options for solving this problem vary depending on the location of the network receiving site. If this is an indoor site, an additional access point may be required. For an outdoor site, the antenna might need to be aligned or replaced with a more directional antenna. You also might be able to reduce impacts of RF interference by changing the access point channel. For example, most microwave ovens emit RF signals in the upper third of the 2.4GHz band. You can generally avoid microwave oven interference by tuning nearby access points to channels 1 or 6.

52. Prepare a memo to your supervisor, explaining why it is important to run encryption on your wireless network.

    The student should report that it is easy for data to be viewed over an unencrypted wireless network. The student could say something about the fact that sensitive information about personnel or the company is being broadcast to the public if encryption is not used.

53. Your company has a suite in a business complex. Another company in the suite next to you has a wireless 802.11b network with the SSID Company A. You can pick up that company's signal from your suite. Your company would like to put up its own wireless network with two access points. Discuss how you would set up these two access points so that your company can obtain optimal performance.

    It is important to determine which of the 802.11b channels the SSID Company A is using. Then you can deploy the wireless access points using different, non-overlapping channels. This will help eliminate interference. Also, it is important to do a site survey within your own suite. You want to place the two wireless access points in such a way that their radio signals provide overlapping coverage for the entire suite and their signal will be minimally reflected by the obstacles within the suite.

Certification Questions

54. True or false: If the signal quality drops from excellent to good, the antenna or access point should be replaced.

    False

55. The network administrator is setting up a wireless network. There is a chance of radio interference. How can the network administrator avoid or minimize potential interference problems?

    a. Perform an RF study prior to installation of the wireless network.
    b. Contact all owners of equipment that may cause interference and ask them to use different systems.

c. Contact the FCC to have the interfering sources shut down.

d. All of these answers are correct.

56. Define MIMO relative to 802.11n.

a. MIMO is a multiplexing technique in which the power is split into multiple parts called spatial currents.

b. MIMO is a frequency-division multiplexing technique in which the data stream is split into multiple parts called spectral streams.

c. MIMO is an OFDM multiplexing technique in which the digital data is portioned into multiple parts called filtered streams.

d. MIMO is a space-division multiplexing technique in which the data stream is split into multiple parts called spatial streams.

57. Which of the following best characterizes CSMA/CA?

a. It replaces CSMA/CD.

b. It provides carrier sense with collision avoidance.

c. It provides carrier sense with congestion avoidance.

d. It provides congestion sensing with collision avoidance.

58. Which of the following are advantages of 802.11g? (Select all that apply.)

a. Compatible with 802.11b

b. Compatible with 802.11a

c. Uses infrared instead of radio

d. High speed

59. Which of the following is used in wireless LANs to identify whether a client is to become a member of the wireless network?

a. SSID

b. MAC address

c. IP address

d. Echo

60. What does the term *last mile* mean in relation to telecommunications?

a. The distance from an RF transmitter to a receiver in WiMAX

b. A measurement of signal coverage for WiMAX and for Wi-Fi

c. A term for the last connection prior to linking to the RF transmitter

d. The last part of the connection from the telecommunications provider to the customer

61. Which of the following is the best way to extend the radio range of a station's wireless link with one access point?

    a. Add multiple access points
    b. Add additional wiring
    c. Add 87BZS encoding
    d. Add B8ZS encoding

62. Which of the following statements is true?

    a. The Wi-Fi Alliance is an organization that assembles and tests wireless equipment before it is shipped to vendors.
    b. The Wi-Fi Alliance is an organization that tests and certifies wireless equipment for compliance with the 803.1 standards.
    c. The Wi-Fi Alliance is an organization that tests and certifies wireless equipment for compliance with the 802.11*x* standards.
    d. None of these answers are correct.

63. Which of the following are current wireless networking standards? (Select all that apply.)

    a. 802.12n
    b. 802.11g
    c. 803.11g
    d. 802.11a
    e. 802.11b
    f. 802.55a
    g. 802.11n
    h. 802.1a
    i. 802.11ac
    j. 802.11ax

This page intentionally left blank

5
CHAPTER

Interconnecting the LANs

Chapter Outline

5-1 Introduction
5-2 The Network Bridge
5-3 The Network Switch
5-4 The Router
5-5 The Console Port Connection
5-6 Interconnecting LANs with the Router
5-7 Interconnecting LANs and WANs
Summary
Questions and Problems

Objectives

- Describe how a bridge is used to interconnect LANs
- Describe how a switch is used to interconnect LANs
- Discuss the advantages of using a switch instead of a hub
- Describe the function of a router when used to interconnect LANs
- Describe the interface associated with a router
- Describe the function of a gateway in a computer network
- Describe the concept of a network segment
- Describe the concept of auto-negotiation

Key Terms

campus network
bridge
bridge table
association
broadcast
ARP
broadcast storm
network slowdown
ARP cache
ARP table
transparent bridge
translation bridge
layer 2 switch
multiport bridge
multicast
managed switch
Cisco Network Assistant (CNA)
dynamic assignment
static assignment
secure addresses
aging time
isolating the collision domains
content-addressable memory (CAM)
flooding
broadcast domain
store-and-forward
switch latency
cut-through
adaptive cut-through
error threshold
multilayer switch (MLS)
wire speed routing
network address
logical address
router interface
RS-232
DB-9
DB-25
console cable
COM1, COM2, …
rollover cable
enterprise network
media converter
FastEthernet port (FA0/0, FA0/1, FA0/2, …)
serial port (S0/0, S0/1, S0/2, …)
routing table
gateway
HSSI
OC
DS-0 to DS-3; T1 to T3
DS
telco
telco cloud
multiplexed
point of presence (POP)
line of demarcation
CSU/DSU
HDLC
PPP
Metro Optical Ethernet (MOE)
Carrier Ethernet

Key Terms continued

Metro Ethernet Forum (MEF)
User–Network Interface (UNI)
Ethernet Service Definition
Ethernet Virtual Connection (EVC)
E-Line Service Type (E-Line)
E-LAN Service Type (E-LAN)
E-Tree Service Type (E-Tree)

Campus Network
A collection of two or more interconnected LANs in a limited geographic area

The utility of LANs led to the desire to connect two or more networks together. For example, a large corporation might have at one time had separate networks for research and engineering and another network for its manufacturing units. These network systems probably used totally different networking technologies and specifications for communicating and were located in different cities, states, or even countries, but it was deemed necessary to "tie" them together. The objective of this and subsequent chapters is to introduce the concepts and issues involved in interconnecting LANs. Interconnecting LANs in a campus network and interconnecting LANs in wide area networks (WANs) involve similar concepts and issues. A **campus network** is a collection of two or more interconnected LANs, either within a building or housed externally in multiple buildings.

5-1 INTRODUCTION

This chapter looks at interconnecting LANs. It discusses bridges, switches, and routers and introduces the function of the network gateway. Students need to understand the network gateway in order to determine where data packets are delivered when they need to exit the LAN. The chapter also covers auto-negotiation and shows how interconnected networking devices negotiate an operating speed.

The OSI model provides a framework that defines the network layers for linking networks together (refer to Chapter 1, "Introduction to Computer Networks"). The OSI model ensures compatibility in the network hardware and software. Concepts related to the hardware technologies used to interconnect LANs are presented in in this chapter. The properties of a networking bridge are defined in Section 5-2, "The Network Bridge." The layer 2 switch is examined in Section 5-3, "The Network Switch," and the router is introduced in Section 5-4, "The Router." The procedure for configuring a router through the router's console port is presented in Section 5-5, "The Console Port Connection." This section provides an overview of configuring a computer's serial communication software and selecting the proper cable and hardware for connecting the console port to a computer. An example of interconnecting LANs is provided in Section 5-6, "Interconnecting LANs with the Router," which examines how routers can be used to interconnect LANs. Section 5-7, "Interconnecting LANs and WANs introduces well-known LAN architecture, data center architecture, and WAN technologies such as high-speed serial connections and Metro Optical Ethernet that are used to connect LANs or to connect the enterprise network to the outside world.

Table 5-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 5-1 **Chapter 5 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.2	Explain the characteristics of network topologies and network types.	5-4, 5-6, 5-7
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes.	5-2, 5-3, 5-6
1.5	Explain common ports and protocols, their application, and encrypted alternatives.	5-3, 5-5
1.6	Explain the use and purpose of network services.	5-3
1.7	Explain basic corporate and datacenter network architecture.	5-7
1.8	Summarize cloud concepts and connectivity options.	5-7
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	5-2, 5-3, 5-4, 5-5, 5-6
2.2	Compare and contrast routing technologies and bandwidth management concepts.	5-4, 5-6
2.3	Given a scenario, configure and deploy common Ethernet switching features.	5-2, 5-5
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	5-2, 5-3, 5-4
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	5-3, 5-4, 5-6
4.0	**Network Security**	
4.5	Explain the importance of physical security.	5-3
5.0	**Network Troubleshooting**	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	5-3, 5-5
5.3	Given a scenario, use the appropriate network software tools and commands.	5-5
5.5	Given a scenario, troubleshoot general networking issues.	5-3, 5-6

5-2 THE NETWORK BRIDGE

This section examines how a bridge is used in computer networks to interconnect LANs. This section describes how a bridge builds a table of connected users on the bridge ports. This concept applies to switches and access points in wireless LANs. It is important for students to understand that a bridge can be used to isolate data traffic.

Bridge
A networking device that uses MAC address information to forward data and interconnect LANs

A bridge can be used in computer networks to interconnect two LANs or separate network segments. Recall that a *segment* is a section of a network separated by bridges, switches, and routers. A **bridge** is a layer 2 device in the OSI model, meaning that it uses MAC address information to make decisions regarding forwarding of data packets. Only the data that needs to be sent across a bridge to the adjacent network segment is forwarded. This makes it possible to isolate or segment the network data traffic. Figure 5-1 provides an example of using a bridge to segment two Ethernet LANs. It shows LAN A connected to port 1 on the bridge and LAN B connected to port 2 on the bridge, creating two segments. There are four computers in LAN A and three computers in LAN B. It is important to note that bridges are now legacy networking devices, but studying them will help you better understand the functionality of switches, especially how data traffic is sent to connected LANs.

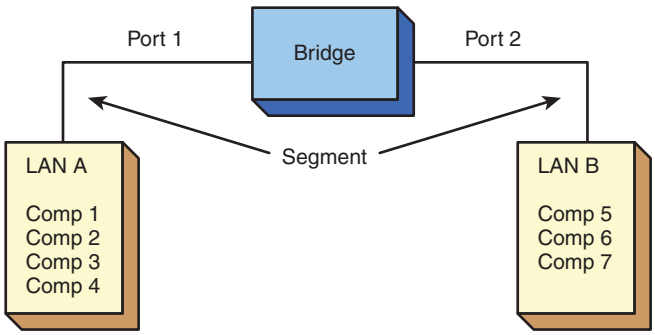


FIGURE 5-1 Using a bridge to interconnect two Ethernet LANs.

Bridge Table
A list of MAC addresses and port locations for hosts connected to the bridge ports

A bridge monitors all data traffic in each of the LAN segments connected to its ports. Recall that a *port* is an input/output connection on a networking device. Bridges use MAC addresses to build a **bridge table** of MAC addresses and port locations for hosts connected to the bridge ports. A sample bridge table is provided in Table 5-2, which shows the stored MAC addresses and the port where each address was obtained.

TABLE 5-2 **Bridge Table**

MAC Address	Port
00-40-96-25-85-BB	1
00-40-96-25-8E-BC	1
00-60-97-61-78-5B	2
00-C0-4F-27-20-C7	2

The source MAC address is stored in the bridge table as soon as a host talks (that is, transmits a data packet) on the LAN. In the example shown in Figure 5-1, if computer 1 in LAN A sends a message to computer 2, the bridge will store the MAC addresses of both computers and record that both of the computers are connected to port 1. If computers 5 or 6 are placing data packets on the network, then the source MAC addresses for computers 5 and 6 are stored in the bridge table, and it is recorded that these computers connect to port 2 on the bridge. The MAC addresses for computers 3 and 4 will not be added to the bridge table until each transmits a data packet.

The bridge monitors the data on its ports to check for an **association** between the destination MAC address of the Ethernet frames and any of the hosts connected to its ports. An association indicates that the destination MAC address for a host is connected to one of the ports on the bridge. If an association is found, the data is forwarded to that port. In the example shown in Figure 5-1, say that computer 1 sends a message to computer 5. The bridge detects an association between the destination MAC address for computer 5 and port 2. The bridge then forwards the data from computer 1 to computer 5 in LAN B via port 2.

Association
An indication that the destination address is for a networking device connected to one of the ports on a bridge

The capability of a bridge to forward data packets only when there is an association is used to isolate data traffic in each segment. For example, say that computer 1 and computer 2 in LAN A generate a lot of data traffic. The computers in LAN B will not see any of the data traffic as long as there is not an association between the destination MAC addresses of the Ethernet packets and any of the hosts in LAN B (computers 5, 6, and 7).

A potential problem with bridges is related to the way broadcasts are handled. With a **broadcast**, a message is sent to all computers on the network; therefore, all broadcasts in a LAN will be forwarded to all hosts connected within the bridged LANs. For example, the broadcast associated with ARP will appear on all hosts. **ARP**, which stands for Address Resolution Protocol, is a protocol used to map an IP address to its MAC address. With ARP, a broadcast is sent to all hosts in a LAN connected to the bridge, as illustrated in Figure 5-2. The bridge forwards all broadcasts; therefore, an ARP request broadcasting the message "Who has this IP address?" is sent to all hosts on the LAN. The data packets associated with ARP requests are small, but computer time is needed to process each request. Excessive numbers of broadcasts being forwarded by the bridge can lead to a **broadcast storm**, resulting in degraded network performance, called a **network slowdown**.

Broadcast
A data transmission sent to all connected devices

ARP
Address Resolution Protocol, a protocol used to map IP addresses to MAC addresses

Broadcast Storm
Excessive numbers of broadcasts

Network Slowdown
Degraded network performance

The MAC address entries stored in a bridge table are temporary. Each MAC address entry in a bridge table remains active as long as there is periodic data traffic activity from that host on its port. However, an entry into the table is deleted if the port becomes inactive. In other words, the entries stored in the table have limited lifetimes. An expiration timer commences once the MAC address is entered into the bridge table. The lifetime for the entry is renewed with new data traffic by the computer, and the MAC address is reentered.

In a similar manner, every networking device (such as a computer) contains an **ARP cache**, also called an **ARP table**, which provides temporary storage for MAC addresses recently contacted. The ARP cache holds the MAC address of a host and enables the message to be sent directly to the destination MAC address without the computer having to issue an ARP request for a MAC address. The following are

ARP Cache
Temporary storage of recently contacted MAC addresses

ARP Table
Another name for the ARP cache

typical steps in the communication process between two computers, computer 1 and computer 2:

1. Computer 1 checks its ARP cache to determine if it already has the MAC address of computer 2. If it does, it skips to step 6; otherwise, it proceeds to step 2.
2. Computer 1 generates an ARP request message for computer 2, with its own MAC and IP address information included.
3. Computer 1 broadcasts the ARP request message on its local network.
4. Every local network device processes the ARP request message. Computers that are not computer 2 discard the message. Only a match, which is computer 2, generates an ARP reply message and updates its ARP cache with computer 1 MAC and IP address information.
5. Computer 2 sends an ARP reply message directly to computer 1.
6. Computer 1 receives the ARP reply message and updates its ARP cache with the MAC and IP addresses of computer 2.

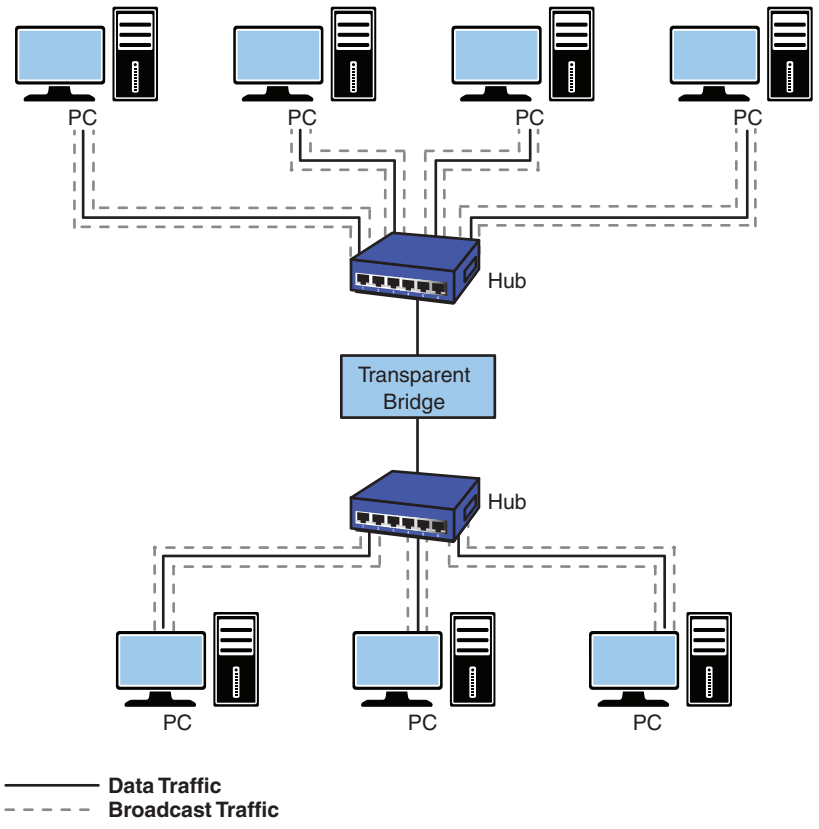


FIGURE 5-2 An example of using a bridge to isolate data traffic.

You can view the contents of the ARP cache on a Windows computer by using the **arp -a** command at the command prompt as follows:

```
C:\arp -a
Interface: 10.10.20.2 on Interface x1000002
Internet Address Physical Address  Type
10.10.20.3       00-08-a3-a7-78-0c dynamic
10.10.20.4       00-03-ba-04-ba-ef dynamic
```

On a macOS computer, you can use the **arp -a** command while in the terminal mode, as shown here:

```
jmac:~mymac$ arp -a
C1.salsa.org (192.168.12.1) at
00-08-a3-a7-78-0c on en1
[ethernet]
C3.salsa.org (192.168.12.1) at
00-08-a3-a7-78-0c on en1
[ethernet]
```

The following message is generated if all the ARP entries have expired:

```
c:\arp -a
No ARP Entries Found
```

A bridge that is used to interconnect two LANs running the same type of protocol (for example, Ethernet) is called a **transparent bridge**. Bridges are also used to interconnect two LANs that are operating two different networking protocols. For example, LAN A could be an Ethernet LAN, and LAN B could be a Token Ring LAN. This type of bridge is called a **translation bridge**, and an example is provided in Figure 5-3. This bridge allows data from one LAN to be transferred to another. Also, the MAC addressing information is standardized so the same address information is used, regardless of the protocol.

Transparent Bridge
A bridge that interconnects two LANs running the same type of protocol

Translation Bridge
A bridge that is used to interconnect two LANs that are operating two different networking protocols

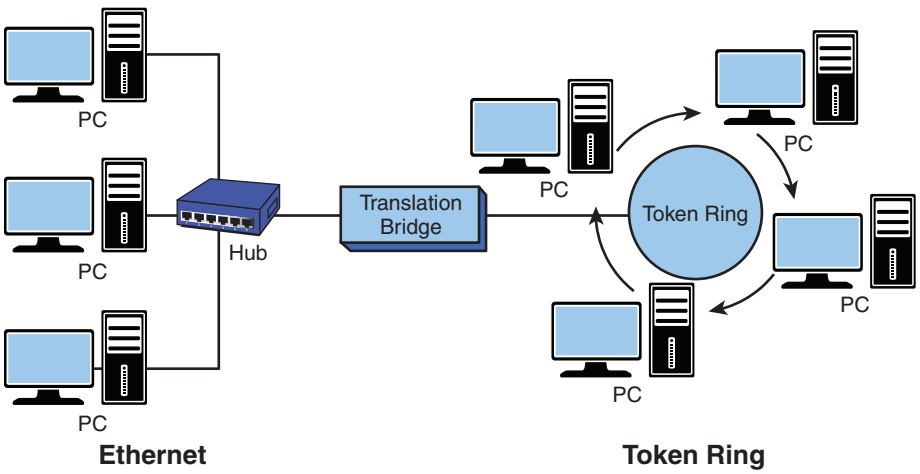


FIGURE 5-3 Using a translation bridge to interconnect an Ethernet LAN and a Token Ring LAN.

A common application for using a bridge today is to interconnect LANs using wireless technology. The use of wireless bridges is a popular choice for interconnecting LANs when the cost of physically connecting them is prohibitive. (Wireless technology and its LAN applications are presented in Chapter 4, "Wireless Networking.")

The use of a bridge is not as common as it used to be except with wireless network applications. New networking technologies are available that provide similar capabilities to a bridge but that are much more powerful. However, bridges are still useful and have several advantages. Table 5-3 provides a summary of the advantages and disadvantages of networking bridges.

TABLE 5-3 **Summary of the Advantages and Disadvantages of Using a Bridge to Interconnect LANs**

Advantages	Disadvantages
Easy to install	Works best in low-traffic areas
Does an excellent job of isolating the data traffic in two segments	Forwards broadcasts and is susceptible to broadcast storms
Relatively inexpensive	
Can be used to interconnect two LANs with different protocols and hardware	
Reduces collision domains (remember how the CSMA/CD protocol works)	

Section 5-2 Review

This section covers the following Network+ exam objectives.

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

An important concept presented in this section is that a bridge passes a broadcast to all devices connected to its ports. Excessive broadcasts can potentially have a negative impact on data traffic and result in network slowdowns.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section presents the advantages and disadvantages of a network bridge. A key concept presented in this section is an association, which indicates that the destination address for a networking device has been obtained.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section mentions the issue of expired ARP entries. IP addresses are stored in the ARP cache for only a limited time. Another important concept presented in this section is that a bridge passes a broadcast to all devices connected to its ports. Excessive broadcasts can potentially have a negative impact on data traffic and result in network slowdowns. As discussed in this section, a bridge table stores the MAC addresses of connected devices. Each MAC address

entry in the bridge table remains active as long as there is periodic data traffic activity from that host on its port. However, an entry in the table is deleted if the port becomes inactive. The data packets associated with ARP requests are small, but computer time is needed to process each request.

Test Your Knowledge

1. Which command is used on a computer to view the contents of the ARP cache?
    a. **arp -c**
    b. **arp -l**
    c. **arp -a**
    d. **arp -b**
    e. **arp**
2. An association indicates that ____.
    a. the destination address for a networking device is connected to one of its ports
    b. the source address is for a networking device connected to one of the ports on the bridge
    c. the destination address is for a networking device connected to one of the ports on the hub
    d. the source address is for a networking device connected to one of the ports on the hub
3. An ARP cache temporarily stores which of the following?
    a. IP addresses for recently contacted networking devices
    b. MAC addresses for networking devices that are to be contacted
    c. IP addresses for networking devices that are to be contacted
    d. MAC addresses for recently contacted networking devices

5-3 THE NETWORK SWITCH

A bridge can be used to isolate the collision domains for interconnected LANs but lacks the capability to provide a direct data connection for the hosts. A bridge forwards the data traffic to all computers connected to its port (refer to Figure 5-2). A networking hub makes it possible to share access to the network with all computers connected to its ports in the LAN but lacks the capability to isolate the data traffic and provide a direct data connection from the source to the destination computer. The increase in the number of computers being used in LANs and the increased data traffic are limiting the usefulness of bridges and hubs in larger LANs. Basically, there is too much data traffic to be shared by the entire network.

Most situations call for a networking device that provides a direct data connection between communicating devices. Neither the bridge nor the hub provides a direct data connection for the hosts. A technology developed to improve the efficiency of data networks and address the need for direct data connections is the layer 2 switch.

Layer 2 Switch
An improved network technology that provides a direct data connection for network devices in a LAN

Multiport Bridge
Another name for a layer 2 switch

A **layer 2 switch** is an improved network technology that addresses the issues of providing direct data connections, minimizing data collisions, and maximizing the use of a LAN's bandwidth; in other words, a layer 2 switch improves the efficiency of the data transfer in the network. It operates at layer 2 of the OSI model and therefore uses the MAC or Ethernet address for making decisions related to forwarding data packets. The switch monitors data traffic on its ports and collects MAC address information in the same way a bridge does to build a table of MAC addresses for the devices connected to its ports. Much like a hub, a switch has multiple ports; much like a bridge, a switch can switch in a data connection from any port to any other port (and, therefore, a switch is sometimes called a **multiport bridge**). A switch minimizes traffic congestion and isolates data traffic in the LAN.

Figure 5-4 shows a switch being used to interconnect the hosts in a LAN. In this figure, the hub has been replaced with a switch. The change from a hub to a switch is relatively easy. The port connections are the same (RJ-45), and once the connections are changed and the device is powered on, the switch begins to make the direct data connections for multiple ports by using layer 2 switching.

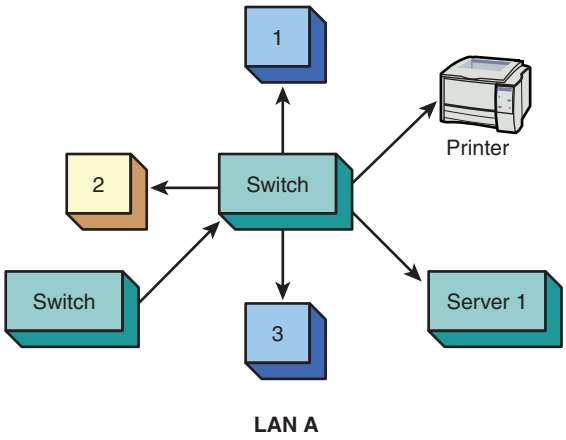


FIGURE 5-4 A switch used to interconnect hosts in a LAN.

The LAN shown in Figure 5-5 contains 14 computers and 2 printers connected to 16 ports on a switch, configured in a star topology. If the computer connected to port 1 is printing a file on the laser printer (port 12), the switch sets up a direct connection between ports 1 and 12. The computer at port 14 could also be communicating with the computer at port 7, and the computer at port 6 could be printing a file on the color printer at port 16. The use of the switch enables simultaneous direct data connections for multiple pairs of hosts connected to the network. Each switch connection provides a link with minimal collisions and therefore makes maximum use of the LAN's bandwidth. A link with minimal collisions is possible because only the two computers that established the link communicate over the channel.

Recall that in the star topology, each host has a direct connection to the switch. Therefore, when the link is established between the two hosts, this link is isolated from any other data traffic. However, there is an exception to this when broadcast or **multicast** messages are sent in the LAN. In the case of a broadcast message, the message is sent to all devices connected to the LAN. A multicast message is sent to a specific group of hosts on the network.

Multicast
Describes a message sent to a specific group of hosts on a network

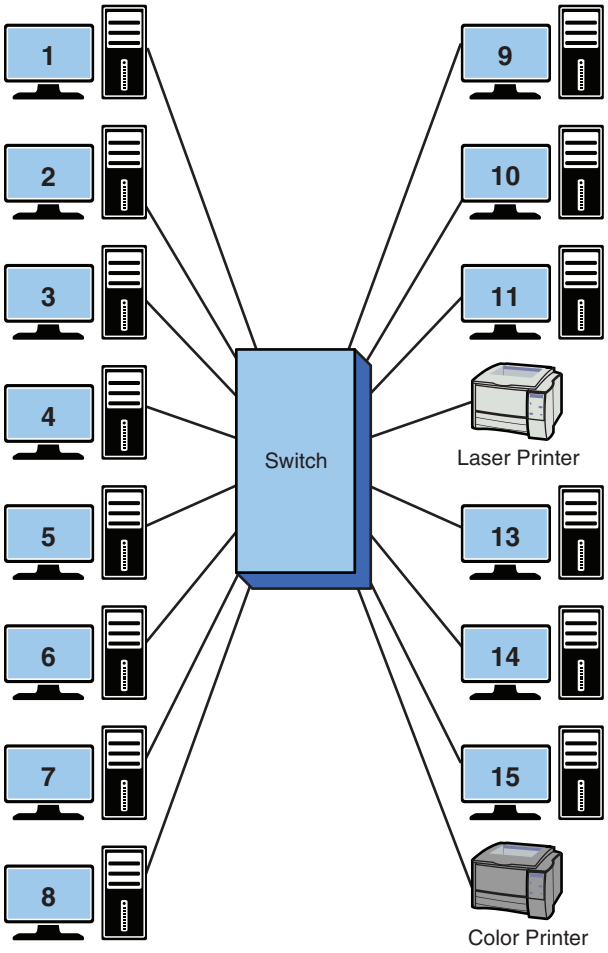


FIGURE 5-5 A switch used to interconnect the networking devices in a LAN.

Hub and Switch Comparison

An experiment was set up to test the data handling characteristics of a hub and a switch, given the same input instructions. The objective of this experiment was to show that data traffic is isolated with a switch but not with a hub. For this experiment, a LAN using a hub and a LAN using a switch were assembled. The LANs are shown in Figure 5-6. Each LAN contains four computers connected in a star topology. The computers are numbered 1–4 for reference. The IP addresses are listed for each host.

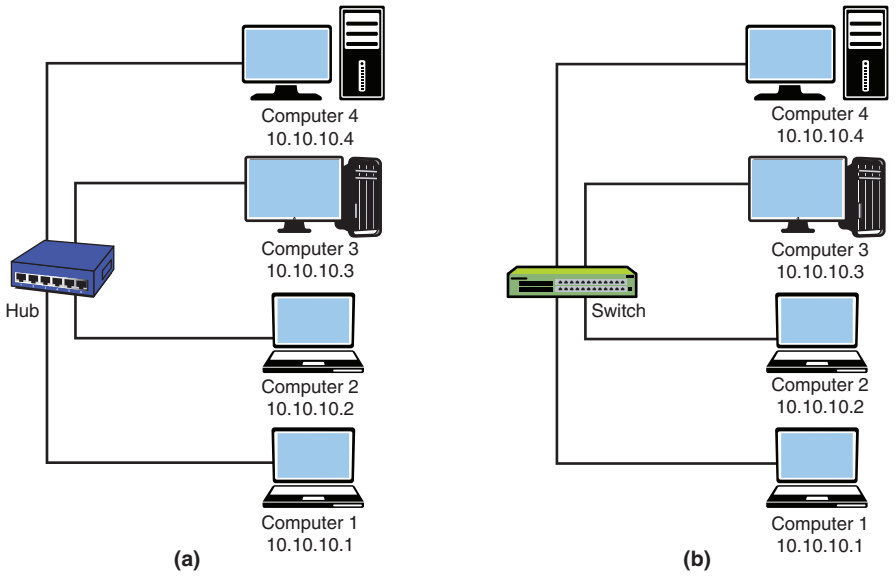


FIGURE 5-6 (a) The LAN experiment with a hub; (b) the LAN experiment with a switch.

Hub Experiment Results In this experiment, computer 1 pinged computer 3. Computer 2 was used to capture the LAN data traffic using a network protocol analyzer. What are the expected results? Remember that a hub is a multiport repeater, and all data traffic input to the hub is passed on to all hosts connected to its ports. (See the "**ping** Command Review" section that follows for a brief review of the use of the **ping** command.)

ping Command Review The **ping** command is used to verify that a network connection exists between two computers. The command format for **ping** is:

```
ping [ip address]
```

This example uses the following command:

```
ping 10.10.10.3
```

After a link is established between the two computers, a series of echo requests and echo replies are issued by the networking devices to determine how much time it takes for data to pass through the link. The protocol used by the **ping** command is Internet Control Message Protocol (ICMP).

The **ping** command is issued to an IP address; however, delivery of this command to the computer designated by the IP address requires that a MAC address be identified for final delivery. The computer issuing the **ping** might not know the MAC address of the computer holding the identified IP address (if it has no entry in the ARP cache table); therefore, an ARP request is issued. An ARP request is broadcast to all computers connected in the LAN. The computer that holds the

IP address replies with its MAC address, and a direct line of communication is then established.

Figure 5-7 shows the data traffic collected by computer 2 when computer 1 pinged computer 3. The first line of the captured data shows the ARP request, asking who has the IP address 10.10.10.3. The second line of the captured data shows the reply from 10.10.10.3 with the MAC address 00-B0-D0-25-BF-48. The next eight lines in the captured data are the series of four echo requests and replies associated with a **ping** request. Even though computer 2 was not being pinged and was not replying to the ARP request, the data traffic was still present on computer 2's hub port. The echo reply is from a Dell network interface card whose MAC address ends with the six characters 25-BF-48. The echo request is coming from a computer with 13-99-2E as the last six hex characters of its MAC address.

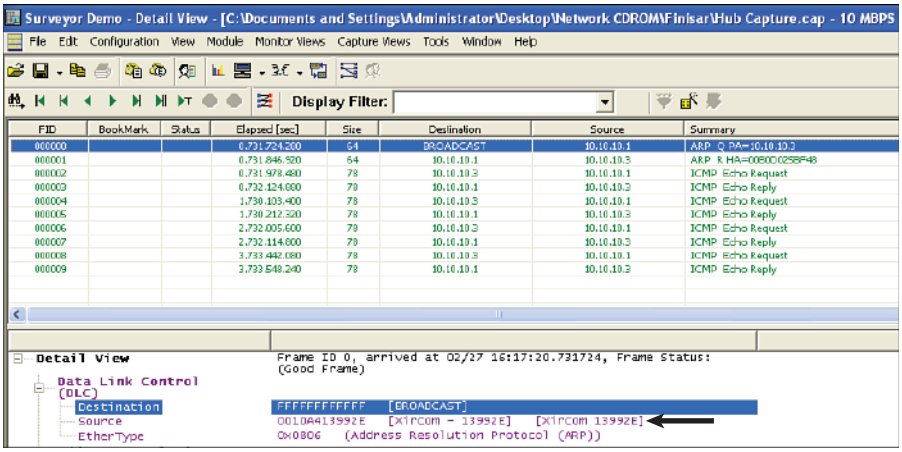


FIGURE 5-7 The data traffic captured by computer 2 for the LAN using a hub [refer to Figure 5-6(a)].

Switch Experiment Results The same experiment just described was repeated for the LAN shown in Figure 5-6(b), this time using a switch instead of a hub to interconnect the computers. This network consists of four computers connected in a star topology, using a switch at the center of the network. The **ping** command **ping 10.10.10.3** was sent from computer 1 to computer 3. The ARP cache for computer 1 is empty; therefore, the MAC address for computer 3 is not known by computer 1. An ARP request is issued by computer 1, and computer 3 replies. The series of echo requests and echo replies follow; however, the data traffic captured by computer 2 (see Figure 5-8) shows the ARP request asking who has the IP address 10.10.10.3. This is the last of the data communications between computers 1 and 3 that is seen by computer 2. A direct line of communication between computers 1 and 3 is established by the switch and prevents computer 2 from seeing the data traffic from computers 1 and 3. The only data traffic seen by computer 2 in this process is the broadcast of the ARP request. This is true for any other hosts in the LAN.

This experiment shows that the use of the switch substantially reduces data traffic—particularly unnecessary data traffic—in the LAN. The experiment shows that the broadcast associated with an ARP request is seen by all computers, but the ARP replies in a LAN using a switch are not seen. This is because a direct data connection is established between the two hosts. This experiment used pings and ARP requests; however, this same advantage of using a switch occurs when transferring files, downloading images, printing files, and so on. The data traffic is isolated from other computers on the LAN. Remember that the switch uses MAC addresses to establish which computers are connected to its ports. The switch then extracts the destination MAC address from the Ethernet data packets to determine to which port to switch the data.

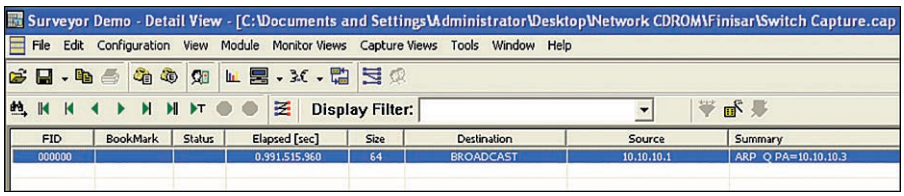


FIGURE 5-8 The data traffic captured by computer 2 for the LAN using a switch [refer to Figure 5-6(b)].

Managed Switches

Managed Switch
A switch that allows a network administrator to monitor, configure, and manage select network features

Cisco Network Assistant (CNA)
A management software tool from Cisco that simplifies switch configuration and troubleshooting

A **managed switch** is a network switch that enables a network administrator to monitor, configure, and manage certain network features, such as which computers are allowed to access the LAN via the switch. Access to the management features for the switch is password protected so that only network administrators can gain entry. This section describes some of the features of the managed interface for a Cisco Catalyst 2960X switch established using the **Cisco Network Assistant (CNA)**. The CNA software provides an easy way to manage the features of Cisco switches.

Note

You can download the CNA software from Cisco if you have a Cisco user account and password. The CNA provides for a centralized mode for completing various network administration tasks for switches, routers, and wireless networking equipment.

Figure 5-9 shows the startup menu for a Cisco Catalyst 2960 switch obtained via the CNA. This figure shows the current setup for the switch. The assigned IP address for the switch is 192.168.1.1, and a router and a switch are interconnected with the switch. (The steps for setting the IP address for an interface on the switch are presented later in this section.)

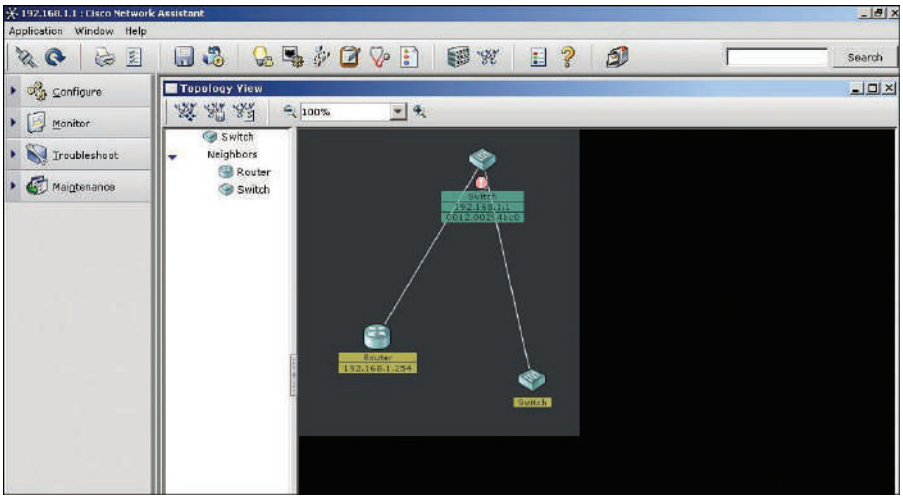


FIGURE 5-9 The startup menu of a Cisco Catalyst switch in the CNA software.

You can view the current connections to the ports on the switch by clicking the **Stacked Switch** icon at the top of the screen, as shown in Figure 5-10. The image of the switch port connections shows ports 1, 2, and 3 brighter, indicating that there are networking devices connected to these ports. The MAC addresses of the devices connected to the switch ports can be displayed by clicking **Configure > Switching > MAC Addresses**, as shown in Figure 5-11. In this case, four MAC addresses are assigned to port 1, one MAC address is assigned to port 2, and one MAC address is assigned to port 3. Multiple networking devices can be connected to a port if the devices are first connected to another switch or hub and the output of the switch or hub is connected to one switch port. The example in Figure 5-12 shows four devices connected through a hub to port 1 on the switch. The output interface information for the MAC address table shows the following information in Figure 5-11:

GigabitEthernet 0/1
GigabitEthernet 0/2
GigabitEthernet 0/3

Notice that the Dynamic Address tab is highlighted in Figure 5-11 to indicate that this is a list of the MAC addresses that have been assigned dynamically. With **dynamic assignment**, a MAC address is assigned to a port when a host is connected. There is also a Static Address tab. With **static assignment**, a MAC address is manually assigned to an interface, and the port assignment does not expire. The Secure Address tab shows what switch ports have been secured. A **secure address** means that a MAC address has been assigned to a port, and the port will automatically disable itself if a device with a different MAC address connects to the secured port.

Dynamic Assignment
A process in which MAC addresses are assigned to a port when a host is connected

Static Assignment
A process in which a MAC address has been manually assigned to a switch port

Secure Address
An address with which a switch port automatically disables itself if a device with a different MAC address connects to the port

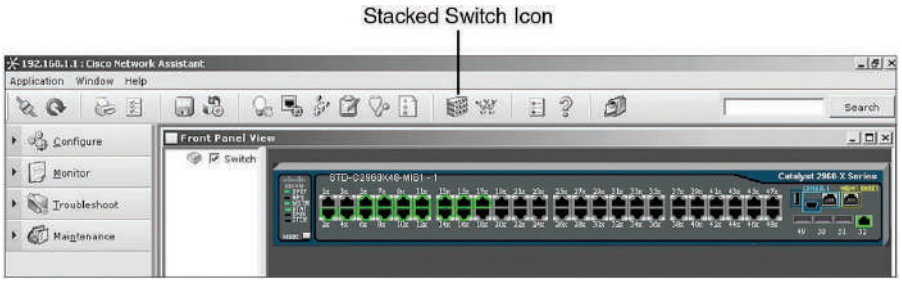


FIGURE 5-10 The highlighted ports showing the current connections and the location of the stacked switches icon.

The GigabitEthernet 0/1, GigabitEthernet 0/2, GigabitEthernet 0/3 notation indicates the [*Interface Type Slot#/Interface#*] on the switch, and *GigabitEthernet* indicates that this interface supports 1000Mbps, 100Mbps, and 10Mbps data rate connections.

Aging Time
The length of time a MAC address remains assigned to a port

In Figure 5-11, aging time is listed as 300 seconds. **Aging time** is the length of time a MAC address remains assigned to a port. If there is no data activity within this time, the assignment of the MAC address is removed. If the computer with the assigned MAC address initiates new data activity, the Aging Time counter is restarted, and the MAC address remains assigned to the port. The management window shows a switch setting for enabling aging. This switch is used to turn off the Aging Time counter so that a MAC address assignment on a port never expires.

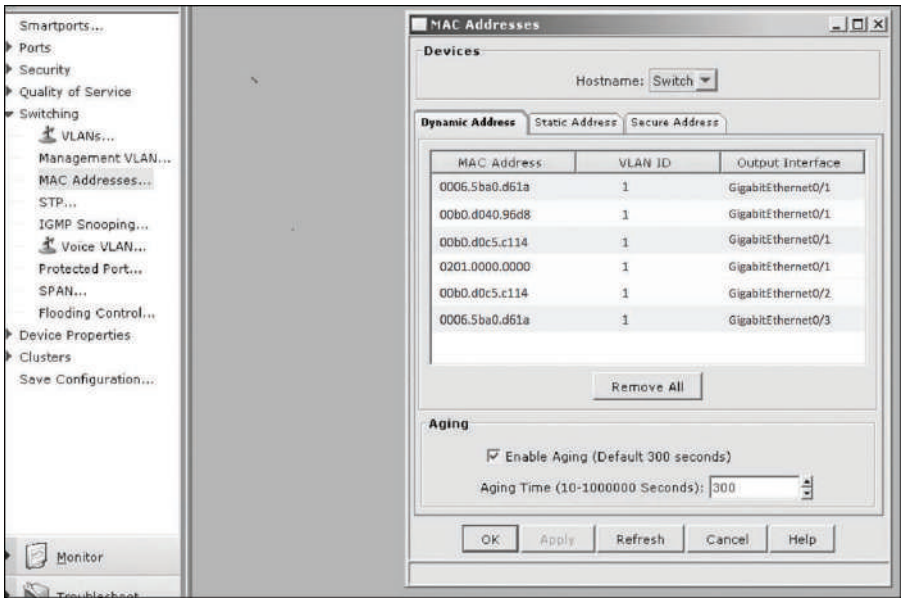


FIGURE 5-11 The window listing the MAC addresses currently connected to a switch.

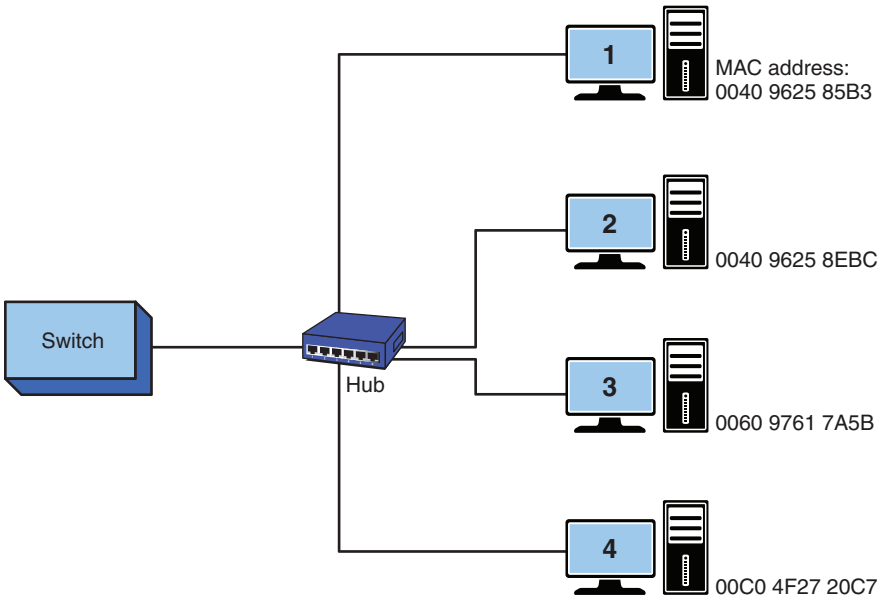


FIGURE 5-12 An example of a hub connected to a switch port, with four computers connected to the hub.

You can configure the IP address on a switch interface by using the Cisco Network Assistant software and clicking **Configure > Device Properties > IP Addresses**. The IP Addresses window shown in Figure 5-13 appears. Clicking the area where the IP address should be entered opens a text box for entering the IP address. After you enter the IP address, click **OK** to save the IP address.

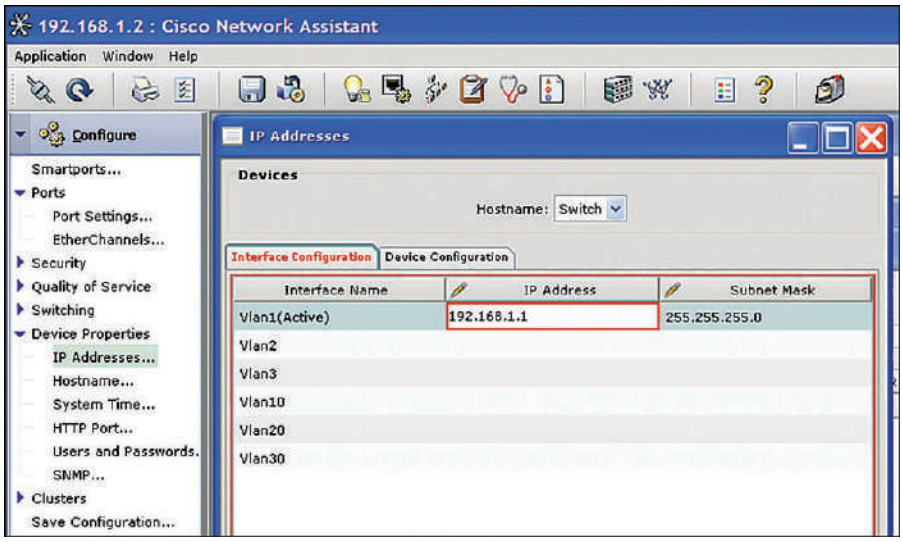


FIGURE 5-13 Configuring an IP address on an interface.

Isolating the Collision Domains
Breaking a network into segments, where a segment is a portion of the network where the data traffic from one part of the network is isolated from the other networking devices

Content-Addressable Memory (CAM)
A table of MAC addresses and port mapping that a switch uses to identify connected networking devices

Flooding
A process that occurs when a switch doesn't have the destination MAC address stored in CAM and transmits a packet out all switch ports except for the port where the packet was received

Broadcast Domain
An area in which any network broadcast sent over the network is seen by all networking devices

Store-and-Forward
A mode in which an entire frame of data is received before any decision is made regarding forwarding the data packet to its destination

Switch Latency
The amount of time a data packet takes from the time it enters a switch until it exits

There are many benefits to using a network switch in a modern computer network. These benefits include less network congestion, faster data transfers, and excellent manageability. A network switch can be used to replace a network hub, and the advantage is that data traffic within a LAN is isolated. The term for this is **isolating the collision domains**, which means breaking the network into segments. A *segment* is a portion of a network where the data traffic from one part of the network is isolated from the other networking devices. A direct benefit of isolating collision domains is that doing so increases the data transfer speed and improves bandwidth/throughput. This is due to the fact that the LAN bandwidth is not being shared and the chances of data collisions are minimized. As a result, the LAN will exhibit faster data transfers and significantly reduced latency. Reduced latency means that the data packets arrive at the destination more quickly.

Switches learn the MAC addresses of connected networks by extracting MAC address information from the headers of transmitted data packets. A switch maps the extracted MAC address to the port where the data packet came in. This information is stored in **content-addressable memory (CAM)**—a table of MAC address and port mapping that the switch uses to identify connected networking devices. The switch then uses the extracted MAC addresses to map direct communication between two network devices connected to its ports. The MAC address and port information remain in CAM as long as the device connected to the switch port remains active. A timestamp establishes the time when the mapping of the MAC address to a switch port is established. However, switches limit the amount of time address and port information are stored in CAM. As mentioned earlier in this section, this is called *aging time*. The mapping information is deleted from the switch's CAM if there is no activity during this set time. This technique keeps the mapping information stored in CAM up to date.

What happens if the destination MAC address is not stored in CAM? In this case, the packet is transmitted out all switch ports except for the port where the packet was received in a process called **flooding**.

Switches minimize the collision domain due to the fact that a direct switch connection is made between networking devices. However, it is important to remember that switches do not reduce the broadcast domain. In a **broadcast domain**, any network broadcast sent over the network will be seen by all networking devices in the same network. Broadcasts within a LAN are passed by switches. (Refer to the discussion of Figures 5-7 and 5-8 for an example.)

A switch can use three modes to forward frames:

- **Store-and-forward:** In this mode, an entire frame of data is received before any decision is made regarding forwarding the data packet to its destination. There is switch latency in this mode because the destination and source MAC addresses must be extracted from the packet, and the entire packet must be received before it is sent to the destination. The term **switch latency** refers to the amount of time a data packet takes from the time it enters a switch until it exits. An advantage of the store-and-forward mode is that the switch checks the data packet for errors before sending it on to the destination. A disadvantage is that lengthy data packets take a longer time before they exit the switch and are sent to the destination.

- **Cut-through:** In this mode, a data packet is forwarded to the destination as soon as the destination MAC address has been read. This minimizes the switch latency; however, no error detection is provided by the switch. There are two forms of cut-through switching:
  - **Fast-forward:** This mode offers the minimum switch latency. The received data packet is sent to the destination as soon as the destination MAC address is extracted.
  - **Fragment-free:** In this mode, fragment collisions are filtered out by the switch. *Fragment collisions* are collisions that occur within the first 64 bytes of the data packet. Recall from Table 1-3 in Chapter 1 that the minimum Ethernet data packet size is 64 bytes. The collisions create packets smaller than 64 bytes, and these packets are discarded. Latency is measured from the time the first bit is received until it is transmitted.
- **Adaptive cut-through:** This mode is a combination of the store-and-forward and cut-through modes. The cut-through mode is used until an **error threshold** (for errors in the data packets) has been exceeded. The switch mode changes from cut-through to store-and-forward when the error threshold has been exceeded.

Cut-Through
A mode in which a data packet is forwarded to the destination as soon as the destination MAC address has been read

Adaptive Cut-Through
A mode that is a combination of the store-and-forward and cut-through modes

Error Threshold
The point at which the number of errors in the data packets has reached a threshold, and the switch changes from cut-through mode to store-and-forward mode

Multilayer Switches

Newer switch technologies, including **multilayer switches (MLSs)**, are available to help further improve the performance of computer networks. An example of a multilayer switch is a layer 3 switch. Layer 3 switches still work at layer 2 but also work at the network layer (layer 3) of the OSI model and use IP addressing for making decisions about routing a data packet in the best direction. The major difference is that the packet switching in basic routers is handled by a programmed microprocessor. A layer 3 switch uses application-specific integrated circuit (ASIC) hardware to handle the packet switching. The advantage of using hardware to handle the packet switching is a significant reduction in processing time compared to using software for packet switching. In fact, the processing time of layer 3 switches can be as fast as the input data rate. With **wire speed routing**, the data packets are processed as fast as they are arriving. Multilayer switches can also work at the upper layers of the OSI model. For example, a layer 4 switch may process data packets at the transport layer of the OSI model.

Multilayer Switch (MLS)
A switch that operates at layer 2 but functions at the higher layers

Wire Speed Routing
A situation in which data packets are processed as quickly as they arrive

Section 5-3 Review

This section covers the following Network+ exam objectives.

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

When a link is established between the two hosts, this link is isolated from any other data traffic. However, there is an exception to this when broadcast or multicast messages are sent in the LAN. In the case of a broadcast message, the message is sent to all devices connected to the LAN.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

*As discussed in this section, the protocol used by the **ping** command is Internet Control Message Protocol (ICMP).*

1.6 Explain the use and purpose of network services.

With dynamic assignment, a MAC address is assigned to a port when a host is connected. With static assignment, a MAC address is manually assigned to an interface, and the port assignment does not expire.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section introduces the use of network switches. It includes a discussion of using a managed switch and the Cisco Network Assistant. This section also provides examples of dynamic MAC address assignment and aging time.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

Network switches are examined in this section. The concept of dynamic MAC assignment and aging time are discussed.

4.5 Explain the importance of physical security.

In cut-through mode, a data packet is forwarded to the destination as soon as the destination MAC address has been read. This minimizes the switch latency; however, no error detection is provided by the switch.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

A direct benefit of isolating collision domains is the increase in the data transfer speed and throughput.

5.5 Given a scenario, troubleshoot general networking issues.

This section discusses circuit-switched and packet-switched networks. In a packet-switched network, data packets are routed based on the associated IP address, and routing is based on programmed routing tables. In a circuit-switched network, there is a dedicated channel for establishing the communications link.

Test Your Knowledge

1. A layer 2 switch does which of the following? (Select all that apply.)
   a. Provides a direct connection for networking devices in a LAN
   b. Uses MAC addressing from the data link layer
   c. Uses MAC addressing from the network layer
   d. Uses IP addressing from the network layer

2. A network administrator wants to verify the network connection at 10.10.20.5. Which of the following commands can be used to verify the connection? (Select all that apply.)

   a. **ping all 10.10.20.5**
   b. **ping 10.10.20.5**
   c. **ping -t 10.10.20.5**
   d. **ping -2 10.10.20.5**

3. What does a managed switch allow a network administrator to do? (Select all that apply.)

   a. Monitor network features.
   b. Configure network features.
   c. Manage certain network features.
   d. All of these answers are correct.
   e. None of these answers are correct.

5-4 THE ROUTER

This section describes the use of a router in a computer network and introduces the basic hardware and interfaces available with a router. Router configuration is described in Chapter 7, "Introduction to Router Configuration."

The router is the most powerful networking device used today to interconnect LANs. A router is a layer 3 device, which means it uses the **network address** (layer 3 addressing) to make routing decisions regarding forwarding of data packets. Remember from Chapter 1 that the OSI model separates network responsibilities into different layers. In the OSI model, layer 3, which is the network layer, is responsible for handling the network address. A network address is also called a *logical address*. Whereas a *physical address* is the hardware or MAC address embedded into a network interface card, a **logical address** describes the IP address location of the network and the address location of the host in the network.

Network Address
A layer 3 address

Logical Address
The IP address location of a network and the address location of a host in a network

Essentially, a router is configured to know how to route data packets entering or exiting a LAN. This differs from a bridge and a layer 2 switch, which use the Ethernet address for making decisions regarding forwarding data packets and only know how to forward data to hosts physically connected to their ports.

Routers are used to interconnect LANs in a campus network. Routers can be used to interconnect networks that use the same protocol (for example, Ethernet), or they can be used to interconnect LANs that use different layer 2 technologies, such as Ethernet and Token Ring. Routers also make it possible to interconnect to LANs around the country and the world and to interconnect many different networking protocols.

Router Interface
The physical connection where a router connects to a network

A router has multiple port connections for connecting to LANs; by definition, a router must have a minimum of three ports. Figure 5-14 shows the symbol commonly used to represent a router in a network drawing. The arrows pointing in and out indicate that data enters and exits the routers through multiple ports. The router ports are *bidirectional,* meaning that data can enter and exit the same router port. Often router ports are called the **router interface**, the physical connection where the router connects to the network.

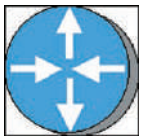


FIGURE 5-14 The network symbol for a router.

The Router Interface

Figure 5-15 shows the rear panel view (interface side) of a Cisco Integrated Services Router (ISR) router.

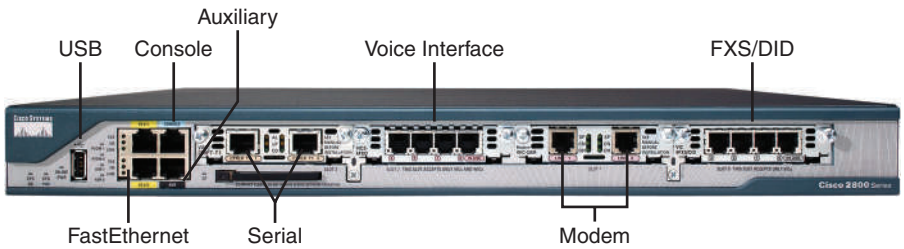


FIGURE 5-15 The rear panel view of a Cisco ISR router.

The following list describes the function of each interface:

- **USB interface:** The USB ports are used for storage and security support.
- **FastEthernet ports:** The ports are FE0/0 for Fast Ethernet 10/100Mbps and FE0/1 for Fast Ethernet 10/100Mbps.
- **Console input:** This 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 can have RJ-45 plugs on each end and requires the use of an RJ-45 to DB9 adapter for connecting to the computer's COM1 or COM2 serial port. The console cable can also have an RJ-45 connector on one end and an integrated DB9 connector on the other end.
- **Auxiliary input:** This input is used to connect a dial-in modem to 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.

- **Serial interface:** CTRLR T1 1 (Controller T1 1) and CTRLR T1 0 (Controller T1 0) are serial controllers with a built-in CSU/DSU. This interface is used to provide a T1 connection to the communications carrier. (CSU/DSU functionality is presented in Chapter 8, "Introduction to Switch Configuration.") The RJ-45 type of connection replaces the older V.35 cabling (shown later in this chapter, in Figure 5-18). There are three LEDs on this interface:
  - **AL**—Alarm
  - **LP**—Loop
  - **CD**—Carrier detect
- **Voice interface card:** This interface shows four phone line connections. This router can be programmed as a small private branch exchange (PBX) for use in a small office.
- **WAN interface card (WIC2AM):** This interface has two RJ-11 jacks and two V.90 analog internal modems. These modems can be used to handle both incoming and outgoing modem calls. This interface is listed as modem in Figure 5-15. (RJ-11 is the common connector used for plugging a telephone into a wall or a modem.)
- **VIC-4FXS/DID:** This interface is a four-port FXS and DID voice/fax interface card. FXS stands for foreign exchange interface and is used for connecting directly to a standard telephone. DID, which stands for direct inward dialing, enables callers to directly call an extension on a PBX. This interface is listed as FXS/DID in Figure 5-15.

The router shown in Figure 5-15 has many interface cards, most notably the voice interface cards, which can enable the router to also become a small VoIP (voice over IP) PBX and voice gateway. VoIP, also called IP telephony, is technology that transports phone conversations over IP networks. A PBX is a user's own telephone system. It manages the internal switching of telephone calls and also interfaces the user's phone to the PSTN (public switched telephone network—the telephone company [telco]). Standard telephones can also be used in IP telephony if the telephones connect to a PBX that supports IP telephony. The interface of the IP telephone system to the PSTN is called a *voice gateway*. The voice data needs to be packaged for transport over the IP network or the PSTN. The gateway also makes sure the proper signaling is included for the voice data packet transport. Signaling is used to establish and terminate telephone calls and to manage many of the advanced features available with telephones. Essentially, this router is capable of supporting VoIP phones and connecting the VoIP phones to external lines such as those of the local telephone company.

Quality of Service

An important issue in the delivery of real-time data over a network (such as with VoIP) is quality of service (QoS). QoS issues for a VoIP network include jitter, queuing/buffering, network latency and network congestion.

Jitter Digitized voice data requires a fixed time interval between data packets for the signal to be properly converted back to an audible analog signal. However, there is a delay problem with voice data transported over a packet network. Variability in data packet arrival introduces jitter in the signal and leads to a poorly reconstructed signal at the receiver. For example, say that a 1000Hz tone is sent over a VoIP network. The tone is digitized at regular time intervals, assembled into frames and packets, and sent out as a Real-Time Transport Protocol (RTP) packet. Random delays in the packets' travel to the destination result in their arriving at irregular time intervals. The reproduced 1000Hz analog tone will contain jitter because the arrival times for the data packets will vary.

Queuing/Buffering Queuing/buffering the data packets long enough for the next data packet to arrive can help minimize the effects of jitter. A buffer is temporary storage for holding data packets until it is time for them to be sent. The buffer enables the data packets to be output at regular time intervals, thereby removing most of the jitter problem. Buffering works as long as the arrival time until the next packet is not too long. If a data packet arrives too late, it might have to be considered lost because real-time data packets can't wait too long for the buffered packet without affecting the quality of the reconstructed signal. Another issue is that the buffering stage introduces delay, and having to wait additional time only introduces more delay.

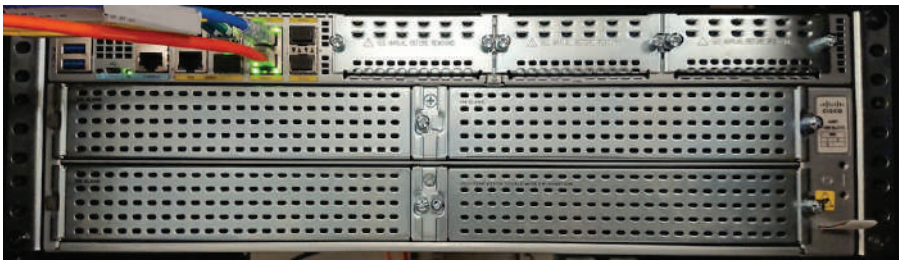
Network Latency It takes time for a data packet to travel from the source to the destination. This time is called network latency, and it is an important issue with VoIP data traffic. Telephones (both traditional and IP) feed a portion of the user's voice into the earpiece. If the round-trip delay of the voice data is too lengthy (more than 50 ms), the user will begin to hear an annoying echo in the earpiece.

Network Congestion Another source of packet delay is network congestion, which can have a negative effect on any type of data traffic but is especially disruptive to VoIP telephony. You must make sure that congestion problems are avoided or at least minimized. You may have the option of configuring routers to optimize routes for IP telephony.

You can minimize delay issues by making sure the network routers and switches are optimized for VoIP data traffic. You can configure a VoIP network so that high-priority data packets (for example, voice packets) are transported first over the IP network. In this case, non-sensitive data packets are given a low-priority status and are transmitted only after the high-priority packets are sent.

Higher-end routers Figure 5-16 shows two Cisco ISR 4400 series routers, which provide adaptable interfaces for connecting to many physical layer technologies, such as Fast Ethernet, Gigabit Ethernet, ATM, and a T1/E1 voice interface. This router is an example of a chassis-based network device that has a fixed number of slots for various types of line cards. Chassis-based network devices are configurable and easy to upgrade; it is also easy to replace their parts.

Some technologies require higher-end routers. One such technology is Multiprotocol Label Switching (MPLS), a data-carrying technique used in telecommunications networks. It can encapsulate data packets from many network protocols—hence the term *multiprotocol*. MPLS assigns tags or labels to a certain type of traffic or network and then handles or switches these distinctive labeled packets across the service provider network backbone.



(a)



(b)

FIGURE 5-16 (a) A Cisco ISR 4461 router; (b) a Cisco ISR 4431 router.

Another useful device for managing data traffic flow is a packet shaper, which is a device that sits between a campus network and the outside network. The device is set up so that all data traffic, incoming and outgoing, passes through it. A packet shaper can be used to set rules to limit download traffic from the Internet. It can also be used to make sure applications such as VoIP are given a higher priority so that the operation and quality of service are not affected.

Section 5-4 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.
Higher-end routers provide support for Multiprotocol Label Switching (MPLS), a data-carrying technique used in telecommunications networks that can encapsulate data packets from many network protocols.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
The router is the most powerful networking device used today to interconnect LANs. A router is a layer 3 device, which means it uses the network address (layer 3 addressing) to make routing decisions regarding forwarding data packets.

2.2 Compare and contrast routing technologies and bandwidth management concepts.
QoS issues for a VoIP network include jitter, network latency and packet loss, and queuing.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.
It takes time for a data packet to travel from the source to the destination. This time is called network latency, and it is an important issue with VoIP data traffic.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

Higher-end routers provide support for Multiprotocol Label Switching (MPLS), a data-carrying technique used in telecommunications networks that can encapsulate data packets from many network protocols.

Test Your Knowledge

1. Which of the following does a router use in order to make routing decisions regarding forwarding of data packets?
   a. Router address
   b. Network address
   c. Fast link pulse
   d. None of these answers are correct.
2. A logical address is which of the following?
   a. MAC address
   b. Router interface address
   c. Network address
   d. The ARP address
3. The physical connection where a router connects to a network is called which of the following?
   a. Console input
   b. Auxiliary input
   c. Router interface
   d. USB interface

5-5 THE CONSOLE PORT CONNECTION

Many students have used a computer's serial port (COM1, COM2, and so on) to connect a mouse, but few are used to configuring HyperTerminal or another serial communications software for establishing a serial connection. This section examines the serial connection from the hardware used to connect to the ports as well as the software configuration. Students need this knowledge when connecting to a router.

RS-232
A serial communications port

The examples in this section are based on a router's console port, but they apply to switches as well. A router's console connection is a slow-speed serial communications link (9600bps) and is the only way to communicate with most routers until the router interfaces have been configured. Specifically, the console connection is an **RS-232** serial communications port that uses an RJ-45 jack to connect to its interface. The RS-232 protocol running on the console port is the same communications protocol format used on a computer's (COM1, COM2) port; however, the

connector for the serial communications port on the computer is either a **DB-9** or **DB-25** connector (although DB-25 connectors are seldom used). Figure 5-17 shows drawings of the DB-9 and DB-25 connector ends. The DB-9 connection uses 9 pins, and the DB-25 connection uses 25 pins.

DB-9
A 9-pin connector

DB-25
A 25-pin connector

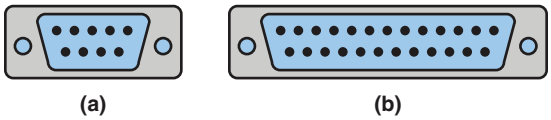


FIGURE 5-17 (a) DB-9 connector; (b) DB-25 connector (courtesy of StarTech.com).

The connection from the router to the serial port on the computer requires a cable to be run from the computer's serial port to the RJ-45 console jack input on the router. This can be accomplished using a cable with the DB-9 and RJ-45 plug ends, as shown in Figure 5-18(a), or using an RJ-45 rollover cable and a DB-9 to RJ-45 adapter, as shown in Figure 5-18(b). Serial connections are increasingly being replaced by USB connections. In such cases, the option is to use a USB to 9-pin RS-232 adapter, as shown in Figure 5-18(c). A cable that connects the router's console port to the computer's serial port is called a **console cable**.

Console Cable
A cable that connects a router's console port to a computer's serial port

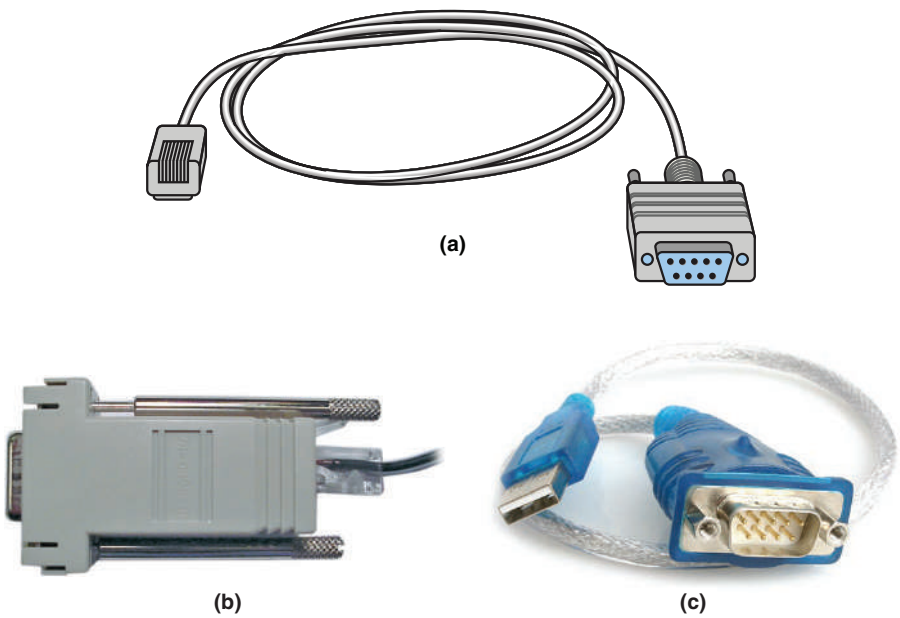


FIGURE 5-18 (a) A console cable with an integrated DB-9 connector; (b) a console cable using an RJ-45 rollover cable and a DB-9 to RJ-45 adapter; (c) a USB to RS-232 adapter (courtesy of StarTech.com).

You connect the DB-9 end of the console cable to any of the available serial ports (**COM1, COM2, ...**) on the computer or to the USB to RS-232 adapter. The router's console input uses an RJ-45 jack, and the console cable must have an RJ-45 plug.

COM1, COM2, ...
The computer's serial communication ports

Rollover Cable
A cable with the signals reversed at each end

The cable used to connect the RJ-45 plug to the computer, called a **rollover cable**, is a flat cable that reverses signals on each cable end (for example, pins 1–8, 2–7, 3–6, and so on). Table 5-4 shows the signal assignments and pin numbers for the ends of a rollover cable. Note that the pin numbers for the cables are swapped at each end.

TABLE 5-4 **Signal and Pin Assignments for Console Rollover Cables**

Signal	Function	RJ-45 End A	RJ-45 End B
RTS	Ready-to-send	1	8
DTR	Data terminal ready	2	7
TXD	Transmit data	3	6
GND	Ground	4	5
GND	Ground	5	4
RXD	Receive data	6	3
DSR	Data send ready	7	2
CTS	Clear-to-send	8	1

A serial communications software package such as HyperTerminal or PuTTY can be used to establish a communications link to a router's console input. Table 5-5 outlines the settings for the serial interface on a Cisco router's console port.

TABLE 5-5 **Settings for the Serial Interface on a Cisco Console Port**

Parameter	Setting
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	none

The next step is to set up the console connection from a computer to the router. This requires that one RJ-45 end of a rollover cable be connected to the console port in the back of the router. The other end of the cable connects to one of the 9-pin serial communication ports (COM ports) of the computer. It is important to note which serial port you connect to. You will have to specify the serial port (for example, COM1, COM2, and so on) when configuring the PuTTY serial communications software.

Configuring the PuTTY Software (Windows)

PuTTY is free terminal emulator software that can be used to connect to the network equipment console via a serial connection. After PuTTY is installed, you can click on the PuTTY program to start. The PuTTY Configuration dialog, shown in Figure 5-19, appears.

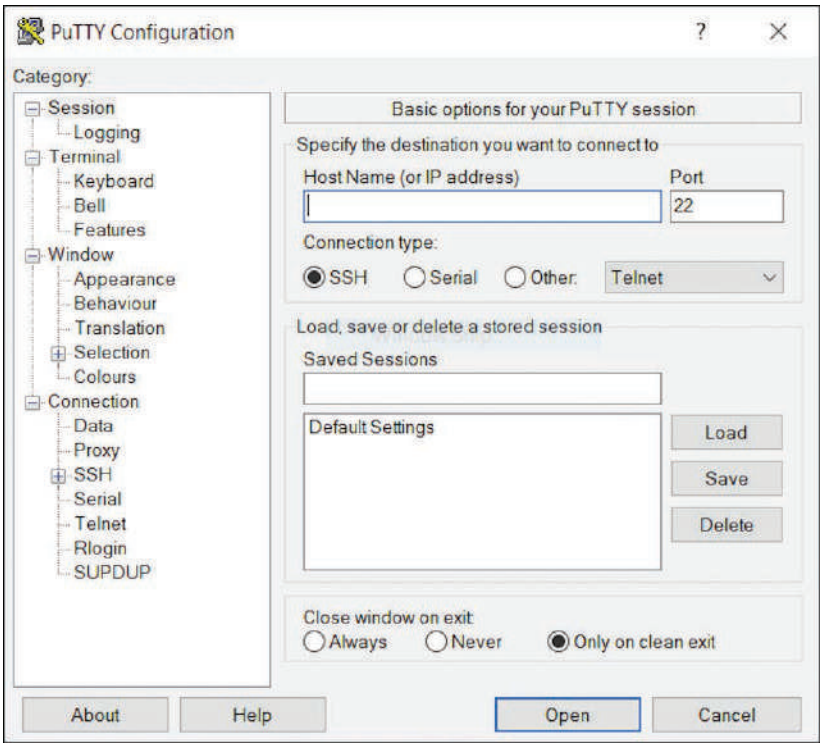


FIGURE 5-19 The PuTTY Configuration dialog.

The PuTTY Configuration dialog lets you specify how you are making the serial connection to the router. In this case, change the Connect Type parameter to **Serial** (see Figure 5-20). This example shows that the connection is configured to use the computer's COM1 serial port. Click **Open** after you've made any other necessary selections.

You can change the properties of a serial connection by selecting **Serial** under Connection in the left pane of the PuTTY Configuration dialog. Recall that the settings for connecting to the router's serial console port are provided in Table 5-5. The COM1 properties have to be set to match those settings (see Figure 5-21). After you change any settings you need to change, you can click **Open**, and the Cisco router screen is displayed. Press **Enter** to start the terminal communications. You should see a window like the one shown in Figure 5-22 when a connection has been established. If the window does not appear, press **Enter** to see whether the router resets itself. You might also see a screen with a **Router>** prompt. In this case, press **Enter**, and if the **Router>** prompt remains, you are connected. If pressing **Enter** doesn't correct the displayed text, the router might need to be restarted.

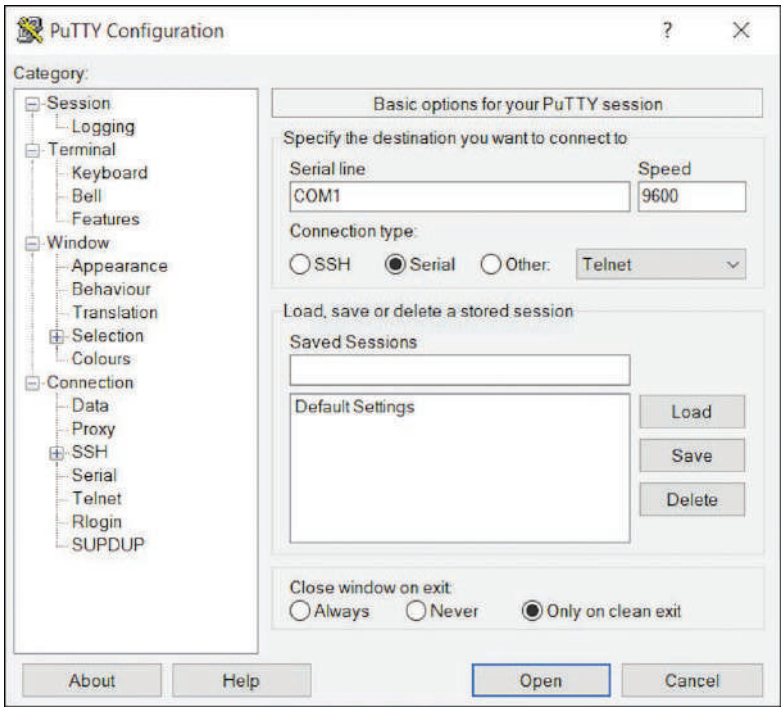


FIGURE 5-20 Changing settings in The PuTTY Configuration dialog.

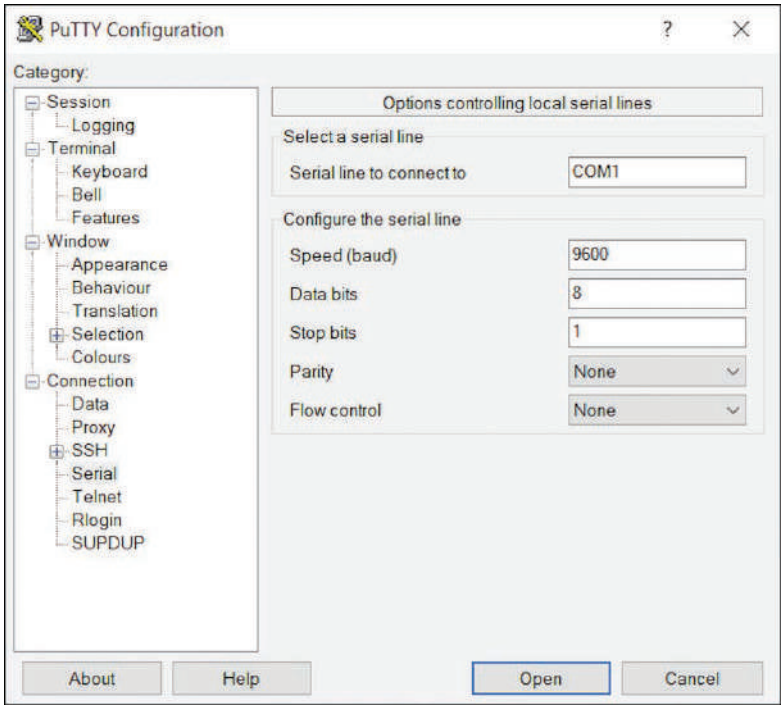


FIGURE 5-21 The PuTTY Configuration dialog for configuring the serial port connection.



FIGURE 5-22 The Cisco router console port screen.

Configuring the ZTerm Serial Communications Software (Mac)

Establishing a console port via the USB serial connection on a macOS computer requires the following:

- Serial communication software such as ZTerm, a shareware program for macOS that can be downloaded from www.dalverson.com/zterm/.
- A USB to a 9-pin RS-232 male serial adapter, such as the USB to 9-pin adapter cable shown earlier, in Figure 5-18(c). (Note that the USB serial adapter may require that an additional driver be installed.)

You need to install the serial communications software and the driver and then start the serial communications software. To do so, select **Settings > Modem Preferences**, as shown in Figure 5-23, to open the window shown in Figure 5-24. You need to change the serial port so that it is set to **PL2303-000** and then click **OK** when the change to usbserial0 has been made. Next, select **Settings > Connection** to open the dialog shown in Figure 5-25. Set the following settings for the serial console connection:

- Set Data Rate to **9600**.
- Set Data Bits to **8**.
- Set Parity to **N**.
- Set Stop Bits to **1**.
- Select **Hardware Handshake**.

When you're done with these settings, click **OK**.

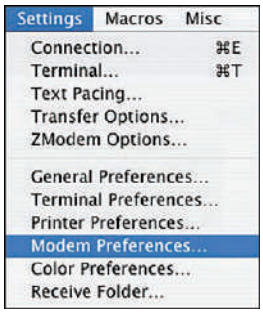


FIGURE 5-23 The macOS dialog for configuring the settings for the serial interface.

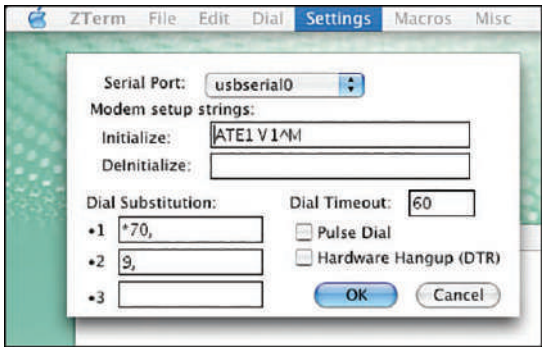


FIGURE 5-24 The macOS dialog for setting the serial port to PL2303-000.

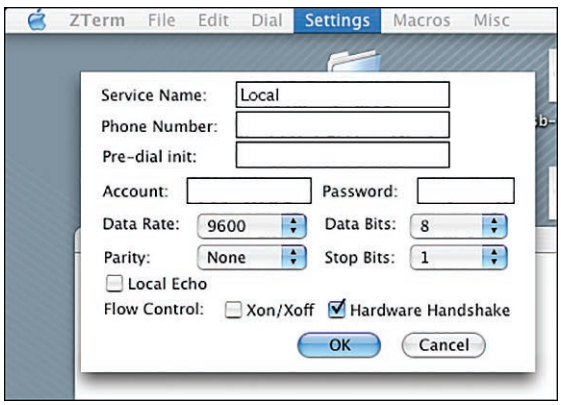


FIGURE 5-25 The macOS window listing the serial communication link settings.

Besides using the console port to configure routers and switches, many small business and home routers and switches offer another way: using the built-in URL management of the device. This is called the HTTPS/management URL port. URL management allows you to connect to a network device via a web browser, using HTTPS to access the device's IP address and its designated TCP port. For example, a manageable network switch with IP address 192.168.0.2 with designated management TCP port 8080 can be reached at https://192.168.0.2:8080. This would take you to the web page of the switch for configuration and management. The default IP address and the management port of the device are often specified in the setup instructions. URL management makes it easier for typical users to configure a network device without using a physical cable connection. Also, a lot of enterprise network equipment offers URL management for management and configuration as well.

Section 5-5 Review

This section covers the following Network+ exam objectives.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

Besides using the console port to configure routers and switches, many small business and home routers and switches offer another way: using the built-in URL management of the device. This is called the HTTPS/management URL port.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

The examples in this section are based on a router's console port, but they apply to switches as well.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

Settings for the serial interface on a Cisco console port are set to have no flow control.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

Table 5-4 provides the signal and pin assignments for console rollover cables.

5.3 Given a scenario, use the appropriate network software tools and commands.

It is important to have a good understanding of the router's command line.

Test Your Knowledge

1. The connection to a router's console port input is typically which of the following?

    a. RS-232

    b. USB

c. DB-9

d. DB-25

e. All of these answers are correct.

2. What cable provides a connection from a wall plate to a computer?

a. RS-232

b. Patch cable

c. Roll-over cable

d. None of the above are correct.

5-6 INTERCONNECTING LANS WITH THE ROUTER

This section examines how routers can be used to interconnect LANs. It introduces concepts such as gateways, routing tables, and network segments. Make sure students understand the terminology and can identify the router hardware. These concepts will be used in Chapters 6, 7, 8, and 9.

As discussed earlier in this chapter, a router routes data based on the destination network address or logical address rather than the physical address used by layer 2 devices (for example, switches, bridges). Information exchanged with bridges and layer 2 switches requires that the MAC address for the hosts be known. Routed networks, such as most enterprise and campus networks, use IP addressing for managing data movement. **Enterprise network** is a term used to describe the network used by a large company. The use of the network or logical address on a computer enables the information to be sent from a LAN to a destination without requiring that the computer know the MAC address of the destination computer. Remember that delivery of data packets is based on knowing the MAC address of the destination.

Enterprise Network
The network used by a large company

As discussed earlier in this chapter, the router interface provides a way to access a router for configuration either locally or remotely. Interfaces are provided for making serial connections to the router and to other devices that require serial communications links. For example, serial interfaces are needed for WAN devices. RJ-45 ports are provided on a router interface for connecting the router to a LAN. Older routers may require the use of an attachment unit interface (AUI) port to establish an Ethernet connection to a UTP cable. This port provides a 10Mbps data connection to Ethernet (10Mbps) networks. An RJ-45 connection is used to connect Ethernet (10Mbps), Fast Ethernet (100Mbps), Gigabit Ethernet (1000Mbps), and 10 Gigabit Ethernet (10Gbps) to a LAN. Although an RJ-45 connection can support Gigabit and 10 Gigabit Ethernet, high-speed data networks can also use a fiber connection.

Figure 5-26 shows an example of a **media converter** used to convert the 15-pin AUI port to the 8-pin RJ-45 connector. Media converters are commonly used in computer networks to adapt layer 1 or physical layer technologies from one technology to another. Examples include AUI to twisted pair (RJ-45), AUI to fiber, and RJ-45 to fiber.

Media Converter
A device used to adapt a layer 1 (physical layer) technology to another layer 1 technology

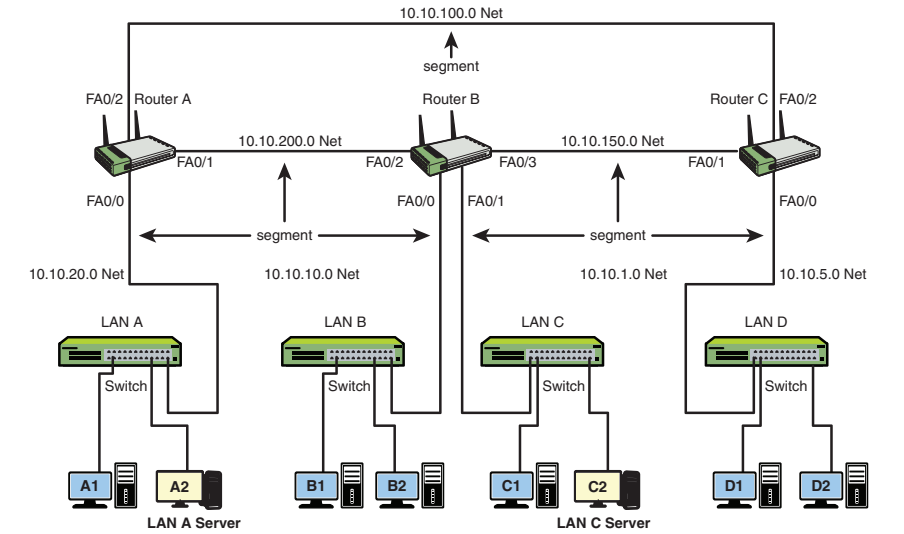


FIGURE 5-26 A CentreCom 210TS AUI to RJ-45 media converter.

When dealing with twisted-pair Ethernet cables, you must also understand the medium dependent interface (MDI) of the NIC of the device. Generally, routers and computers use an MDI interface, whereas switches use MDI-X (medium dependent interface crossover). In order for these two types of devices to communicate, the transmit pair pins on one end of the twisted-pair cable must connect to the receive pair pins on the other end. This is why you can use a straight-through twisted-pair cable to connect a router or a computer to a switch, as discussed in Chapter 2, "Physical Layer Cabling: Twisted-Pair." Today, many NICs and network devices are equipped with the Auto-MDI-X (auto-medium-dependent interface crossover) feature, which detects the crossover and changes its interface to MDI or MDI-X automatically.

This section provides the information on how to design, manage, and configure campus networks. Figure 5-27 shows an example of a small interconnected LAN. This example shows four Ethernet LANs interconnected using three routers. The LANs are configured in a star topology, using switches at the center of the LAN. The LANs are labeled LAN A, LAN B, LAN C, and LAN D. The routers are labeled RouterA, RouterB, and RouterC. (Router naming protocols are discussed in Chapter 9, "Routing Protocols.") Connection of the routers to the LANs is provided by the router's **FastEthernet port (FA0/0, FA0/1, FA0/2, ...)**. Look for the FA labels in Figure 5-27.

FastEthernet Port (FA0/0, FA0/1, FA0/2, ...)
FastEthernet ports on a router



Router A Port Addresses (LAN A)	
FastEthernet 0/0 (Gateway Address)	10.10.20.250
FastEthernet 0/1	10.10.200.1
FastEthernet 0/2	10.10.100.1
LAN A Computers	
Computer A1	10.10.20.1
Computer A2	10.10.20.2
Subnet Mask	***255.255.255.0***

Router B Port Addresses (LAN B)	
FastEthernet 0/0 (Gateway Address)	10.10.10.250
FastEthernet 0/2	10.10.200.2
FastEthernet 0/3	10.10.150.1
LAN B Computers	
Computer A1	10.10.10.1
Computer A2	10.10.10.2
Subnet Mask	***255.255.255.0***

Router B Port Addresses (LAN C)	
FastEthernet 0/1 (Gateway Address)	10.10.1.250
FastEthernet 0/2	10.10.200.2
FastEthernet 0/3	10.10.150.1
LAN C Computers	
Computer A1	10.10.1.1
Computer A2	10.10.1.2
Subnet Mask	***255.255.255.0***

Router Port Addresses (LAN D)	
FastEthernet 0/0 (Gateway Address)	10.10.5.250
FastEthernet 0/1	10.10.150.2
FastEthernet 0/2	10.10.100.2
LAN D Computers	
Computer A1	10.10.5.1
Computer A2	10.10.5.2
Subnet Mask	***255.255.255.0***

FIGURE 5-27 A small interconnected LAN.

The interconnections for the routers and the LANs are summarized as follows:

- RouterA connects directly to the LAN A switch via port FA0/0. RouterA also connects directly to RouterB via port FA0/1 and connects to RouterC via port FA0/2.
- RouterB connects directly to the LAN B switch via port FA0/0. RouterB connects to the LAN C switch via port FA0/1. RouterB connects directly to RouterA via port FA0/2 and connects to RouterC via port FA0/3.
- RouterC connects directly to the LAN D switch via port FA0/0. Connection to RouterB is provided via port FA0/1. RouterC connects to RouterA via port FA0/2.

Serial Port (S0/0, S0/1, S0/2, ...)
The serial ports on a router

The **serial ports (S0/0, S0/1, S0/2, ...)** are not being used to interconnect the routers in this sample campus network. The serial interfaces are typically used to interconnect LANs that connect through a data communications carrier such as a telephone company (telco).

The network configuration shown in Figure 5-27 enables data packets to be sent and received from any host on the network after the routers in the network have been properly configured. For example, computer A1 in LAN A could be sending data to computer D1 in LAN D. This requires that the IP address for computer D1

be known by the user sending the data from computer A1. The data from computer A1 first travels to the switch where the data is passed to RouterA via the FA0/0 data port. RouterA examines the network address of the data packet and uses configured routing instructions stored in routing tables to decide where to forward the data. RouterA determines an available path to RouterC via the FA0/2 port connection. The data is then sent directly to RouterC. RouterC determines that the data packet should be forwarded to the FA0/0 port to reach computer D1 in LAN D. The data is then sent to D1. Alternatively, RouterA could have sent the data to RouterC through RouterB via Router A's FA0/1 port. (Path selection for data packets is examined in Chapter 9 "Routing Protocols."

Delivery of the information over the network is made possible by the use of an IP address and **routing tables**. Routing tables keep track of the routes used for forwarding data to its destination. RouterA used its routing table to determine a network data path so computer A1's data could reach computer D1 in LAN D. RouterA determines that a path to the network where computer D1 is located can be obtained via RouterA's FA0/2 port to the FA0/2 port on RouterC. RouterC determines that computer D1 is on LAN D, which connects to RouterC's FA0/0 port. RouterC issues an ARP request to determine the MAC address of computer D1. The MAC address is then used for final delivery of the data to computer D1.

Routing Table
A table that keeps track of the routes to use for forwarding data to its destination

If RouterA determines that the network path to RouterC is down, RouterA can route the data packet to RouterC through RouterB. After RouterB receives the data packet from RouterA, it uses its routing tables to determine where to forward the data packet. RouterB determines that the data needs to be sent to RouterC, and it uses the FA0/3 port to forward the data.

Gateway Address

The term **gateway** is used to describe the address of the networking device that enables the hosts in a LAN to connect to networks and hosts outside the LAN. For example, for all hosts in LAN A, the gateway address is 10.10.10.250. This address is configured on the host computer. Any IP packets with a destination outside the LAN are sent to the gateway address. The gateway address is referred to as the *default gateway* in Windows OS and as the *router* in macOS.

Gateway
A networking device that enables hosts in a LAN to connect to networks (and hosts) outside the LAN

Network Segments

A *network segment* is the networking link between two LANs. There is a segment associated with each connection of an internetworking device (for example, router–hub, router–switch, router–router). For example, the IP address for the network segment connecting LAN A to the router is 10.10.20.0. All hosts connected to this segment must contain a 10.10.20.*x* because the subnet mask 255.255.255.0 is being used. (Subnet masking is fully explained in Chapter 6, "TCP/IP.")

Routers use the information about the network segments to determine where to forward data packets. For example, the network segments that connect to RouterA include the following:

10.10.20.0
10.10.200.0
10.10.100.0

The computers in LAN A are in the 10.10.20.0 network, which means every computer in this network must contain a 10.10.20.*x* IP address. For example, computer A1 in LAN A will have the assigned IP address 10.10.20.1 and gateway address 10.10.20.250. The computers in LAN B are located in the 10.10.10.0 network. This means that every computer in this network must contain a 10.10.10.*x* IP address. The *x* part of the IP address is assigned for each host. The gateway address for the hosts in LAN B is 10.10.10.250.

Section 5-6 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.
A network segment is the networking link between two LANs. There is a segment associated with each connection of an internetworking device (for example, router–hub, router–switch, router–router).

1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
The gateway address is referred to as the default gateway in Windows OS and as the router in macOS.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
A router routes data based on the destination network address or logical address rather than the physical address used by layer 2 devices (for example, switches, bridges).

2.2 Compare and contrast routing technologies and bandwidth management concepts.
This section introduces the router. It is important to remember that the purpose of the routing table is to keep track of the routes used to forward data to its destination.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.
This section mentions that a router routes data based on the destination network address or logical address rather than the physical address used by layer 2 devices.

5.5 Given a scenario, troubleshoot general networking issues.
This section introduces the routing table, which keeps track of the routes to use for forwarding data to its destination

Test Your Knowledge

1. What does a router's routing table do?
   a. Keeps track of the routes to forward data to its destination
   b. Keeps track of the IP addresses to forward data to its destination

c. Keeps track of the MAC addresses to forward data to its destination

d. None of these answers are correct.

2. True or false: The term *enterprise network* is used to describe the network used by a large company.

   True

3. A gateway address defines which of the following?

   a. The networking links between two LANs

   b. The networking device that enables hosts in a LAN to connect to networks outside the LAN

   c. The networking device that enables hosts in a LAN to connect to networks inside the LAN

   d. All of these answers are correct.

5-7 INTERCONNECTING LANS AND WANS

This section explores the basics of telecommunication data rates and line connections. This is a good time to ensure that students understand T1 and T3 and DS-0 and DS-3. At a minimum, make sure students know the data rates for each data channel. Most WANs are interconnected via telco, the telecommunications carrier. Students should understand the concepts of point of presence and line of demarcation. The CSU/DSU is an important piece of technology used to facilitate WANs, or "broadband" networks. It might be worthwhile for students to prepare a short report of the current role of CSUs/DSUs in wide area networking. Information on line encoding formats is presented to ensure that students have at least some understanding of data encapsulation. This section provides an example of configuring the data encapsulation for a router.

This section also introduces the extension of the Ethernet infrastructure beyond the internal network. It introduces Metro Optical Ethernet and the Ethernet service types, including E-Line, E-LAN, and E-Tree. This section also introduces the four service attributes: CIR, CBS, EIR, and EBS.

This section introduces well-known LAN architecture, data center architecture, and WAN technologies such as high-speed serial connections and Metro Optical Ethernet that are used to connect LANs or to connect the enterprise network to the outside world.

Three-Tiered LAN Architecture

Most enterprise networks use a three-tiered design that has core, distribution, and access layers (see Figure 5-28). These layers can be spread out into more layers or compacted into fewer, depending on the size of these networks. This three-tiered network structure is used in campus networks to improve data handling and routing within the network.

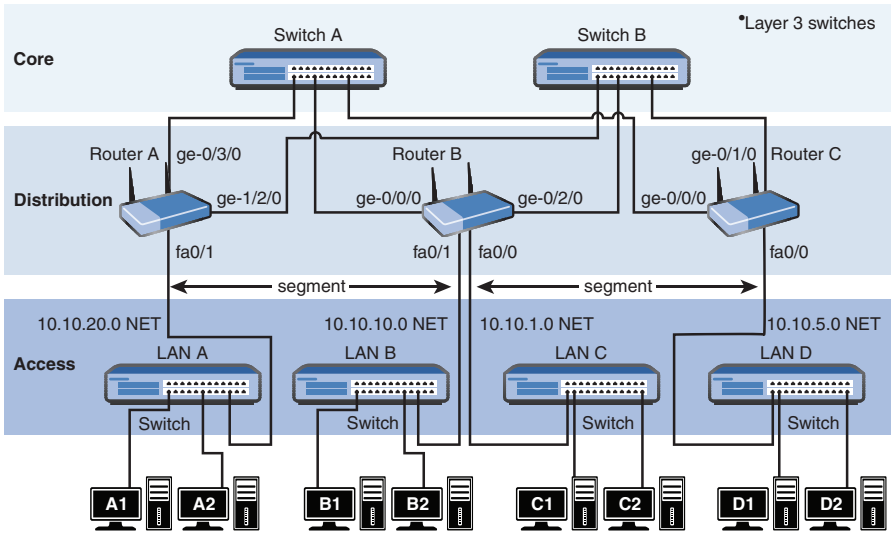


FIGURE 5-28 The core, distribution, and access layers of a network.

Core

The network core usually contains high-end layer 3 switches or routers. The core is the heart, or backbone, of the network. The major portion of a network's data traffic passes through the core. The core must be able to quickly forward data to other parts of the network. Data congestion should be avoided at the core, if possible. This means that unnecessary route policies should be avoided. (An example of a route policy is *traffic filtering,* which limits what traffic can pass from one part of a network to another.) It takes time for a router to examine each data packet, and unnecessary route policies can slow down the network's data traffic.

As mentioned earlier, high-end routers and layer 3 switches are typically selected for use in the core. Of the two, the layer 3 switch is the better choice. A layer 3 switch is essentially a router that uses electronic hardware instead of software to make routing decisions. The advantage of the layer 3 switch is the speed at which it can make a routing decision and establish a network connection.

Another alternative for networking hardware in the core is a layer 2 switch. A layer 2 switch does not make any routing decisions and can quickly make network connection decisions based on the network hardware connected to its ports. The advantage of using a layer 2 switch in the core is cost. The disadvantage is that a layer 2 switch does not route data packets; however, high-speed layer 2 switches are more affordable than high-speed routers and layer 3 switches.

An important design issue in a campus network and the core is redundancy. *Redundancy* is a way to provide a backup route or network connection in the event of a link failure. The core hardware is typically interconnected to all distribution network hardware, as shown in Figure 5-28. The objective is to ensure that data traffic continues for the entire network, even if a core networking device or link fails.

Each layer beyond the core breaks the network into smaller networks, with the final result being a group of networks that are capable of handling the amount of traffic generated. The design should thus incorporate some level of redundancy.

Distribution/Aggregation Layer

The distribution/aggregation layer in a network is the point where the individual LANs connect to the campus network routers or layer 3 switches. Routing and filtering policies are more easily implemented at the distribution layer without having a negative impact on the performance of the network data traffic. Also, the speed of the network data connections at the distribution layer is typically slower than at the core. For example, connection speeds at the core should be the highest possible, such as 1Gbps or 10Gbps, whereas the data speed connections at the distribution layer could be 100Mbps or 1Gbps. Figure 5-28 shows the connections to the access and core layers via the router's Ethernet interfaces.

Access/Edge Layer

The access/edge layer is where the networking devices in a LAN connect together. The network hardware used in this layer is typically a layer 2 switch. Remember that a switch is a good choice because it forwards data packets directly to destination hosts connected to its ports, and network data traffic is not forwarded to all hosts in the network. The exception to this is with a broadcast, where data packets are sent to all hosts connected to the switch.

Traffic Flow

An important networking issue is how data traffic flows in the core, distribution, and access layers of a campus LAN. In Figure 5-28, if computer A1 in LAN A sends data to computer D1 in LAN D, the data is first sent through the switch in LAN A and then to Router A in the distribution layer. Router A then forwards the data to one of the core switches, Switch A or Switch B. Switch A or Switch B then forwards the data to Router C. The data packet is then sent to the destination host in LAN D.

Data Center Architecture

In most networks, the data center is unique in its design architecture. Because the data center houses the critical enterprise servers and storage, with data constantly moving from server to server, it requires a design that can optimize these flows with great speed. Rather than using a three-tiered architecture, a data center network is likely to use a two-tiered architecture, such as the spine and leaf architecture.

At the leaf layer, each server rack has one or more access/edge switches, typically affixed at top-of-rack (ToR). The servers within the rack are connected and aggregate traffic from servers. The leaf layer is then connected to the spine layer, which is the backbone of the network and provides core switching functions. Each leaf switch connects to every spine switch in the network, creating multipath redundancy and load sharing performance.

Traditional data center traffic is from client to server and moves in and out of the data center; this is called north–south traffic. East–west traffic is the traffic flow from server to server or server to storage within the data center network. Today, we are seeing more and more east–west traffic due to the rise in popularity of virtualized and containerized systems in modern data centers. The spine and leaf architecture lends itself very well to this type of traffic flow as it reduces the number of hops between any devices in the data center network to only one.

WAN High-Speed Serial Connections

The term *high-speed* is relative. For large networks, a high-speed connection could be a DS-3 line, which offers 44.7Mbps+, or a connection to a high-speed serial interface (**HSSI**) that supports data rates from 300Kbps to 52Mbps. For small networks, a high-speed serial connection out of the network could be a T1 line (1.544Mbps). The T1 data rate is fast relative to the connection speed provided by a dial-up phone modem, so some users would call this a "high-speed" connection. This section provides an introduction to the data standards currently being used in data communications and the data formats being used. These data standards include T1 to T3, DS-1 to DS-3, E1, E3, and the **OC** (optical carrier) data rates OC-1 to OC-192.

HSSI
High-speed serial interface

OC
Optical carrier

Data Channels

The most common communications data rates for end users are **DS-0 to DS-3** and **T1 to T3**. The T1/DS-1 and T3/DS-3 designations are actually the same data rates, and the terms are used interchangeably. The Bell system T carriers were established in the 1960s primarily for transporting digitized telephone conversations. In the early 1980s, digital signal (**DS**) subscriber lines became available. Table 5-6 lists the data rates for the T/DS carriers. The DS-0 designation is for the base rate of the digital signal lines—basically the data rate of a digitized telephone call.

DS-0 to DS-3; T1 to T3
Common telecommunication data rates

DS
Digital signal

TABLE 5-6 **Data Rates for the T and DS Carriers**

Designation	Data Rate
DS-0	64Kbps (56Kbps)
T1 (DS-1)	1.544Mbps
T2 (DS-2)	6.312Mbps
T3 (DS-3)	44.736Mbps
T4 (DS-4)	274.176Mbps

A T1 line is capable of carrying 24 DS-0 transmissions, or 24 voice channels. Each DS-0 line uses 64Kbps (56Kbps) of data, but the data rate of 56Kbps in parentheses after 64Kbps indicates the rate actually available to the user in some cases. In other words, the DS-0 line does not guarantee that the full 64Kbps line is available. It depends on the connection provided by the telecommunications carrier (**telco**—the local telephone company) and the equipment used to make the connection. When a 56Kbps connection is used, the additional part of the data is for the overhead (synchronization and framing) required for the digital transmission.

Telco
The local telephone company

The data lines are leased from a telecommunications carrier for carrying any type of data, including voice, data, and video. It is important to note that when you lease a T1 (DS-1) line from a telecommunications carrier to provide a data connection from point A to point B, the telecommunications carrier does not provide you with your own point-to-point private physical connection. The telecommunications carrier provides you with sufficient data bandwidth and a switched connection in its system to carry your data traffic to the destination. You data is likely to be multiplexed with hundreds of other T1/DS-1 data channels. For example, in Figure 5-29,

networks A and B each have established and configured a T1 data connection to the **telco cloud**—the switched network the telecommunications carrier uses to get the data to its destination. The data from network A enters the telco cloud and is routed to the destination, network B. The term *cloud* is often used to describe the interconnection of networks via the Internet.

Telco Cloud
The telecommunications carrier's switched network, which is used to transport data to its destination; also, the interconnected networks on the Internet

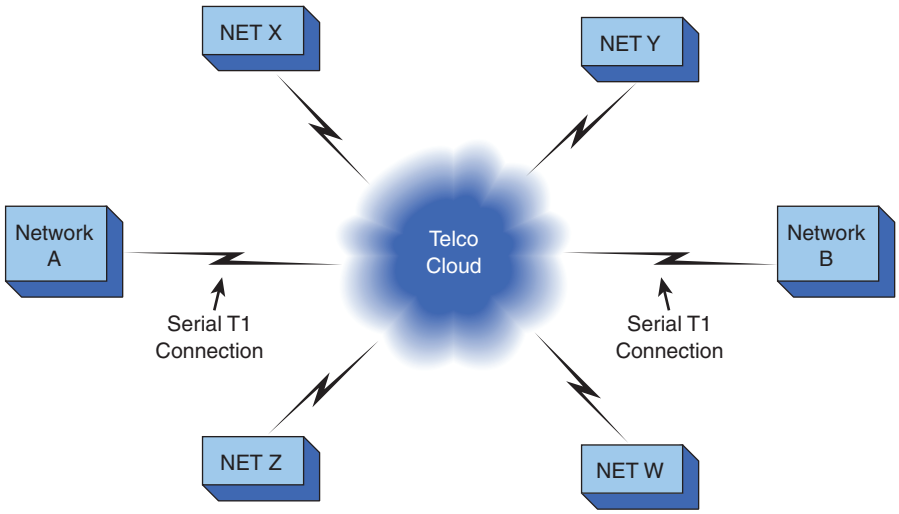


FIGURE 5-29 Transporting data over a T1/DS-1 line to the destination.

Note in Figure 5-29 that networks W, X, Y, and Z also interconnect to the telco cloud. These networks can also be exchanging data packets—possibly over the same lines carrying data to and from networks A and B. In other words, the data from the networks is being **multiplexed** together to reach the destination.

Multiplexed
Combined data packets for transport

Two other designations for data rates are E1 and E3. These designations are used throughout the world where the T-carrier designation is not used, such as Europe. Table 5-7 lists the data rates for E1 and E3.

TABLE 5-7 **E1 and E3 Data Transmission Rates**

Designation	Data Rate
E1	2.048Mbps
E3	34.368Mbps

Point of Presence

The place where the telecommunications carrier brings in service to a facility is called the **point of presence (POP)**. This is where users connect their networks to the telecommunications carrier. The link to the telecommunications carrier can be copper, fiber, digital microwave, or digital satellite. A related term is **line of demarcation**, which refers to the point where ownership of the telecommunications equipment changes from the telecommunications carrier to the customer.

Point of Presence (POP)
The point where a customer connects network data traffic to a telecommunications carrier

Line of Demarcation
The point where ownership of telecommunications equipment changes from the telecommunications carrier to the user

CSU/DSU
Channel service unit/data service unit

A telecommunications carrier requires that a data connection be made through a channel service unit/data service unit (**CSU/DSU**), which provides the hardware data interface to the carrier. This includes adding the framing information for maintaining the data flow, storing performance data, and providing line management. Figure 5-30 provides an example of inserting a CSU/DSU in the connection to the telco cloud.

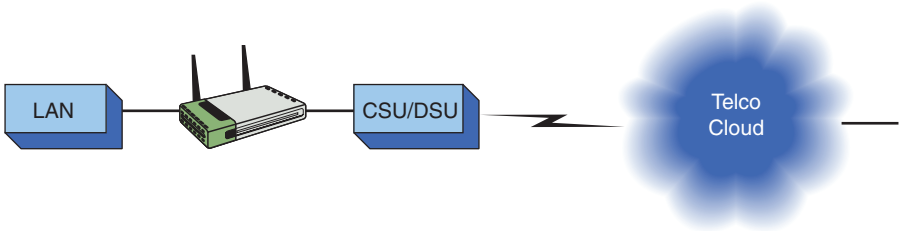


FIGURE 5-30 The placement of a CSU/DSU in the connection to the telco cloud.

The CSU/DSU also has three alarm modes for advising the user of problems on the link: red, yellow, and blue. Table 5-8 defines the conditions for each alarm.

TABLE 5-8 **CSU/DSU Alarms**

Alarm	Description
Red	Indicates that the incoming signal has been corrupted
Yellow	Indicates that a failure in the link has been detected
Blue	Indicates a total loss of incoming signal

HDLC
High-Level Data Link Control

PPP
Point-to-Point Protocol

Two serial line protocols commonly used in wide area networking are High-Level Data Link Control (**HDLC**) and Point-to-Point Protocol (**PPP**). Routers use these two protocols to carry data over a serial line connection, typically over direct connections such as with T1. PPP is used for serial interface connections such as that provided by modems. PPP is a full-duplex protocol and is a subset of the HDLC data encapsulation. Point-to-Point Protocol over Ethernet (PPPoE) enables users on an Ethernet network to connect to a remote site over the telco's customer premises equipment. Figure 5-31 illustrates direct connections using HDLC and PPP.

The routers at each end must be configured with the proper data encapsulation. That is, the data must be properly packaged for transport over a serial telecommunications line. The type of encapsulation depends on the hardware being used to make the connection.

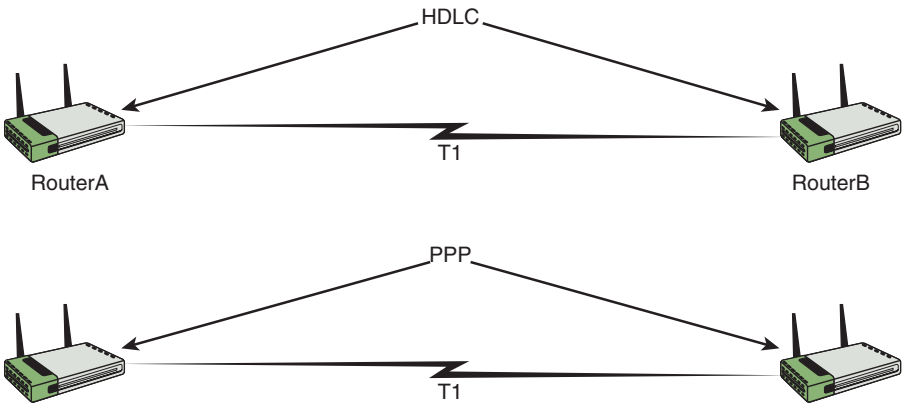


FIGURE 5-31 Examples of direct connections.

The type of network being configured and the equipment being used to make the direct connection determine what format is used for data encapsulation. For example, Cisco routers automatically configure the serial interfaces to run HDLC, but Cisco routers support many data encapsulation formats. HDLC data encapsulation formats are implemented differently by some vendors, and sometimes some equipment is not interoperable with other equipment, even if all the equipment has specified the HDLC encapsulation. In such a case, another encapsulation format, such as PPP, can be used to make a direct connection. Using incorrect encapsulation at either end will result in encapsulation errors and no connection.

Metro Optical Ethernet/Carrier Ethernet

The number of Internet users is growing at a staggering rate. One key factor that brings people to the Internet is its application. The systems have evolved greatly from the days of stand-alone applications running on computers to the days of real-time and collaborative applications that connect via the Internet. Many applications on the Internet are available for people to download and add to their computer systems. Coupled with the wealth of applications is the ever-increasing need for more bandwidth. It is no longer sufficient for some of these applications to run on lower-bandwidth modem connections. In a business environment, even T1 speed (1.544Mbps) is not adequate to accommodate the number of concurrent users and the increased data demands of many applications. As discussed in the previous sections, there have been many developments on both the commercial and residential sides (for example, fiber-to-the-business [FTTB]) to bring more bandwidth to consumers.

What every network infrastructure has in common is the Ethernet infrastructure. The design might be different, the equipment might be from different vendors, and the backbone speeds might not be the same; however, everyone is running the same Ethernet-based infrastructure. The IT world has invested a lot of time and money in improving Ethernet speeds. Ethernet has come a long way from the old 10BASE5 technology running over coaxial (coax) cable to the high-speed 10 Gigabit fiber-optic networks we have today. Ethernet is a standard network protocol used to connect virtually all networking devices. So, wouldn't it be logical to extend the

Metro Optical Ethernet (MOE)
An extension of the Ethernet infrastructure via optical technologies beyond the internal network infrastructure

Carrier Ethernet
An extension of the Ethernet infrastructure that covers much more than just a metropolitan area

Ethernet infrastructure beyond the internal network infrastructure? Why not use Ethernet as a WAN connection? **Metro Optical Ethernet (MOE)** was originally conceived to connect subscribers and businesses in metropolitan area networks (MANs). Metro Optical Ethernet has now evolved to **Carrier Ethernet**, which covers much more than just a metropolitan area.

Metro Ethernet and Carrier Ethernet specifications are defined by a nonprofit organization called the **Metro Ethernet Forum (MEF)**. Ethernet service is provided by the Carrier Ethernet provider and is delivered at the **user–network interface (UNI)**, where the customer equipment (CE) attaches to the network. The MEF defines the UNI as the demarcation point between the customer equipment and the service provider. Sometimes, it is referred to as a *subscriber site*. Generally, the UNI is an Ethernet physical interface operating at 10Mbps, 100Mbps, 1Gbps, or 10Gbps.

Metro Ethernet Forum (MEF)
A nonprofit organization that defines Metro/Carrier Ethernet specifications

User–Network Interface (UNI)
The demarcation point between customer equipment and a service provider

Note

In the context of the MEF specifications, the terms *Metro Ethernet* and *Carrier Ethernet* can be used interchangeably. The term *Carrier Ethernet* is used for the rest of this chapter.

The MEF develops the **Ethernet Service Definition** framework, which defines the Ethernet service types. These services are based on the types of **Ethernet virtual connections (EVCs)**. The MEF defines an EVC as "an association of two or more UNIs" which essentially creates a logical path that connects two or more subscriber sites. Because the UNI is a physical connection and the EVC is a logical connection, a UNI might contain more than one EVC, as illustrated in Figure 5-32.

Ethernet Service Definition
An MEF framework that defines the Ethernet service types

Ethernet Virtual Connection (EVC)
An association of two or more UNIs that essentially creates a logical path that connects two or more subscriber sites

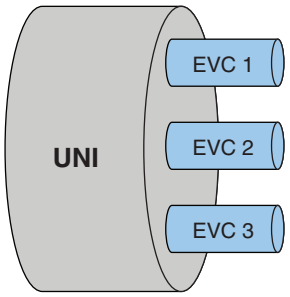


FIGURE 5-32 The UNI/EVC relationship.

Ethernet Service Types

Much like a Frame Relay or ATM permanent virtual circuit (PVC), an EVC creates protection and data privacy for the subscriber sites on the same EVC and prevents data transfer between subscriber sites that are not part of the same EVC. From the EVC types, the MEF derived the following three Ethernet service types:

- **Ethernet line service (E-Line)**—Point-to-point Ethernet service based on a point-to-point EVC

- **Ethernet LAN service (E-LAN)**—Multipoint-to-multipoint service based on a multipoint-to-multipoint EVC
- **Ethernet tree service (E-Tree)**—Point-to-multipoint service based on a routed-multipoint EVC

The **E-Line service type** provides a point-to-point Ethernet virtual connection between two UNIs or subscriber sites, as shown in Figure 5-33. It is analogous to a dedicated leased line or a Frame Relay PVC. This type of Carrier Ethernet service is the most popular one of all due to its simplicity. Internet service is usually provided using the E-Line service type.

E-Line Service Type (E-Line)
A service type that provides a point-to-point Ethernet virtual connection between two UNIs

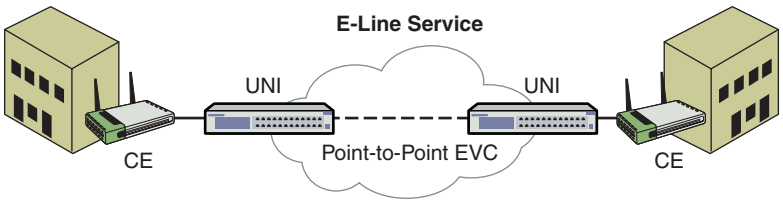


FIGURE 5-33 E-Line service.

The **E-LAN service type** can provide connectivity to two or more subscriber sites by using the same EVC, as shown in Figure 5-34. This type of service is more advantageous when adding new subscriber sites as they can be added to the same multipoint EVC without disturbing the existing subscriber sites on the same EVC. A transparent LAN service is a well-known service offered by the E-LAN service type. From the subscriber's standpoint, it appears as though everyone is on the same LAN.

E-LAN Service Type (E-LAN)
A service type that provides connectivity to two or more subscriber sites using the same EVC

The **E-Tree service type** provides a hub-and-spoke environment or a root-and-leaf environment. The E-Tree provides traffic separation between subscriber sites. Traffic from any leaf can only be sent to and received from a root. Traffic can never be forwarded directly to other leaves in the EVC. This service type is geared toward ISPs that want to provide multicast-type service such as video on demand. Figure 5-35 illustrates the E-Tree service type.

E-Tree Service Type (E-Tree)
A service type that provides a hub-and-spoke environment or a root-and-leaf environment

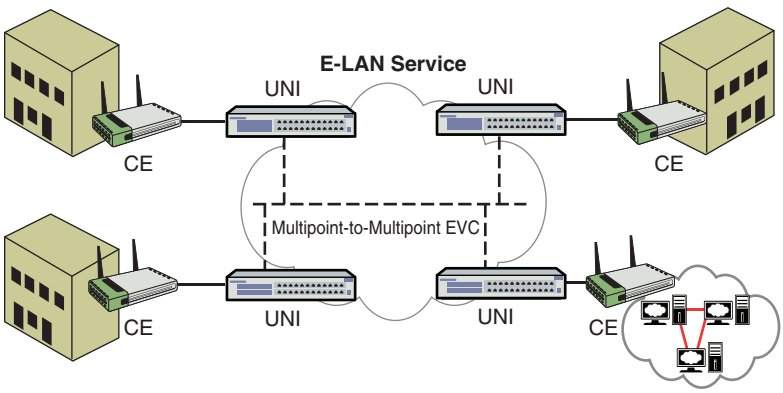


FIGURE 5-34 E-LAN service.

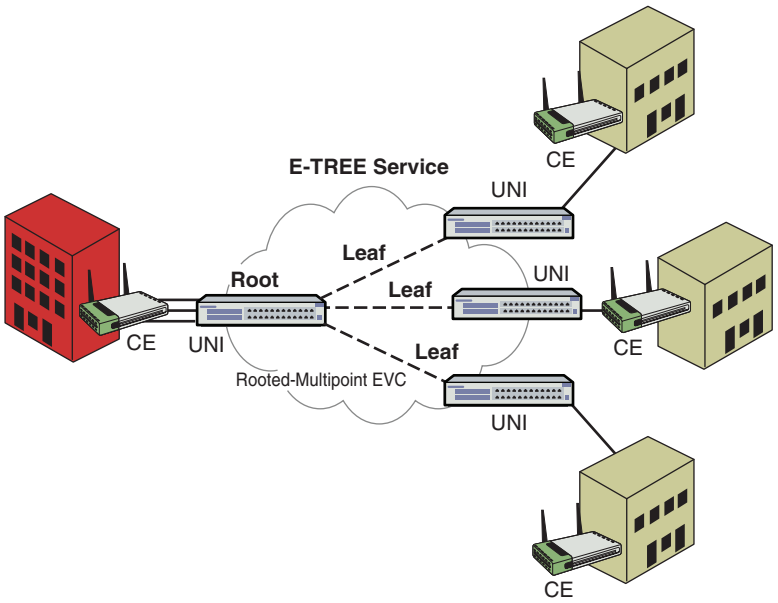


FIGURE 5-35 E-Tree service.

Service Attributes

Many service attributes define the capabilities of the previously mentioned Ethernet service types. These attributes are under constant revision by the MEF. This section details some of the attributes that are most pertinent to typical IT users.

The bandwidth profile service attribute is a commonly used attribute. As a matter of fact, the first thing a subscriber must do when ordering the Carrier Ethernet service is to choose the bandwidth. The bandwidth profile service attribute is either applied at the UNI or to an EVC to limit the rate at which the Ethernet frames can transverse the applied point. Even though the UNI might be delivered as a 1Gbps physical connection, the subscriber might choose to subscribe to only 500Mbps worth of bandwidth. Traffic rate limiting is needed in such situations. The bandwidth profile service attribute uses the following parameters to for traffic rate limiting:

- **Committed information rate (CIR):** This is the same parameter used in Frame Relay. It is an average rate measured in bits per second that is used to guarantee the bandwidth the network must deliver.
- **Committed burst size (CBS):** This is the traffic size, in kilobytes, that is allowed to burst and is not discarded or shaped by the profile.
- **Excess information rate (EIR):** This is an average rate parameter, in bits per second, that is used to allow traffic greater than the CIR to traverse and may deliver it when the network is not congested.
- **Excess burst size (EBS):** This is the burstable size allowed when the traffic is in the EIR mode.

Another useful service attribute is VLAN tag preservations. In a typical campus infrastructure, VLANs are used to separate physical segments into many logical segments. These VLANs reside locally. When connecting multiple campuses across the WAN, the VLANs cannot be extended; the separation has to be done at the higher OSI layer. It is typically carried out as different routed networks. With a Carrier Ethernet network, LAN extension is no longer an issue. The VLAN tag preservations service attribute can be used to carry out the mission. With this attribute, all Ethernet frames received from a subscriber traverse untouched across the EVC. Therefore, when an 802.1Q VLAN tag is provisioned and applied at the customer equipment (CE), its customer edge VLAN ID (CE-VLAN ID) is preserved.

Section 5-7 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.
This section discusses Metro Optical Ethernet (MOE), an extension of the Ethernet infrastructure via optical technologies beyond the internal network infrastructure. This section also presents the concept of a demarcation point.

1.7 Explain basic corporate and datacenter network architecture.
This section presents a three-tiered design that has core, distribution, and access layers.

1.8 Summarize cloud concepts and connectivity options.
This section presents the telco cloud, which is the telecommunications carrier's switched network, used to transport data to its destination. Telco cloud also refers to the interconnected networks on the Internet.

Test Your Knowledge

1. What is the data rate of a DS-3 line?
   a. 44,735Mbps
   b. 44.736Mbps
   c. 44.735Mbps
   d. 1.544Mbps
2. Which alarm indicates a total loss of the incoming signal on a CSU/DSU?
   a. Red
   b. Blue
   c. Yellow
   d. All of these answers are correct.

3. How does Carrier Ethernet differ from Metro Ethernet?

   a. They are exactly the same.
   b. Carrier Ethernet covers much more than just a metropolitan area.
   c. Metro Ethernet covers much more than just a metropolitan area.
   d. None of these answers are correct.

4. Which service type can provide connectivity to two or more subscriber sites using the same EVC?

   a. E-Tree
   b. E-Line
   c. E-LAN
   d. All of these answers are correct.

SUMMARY

This chapter establishes how LANs are interconnected. It discusses LAN architecture and data center architecture. This chapter discusses internetworking hardware such as bridges, switches, and routers and presents examples of using these technologies. It also discusses various WAN technologies.

This chapter presents a technique for internetworking LANs using routers. In addition, it defines the purpose of a router and its hardware interface. This chapter also demonstrates the use of switches and hubs to connect to routers and explains the purpose of a gateway and the concept of a network segment.

You should understand the following concepts from this chapter:

- How bridges are used to interconnect separate LANs
- How a switch is used in a network and why the switch improves network performance
- The various connections on a router interface
- How a router is used to interconnect LANs
- The purpose of a gateway in a computer network
- The concept of a network segment
- The concept of auto-negotiation
- The steps involved in establishing a console connection

QUESTIONS AND PROBLEMS

Section 5-2

1. What is a bridge?

   A bridge is a layer 2 device used to interconnect LANs.

2. Define segment.

   A segment is a section of a network separated by bridges, switches, and routers.

3. What information is stored in a bridge table?

   A bridge table stores the MAC addresses and port locations for hosts connected to the bridge ports.

4. What is an association on a bridge, and how is it used?

   Association indicates that the destination address is for one of the networking devices connected to one of its ports. If an association is detected, the data packet is forwarded to the port.

5. What term is used for excessive broadcasts on a network?

   Broadcast storm

6. What command is used on a computer to view the contents of the ARP cache?

   arp -a

7. What does an empty ARP cache indicate?

   All of the ARP entries have expired.

8. Why do entries in a bridge table have a limited lifetime?

   Each MAC address entry in a bridge table remains active as long as there is periodic data traffic activity. The entries expire so that the table lists only the MAC addresses for the networking devices that have been active in the network recently.

9. Which of the following are advantages of using a bridge to interconnect LANs? (Select all that apply.)

   a. Works best in low-traffic areas
   b. Relatively inexpensive
   c. Can be used to route data traffic
   d. Easy to install
   e. Reduces collision domains

Section 5-3

10. When a network switch uses a MAC or Ethernet address for making decisions related to forwarding data packets, at which layer of the OSI model does it operate?

    Layer 2, the data link layer

11. Which of the following is another name for a switch?

    a. Multiport repeater
    b. Multiport bridge
    c. Multiport router
    d. Multiport hub

12. How does a switch provide a link with minimal collisions?

    Only the two computers or networking devices that established the link communicate on the channel.

13. The link for a switch connection is isolated from other data traffic except for what type of messages?

    Broadcast and multicast

14. What data traffic is sent across a network when a computer pings another computer and a hub is used to interconnect the computers?

    Line 1 ARP request

    Line 2 ARP reply

    Line 3 Echo request/Echo reply (repeats 4 times)

    …

    …

    Line 10

15. Explain what data traffic is seen by computer 3 when computer 1 pings computer 2 in a LAN if a switch is used to interconnect the computers.

    Line 1 ARP request

16. Define dynamic assignment on a switch.

    Assignment of a MAC address to a port when the device is connected

17. Define aging time on a switch.

    The length of the time a MAC address remains assigned to a port

18. Explain how a switch learns MAC addresses and where a switch stores the addresses.

    A switch learns the MAC addresses of the connected networking devices by extracting the MAC address information from the headers of transmitted Ethernet data packets. The switch maps an extracted MAC address to the port where the data packet came in. This information is stored in content-addressable memory (CAM).

19. What happens if a MAC address is not stored in CAM on a switch?

    Flooding occurs: The packet is transmitted out all switch ports except for the port where the packet was received.

20. Which two modes does a switch use to forward frames?

    Store-and-forward and cut-through

21. Which switch mode offers minimum latency?

    Fast-forward mode offers the minimum switch latency. The received data packet is sent to the destination as soon as the destination MAC address is extracted.

22. What is an error threshold, and which switch mode is it associated with?

    Cut-through mode is used until an error threshold (errors in the data packets) has been exceeded. The switch mode changes from cut-through to store-and-forward after the error threshold has been exceeded.

23. Explain the difference between store-and-forward and the cut-through modes on a switch.

In store-and-forward mode, the entire frame of data is received before any decision is made regarding forwarding the data packet to its destination. An advantage of store-and-forward mode is that the switch checks the data packet for errors before it is sent on to the destination. A disadvantage is that lengthy data packets take a longer time to exit the switch and be sent to the destination.

In cut-through mode, a data packet is forwarded to the destination as soon as the destination MAC address has been read. This minimizes the switch latency; however, no error detection is provided by the switch.

24. How does a layer 3 switch differ from a layer 2 switch?

Layer 3 switches work at layer 2 but also work at the network layer (layer 3) of the OSI model and use IP addressing for making decisions to route a data packet in the best direction. The major difference is that the packet switching in basic routers is handled by a programmed microprocessor. A layer 3 switch uses application-specific integrated circuit (ASIC) hardware to handle packet switching. The advantage of using hardware to handle the packet switching is a significant reduction in processing time compared to using software.

25. What is meant by the term wire-speed routing?

Data packets are processed as quickly as they arrive.

Section 5-4

26. A router uses the network address on a data packet for what purpose?

To make routing decisions about the router interface to which to forward the data

27. What is a logical address?

It is the IP address location of the network and the address location of the host in the network.

28. The physical connection where a router connects to a network is called the ____.

    a. router port
    b. network port
    c. network interface
    d. router interface

29. The connection to a router's console input is typically which of the following? (Select all that apply.)

    a. RS-232
    b. RJ-45
    c. DB-9
    d. RJ-11

30. What does AUI stand for?

    a. Auxiliary unit input
    b. Attachment unit interconnect
    c. Auxiliary unit interface
    d. Attachment unit interface

31. The AUI port on a router connects to which networking protocol?

    a. 100BASE-T
    b. 10BASE-T
    c. Token Ring
    d. Ethernet

Section 5-5

32. What is a rollover cable?

    A flat cable that reverses the pin number assignments on each end of the cable.

    1—8

    …

    …

    8—1

33. What values are used when configuring HyperTerminal for connecting to a Cisco router's console port?

    9600 bps

    8 data bits

    No parity

    1 stop bit

    No flow control

Section 5-6

34. Define enterprise network.

    A network used by a large company

35. What router interface is most commonly used to interconnect LANs in a campus network?

    a. Serial
    b. Console port
    c. Ethernet
    d. ATM

36. Serial interfaces on a router are typically used for which of the following?

    a. To interconnect routers
    b. To interconnect hubs
    c. To connect to communication carriers
    d. To connect to auxiliary ports

37. The designation E0 indicates ____.

    a. Ethernet port 0
    b. Ethernet input
    c. External port 0
    d. Exit port 0

38. Routing tables on a router keep track of ____.

    a. port assignments
    b. MAC address assignments
    c. gateway addresses of LANs
    d. routes to use for forwarding data to its destination

39. By convention, what is the name of serial port 0 on a router?

    a. S0
    b. System 0
    c. Serial interface 0
    d. Serial AUI 0

40. Define the term gateway.

    A networking device that enables hosts in a LAN to connect to networks and hosts outside the LAN

Section 5-7

41. What networking equipment is usually found in the core of a campus network?

    High-end layer 3 switches or routers

42. How are route policies applied in the core?

    Route policies should be avoided in the core because it takes time to examine each data packet.

43. What is the advantage of using a layer 3 switch in the core of the campus network?

    Speed

44. Can a layer 2 switch be used in the core of a campus network? Why or why not?

    Yes, a layer 2 switch can be used. It may be used for its cost advantage.

45. What is the function of the distribution layer in a campus network?

    The distribution layer is the point where the LANs connect to the campus network routers or layer 3 switches.

46. Can routing policies be implemented in the distribution layer? Why or why not?

    Yes, routing policies can be implemented without degrading the performance of the network. The networking devices in the distribution layer typically run at slower data speeds than the core.

47. What is the purpose of the access layer?

    The access layer is where the networking devices in a LAN connect together.

48. The campus network servers are typically located in what layer?

    The access layer

49. Why are routers typically not interconnected at the distribution layer?

    Interconnecting separate networks at the distribution layer can lead to network stability problems.

50. What is the name for the part of the campus network that carries the bulk of the routed data traffic?

    The campus backbone

51. List three criteria for selecting the network media. Which is the final decision factor?

    Data speed

    Distance

    Budget

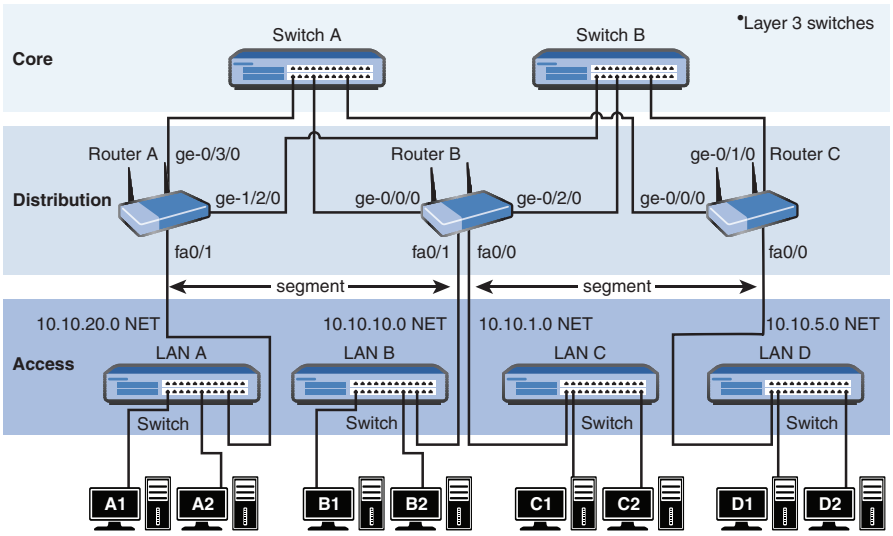
    The available budget is always the final decision factor.

52. Which media is the best choice in a campus network?

    Fiber has the advantage because it will always be capable of carrying more data bandwidth than twisted-pair.

53. The following figure illustrates how data flows from a computer in LAN B to a computer in LAN C. Assume that Switch A has been configured to be the preferred switch. Describe the data flow.

    The data will flow to Router B (FA0/0) and then the data will then exit Router B (FA0/1) and will travel to LAN C.



54. What is the data rate of a DS-3 line?

    44.736 Mbps

55. What is the data rate of a T1 line?

    1.544 Mbps

56. Define telco cloud.

    The telecommunications carrier switched network used to transport data to its destination; or the interconnected networks on the Internet

57. Define fractional T1.

    This term indicates that only a portion of the T1 bandwidth is being used.

58. Define point of presence.

    POP is the point where the customer connects network data traffic to the communications carrier.

59. Explain the difference between line of demarcation and point of presence.

    Line of demarcation is the point where ownership of communications equipment changes.

    Point of presence is the connection point to the communications carrier.

60. A CSU/DSU has a blue alarm. What does this indicate?

    A total loss of the incoming signal.

61. What is Metro Optical Ethernet?

    An extension of the Ethernet infrastructure beyond the internal network infrastructure

62. How does Carrier Ethernet differ from Metro Optical Ethernet?

    They are basically the same except Carrier Ethernet covers more than just the metropolitan area.

63. What is an Ethernet virtual connection?

    An EVC is defined by the MEF as "an association of two or more UNIs" which essentially creates a logical path that connects two or more subscriber sites.

64. Which type of Carrier Ethernet service is the most popular due to its simplicity?

    The E-Line service type

65. What is a committed information rate (CIR)?

    A CIR is used to guarantee the bandwidth a network must deliver.

Critical Thinking

66. How can a network administrator use the OSI model to isolate a network problem?

    The student should discuss how the network administrator looks for problems at different layers using the **ping** command, Telnet, and so on.

67. Why is auto-negotiation not recommended for use in critical network data paths?

    The data speeds should be fixed for critical data paths. You don't want to take the chance of the networking equipment negotiating a slower speed.

68. What happens if the local network devices do not have a local ARP cache?

    The broadcasts will increase dramatically, depending on the size of the network. Broadcasts lead to network degradation. Also, every network device will have to process more broadcast messages, which requires CPU power.

Certification Questions

69. Which of the following best defines bridge table?

    a. A list of MAC addresses and port locations for hosts connected to the bridge ports
    b. A list of IP addresses and port locations for hosts connected to the bridge ports
    c. A list of IP addresses and port locations for hosts connected to the hub ports
    d. A list of MAC addresses and port locations for hosts connected to the hub ports

70. Which of the following best defines aging time?

    a. The length of time a MAC address remains assigned to a port
    b. The length of time an IP address remains assigned to a port
    c. The length of time a MAC address remains assigned to a hub
    d. The length of time an IP address remains assigned to a hub

71. Dynamic assignment on a switch implies which of the following?

    a. MAC addresses are assigned to a port when a host is connected.
    b. IP addresses are assigned to a port when a host is connected.
    c. MAC addresses are assigned to a switch when a host is connected.
    d. IP addresses are assigned to a switch when a host is connected.

72. Which of the following terms is used for a MAC address being manually assigned?

    a. Dynamic assignment
    b. ARP assignment
    c. DHCP assignment
    d. Static assignment

73. What is the purpose of a secure address on a switch?

    a. The switch port will use port discovery to assign a MAC address to the port.
    b. The switch port will automatically disable itself if a device with a different MAC address connects to the port.
    c. The switch port will use a different MAC address than the one connected to the port.
    d. The switch can determine what networking devices have selectable IP addresses.

74. What is the length of time an IP address is assigned to a switch port called?

    a. Delay time
    b. Enable time
    c. Aging time
    d. Access time

75. Which of the following is a table of MAC addresses and port mapping used by a switch to identify connected network devices?

    a. CAM
    b. ARP
    c. ARP-A
    d. **ipconfig /all**

76. Which of the following best defines store-and-forward relative to switch operation?

    a. The frame is stored in CAM and then forwarded to the source for confirmation.

    b. The frame is stored in CAM and then forwarded to the destination for confirmation.

    c. The header is received before being forwarded to the destination.

    d. The entire frame is received before a decision is made regarding forwarding to the destination.

77. In which switch mode is a data packet forwarded to the destination as soon as the MAC address has been read?

    a. Store-and-forward

    b. Adaptive fast-forward

    c. Cut-through

    d. Fast-forward

78. Which switch mode offers the minimum switch latency?

    a. Cut-through

    b. Fast-forward

    c. Store-and-forward

    d. Adaptive cut-through

6
CHAPTER

TCP/IP

Chapter Outline

6-1 Introduction
6-2 The TCP/IP Layers
6-3 Number Conversion
6-4 IPv4 Addressing
6-5 Subnet Masks: Subnetting and Supernetting
6-6 Supernetting, CIDR Blocks, and VLSM
6-7 IPv6 Addressing
Summary
Questions and Problems

Objectives

- Develop an understanding of the four layers of the TCP/IP model
- Define how a TCP connection is established, maintained, and terminated
- Investigate the properties of the UDP connectionless protocol
- Define the five classes of IPv4 addresses
- Investigate the properties of basic number conversion
- Define the purpose of subnet masking
- Investigate the implementation of CIDR blocks and supernetting
- Apply subnet masking concepts to allocate space for hosts in a subnet
- Define the structure of IPv6

Key Terms

NCP
ARPANET
well-known ports
ICANN
transport layer protocols
TCP
connection-oriented protocol
SYN, SYN ACK, ACK
UDP
Internet layer
Internet Protocol (IP)
ARP
IGMP
multicasting
multicast address
network interface layer
hex
IPv4
Classes A, B, C, D, and E
RIRs
ARIN
non-Internet-routable IP address
classful
subnet mask
subnetting
supernetting
CIDR
CIDR block
VLSM
Subnet
Supernet
IPv6
IPng
full IPv6 address
unicast address
multicast address
anycast address
link-local address
6to4 prefix
stateless address autoconfiguration (SLAAC)

Transmission Control Protocol/Internet Protocol (TCP/IP) is the protocol suite used for communications between hosts in most local networks and on the Internet. TCP/IP can be used to enable network communications in LANs, campus networks, and wide area networks (WANs) as long as the hosts support the protocol. TCP/IP is widely supported and is included in operating systems such as Windows 10, macOS, Linux, and Unix.

NCP
Network Control Protocol, a protocol developed by the Defense Advanced Research Projects Agency to provide a way to network the computers of government researchers

Network Control Protocol (**NCP**) was developed by the Defense Advanced Research Projects Agency (DARPA) to provide a way to network the computers of government researchers. The DARPA-funded initiative forced the use of a standard networking protocol by all defense contractors.

6-1 INTRODUCTION

This chapter examines TCP/IP. It includes an overview of the layers of the TCP/IP model and the very important issue of subnet masks. Most students already understand the basics of number conversion, but a review is presented in Section 6-3 just in case. Sections 6-5 and 6-6 on subnet masks and CIDR blocks are probably the most challenging sections in the chapter. Section 6-5 shows students how to create subnets and the proper subnet masks for a network. It is important for students to understand subnet mask concepts because they are used in the remainder of the book.

Transmission Control Protocol (TCP) was first proposed in 1974 in a paper by Vint Cerf and Bob Kahn. The suite of protocols called TCP/IP was introduced in 1978. In 1983, TCP/IP replaced NCP as the standard networking protocol used by the Advanced Research Projects Agency Network (**ARPANET**), considered the predecessor to today's Internet.

ARPANET
Advanced Research Projects Agency Network, the predecessor to today's Internet

This chapter examines the fundamentals of the TCP/IP protocol suite. The relationship of the TCP/IP model to the OSI model is presented in Section 6-2, "The TCP/IP Layers." That section also examines the layers of the TCP/IP model: the application layer, the transport layer, the Internet layer, and the network interface layer. Section 6-3, "Number Conversion," discusses the numbering systems used in TCP/IP networks, including examples of converting decimal, hexadecimal, and binary numbers. The fundamentals of IP addressing are reintroduced in Section 6-4, "IPv4 Addressing." (The concept of IP addressing was first introduced in Chapter 1, "Introduction to Computer Networks.") Section 6-4 examines the 32-bit structure of IPv4 addressing, which is the version predominantly used on the Internet today. This section goes into detail about the role and features of IP addressing in computer networks.

The concept of subnet masking is examined in Section 6-5, "Subnet Masks: Subnetting and Supernetting." This section presents many examples of calculating and applying subnet masks to networks. The material presented will give you the knowledge base you need to master subnet masking–related concepts that are presented later in the book. The fundamentals of CIDR blocks and supernetting are examined in Section 6-6, "Supernetting, CIDR Blocks, and VLSM." The chapter concludes with Section 6-7, "IPv6 Addressing," which provides an overview of the newer IP addressing standard, IPv6.

Table 6-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 6-1 **Chapter 6 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.1	Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.	6-2
1.2	Explain the characteristics of network topologies and network types.	6-2
1.3	Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	6-2
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes.	6-3, 6-4, 6-5, 6-6, 6-7
1.5	Explain common ports and protocols, their application, and encrypted alternatives.	6-2, 6-4, 6-7
1.6	Explain the use and purpose of network services.	6-2, 6-7
1.7	Explain basic corporate and datacenter network architecture.	6-2
1.8	Summarize cloud concepts and connectivity options.	6-4, 6-7
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	6-2, 6-5
2.3	Given a scenario, configure and deploy common Ethernet switching features.	6-2
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	6-2
4.0	**Network Security**	
4.3	Given a scenario, apply network hardening techniques.	6-7
4.4	Compare and contrast remote access methods and security implications.	6-2
4.5	Explain the importance of physical security.	6-7
5.0	**Network Troubleshooting**	
5.3	Given a scenario, use the appropriate network software tools and commands.	6-2, 6-3, 6-5

6-2 THE TCP/IP LAYERS

This section examines the four layers of the TCP/IP model (network interface, Internet, transport, and application). Each layer is examined in sufficient detail to provide students with a good understanding of TCP/IP. This section examines many TCP/IP concepts, such as the TCP connection-oriented and UDP connectionless protocols. It is very important that students understand how a TCP connection is established. This process is illustrated with block diagrams and with screenshots of network protocol analyzer software. Many examples of the TCP/IP protocols are examined, and it is important to ensure that students understand the purpose of each layer of the TCP/IP model.

This section examines the various protocol types, as well as the four layers of the TCP/IP model: the application, transport, Internet, and network interface layers (see Table 6-2). The TCP/IP protocol was established in 1978, prior to the final release of the OSI model (refer to Chapter 1); the four layers of the TCP/IP model correlate with the seven layers of the OSI model as shown in Figure 6-1.

TABLE 6-2 **The Four Layers of the TCP/IP Model**

Layer	Purpose of the Layer
Application layer	Defines the applications used to process requests and which ports and sockets are used
Transport layer	Defines the type of connection established between hosts and how acknowledgments are sent
Internet layer	Defines the protocols used for addressing and routing the data packets
Network interface layer	Defines how a host connects to the network

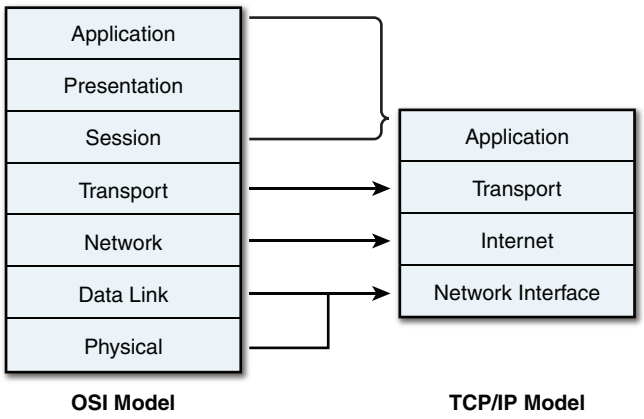


FIGURE 6-1 The layers of the TCP/IP model and their relationships to the OSI model.

The Application Layer

The top level of the TCP/IP stack is the *application* layer. This layer is used to process requests from hosts and to ensure that connections are made to appropriate ports. A *port* is basically an address used to direct data to the proper destination application.

There are 65,536 possible TCP/UDP ports. Ports 1–1023 are called **well-known ports**, or *reserved* ports. These ports are reserved by Internet Corporation for Assigned Names and Numbers (**ICANN**). Ports 1024–49,151 are called *registered* ports, and they are registered with ICANN. Ports 49,152–65,535 are called *dynamic* or *private* ports. Table 6-3 summarizes the port numbers.

Well-known Ports
Ports reserved by ICANN

ICANN
Internet Corporation for Assigned Names and Numbers

TABLE 6-3 **Port Number Assignments**

Port Numbers	Description
1–1023	Well-known ports
1024–49,151	Registered ports
49,152–65,535	Private ports

Examples of well-known ports include TCP port 80 (for HTTP), TCP port 443 (for HTTPS), and TCP port 22 (for SSH). Applications use these port numbers when communicating with other applications, as illustrated in Figure 6-2. In this figure, Host B is passing to Host A data that is destined for TCP port 80 (HTTP). Hypertext Transfer Protocol (HTTP) is used for transferring non-secure web-based documents to a web browser such as Internet Explorer or Mozilla Firefox. Host A receives the packet and passes the application up to the port 80 application. Table 6-4 lists some popular applications and their port numbers for TCP/IP, including FTP, SSH, SMTP, DNS, DHCP, HTTP, and HTTPS.

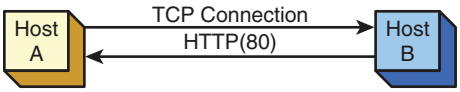


FIGURE 6-2 An example of two hosts connected for a TCP transmission.

TABLE 6-4 **Common Applications and Their Port Numbers**

Transport Protocol	Port Number(s)	Application	Description
TCP	20 (data port) 21 (command/ control port)	FTP	File Transfer Protocol
TCP	22	SSH	Secure Shell
TCP	23	Telnet	Virtual terminal connection
TCP	25	SMTP	Simple Mail Transfer Protocol
TCP/UDP	53	DNS	Domain Name System
UDP	67, 68	(BOOTP-Server)	Dynamic Host Configuration Protocol (DHCP)

Transport Protocol	Port Number(s)	Application	Description
UDP	69	TFTP	Trivial File Transfer Protocol
TCP/UDP	80	HTTP	Hypertext Transfer Protocol
TCP	110	POP3	Post Office Protocol
TCP	123	NTP	Network Time Protocol
UDP TCP	137, 138 139	NetBIOS	Network Basic Input/Output System
TCP	143	IMAP	Internet Message Access Protocol
UDP	161	SNMP	Simple Network Management Protocol
TCP/UDP	389	LDAP	Lightweight Directory Access Protocol
TCP	443	HTTPS	Secure HTTP
TCP	445	SMB	Server Message Block
UDP	514		Syslog
TCP/UDP	636	LDAP over SSL	Lightweight Directory Access Protocol over Secure Sockets Layer
TCP	993	IMAP over SSL	Secure IMAP Email
TCP	995	POP3 over SSL	Secure POP3 Email
TCP	1433	SQL Server	MS SQL Server Database Connection
TCP	1521	Oracle/SQLnet	ODBC connection
UDP	1701	L2TP	Layer 2 Tunneling Protocol
TCP	1720	H.323/Q.931	Voice over IP
TCP/UDP	1723	PPTP	Point-to-Point Tunneling Protocol
TCP/UDP	2427/2727	MGCP	Media Gateway Control Protocol
TCP	3303	MySQL Server	MySQL Server Database Connection
TCP/UDP	3389	RDP	Remote Desktop Protocol
UDP	5004/5005	RTP	Real-Time Transport Protocol
TCP/UDP	5060/5061	SIP	Session Initiation Protocol (which is involved in making and delivering phone calls)
TCP/UDP	5900	VNC	Virtual Network Computing for Remote Desktop

Transport Layer Protocol
A type of protocol that defines the type of connection established between hosts and how acknowledgments are sent

Note

For a complete list of ports, see www.iana.org/assignments/port-numbers.

The Transport Layer

The **transport layer protocols** in TCP/IP are very important in establishing network connections, managing the delivery of data between source and destination hosts, and terminating data connections. There are two transport protocols within the

TCP/IP transport layer, TCP and UDP. Transmission Control Protocol (**TCP**) is a **connection-oriented protocol**, which means it establishes network connections, manages data transfer, and terminates connections. TCP establishes a set of rules or guidelines for establishing connections. TCP verifies the delivery of data packets through the network and includes support for error checking and recovery of lost data. TCP then specifies a procedure for terminating the network connection. The TCP header is shown in Figure 6-3.

TCP
Transmission Control Protocol, a connection-oriented protocol that establishes a set of rules or guidelines for establishing connections and verifies the delivery of data packets through the network

Connection-Oriented Protocol
A type of protocol that establishes network connections, manages the delivery of data, and terminates connections

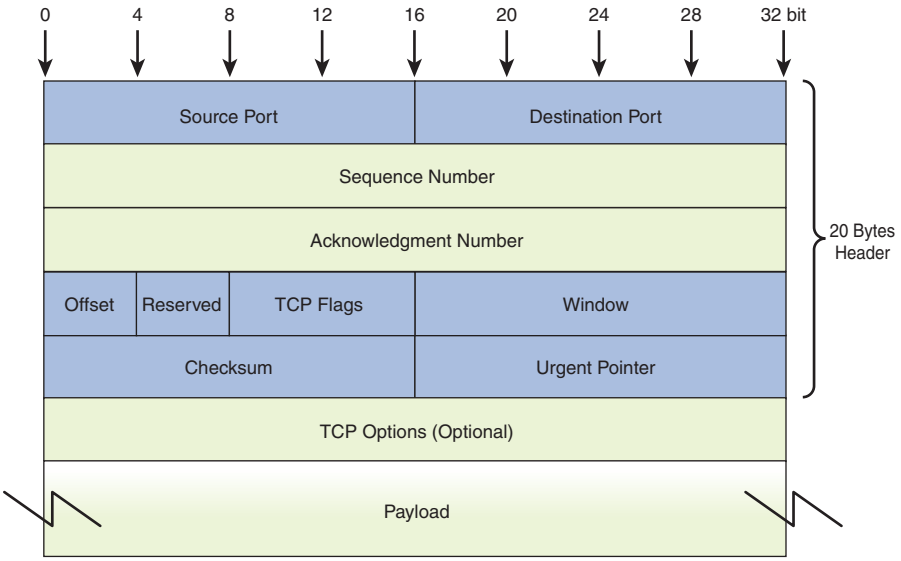


FIGURE 6-3 The TCP header.

A unique sequence of three data packets is exchanged at the beginning of a TCP connection between two hosts, as shown in Figure 6-4. This process, called the TCP three-way connection handshake, forms a virtual connection that is made over the network. It makes use of the TCP flags to signal the start of the connection. This sequence is as follows:

1. The **SYN** (synchronizing) packet
2. The **SYN ACK** (synchronizing acknowledgment) packet
3. The **ACK** (acknowledgment) packet

SYN
Synchronizing packet, a packet in the TCP three-way connection handshake

SYN ACK
Synchronizing acknowledgment packet, a packet in the TCP three-way connection handshake

ACK
Acknowledgment packet, a packet in the TCP three-way connection handshake

The host initiating the connection sends a synchronizing packet, which has a TCP SYN flag set to 1. This is called a SYN packet. In the example shown in Figure 6-4, Host A issues a SYN packet to initiate the TCP handshake. The SYN has a sequence number (SEQ) associated with it. In this example, the sequence number is *x*, and it is used to keep track of the data packets being transferred from

Host A to Host B. The length of the packet being sent by Host A is 0 (LEN 0), which indicates that the packet contains no data.

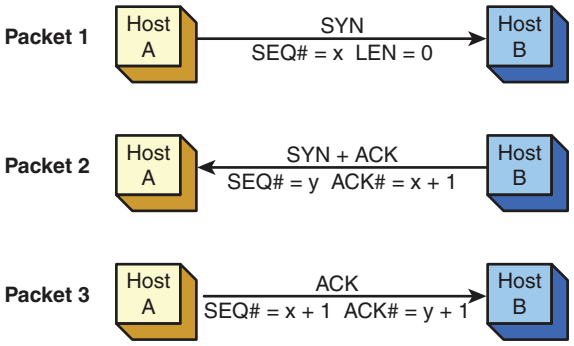


FIGURE 6-4 The initial three-packet TCP handshake.

In packet 2, Host B replies with a SYN ACK packet, which has both the TCP SYN flag and the TCP ACK flag set to 1. The ACK is an acknowledgment that Host B received the packet from Host A. A number is attached to the ACK with the value (x + 1), which should be the sum of the SEQ from packet 1 plus the length (LEN) of packet 1. Recall that the length of packet 1 is 0 (LEN 0), but packet 1 counts as one packet; therefore, Host B replies with an acknowledgment of the packet 1 sequence number plus 1 (x + 1). This acknowledgment notifies Host A that the packet (packet 1) was received. Packet 2 from Host B also has a sequence number issued by Host B. In this packet, the sequence number has the value y. This sequence number is used to keep track of packets transferred by Host B.

In packet 3, Host A acknowledges receipt of Host B's packet by sending an ACK packet with a TCP ACK flag set. The ACK number is an increment of one higher than the SEQ sent by Host B in packet 2 (y + 1). Host A also sends an updated SEQ that is one larger than the SEQ Host A sent in packet 1 (x + 1). Remember that Host A and Host B each has its own sequence number. This completes the three-way handshake that establishes the TCP connection. Such a handshake appears at the beginning of every TCP data transfer.

Figure 6-5 shows the network setup for an example of a TCP packet transmission captured using a network protocol analyzer. Host A (the client) is establishing an FTP connection with Host B. (The captured file, 6-a.cap, is provided at the companion website. See the Introduction for information on how to access this site.) Figure 6-6 shows portions of the captured data packets.

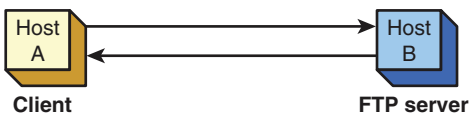


FIGURE 6-5 The setup for the capture of the TCP connection.

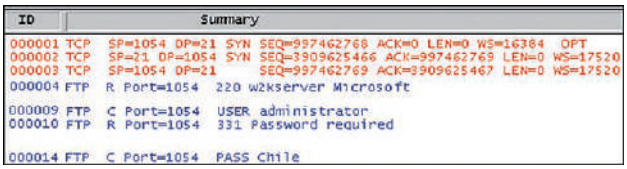


FIGURE 6-6 An example of the three packets exchanged in the initial TCP handshake.

Packet 1 (ID 000001) is the SYN, or synchronizing, packet. This packet is sent from the host computer on the network that wants to establish a TCP network connection. In this example, Host A is making a TCP connection for an FTP file transfer. The summary information for packet 1 specifies that this is a TCP packet, the source port is 1054 (SP=1054), and the destination port is 21 (DP=21). Port 1054 is an arbitrary port number that the FTP client picks or is assigned by the operating system. The destination port 21 (command/control) is the well-known FTP port (see Table 6-4). The packet has a starting sequence number, 997462768, and there is no acknowledgment (ACK=0). The length of the data packet is 0 (LEN=0). This indicates that the packet does not contain any data. The window size—which indicates how many data packets can be transferred without an acknowledgment—is 16384 (WS=16384).

Packet 2 is the SYN ACK packet from the FTP server. The sequence number SEQ=3909625466 is the start of a new sequence for the data packet transfers from Host B. The source port is 21 (SP=21), and the destination port for packet 2 is 1054 (DP=1054). ACK=997462769 is an acknowledgment by Host B (the FTP server) that the first TCP transmission was received. Note that this acknowledgment shows an increment of 1 from the starting sequence number provided by Host A in packet 1.

Packet 3 is an acknowledgment from the client (Host A) back to the FTP server (Host B) that packet 2 was received. Note that the acknowledgment is ACK=3909625467, 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 first thing that happens is that a host sends a FIN (finish) packet to the other connected host. This is shown in Figure 6-7. Host B sends a FIN packet to Host A, indicating that the data transmission 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 that the connection is being terminated. Host B replies with an ACK packet.

Figure 6-8 shows an example of terminating a TCP connection. This example was captured with a network protocol analyzer. (The captured file, 6-a.cap, is provided at the companion website.)

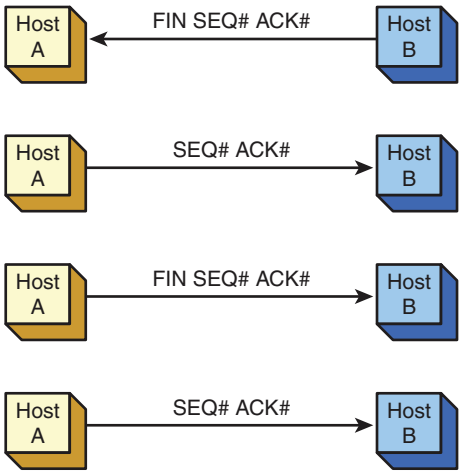


FIGURE 6-7 Terminating the TCP connection.

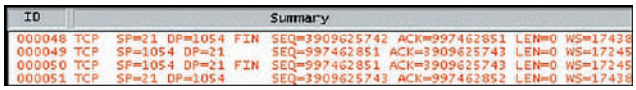


FIGURE 6-8 An example of the four-packet TCP connection termination.

Packet 48 (see Figure 6-8) is a TCP packet with the source port 21 (SP=21) and the destination port 1054 (DP=1054). The FIN statement is shown, followed by SEQ and ACK numbers. Remember that the SEQ and ACK numbers are used to keep track of the number of packets transmitted and an acknowledgment of the number received. The LEN of packet 48 is 0, which means the packet does not contain any data. Packet 49 is an acknowledgment from the host, at port 1054, of the FIN packet. Remember that the FIN packet was sent by the host at the source port 21. In packet 50, the host at port 1054 sends a FIN packet to the host at the destination port 21. In packet 51, the host at port 21 acknowledges receipt of the FIN packet, and the four-packet sequence closes the TCP connection.

UDP
User Datagram Protocol

User Datagram Protocol (**UDP**) is a *connectionless* protocol. This means UDP packets are transported over the network without a connection being established and without any acknowledgment that the data packets arrived at the destination. UDP is useful in applications such as videoconferencing and audio feeds, where such acknowledgments are not necessary. The UDP header is shown in Figure 6-9.

Figure 6-10 provides an example of a UDP packet transfer. Packet 136 is the start of a UDP packet transfer of an Internet audio feed. A TCP connection to the Internet was made first, and then the feed was started. At that time, the UDP connectionless packets started. Packets 138, 139, and 140 are the same types of packets and have a length of 789. No acknowledgments are sent back from the client because all the packets are coming from the Internet source. UDP does not have a procedure for terminating the data transfer; either the source stops delivery of the data packets or the client terminates the connection.

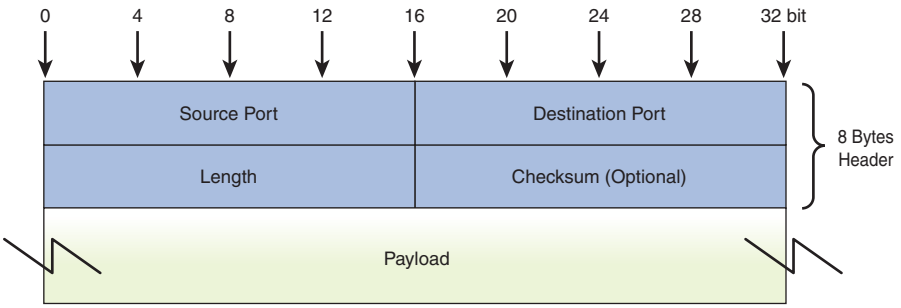


FIGURE 6-9 UDP header.

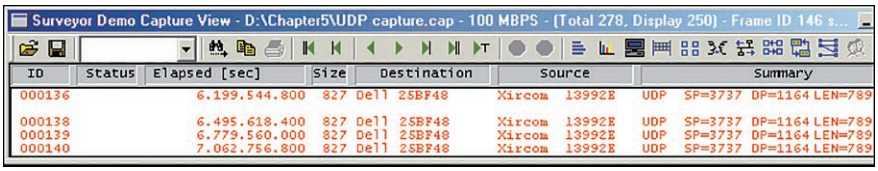


FIGURE 6-10 An example of a UDP packet transfer.

The Internet Layer

The TCP/IP **Internet layer** defines the protocols used for addressing and routing data packets. Protocols that are part of the TCP/IP Internet layer include IP, ARP, ICMP, and IGMP. These protocols are examined in the following sections.

Internet Layer
The layer of the TCP/IP model that defines the protocols used for addressing and routing data packets

IP **Internet Protocol (IP)** defines the addressing used to identify the source and destination addresses of data packets being delivered over an IP network. The IP header is shown in Figure 6-11. An IP address is a logical address that consists of a network address portion and a host address portion. The network portion is used to direct the data to the proper network. The host address identifies the address locally assigned to the host. The network portion of the address is similar to the area code for a telephone number. The host address is similar to the local exchange number. The network and host portions of the IP address are used to route the data packets to the destination. (IP addressing and subnet masking are examined in detail in Sections 6-4 and 6-5.)

Internet Protocol (IP)
A protocol that defines the addressing used to identify the source and destination addresses of data packets being delivered over an IP network

ARP Address Resolution Protocol (**ARP**) is used to resolve an IP address to a hardware address for final delivery of data packets to the destination. ARP issues a query in a network called an *ARP request*, asking which network interface has this IP address. The host assigned the IP address replies with an *ARP reply*, the protocol that contains the hardware address for the destination host. Figure 6-12 provides an example of an ARP request captured with a protocol analyzer. As shown highlighted in Figure 6-12(a), an ARP request is issued on the LAN. The source MAC address of the packet is 00-10-A4-13-99-2E. The destination address on the local area network shown is BROADCAST, which means this message is being sent to all computers in the local area network. A query (Q) is asking who has the IP address 10.10.10.1 (PA=). *PA* is an abbreviation for *protocol address*.

ARP
Address Resolution Protocol, a protocol that is used to map an IP address to a MAC address

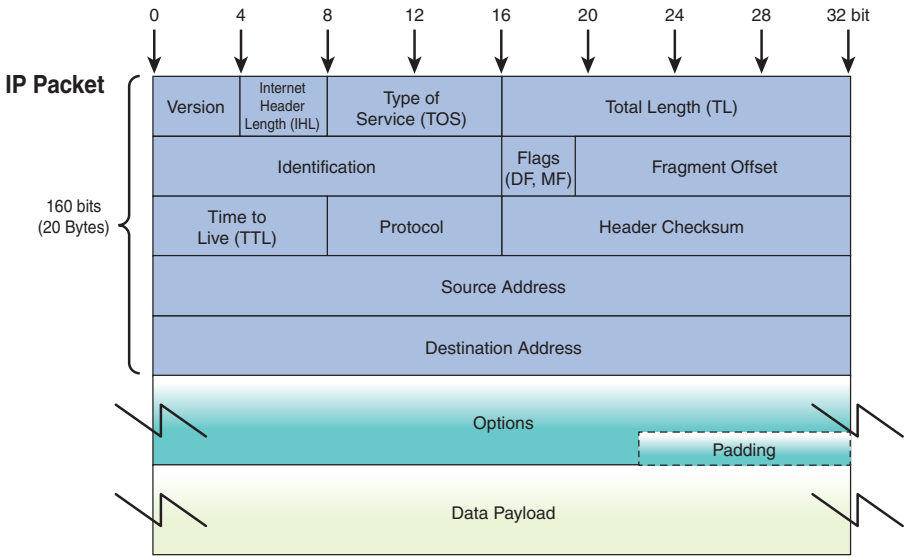


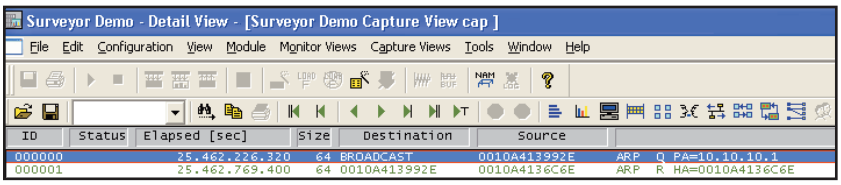
FIGURE 6-11 IP Header

The highlighted area in Figure 6-12(b) shows the destination computer's ARP reply, in which the computer sends its MAC address back to the source that issued the ARP request. (The *R* after ARP indicates this is an ARP reply.) The source of the ARP reply is 00-10-A4-13-6C-6E, which indicates that the MAC address for 10.10.10.1 is 00-10-A4-13-6C-6E (HA=). HA is an abbreviation for *hardware address*. In this case, the owner of the IP address replied to the message, but that does not always happen. Sometimes another networking device, such as a router, can provide the MAC address information. In that case, the MAC address returned is for the next networking device in the route to the destination.

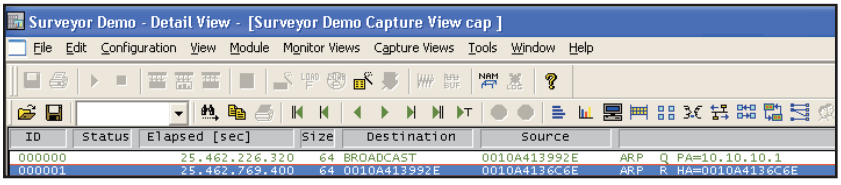
Figure 6-13 provides a breakdown of the packet details of the ARP request. The description of the ARP request is a broadcast that is the uppercase letter *F*. This means that all binary data bits are set to a logical 1. The data packet with all Fs is highlighted at the bottom of the image. Can you find the source address for the ARP request? The source address 00-10-A4-13-99-2E immediately follows the destination address. The hexadecimal number 0x0806 identifies this as an ARP packet. (The 0x indicates that the 0806 is a hexadecimal number. Section 6-3 discusses hexadecimal numbers in more detail.)

ICMP Internet Control Message Protocol (ICMP) is used to control the flow of data in a network, report errors, and perform diagnostics. A networking device, such as a router, sends an ICMP *source-quench* packet to a host that requests a slowdown in the data transfer.

An important troubleshooting tool within the ICMP protocol is **ping**, the packet Internet groper. The **ping** command is used to verify connectivity with another host in the network. The destination host could be in a LAN, in a campus LAN, or on the Internet. (The **ping** command was introduced in Chapter 1 and used in Chapter 4, "Wireless Networking," to test data packet deliveries in a LAN using a hub or switch.)



(a)



(b)

FIGURE 6-12 Captured packets showing the (a) ARP request and the (b) ARP reply.

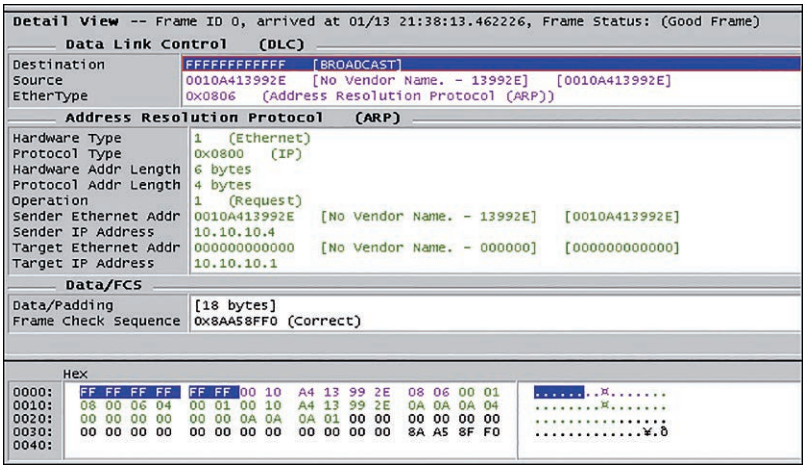


FIGURE 6-13 The details of the ARP broadcast packet.

The **ping** command uses a series of echo requests, and the networking device receiving the echo requests responds with a series of echo replies to test a network connection. Refer to Chapters 1 and 4 for examples.

IGMP Internet Group Management Protocol (**IGMP**) is used when one host needs to send data to many destination hosts. This is called **multicasting**. The addresses used to send a multicast data packet, called **multicast addresses**, are reserved addresses that are not assigned to hosts in a network. An example of an application that uses IGMP packets is a router using multicasting to share routing tables. This is explained in Chapter 9, "Routing Protocols," which examines routing protocols.

Another application of IGMP packets is when a host wants to stream data—such as audio and video files—to multiple hosts. *Streaming* means the data is sent without waiting for any acknowledgment that the data packets were delivered. In fact, in

IGMP
Internet Group Management Protocol, a protocol used for multicasting

Multicasting
A process in which one host sends data to many destination hosts

Multicast Address
An address that is used to send multicast data packets

IGMP, the source doesn't care whether the destination receives a packet. Another feature of IGMP is that the data is handed off to the application layer as it arrives. This enables the appropriate application to begin processing the data for playback.

The Network Interface Layer

Network Interface Layer
The layer of the TCP/IP model that defines how a host connects to a network

The **network interface layer** of the TCP/IP model defines how a host connects to the network. Recall that a host can be a computer or a networking device such as a router. The type of network to which the host connects is not dictated by TCP/IP. The host could be a computer connected to an Ethernet or Token Ring network or a router connected to a Frame Relay WAN. TCP/IP is not dependent on a specific networking technology; therefore, TCP/IP can be adapted to run on newer networking technologies such as Asynchronous Transfer Mode (ATM).

In the network interface layer, every TCP/IP data packet must have a destination and a source MAC address in the TCP/IP header. The MAC, or hardware, address is found on the host's network interface card or connection and is 12 hexadecimal characters in length. For example, the network interface could have this MAC address:

00-10-A4-13-99-2E

The hardware address is used for final delivery of data packets to the next destination in a network. The first six hexadecimal numbers represent the organization that manufactured the card. This is called the *organizational unit identifier* (*OUI*). The last six digits are unique numbers assigned by the manufacturer of the network interface. (The concept of the MAC address is fully explained in Chapter 1, and you are encouraged to refer to that material for a thorough review.)

Section 6-2 Review

This section covers the following Network+ exam objectives.

1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
This section discusses the TCP header, the TCP and UDP protocols, and TCP flags.

1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
The details of the ARP broadcast packet are presented in this section.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.
This section discusses RDP, SSH, Telnet, TFTP, HTTP, HTTPS, POP3, NTP, IMAP, and SMB.

1.6 Explain the use and purpose of network services.
This section introduces NTP.

1.7 Explain basic corporate and datacenter network architecture.

This section discusses the application layer, which is the top layer of the TCP/IP stack. This layer is used to process requests from hosts and to ensure that connections to appropriate ports are made.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

A networking device, such as a router, sends an ICMP source-quench packet to a host that requests a slowdown in the data transfer.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

ARP is used to resolve an IP address to a hardware address for final delivery of data packets to the destination.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section introduces SNMP.

4.4 Compare and contrast remote access methods and security implications.

This section introduces common applications and their port numbers, including port 5900, which is for Virtual Network Computing for Remote Desktop.

5.3 Given a scenario, use the appropriate network software tools and commands.

This section provides an example of an ARP request captured with a protocol analyzer.

Test Your Knowledge

1. True or false: The four layers of the TCP/IP model are application, network, Internet, and data link.

   False

2. Which layer of the TCP/IP model processes requests from hosts to ensure that a connection is made to the appropriate port?

   a. Application
   b. Internet
   c. Transport
   d. None of these answers are correct.

3. Which of the following are the three packets exchanged at the beginning of a TCP connection between two ports?

   a. SYN, SYN ACK, ACK
   b. SYN, SYN, ACK
   c. SYN, ACK, ACK
   d. TCP does not use SYN packets.

6-3 NUMBER CONVERSION

This section reviews the numbering systems used in computer networking, with a focus on converting binary, decimal, and hexadecimal numbers.

Binary-to-Decimal Conversion

Binary numbers are represented as a logical 0 or logical 1 in base 2 format. This means that each number has a place value of 2n, where *n* is the place value position of the binary digit. The place values start at 2^0 with the least significant bit (LSB) position. For example, the binary number 1011 has the place values of 2^0 for the LSB position to 2^3 for the most significant bit (MSB) position:

Place value	2^3	2^2	2^1	2^0
Binary digit	1	0	1	1
MSB→LSB	MSB			LSB

The 1 and 0 are used as multipliers with the place value. For example, the conversion of 1011 to decimal is as follows:

$$1 \times 2^3 = 8$$
$$0 \times 2^2 = 0$$
$$1 \times 2^1 = 2$$
$$\underline{1 \times 2^0 = 1}$$
$$\text{sum} = 11$$

Note here that each place value is multiplied by the value of the binary digit.

Instead of writing 2^0, 2^1, 2^2,…, it is easier to write the decimal equivalent for each place value (for example, 1, 2, 4, 8, 16, 32, 64, 128). The calculations for determining each place value are as follows:

$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$
$2^4 = 16$	$2^5 = 32$	$2^6 = 64$	$2^7 = 128$

The place values for eight binary numbers (an octet) are as follows:

Place value (decimal)	128	64	32	16	8	4	2	1
Place value	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
MSB→LSB	MSB							LSB

For example, the place values for the binary number 100100 can be set up as follows:

Place value (decimal)	32	16	8	4	2	1
Place value	2^5	2^4	2^3	2^2	2^1	2^0
Binary digit	1	0	0	1	0	0
MSB→LSB	MSB					LSB

Every place value that has a binary digit 1 is used to sum a total for determining the decimal equivalent for the binary number. In this example, the decimal equivalent is 32 + 4 = 36. After working a few examples, it becomes obvious that the base 2 place values can be written by inspection in their decimal equivalence. The rightmost place value is 1, the next place value is 2, the next is 4, and so on.

The 8-bit octet numbers used in IP addressing are converted from binary to decimal in the same manner. The following example demonstrates this.

Example 6-1

Given the following 32-bit IP address expressed in binary format, convert the number to dotted-decimal format:

11000000	10101000	00100000	00001100
Octet 4	Octet 3	Octet 2	Octet 1

Solution

First, assign the place value for each binary position:

	128	64	32	16	8	4	2	1
Octet 1	0	0	0	0	1	1	0	0

$(1 \times 8) + (1 \times 4) = 8 + 4 = 12$

	128	64	32	16	8	4	2	1
Octet 2	0	0	1	0	0	0	0	0

$(1 \times 32) = 32$

	128	64	32	16	8	4	2	1
Octet 3	1	0	1	0	1	0	0	0

$(1 \times 128) + (1 \times 32)\ (1 \times 8) = 128 + 32 + 8 = 168$

	128	64	32	16	8	4	2	1
Octet 4	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 by using division: You repeatedly divide the decimal number by 2 until the quotient is 0. The steps for converting decimal numbers to binary by using division are as follows:

1. Divide the decimal number by 2, record the remainder (0 or 1), and write the quotient or result of the division by 2.
2. Divide the quotient by 2 and record the remainder (0 or 1). Write the quotient and repeat this step until the quotient is 0.
3. 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 the value 1100. The calculation for this is shown:

12/2	
6/2	0
3/2	0
1/2	1
0	1

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

8	4	2	1
1	1	0	0

$(1 \times 8) + (1 \times 4) = 12$

Example 6-3

Convert 33 to its binary equivalent.

Solution

Use the decimal-to-binary steps listed previously.

33/2	
16/2	1
8/2	0
4/2	0
2/2	0
1/2	0
0	1

The answer is 100001.

Example 6-4

Convert the decimal number 254 to binary.

Solution

Use the decimal-to-binary steps listed previously.

254/2	
127/2	0
63/2	1
31/2	1
15/2	1
7/2	1
3/2	1
1/2	1
0	1

The answer is 11111110.

Hexadecimal Numbers

Hexadecimal (**hex**) numbers are base 16 numbers. Table 6-5 provides a conversion lookup table for hexadecimal. A hexadecimal number is represented by four binary numbers. Notice that the letters A–F are used to represent the decimal numbers 10–15.

Hex
Hexadecimal, base 16

Converting Hexadecimal

The simplest way to convert hexadecimal numbers to binary is through the use of either a calculator or a lookup table, such as Table 6-5.

TABLE 6-5 **Hexadecimal Conversion Table**

Decimal	Hexadecimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001

Decimal	Hexadecimal	Binary
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Hexadecimal numbers are used in computer networks to represent a computer's 12-hex-character MAC address and are used to display the packet details in a protocol analyzer, as shown in Figure 6-11. Hex numbers are also used in IPv6 addressing (discussed in Section 6-7).

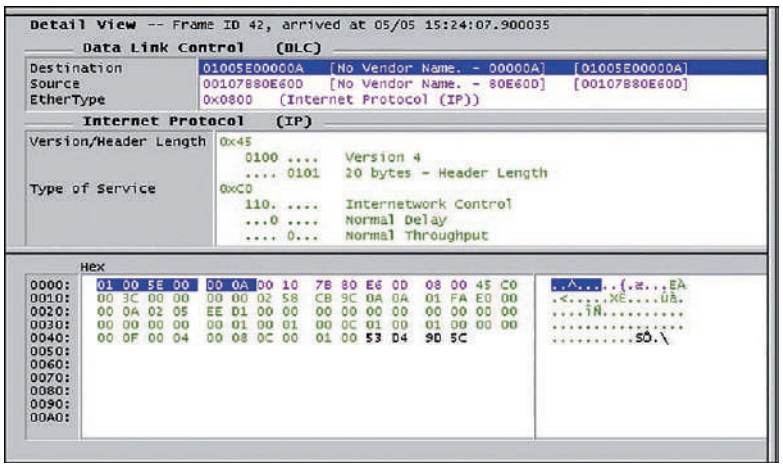


FIGURE 6-14 An example of the use of hex numbers in data packets.

The highlighted region in Figure 6-14 shows the destination MAC address 01005E00000A, which is a 12-digit hexadecimal code. Notice that the EtherType number is 0x0800, which indicates that this is an Internet Protocol packet. Also note that the numbers at the bottom of the screen are expressed in hex format. These numbers are the values in the data packets:

> **0x800**—The 0x indicates that this is a hexadecimal number.
> **$0x800_H$**—The subscript H is sometimes used to indicate a hexadecimal number. The subscript notation is not always practical to display in text format, however, so this style is of limited use.

The following examples show how to convert hexadecimal numbers to binary.

Example 6-5

Convert the hexadecimal number 0x48AF to binary.

Solution

Use Table 6-5 to convert the hex numbers.

Hex:	4	8	A	F
Binary:	0100	1000	1010	1111

Example 6-6

Convert the hexadecimal number 0x0800 to binary.

Solution

Use Table 6-5 to convert the hex numbers.

Hex:	0	8	0	0
Binary:	0000	1000	0000	0000

Converting binary numbers to hexadecimal requires that the binary numbers be separated into groups of four, beginning with the LSB position. If a binary sequence doesn't have 4 bits, you use leading 0s to pad the number. The binary numbers used in computer networks are always multiples of four in length; therefore, you don't have to pad any of the numbers with leading 0s.

Example 6-7

Convert the binary number 010011001010 to hexadecimal.

Solution

Separate the binary numbers into groups of four, beginning with the LSB position. Next, use the conversion lookup table (refer to Table 6-5) to convert each 4-bit binary group to hexadecimal.

0100	1100	1010
4	C	A

The answer is 0x4CA

Section 6-3 Review

This section covers the following Network+ exam objective.

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

This section introduces hex numbers, which are used with IPv6.

5.3 Given a scenario, use the appropriate network software tools and commands.

This section shows an example of a protocol analyzer being used to examine hex numbers. The focus of this section is number conversion. An important relationship is the structure of the MAC address, which is made up of 12 hexadecimal characters. Also, EtherType 0x0800 is expressed in hexadecimal.

Test Your Knowledge

1. What is the hexadecimal equivalent to the binary number 1011011011110001?

   a. B6F1

   b. A6F1

   c. AAF1

   d. BAF1

   e. None of these answers are correct.

2. True or false: Converting 65 to its binary equivalent yields 1000001.

   True

6-4 IPV4 ADDRESSING

Networking devices on the Internet and in LANs currently use IPv4 addresses. Students should understand the address range for the five classes of IP addresses: Classes A, B, C, D, and E. This section describes IPv4 addressing and the role of each octet.

IP addressing provides a standardized format for assigning a unique routable address for each host in a TCP/IP network. The host in a TCP/IP network already has a hardware (MAC) address, so why is an IP address needed? An internetworking device needs a routable network address to deliver data packets outside the LAN. An IP address is similar to a telephone number. The network portion of the IP address is like the telephone number's area code. The host portion of the IP address is like the telephone number's 7-bit local exchange number. This section identifies the network and host portions of an IP address and describes how IP addressing is used to identify the address for a host in a network.

The predominant IP addressing version currently being used on the Internet and for TCP/IP data traffic is **IPv4**. There are five classes of IPv4 addresses: **Classes A, B, C, D, and E**. Table 6-6 provides the address breakdown for the classes. Classes A, B, and C are the primary addresses used over the Internet and for TCP/IP data traffic. Class D is used for multicasting (explained in Chapter 9), and the Class E range is experimental and is not used on the Internet. A newer IP addressing scheme called IPv6 has been developed for use on the Internet. Section 6-7 covers this addressing scheme in more detail.

IPv4
Internet Protocol version 4, the IP version currently being used on the Internet

Classes A, B, C, D, and E
The five classes of IPv4 addresses

TABLE 6-6 **IPv4 Address Classes and Ranges**

Class	IP Address Range
A	0.0.0.0–127.255.255.255
B	128.0.0.0–191.255.255.255
C	192.0.0.0–223.255.255.255
D	224.0.0.0–239.255.255.255
E	240.0.0.0 –254.255.255.255

Note

The 0.0.0.0 and 127.*x.x.x* addresses are special-purpose addresses. The 0.0.0.0 IP address refers to the source host on the current network. The 127.*x.x.x* addresses are used as Internet host loopback addresses. A datagram sent by a higher-level protocol to an address anywhere within this block should loop back inside the host. The loopback address used most commonly is 127.0.0.1. The 127.*x.x.x* addresses should never appear on a network.

Each IP address consists of four 8-bit octets, providing a total binary data length of 32 bits. Figure 6-15 shows the 32-bit structure for an IP address. Each octet in the IP address is expressed in terms of its decimal equivalent. Each octet can range from 00000000 to 11111111 in binary or 0 to 255 in decimal. The decimal equivalent representation of the four octets shown in Figure 6-12 is 10.10.20.1. Table 6-7 provides a breakdown for determining each octet in decimal and binary.

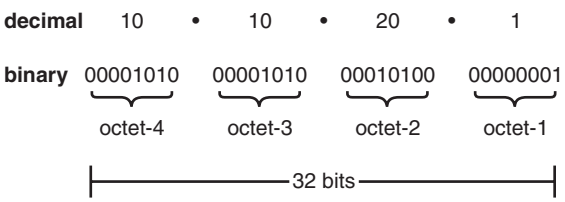


FIGURE 6-15 The structure of a 32-bit IPv4 address.

TABLE 6-7 **Decimal/Binary Octet Breakdown for the 10.10.20.1 IPv4 Address**

Octet	Decimal	Binary
4	10	00001010
3	10	00001010
2	20	00010100
1	1	00000001

Representing binary data in decimal form simplifies the user interface. TCP/IP uses the binary form (represented as 32 1/0 bits) for transporting the IP address, but the user interface is typically expressed in *dotted-decimal* format. The IP address 10.10.20.1 is an example of dotted-decimal format.

Each of the four octets of an IPv4 address represents either a network or a host portion of the IP address. Figure 6-16 and Table 6-8 illustrate the breakdown in each of the address classes for network and host bits. Class A has 8 bits assigned for the network address and 24 bits for the host. Class B has 16 bits for the network address and 16 bits for the host. Class C has 24 bits assigned for the network address and 8 bits for the host.

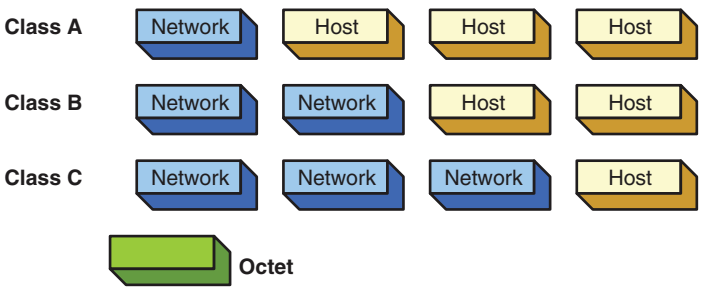


FIGURE 6-16 The octets making up the network and host portions of the IPv4 address for Classes A, B, and C.

TABLE 6-8 **Breakdown of the Network and Host Bits by Class**

Class	Number of Network Bits	Number of Host Bits
A	8	24
B	16	16
C	24	8

The number of host bits in the IP address classes determines how many hosts can be created for each class of address. You can use this equation to calculate the number of usable IP addresses or host IP addresses that can be created for a network:

$2^n - 2$, where n = number of host bits

For example, a Class C address has 8 host bits; therefore, $2^8 - 2 = 254$ host IP addresses can be assigned to a Class C network. The reason for the "– 2" value in the equation when calculating the number of host addresses is that the host IP address cannot be all 1s or all 0s. The all-1s state is reserved for network broadcasts, and the all-0s state is reserved for the network address.

Table 6-9 lists the total number of available host IP addresses for each class of network. (A technique called *subnetting* is introduced in Section 6-5. This technique involves borrowing and adding host bits to the network address bits to create subnets in a network.)

TABLE 6-9 **Numbers of Host IP Addresses by Class**

Class	Number of Host Bits	Number of Hosts
A	24	16,777,214
B	16	65,534
C	8	254

IP Address Assignment IP address allocation is governed by the Internet Assigned Numbers Authority (IANA). To coordinate the global hierarchy effort of IP allocation more effectively, IANA delegates the allocation to the regional Internet registries (**RIRs**), each of which is responsible for a particular area. The five RIRs accounting for the different regions of the world are as follows:

RIRs
Regional Internet Registries, IANA-designated governing organizations responsible for IP address allocation by geographic location

- **AFRINIC:** Africa region
- **APNIC:** Asia/Pacific region
- **ARIN:** North America region
- **LACNIC:** Latin America and some Caribbean islands
- **RIPE NCC:** Europe, the Middle East, and Central Asia

In North America, IP addresses are assigned by the American Registry for Internet Numbers (**ARIN**; see www.arin.net). ARIN assigns IP address space to Internet service providers (ISPs) and end users. However, an ISP or end user must be large enough to merit a block of addresses. After ARIN allocates blocks of addresses to ISPs, the ISPs issue addresses to their customers. For example, a telco could be the ISP that has a large block of IP addresses and issues an IP address to a user. A local ISP could also be assigned a block of IP addresses from ARIN, but the local ISP must have a large number of users.

ARIN
American Registry for Internet Numbers

ARIN also assigns end users' IP addresses. Once again, an end user must qualify to receive a block of addresses from ARIN. This usually means that the end user must be large. For example, many universities and large businesses can receive blocks of IP addresses from ARIN. However, most end users get their IP addresses from an ISP (such as a telco) or have IP addresses assigned dynamically when they connect to the ISP.

Private IP Addresses Unlike the public IP address ranges assigned to RIRs, ISPs, or users, there are address ranges in Classes A, B, and C that have been set aside for private use. The Internet Engineering Task Force (IETF) proposed RFC 1918 for address allocation for private Internets in 1996. These addresses, called *private addresses*, are not used for Internet data traffic but are intended to be used specifically on internal networks called *intranets.* Table 6-10 lists the private address ranges.

TABLE 6-10 **Private IP Addresses**

Class	Address Range
A	10.0.0.0–10.255.255.255
B	172.16.0.0–172.31.255.255
C	192.168.0.0–192.168.255.255

Non-Internet-Routable IP Address
An IP address that cannot be routed on the Internet

One popular private IP address is the Class C address 192.168.0.0, which is used by many home routers for home private LANs. Functionally, private addresses work the same as public addresses except that they are not routed on the Internet. They are called **non-Internet-routable IP addresses** and are blocked by ISPs. (The IP addresses used in this book are in the private address range.)

Section 6-4 Review

This section covers the following Network+ exam objective.

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

This section mentions the fact that the IETF proposed RFC 1918 on address allocation for private networks in 1996.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

This section states that IP addressing provides a standardized format for assigning a unique routable address for every host in a TCP/IP network.

Test Your Knowledge

1. The home IP address for a network is assigned by which of the following?
   a. ARIN, the Association of Registered Internet Numbers
   b. ARIN, the American Registry for Internet Names
   c. ARIN, the American Registry for Internet Numbers
   d. ARNN, the American Registry for Internet Names and Numbers

2. The IP address 192.168.20.5 is an example of which of the following? (Select all that apply.)

   a. A Class C IP address
   b. A Class B IP address
   c. A Class A IP address
   d. A private IP address

6-5 SUBNET MASKS: SUBNETTING AND SUPERNETTING

Subnetting and supernetting are difficult concepts for students to master. This section provides many examples for students to follow and learn. This section demonstrates the concept of borrowing bits from the host to create subnets, as well as how to apply subnet masks. This section includes a discussion on selecting a subnet mask to prevent the waste of host addresses.

The goal of this section is to demonstrate how to establish subnet masks for use in computer networks and how to create subnet masks for subnetting and supernetting. Up to this point, this chapter has focused on **classful** networks, which means that the IP addresses and subnets are within the same network. The problem with classful addressing is that it leaves a lot of unused IP address space. For example, a Class A IP network has more than 16 million possible host addresses. A Class B network has more than 65,000 host addresses. However, only a limited amount of Class A and Class B address space has been allocated for Internet use.

Classful
Indicates that IP and subnet addresses are within the same network

A **subnet mask** identifies which bits in an IP address are to be used to represent the network/subnet portion of an IP address. Essentially, a subnet mask defines the boundary of a network.

Subnet Mask
A number that identifies the network/subnet portion of an IP address

To understand subnet masks, we need to begin with the subnet masks for the classful IP address ranges:

- **Class A:** 255.0.0.0, where the first octet (8 bits) represents the network bits, and the last three octets (24 bits) represent the host bits.
- **Class B:** 255.255.0.0, where the first two octets (16 bits) represent the network bits and the last two octets (16 bits) represent the host bits.
- **Class C:** 255.255.255.0, where the first three octets (24 bits) represent the network bits, and the last octet (8 bits) represents the host bits.

It is important to understand that a subnet mask consists of bit position values set to either 1 or 0. A bit position set to 1 indicates that the bit position is used to identify a network or subnet, whereas a 0 bit position represents a host.

The boundary of each network can be found by applying a subnet mask to an IP address. This is simply a logical AND operation—or "ANDing" an IP address with the subnet mask. Setting the subnet mask bit position to 1 enables the bit value from the IP address to pass. Setting the subnet mask bit value to 0 disables the bit value from appearing on the output. This is illustrated in Table 6-11.

TABLE 6-11 **Applying a Subnet Mask**

Subnet Mask Bit	IP Address Bit	Output
0	0	0
0	1	0
1	0	0
1	1	1

Notice that when the subnet mask bit is set to 0, the output is forced to 0. When the subnet mask bit is set to 1, the output follows the IP address bit.

For example, let's use the Class B IP address 172.16.1.2 and with it the Class B subnet mask 255.255.0.0:

- 172.16.1.2 ↔ 1010 1100.0001 0000.0000 0001.0000 0010
- 255.255.0.0 ↔ 1111 1111.1111 1111.0000 0000.0000 0000
- 172.16.0.0 ↔ 1010 1100.0001 0000.0000 0000.0000 0000

The result, 172.16.0.0, is the network address, which identifies the start of the network boundary. Next, you need to find the end of the network boundary. You can obtain this by inverting the host bits of the network address to 1s. The host bits are given according to the subnet mask, which in this case is the last two octets, or 16 bits, as underlined above. 172.16.255.255 is the end of this network boundary, and this IP address is also called the broadcast address:

172.16.255.255 ↔ 1010 1100.0001 0000.1111 1111.1111 1111

The boundary or range of this network is, therefore, 172.16.0.0–172.16.255.255. The usable IP address range is 172.16.0.1–172.16.255.254.

Subnetting

Sometimes, a network needs to be made smaller—possibly to make efficient use of the IP addresses or perhaps to accommodate network design requirements. *Subnetting* is a technique that can be used to break down or partition the original network into smaller networks called *subnets*. The key to subnetting is the subnet mask. Because a subnet mask defines the boundary of a network, by creating a new subnet mask or a custom subnet mask, you end up with a new subnet. You can create a custom subnet mask from the original or default subnet mask of a classful address (that is, Class A, B, or C address) by borrowing bits from the host portion

of the IP address, as shown in Figure 6-17. The network portion of the IP address and the new subnet bits are used to define the new subnet. When you change a classful address into new smaller subnets, these subnets become classless. Routers use this address information to properly forward data packets to the proper subnet.

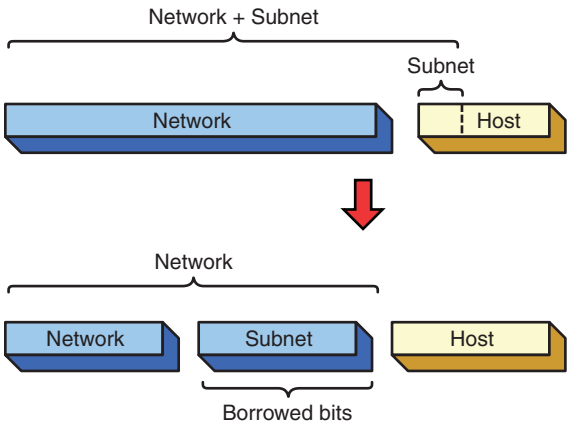


FIGURE 6-17 Borrowing bits from the host to create subnets.

How to Accomplish Subnetting You can accomplish subnetting by manipulating the subnet mask as described in the following subsections.

Step 1: Know the Original/Default Subnet Mask This is the most important step: You begin with the original or the default subnet mask. The subnet mask is obtained from the class (A, B, or C) of the given IP address. At the beginning, it is all about the classful boundary of these classes and their respective subnet masks, which are 255.0.0.0, 255.255.0.0, and 255.255.255.0. Figure 6-15 shows the Class C network address 192.168.12.0. By default, the original subnet mask for this Class C address is 255.255.255.0.

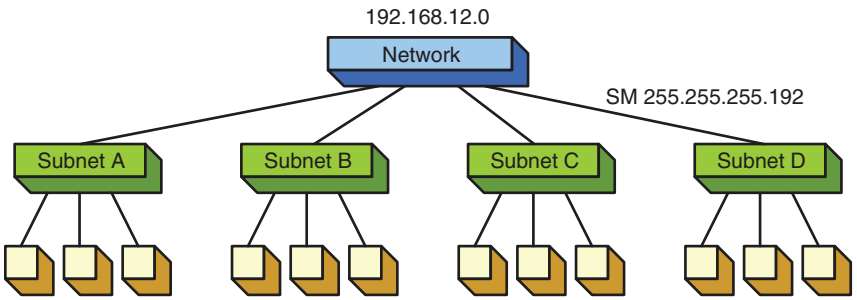


FIGURE 6-18 Partitioning a network into subnets.

Step 2. Find the New Subnet Requirements The purpose of subnetting is to create new subnets. You need to determine how many subnets or how many IP addresses are needed per subnet. The Class C network shown in Figure 6-18 is partitioned into four subnets.

Step 3. Find the Number of Borrowed Host Bits Remember that there is only one network/subnet in the original classful address. In order to create four subnets from the original single Class C network, 192.168.12.0, you need to borrow from the host bits portion, thus reducing the number of bits available for host IP addresses, as shown in Figure 6-19.

Equations 6-1 and 6-2 show how to calculate the number of subnets created and the number of hosts per subnet:

$$\text{Number of subnets created} = 2^x \quad \textbf{[Equation 6-1]}$$
$$\text{Number of hosts per subnet} = 2^{(y-x)} \quad \textbf{[Equation 6-2]}$$

where:

x = number of bits borrowed from the host bits
y = number of host bits for the class of network (A = 24, B = 16, C = 8)

Using the first of the equations above to break down the 192.168.12.0 network into four subnets yields the following:

$$\text{Number of subnets created} = 2^x = 4$$

Then you solve for x:

$$2^{(2)} = 4$$

Therefore, $x = 2$ requires borrowing 2 host bits.

Applying these values to the second of the equations above yields the following:

$$\text{Number of hosts/subnet} = 2^{(y-x)} = 2^{(8-2)} = 64$$

When creating subnets, it is important to note that each subnet has both a network address and a broadcast address. Taking this into consideration, the equations for calculating the number of hosts per subnet are modified to account for the number of usable hosts per subnet. The modified equations are as follows:

$$\text{Number of usable hosts per subnet} = 2^{(y-x)} - 2 \quad \textbf{[Equation 6-3]}$$
$$= 2^{(8-2)} - 2 = 64 - 2 = 62$$

Therefore, it requires 2 bits borrowed from the host bits to provide four possible subnets. These borrowed bits are also known as *subnet bits*. Each subnet has 2^6 (or 64) available hosts or IP addresses, and each subnet has 62 usable hosts or IP addresses. The number of bits borrowed and the new host bits are shown in Figure 6-19.

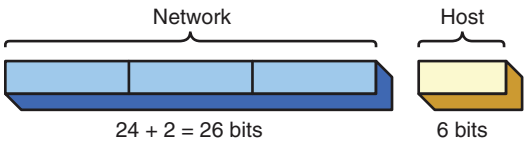


FIGURE 6-19 The breakdown of an IP address to allow for the creation of four subnets.

Step 4. Create the Custom Subnet Mask The network 192.168.12.0 has 2 bits borrowed from the host portion of the IP address to create the four subnets. The Class C network has 24 network bits and 8 host bits. Then 2 bits are borrowed from the host address to create the four subnets. The network plus subnet portion of the IP address is now 24 + 2 = 26 bits in length, and the host portion is now 6 bits. The breakdown of the 32-bit IP address is shown in Figure 6-19.

A custom subnet mask can be created by using the 2 borrowed bits. The two most significant bit (MSB) positions, borrowed from the host and network portion of the IP address, must be included in the subnet mask selection. The purpose of the subnet mask is to specify the bit positions used to identify the network and subnet bits. The subnet mask for identifying the Class C network 192.168.12.0 is 255.255.255.0, as shown with this binary conversion:

First Octet	Second Octet	Third Octet	Fourth Octet
255	.255	.255	.0
1111 1111	.1111 1111	.1111 1111	.**00**000 0000

Figure 6-20 shows the fourth octet of the Class C subnet mask, which identifies the host bits. When borrowing a host bit, you simply change or set the bit from 0 to 1, which is much better illustrated in binary format.

The two MSBs are borrowed from the host bits; therefore, the last octet of the subnet mask is where the 1 indicates that this place is used for the subnet mask, and the *x* means that the place value is left for the host address. Summing the two bit position values that have a 1 yields 128 + 64 = 192. The 192 is placed in the last octet of the subnet mask. The complete subnet mask is 255.255.255.192.

	|————Subnet————|		|——Host Addresses——|				
Place Value	128	64	32	16	8	4	2	1
	1	1	x	x	x	x	x	x

FIGURE 6-20 An example showing the 2 bits borrowed from the host for subnetting.

The custom subnet mask created form the 2 borrowed host bits is 255.255.255.192, as shown with the following binary conversion:

First Octet	Second Octet	Third Octet	Fourth Octet
255	.255	.255	.192
1111 1111	.1111 1111	.1111 1111	.**11**00 0000

Step 5. Derive the Subnets In step 2, you specified four new subnets, which can also be verified with Equation 6-1 using the 2 borrowed bits. Each subnet has its own network address. The network addresses are used to route data packets to the correct subnet. Table 6-12 shows the four subnet addresses listed in both binary and decimal formats.

Note

The 6 host bits are all set at 0 in a subnet's network address.

TABLE 6-12 **Binary and Decimal Equivalents for a Subnet's Network Address**

Place Value			
128	**64**	**Host Bits**	**Subnet/Network Address**
0	0	000000	0
0	1	000000	64
1	0	000000	128
1	1	000000	192

Each subnet also has its own broadcast address. The broadcast address for the subnet is used to broadcast packets to all hosts in the subnet. (Note: All host bits are set to 1 for a broadcast.) Table 6-13 shows the binary and decimal equivalents for the subnet's broadcast address.

TABLE 6-13 **Binary and Decimal Equivalents for a Subnet's Broadcast Address**

	Subnet		Host Bits						Decimal Equivalent
Place Value	128	64	32	16	8	4	2	1	
	0	0	1	1	1	1	1	1	63
	0	1	1	1	1	1	1	1	127
	1	0	1	1	1	1	1	1	191
	1	1	1	1	1	1	1	1	255
Place Value	128	64	32	16	8	4	2	1	

Given this information, the network and broadcast addresses can be defined for the four subnets of the 192.168.12.0 network. With four subnets, each subnet has 64 total IP addresses. These parameters now set a new boundary for each new custom subnet. Because the IP address numbers have to be contiguous, the first subnet with 64 IP addresses will start from 192.168.1.0 and go to 192.168.1.63. The next subnet will be 192.168.1.64 through 192.168.1.127 (for another 64 IP addresses and so on and so forth).

Next, we can compare the original network and the four new subnets. This is the original Class C network with subnet mask 255.255.255.0:

Number of Subnet	Network Address	Broadcast Address	Usable IP Address Range
1	192.168.1.0	192.168.1.255	192.168.1.1–192.168.1.254

This is four subnets with the custom subnet mask 255.255.255.192:

Number of Subnet	Network Address	Broadcast Address	Usable IP Address Range
1	192.168.1.0	192.168.1.63	192.168.1.1–192.168.1.62
2	192.168.1.64	192.168.1.127	192.168.1.65–192.168.1.126
3	192.168.1.128	192.168.1.191	192.168.1.129–192.168.1.190
4	192.168.1.192	192.168.1.255	192.168.1.193–192.168.1.254

Alternative Technique to Derive the Subnets: Magic Number

Instead of using binary math to find the network address and broadcast address of each new subnet, there is another popular technique to derive each new subnet: the magic number technique. The magic number defines the number increment of each subnet and can be obtained by subtracting the custom subnet mask octet from 256. For example, say that the custom subnet mask is 255.255.255.192. The magic number is as follows:

256 – 192 = 64

This means each subnet will be an increment of 64, starting from 192.168.1.0, which yields the following:

192.168.1.0
192.168.1.64
192.168.1.128
192.168.1.192

Each of these network addresses is the beginning IP address for a network. Then, the broadcast IP address is the last IP address of each subnet range. It can be obtained by adding the magic number minus 1 (in this case, 64 – 1) to the network address. In this case, it would yield the following:

192.168.1.0 + 63 = 192.168.1.63
192.168.1.64 + 63 = 192.168.1.127
192.168.1.128 + 63 = 192.168.1.191
192.168.1.192 + 63 = = 192.168.1.255

Subnet Masking Examples

The division and magic number techniques for subnet masking can be applied to Class A, Class B, or Class C addresses. The following examples demonstrate subnet mask selection in a network.

Example 6-8

Given the network address 10.0.0.0, divide the network into eight subnets. Specify the subnet mask, the network and broadcast addresses, and the number of usable hosts per subnet.

Solution

Creating eight subnets requires borrowing 3 host bits; therefore, $x = 3$. This is a Class A network, so $y = 24$.

Using Equation 6-1, the number of subnets = $2^3 = 8$.

Using Equation 6-3, the number of usable hosts = $2^{(24-3)} - 2 = 2097150$.

The 8 subnets are as follows:

128	64	32	Host Bits	Subnet
0	0	0	*xxxxx*	0
0	0	1	*xxxxx*	32
0	1	0	*xxxxx*	64
0	1	1	*xxxxx*	96
1	0	0	*xxxxx*	128
1	0	1	*xxxxx*	160
1	1	0	*xxxxx*	192
1	1	1	*xxxxx*	224

Therefore, the network and broadcast addresses for the eight subnets are as follows:

Subnet	Network Address	Broadcast Address
0 subnet (000)	10.0.0.0	10.31.255.255
32 subnet (001)	10.32.0.0	10.63.255.255
64 subnet (010)	10.64.0.0	10.95.255.255
96 subnet (011)	10.96.0.0	10.127.255.255
128 subnet (100)	10.128.0.0	10.159.255.255
160 subnet (101)	10.160.0.0	10.191.255.255
192 subnet (110)	10.192.0.0	10.223.255.255
224 subnet (111)	10.224.0.0	10.255.255.255

The subnet mask for creating the eight subnets is 255.224.0.0.

The 224 in Example 6-8 comes from setting the subnet mask to select the three MSB positions in the host portion of the address, as shown in Figure 6-21.

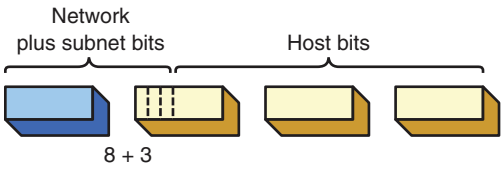


FIGURE 6-21 The network, subnet, and host bit positions for creating the eight subnets in Example 6-8.

Another way to select a subnet mask is to specify how many usable hosts are available to be assigned in a subnet. For example, assume that 62 usable host addresses are to be available in a subnet and also assume a Class C network. Use Equation 6-3:

$$62 = 2^{(8-x)} - 2$$
$$64 = 2^{(8-x)}$$

Use logarithms to solve for x:

$$\log 64 = (8 - x)(\log 2)$$
$$\log 64/(\log 2) = 8 - x$$
$$6 = 8 - x$$
therefore, $x = 2$

Instead of using logarithms, however, you can use a table such as Table 6-14. Example 6-9 shows how to use a table like this one to determine the subnet mask.

TABLE 6-14 **Number of Bits Borrowed to Create a Specific Number of Usable Hosts**

Number of Usable Hosts	Number of Host Bits Needed		
	Class A	Class B	Class C
1022	14	6	—
510	15	7	—
254	16	8	—
126	17	9	—
62	18	10	2
30	19	11	3
14	20	12	4
6	21	13	5
2	22	14	6

Example 6-9

Determine the subnet mask required for the router-to-router link shown in Figure 6-22 if only two host addresses are required for this link.



FIGURE 6-22 Setting a subnet mask for a router-to-router link that provides two host addresses.

Solution

Using Table 6-14 to determine the number of host bits borrowed for creating a subnet with two usable hosts, notice that 14 host bits are borrowed for this Class B network. This means the first three octets plus the 6 MSB positions of the fourth octet will be used to create the subnet mask. The decimal equivalent for the 6 MSB bit positions is 128 + 64 + 32 + 16 + 8 + 4 = 252.

Binary	11111111	11111111	11111111	111111*xx*
Decimal	255	255	255	252

Therefore, the subnet mask is 255.255.255.252.

Gateway IP Address

A Gateway IP address is the IP address of the network device that enables the hosts in a LAN to connect to networks and host outside the LAN. Computers use subnet masks to control data flow within networks. Computers in a LAN use subnet masks to determine whether a destination IP address is intended for a host in the same LAN or if a data packet should be sent to the gateway IP address of the LAN. The gateway IP address is typically the physical network interface on a layer 3 switch or a router.

For example, say that the IP address of a computer in a LAN is 172.16.35.3. The subnet mask 255.255.255.0 is being used. The 255.255.255.0 subnet mask indicates that all bits in the first three octets must match each other to stay in this LAN. This can be verified by ANDing the subnet mask with the destination address to obtain the network address as shown below. This means that all data packets with an IP address between 172.16.35.0 and 172.16.35.255 stay in the LAN and can communicate directly with each other without using the LAN gateway. A data packet with destination IP address 172.16.34.15 is not in the same LAN and must be sent to the LAN gateway.

	Computer	Destination 1	Destination 2
IP Address	172.16.35.3	172.16.35.200	172.16.34.15
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Network Address	172.16.35.0	172.16.35.0	172.16.34.0

This section demonstrates techniques for establishing subnets and subnet masks in computer networks. It provides examples of the process of borrowing bits to determine the number of available hosts in a subnet. The next section examines the concepts of expanding a subnet IP address range beyond class boundaries by using CIDR blocks.

Section 6-5 Review

This section covers the following Network+ exam objective.

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

This section presents techniques for subnetting networks. Make sure you understand the concept of borrowing bits to create a subnet and can identify how many host IP addresses are available for a given subnet. This section also shows how to use a subnet mask to determine whether a destination IP address is in the same LAN or whether a data packet is sent to the gateway address for a LAN. This is an important concept when tracking data packet travel.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section states that the gateway IP address is typically the physical network interface on a layer 3–capable switch or a router. The network portion of the IP address and the new subnet bits are used to define the new subnet. When you change a classful address into new smaller subnets, the subnets become classless. Routers use this information to properly forward data packets to the proper subnets.

Test Your Knowledge

1. The subnet mask 255.255.255.0 is applied to the IP address 10.20.35.12. Which subnet is the packet sent to?

   a. 10.20.35.32

   b. 10.20.0.0

   c. 10.0.0.0

   d. 10.20.35.192

   e. None of these answers are correct.

2. What is the network address for a host with IP address 192.168.50.146 using subnet mask 255.255.255.192?

   a. 192.168.50.128
   b. 192.168.50.191
   c. 192.168.128.0
   d. 192.168.128.192
   e. None of these answers are correct.

3. Given network IP address 172.16.0.0 and subnet mask 255.255.192.0, how many subnets are in this network?

   a. 2
   b. 4
   c. 8
   d. 16

6-6 SUPERNETTING, CIDR BLOCKS, AND VLSM

This section introduces supernetting, CIDR blocks, and VLSM. It shows how to borrow network bits to create CIDR blocks. An example shows how to verify that CIDR blocks have not crossed boundaries. This is an important concept because a CIDR block crossing a boundary will result in an IP address being mapped to the wrong subnet.

Supernetting
A technique that allows multiple contiguous classful networks to be combined into one larger network

A technique called **supernetting** was proposed in 1992 to eliminate class boundaries and to make available the unused IP address space. Supernetting allows multiple contiguous classful networks to be combined into one larger network, called a *supernet*. Supernetting is very useful in Internet routing and routing optimization because it means more network routes can be combined or summarized. Supernetting, also referred to as *route summarization* or *route aggregation*, is the opposite of subnetting, which involves partitioning a network into smaller subnets. Both subnetting and supernetting use custom subnet masks to overcome class boundaries.

With subnetting, you borrow from the host bits of the subnet mask to increase the network bits or create subnet bits. With supernetting, you increase the host bits of the subnet mask and borrow from the network bits instead. Also, whereas with subnetting, the result is multiple subnets, supernetting yields only one network or supernet as a result.

There are two basic rules involved in supernetting:

- The combined classful networks must be contiguous.
- The number of combined classful networks must be 2^n, where n is the number of network bits borrowed.

For example, two Class C networks, 192.168.2.0 and 192.168.3.0, can be combined:

The number of combined networks = $2n = 2$

Solving for n, $n = 1$. Therefore, the number of network bits borrowed is 1.

Borrowing 1 network bit from the original Class C subnet mask 255.255.255.0 yields a custom subnet mask, as shown here:

First Octet	Second Octet	Third Octet	Fourth Octet
255	.255	.254	.0
1111 1111	.1111 1111	.1111 1110	.0000 0000

This new supernet 192.168.2.0 has the custom subnet mask 255.255.254.0. The network address can be obtained the same way as in subnetting: by ANDing the Class C address 192.168.2.0 or 192.168.3.0 with the custom subnet mask. Inverting the host bits of the network address to 1s yields the broadcast address.

Borrowing a network bit increases the number of available IP addresses as well. A Class C address has 8 host bits, which yields $2^8 = 256$ available IP addresses. With this new supernet, there are now 9 host bits; therefore, the number of available hosts is $2^9 = 512$. The following table shows information about this new supernet:

Network Address	Broadcast Address	Usable IP Address Range
192.168.2.0	192.168.3.255	192.168.2.1–192.168.3.254

Supernetting requires a simpler way to indicate the subnet mask. The technique that has been developed for this is called *classless interdomain routing* (**CIDR**). CIDR (pronounced "cider") notation specifies the number of network bits set to 1 that make up the subnet mask. For example, the Class C size subnet mask 255.255.255.0 is listed in CIDR notation as /24. This indicates that 24 bits are all set to 1. A Class B size subnet is written as /16, and a Class A subnet is written as /8. CIDR can also be used to represent subnets that identify only part of the octet bits in an IP address. For example, the subnet mask 255.255.254.0, discussed earlier, is written in CIDR notation as /23. The /23 comes from the 23 bits that are set to a 1, as shown above.

CIDR
Classless interdomain routing

CIDR notation has now become a shorthand technique for writing subnet masks; it is not used only for supernetting. For example, the subnet mask 255.255.255.192 is written as /26. This notation shows the number of network and host bits used to create the subnet mask. In the case of a /26 subnet mask, 24 network bits and 2 host bits are being used. /26 is another custom subnet mask where class boundaries are not being crossed and network bits are not being borrowed.

A network address and the subnet mask 192.168.12.0 255.255.252.0 can be written in CIDR notation as 192.168.12.0/22. Table 6-15 provides the CIDR notations for the most common subnet masks.

TABLE 6-15 **CIDR–Subnet Mask Conversion**

CIDR Notation	Subnet Mask	CIDR Notation	Subnet Mask
/8	255.0.0.0	/21	255.255.248.0
/9	255.128.0.0	/22	255.255.252.0
/10	255.192.0.0	/23	255.255.254.0
/11	255.224.0.0	/24	255.255.255.0
/12	255.240.0.0	/25	255.255.255.128
/13	255.248.0.0	/26	255.255.255.192
/14	255.252.0.0	/27	255.255.255.224
/15	255.254.0.0	/28	255.255.255.240
/16	255.255.0.0	/29	255.255.255.248
/17	255.255.128.0	/30	255.255.255.252
/18	255.255.192.0	/31	255.255.255.254
/19	255.255.224.0	/32	255.255.255.255
/20	255.255.240.0		

CIDR Block
Used to break down class barriers in IP addressing

Two Class C networks, such as 192.168.2.0/24 and 192.168.3.0/24, can be grouped together as one supernet. You can group these two networks together by modifying the /24 CIDR number to /23. Writing these two networks in CIDR notation provides 192.168.2.0/23. This reduces the two Class C subnets to one larger network. A group of networks defined by CIDR notation is called a **CIDR block**. CIDR blocks are used to break down class barriers in IP addressing. The group of four IP addresses from 192.168.76.0 to 192.168.79.0 with CIDR notation /22 is a supernet. The CIDR block in this case can be represented as 192.168.76.0/22.

The problem with randomly applying CIDR blocks to Class A, B, and C addresses is that there are boundaries in each class, and these boundaries can't be crossed. If a boundary is crossed, the IP address maps to another subnet. For example, the CIDR block may be expanded to include four Class C networks. This means that all four Class C networks need to be specified by the same CIDR subnet mask to avoid crossing boundaries. The new subnet mask is 255.255.252.0. The following example demonstrates what happens if a boundary is crossed.

Example 6-10

Explore what happens if the boundary in IP addresses for Class C subnets is crossed. For this example, the subnets have the following IP addresses:

192.168.78.0/22

192.168.79.0/22

192.168.80.0/22

192.168.81.0/22

Solution

Applying the /22 subnet mask to 192.168.78.0 and 192.168.80.0 provides the following:

	Place Value	128	64	32	16	8	4	2	1
192.168.78.0	IP address	0	1	0	0	1	1	1	1
255.255.252.0	Subnet mask	1	1	1	1	1	1	0	0
192.168.76.0		0	1	0	0	1	1	0	0 (76)
					64 + 8 + 4 = 76				

Note

The binary values of the affected octet are shown, and applying the subnet mask means that the binary values of the IP address and the subnet mask are ANDed together.

Now the same subnet mask is applied to the 192.168.80.0 subnet:

	Place Value	128	64	32	16	8	4	2	1
192.168.80.0	IP address	0	1	0	1	0	0	0	0
255.255.252.0	Subnet mask	1	1	1	1	1	1	0	0
192.168.80.0		0	1	0	1	0	0	0	0 (80)
						64 + 16 = 80			

Applying the /22 subnet mask places these two IP addresses in different subnets. The first IP address is placed in the 76 subnet, and the second IP address is placed in the 80 subnet. The boundary line has been crossed: The IP addresses are in different subnets when /22 is applied.

This example shows what happens if a boundary is crossed in IP addressing. If four Class C subnets need to be grouped into one CIDR block, IP addresses from these ranges could be used:

192.168.76.0–192.168.79.0 (all of which will be in the 76 subnet)
192.168.80.0–192.168.83.0 (all of which will be in the 80 subnet)

In the earlier subnetting examples in this chapter, all subnets have used the same subnet mask when created. This means every subnet has the same number of hosts. However, in a real-world scenario, the requirements for each subnet may be different. Variable-length subnet masking (**VLSM**) was developed to enable the use of subnet masks to better fit the needs of the network and to efficiently use the IP address space. For example, with VLSM, a Class C network can be subnetted into four subnets of different sizes. Using the techniques described earlier in this section, you can create different sized subnets by using different custom subnet masks, as shown in Table 6-16.

VLSM
Variable-length subnet masking

TABLE 6-16 **Creating Subnets of Different Sizes**

Network Address	Broadcast Address	Custom Subnet Mask	Number of Available Hosts
192.168.1.0	192.168.1.127	255.255.255.128	128
192.168.1.128	192.168.1.191	255.255.255.192	64
192.168.1.192	192.168.1.223	255.255.255.224	32
192.168.1.224	192.168.1.255	255.255.255.224	32

Notice that these subnets do not overlap, and the subnets' boundaries are not violated. These subnets can be represented using the following CIDR blocks:

192.168.1.0/25
192.168.1.128/26
192.168.1.192/27
192.168.1.224/27

Careful planning is required to ensure that the IP addresses can all be specified by the same subnet mask. After reading this section, you should have an understanding of supernets, classless routing, and CIDR blocks. You should also understand CIDR notation and be able to determine whether a group of IP addresses is in the same subnet.

Section 6-6 Review

This section covers the following Network+ exam objective.

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

This section presents a technique for creating classless CIDR blocks. It is important to understand that to create CIDR blocks, bits are borrowed from the network bits.

Test Your Knowledge

1. Which of the following is the CIDR notation for the network address 192.168.6.0 and the subnet mask 255.255.254.0?
   a. 192.168.6.0/23
   b. 192.168.6.0/12
   c. 192.168.6.0/15
   d. 192.168.6.0/20
2. Which of the following is the subnet mask for CIDR block /22?
   a. 255.255.255.252
   b. 255.252.0.0
   c. 255.255.255.254
   d. 255.255.252.0

6-7 IPV6 ADDRESSING

This section examines the basics of IPv6 that students need to know. There are three types of IPv6 addresses: unicast, multicast, and anycast. Students should be aware of these address types as well as the 6to4 prefix, which has been proposed for use in the IPv4 to IPv6 transition. A good task is to have students research the current status of IPv6 on the Internet or have them ask their ISPs about IPv6.

Even though available address space for IPv4 has run out due to the rapid growth of the Internet and the development of many new Internet-compatible devices, IP version 4 (IPv4) is still the predominant TCP/IP addressing technique used on the Internet today. IP version 6 (**IPv6**) is the solution for expanding the possible number of users on the Internet. IPv6 is also called **IPng**, or IP Next Generation.

IPv6
IP version 6

IPng
IP Next Generation

Whereas IPv4 has a 32-bit address structure, IPv6 uses 128-bit addressing. IPv6 provides for a large number of IP addresses (2^{128}), which is roughly 3.4×10^{38} IP addresses. IPv6 numbers are written in hexadecimal rather than dotted decimal. For example, the following is a 32-hexadecimal-digit IPv6 address:

6789:ABCD:1234:EF98:7654:321F:EDCB:AF21

This address is classified as a **full IPv6 address** because each of the 32 hexadecimal positions contains a value other than 0.

Full IPv6 Address
An address in which all 32 hexadecimal positions contain a value other than 0

Note

Keep in mind that 32 hex digits × 4 bits per hex digit = 128 bits.

IPv6 use the dotted-decimal format of IPv4 because it would take many decimal numbers to represent an IPv6 address. Each decimal number takes at least 7 binary bits in American Standard Code for Information Interchange (ASCII) code. For example, the decimal equivalent of the first 8 hexadecimal characters in the previous full IPv6 address is as follows:

6	7	8	9	:A	B	C	D
103		.137		.171		.205	

This is the complete decimal equivalent number for the full IPv6 address shown earlier:

103.137.171.205.18.52.239.152.118.84.50.31.237.203.175.33

This decimal number is 42 characters long. In fact, the decimal equivalent number could be 48 decimal numbers long.

IPv6 uses seven colons (:) as separators to group the 32 hex characters into eight groups of four. Some IPv6 addresses contain one or more zeros. IPv6 addresses that contain zeros can be compressed to make them easier to write. For example, consider this IPv6 number:

6789:0000:0000:EF98:7654:321F:EDCB:AF21

You can drop consecutive 0s and replace them with a double-colon notation:

6789::EF98:7654:321F:EDCB:AF21

Recovering a compressed number from double-colon notation simply requires that all numbers to the left of the double notation be entered, beginning with the leftmost slot of the IPv6 address. Next, you can move on to the numbers to the right of the double colon. Begin with the rightmost slot of the IPv6 address slots and enter the numbers from right to left until the double colon is reached. Enter zeros into any empty slots, as shown here:

6789 :0 :0 :EF98 :7654 :321F :EDCB :AF21

You can convert an IPv4 number to IPv6 form by writing the IPv4 number in hexadecimal and placing the number to the right of a double colon. Example 6-11 demonstrates how to convert a dotted-decimal IP address to IPv6 hexadecimal.

Example 6-11

Convert the IPv4 address 192.168.5.20 to an IPv6 hexadecimal address.

Solution

First, convert each dotted-decimal number to hexadecimal:

Decimal	Hex
192	C0
168	A8
5	05
20	14

(*Hint: U*se a calculator or a lookup table to convert the decimal numbers to hexadecimal.) The IPv6 address will have many leading 0s; therefore, the IPv6 hex address can be written in double-colon notation:

::C0A8:0514

You can also write IPv4 numbers in IPv6 form by writing the IPv4 number in dotted-decimal format as shown here, with the number preceded by 24 hexadecimal 0s:

0000: 0000: 0000: 0000: 0000: 0000:192.168.5.20

This number can be reduced as follows:

::192.168.5.20

Much like IPv4 classless addresses, IPv6 addresses are fundamentally divided into a network portion followed by a host portion. The network portion is called the *network prefix,* and the number of bits used is the *prefix length*. The prefix is represented with a slash followed by the prefix length. (This is the same notation used with CIDR in IPv4.) For example, the IPv6 address 2001:DB8:FEED:BEEF::12 has a 64-bit network prefix. It can be represented as 2001:DB8:FEED:BEEF::12/64. In IPv6, the host portion of the address is called the *interface identifier*, or sometimes the *host identifier*. It is always 64 bits in length and is the last 64 bits of the 128-bit address. This automatically leaves 64 bits as the network prefix.

There are three types of IPv6 addresses: **unicast address**, **multicast address**, and **anycast address**. A unicast IPv6 address is used to identify a single network interface address, and data packets are sent directly to the computer with the specified IPv6 address. There are several types of unicast addresses, including **link-local addresses**, global unicast addresses, and unique local addresses. Link-local addresses are designed to be used for and are limited to communications on the local link. Every IPv6 interface has one link-local address.

A multicast IPv6 address is defined for a group of networking devices. Data packets sent to a multicast address are sent to the entire group of networking devices, such as a group of routers running the same routing protocol. Multicast addresses all start with the prefix FF00::/8. The next group of characters in the IPv6 multicast address (the second octet) is called the *scope*, or *scope options*. The scope bits are used to identify which ISP should carry the data traffic. The anycast IPv6 address is obtained from a list of addresses but is delivered only to the nearest node.

Unicast Address
An address that is used to identify a single network interface address, with data packets sent directly to the computer that has the specified IPv6 address

Multicast Address
An address that is used to send data packets to an entire group of networking devices, such as a group of routers running the same routing protocol

Anycast Address
An address obtained from a list of addresses

Link-Local Address
An address that is designed to be used for and is limited to communications on the local link

Transitioning to IPv6

Although IPv6 is increasingly being adopted and is being used in a number of major network sites, the Internet is still running IPv4 and will continue to do so for some time. A number of strategies are in place to help with the IPv4-to-IPv6 transition.

One possible technique for transitioning to IPv6 is to use the **6to4 prefix**, which essentially enables IPv6 sites to communicate over the IPv4 Internet. It requires the use of a 6to4-enabled router and 6to4 tunneling. It also requires the use of a 6to4 relay router that forwards 6to4 data traffic to other 6to4 routers on the Internet.

6to4 Prefix
A globally routable address that enables IPv6 hosts to communicate over the IPv4 Internet

Figure 6-23 illustrates the structure of the 6to4 prefix for hosts. The 32 bits of the IPv4 address fit into the first 48 bits of the IPv6 address.

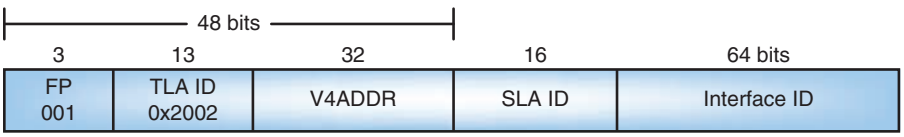


FIGURE 6-23 The 6to4 prefix format.

Note the following in Figure 6-23:

- **FP:** This is the format prefix, which is made up of the higher-order bits. The 001 indicates that this is a global unicast address.

Note

The current IPv6 address allocation can be viewed at www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml.

- **TLA ID (0x2002):** This is a top-level identifier issued to a local Internet registries. These IDs are administered by IANA (www.iana.org). The TLA ID, which is used to identify the highest level in the routing hierarchy, is 13 bits long.
- **V4ADDR:** This is the IPv4 address of the 6to4 endpoint and is 32 bits long.
- **SLA ID:** This is the site-level aggregation identifier that is used by individual organizations to identify subnets within their sites. The SLA ID is 16 bits long.
- **Interface:** This ID is the link-level host identifier, which is used to indicate an interface on a specific subnet. The interface ID is equivalent to the host IP address in IPv4.

The 6to4 prefix format enables IPv6 domains to communicate with each other even if they don't have an IPv6 ISP. In addition, IPv6 can be used within an intranet, but access to the Internet is still available. 6to4 provides unicast IPv6 connectivity between IPv6 host and via the IPv4 Internet.

Note

The term *dual stack* indicates that IPv4 and IPv6 are running at that same time.

Another notable transition technology is Toredo. Toredo is sometimes referred to as Microsoft Toredo as it was developed by Microsoft, and it is enabled by default on Microsoft operating systems. Toredo is a tunneling protocol that provides IPv6 connectivity for IPv6-capable devices that are on an IPv4 platform, and it works behind NAT (network address translation) devices. Toredo uses the IPv6 network prefix 2001::/32.

Stateless Address Autoconfiguration (SLAAC)
An IPv6 technique that enables serverless basic network configuration of IPv6 computers

Stateless address autoconfiguration (SLAAC) is another important feature of IPv6. SLAAC allows for a serverless basic network configuration of IPv6 computers. This means that even though an IPv6 DHCP server and an IPv6-enabled router are not involved, any IPv6 computer can self-configure its own link-local address. The term *link-local address* indicates that the IP address is self-configured. This means that any IPv6 host should be able to communicate with other IPv6 hosts on its local link or network.

The network prefix for link-local addresses is defined as FE80::/10. The interface identifier of the link-local address can be derived by transforming the 48 bits of the MAC address to 64 bits of the IEEE's EUI-64 (64-bit Extended Unique Identifier) format. If the privacy extensions for SLAAC are enabled on the operating system, the interface identifier is randomly generated. To complete the autoconfiguration, the subnet prefix FE80::/64 is then prepended to the interface identifier, creating a 128-bit link-local address.

To ensure that there is no duplicate address on the same link, the computer sends a neighbor solicitation (NS) message out on the link. The purpose of this solicitation is to discover the link-layer address of another IPv6 node or to confirm a previously determined link-layer address. If there is no response to the message, the computer assumes that the address is unique and therefore assigns the link-local address to its interface. The process of detecting another computer with the same IPv6 address is called *duplicate address detection* (*DAD*).

The EUI-64 transform algorithm is also used to derive the interface identifier for the global unicast address. With IPv4, a computer generally obtains its network settings from a DHCP server. With IPv6, SLAAC allows IPv6-enabled devices to connect to the network without requiring support of an IPv6 DHCP server; a device can automatically configure its network settings without a DHCP server by sending a router solicitation (RS) message to its IPv6 router. The router then sends back its router advertisement (RA) message, which contains network prefix information (the first 64 bits) that a computer can use with its own EUI-64 address (the last 64 bits).

SLAAC helps significantly simplify the deployment of IPv6 devices, especially in transient environments such as airports, train stations, stadiums, and hotspots.

The following example demonstrates how to convert the 48-bit MAC address 000C291CF2F7 to EUI-64 format:

1. Expand the 48-bit MAC address to 64-bit format by inserting FFFE in the middle of the 48 bits:

   000C29 **FFFE** 1CF2F7

2. Change the seventh bit, starting with the leftmost bit of the address, from 0 to 1. This seventh bit is referred to as the U/L bit (universal/local bit). 000C29 is 0000 0000 0000 1100 0010 1001 in binary format. When its seventh bit is changed to 1, it becomes 0000 0010 0000 1100 0010 1001, which is 020C29 in hexadecimal. The result is the EUI-64 address 020C29FFFE1CF2F7.

CIDR for IPv6

The concept of CIDR for IPv6 is the same as the concept of CIDR for IPv4. The biggest difference between IPv4 CIDR and IPv6 CIDR is in the network prefix representation. Remember that IPv4 uses a 32-bit address that can have a variable-length network prefix, with its maximum network prefix size being 32, represented as /32. This matches with its IP addressing bit. By design, IPv6 is structured to have 64 bits of network prefix for each LAN segment or subnet. This leaves 64 bits for IPv6 hosts on the subnet. To put this into perspective, one IPv6 subnet can have up to 2^{64} (18,446,744,073,709,551,616) IPv6 addresses.

The IPv4 CIDR notation is a network address followed by a slash (/) and then a network prefix—for example, 192.168.1.0/25. The IPv6 CIDR notation is very similar; it contains the IPv6 network address followed by a double colon (::), a slash (/), and then a network prefix. For example, a standard IPv6 subnet with a 64-bit prefix can be represented as 2001:db8::/64.

Table 6-17 shows a typical allocation of different IPv6 CIDR sizes.

TABLE 6-17 **Typical Allocation of Different IPv6 CIDR Sizes**

CIDR	Number of IPv6 Subnets
/64	1 IPv6 subnet
/56	256 IPv6 subnets (2^8)
/48	65,536 IPv6 subnets (2^{16})
/32	4,294,967,296 IPv6 subnets (2^{32})
/24	1,099,511,627,776 IPv6 subnets (2^{40})

When will the Internet switch to IPv6? The answer is not clear, but the networking community recognizes that something must be done to address the limited availability of current IP address space. As of late 2021, manufacturers had already incorporated IPv6 capabilities into their routers and operating systems, and it was estimated that 30% of networks had adopted IPv6. The switch to IPv6 will involve providing some way for IPv4 networks to continue to function. In addition, techniques such as NAT (refer to Chapter 1) have made it possible for intranets to use private address space and remain connected to the Internet. Such techniques have significantly reduced the number of IP addresses required for each network.

Section 6-7 Review

This section covers the following Network+ exam objectives.

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

This section provides an overview of IPv6 addressing. Make sure you understand the structure of IPv6 addressing. Key topics include the structure of an IPv6 address, tunneling for 6to4, and the three types of IPv6 addresses.

1.6 Explain the use and purpose of network services.

In the IPv6 multicast address, the second octet is called the scope, or scope options. The scope bits are used to identify which ISP should carry the data traffic. The EUI-64 transform algorithm is used to derive the interface identifier for the global unicast address. This feature helps significantly simplify the deployment of IPv6 devices, especially in transient environments such as airports, train stations, stadiums, and hotspots.

4.3 Given a scenario, apply network hardening techniques.

IPv6 has a router advertisement (RA) message, which contains network prefix information (the first 64 bits) that a computer can use with its own EUI-64 address (the last 64 bits).

Test Your Knowledge

1. What is a 6to4 prefix?
    a. An address that enables IPv4 hosts to communicate over the IPv6 Internet
    b. An address that enables IPv6 hosts to communicate over the IPv4 Internet
    c. An address used to separate an IPv6 address from a hex MAC address
    d. An address used to separate a MAC address from an IPv4 address
2. In regard to IPv6, what is the SLA ID?
    a. It replaces the MAC address in IPv6 and is 32 bits long.
    b. It is the site-level aggregation ID and 128 bits in length, and it replaces the 32-bit IPv4 address.
    c. It is the site-level aggregation ID and is used by individual networks to identify the subnets within their sites.
    d. It replaces the IP address in IPv6 and is 128 bits in length.

SUMMARY

This chapter presents an overview of the fundamentals of the TCP/IP protocol suite. TCP/IP is well established for carrying data traffic over the Internet. You should understand the following:

- The layers of the TCP/IP model and their relationship to the OSI model layers
- The basic structure of a 32-bit IPv4 address
- How to subnet a network
- How to apply subnet masks in networks
- The purpose of CIDR blocks and supernetting
- The data structure of an IPv6 hexadecimal address
- The structure and purpose of the 6to4 prefix

QUESTIONS AND PROBLEMS

Section 6-2

1. What are the four layers of the TCP/IP model?

   Application

   Transport

   Internet

   Network interface

2. Which layer of the TCP/IP model processes requests from hosts to ensure that a connection is made to the appropriate port?

   Application layer

3. What are well-known ports?

   Ports reserved by ICANN, ports 1–1023

4. Identify the port numbers for the following applications:

   a. Telnet

      23

   b. HTTP

      80

   c. FTP

      20, 21

d. DNS

53

e. DHCP

67, 68

5. Define the purpose of a *connection-oriented protocol* and give an example.

A connection-oriented protocol establishes a network connection, manages the data transfer, and terminates the connection. TCP is a connection-oriented protocol.

6. Which three packets are exchanged between two hosts when establishing a TCP connection?

SYN

SYN + ACK

ACK

7. What is the purpose of a sequence number (SEQ) in TCP data packets?

The sequence number is used to keep track of the data packets being transferred by the hosts.

8. Explain how a host knows that a data packet was not received.

The host that receives the data packets sends back an acknowledgment (ACK) that should contain the sum of sequence numbers in the previous packet plus the length of the current packet. The host that transmits the packet knows from the acknowledgment whether a packet was received.

9. Describe how a TCP connection is terminated.

The host terminating the connection sends a FIN packet. The other end host sends an ACK and then sends a FIN packet. This is acknowledged by the original host, and the connection is terminated.

10. What does *UDP* stand for, and what is it?

UDP stands for User Datagram Protocol. UDP is a protocol used to transport packets over a network without a connection being established and without any acknowledgment that the data packets arrived at the destination.

11. What is the purpose of the Internet layer in the TCP/IP suite?

The Internet layer defines the protocol used for addressing and routing the data packets.

12. What is the purpose of an ARP request?

It is a query asking which network interface has a specified IP address.

13. What is the purpose of an ARP reply?

An ARP reply returns the MAC address of a device.

14. Which important networking troubleshooting tool is part of ICMP, and how does it test a network connection?

    ping is a command that issues a series of echo requests, and the networking device receiving the echo request responds with echo replies.

15. When is IGMP used?

    IGMP is used when one host needs to send data packets to many destination hosts.

16. The network interface layer of the TCP/IP model defines how the host connects to which network?

    The type of network is not dictated by TCP/IP.

Section 6-3

17. Convert the following 8-bit binary number to decimal: 10010011.

128	64	32	16	8	4	2	1
1	0	0	1	0	0	1	1

    128 + 16 + 2 + 1 = 147

18. Convert the following octet to decimal: 11000000.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

    128 + 64 = 192

19. Convert the following 8-bit number to decimal: 11111100.

128	64	32	16	8	4	2	1
1	1	1	1	1	1	0	0

    128 + 64 + 32 + 16 + 8 + 4 = 252

20. Convert the following binary number to decimal: 11111111.

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

    128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

21. Convert the number 192 to its binary equivalent.

2	192	
2	96	0
2	48	0
2	24	0
2	12	0

2	6	0
2	3	0
2	1	1
	0	1

The binary equivalent is 11000000.

22. Convert the number 65 to its binary equivalent.

2	65	
2	32	1
2	16	0
2	8	0
2	4	0
2	2	0
2	1	0
	0	1

The binary equivalent is 1000001.

23. Convert the number 96 to its binary equivalent.

2	96	
2	48	0
2	24	0
2	12	0
2	6	0
2	3	0
2	1	1
0	1	

The binary equivalent is 1100000.

24. What is the hexadecimal equivalent of 13? (Refer to Table 6-5.)

The hexadecimal equivalent is D.

25. Convert 0x5AF3 to binary. Use Table 6-5.

Hex	5	A	F	3
Binary	0101	1010	1111	0011

26. Convert 1011011011110001 to hexadecimal.

Put binary digits in groups of four and use Table 6-5.

Binary	1011	0110	1111	0001
Hex	B	6	F	1

Section 6-4

27. What is the IP address range for Class C addresses?

    192.0.0.0–223.255.255.255

28. What is the purpose of Class D IP addresses?

    Class D addresses are used for multicasting.

29. How many bits are in an IPv4 address? How many octets (refer Table 6-5)?

    32 bits and 4 octets

30. An IPv4 address is typically expressed in what format?

    Dotted decimal

31. The IPv4 address 192.168.12.2 is an example of what address format?

    Dotted decimal

32. How many network bits are in each of the following classes?

    a. Class A

       8 bits

    b. Class B

       16 bits

33. How many network and host bits are in a Class C network address?

    24 network bits and 8 host bits

34. What is the purpose of a private IP address?

    It is intended for use in an intranet.

35. Can private IP addresses be routed?

    Yes, but only on intranets, not on the Internet.

36. How are private IP addresses handled on the Internet?

    They are blocked by the Internet service providers.

37. Which organization assigns IP addresses for North America?

    ARIN (American Registry for Internet Numbers)

Section 6-5

38. How many host bits are borrowed if four subnets are created?

    2 host bits are borrowed ($x = 2$).

39. What is the purpose of a subnet mask?

    A subnet mask identifies the network/subnet portion of an IP address.

40. A host computer is assigned IP address 192.168.12.8 and subnet mask 255.255.255.192. The host sends a packet to another host with IP address 192.168.12.65. Is the destination IP address in the same subnet as 192.168.12.8? Show why or why not.

No, it is not in the same subnet. The 192.168.12.65 address is in the 64 subnet:

192 .168 .12 .65

255 .255 .255 .192

192 .168 .12 .64

128	64	32	16	8	4	2	1	
0	1	0	0	0	0	0	1	**(65)**
1	1	0	0	0	0	0	0	**(192)**
0	1	0	0	0	0	0	0	**(64)**

41. The subnet mask 255.255.255.224 is applied to a packet with destination IP address 192.168.12.135. Which subnet is the packet sent to? Show your work.

The packet is sent to the 192.168.12.128 subnet.

192 .168 .12 .135

255 .255 .255 .224

192 .168 .12

128	64	32	16	8	4	2	1	
1	0	0	0	0	1	1	1	**(135)**
1	1	1	0	0	0	0	0	**(224)**
1	0	0	0	0	0	0	0	**(128)**

42. The subnet mask 255.255.255.0 is applied to packets with the following IP addresses. Which subnet is each packet sent to? Show your work.

a. 10.20.35.12

10 .20 .35 .12

255 .255 .255 .0

10 .20 .35 .0 subnet

b. 10.20.35.3

10 .20 .35 .3

255 .255 .255 .0

10 .20 .35 .0 subnet

c. 10.50.35.6

10 .50 .35 .6

255 .255 .255 .0

10 .50 .35 .0 subnet

d. 192.168.12.8

192 .168 .12 .8

255 .255 .255 .0

192 .168 .12 .0 subnet

43. Given the IP address 193.10.10.0 and assuming that four subnets are to be created, answer the following questions.

a. What are the network address and the broadcast address for each subnet?

	Network Address	Broadcast Address
First subnet	193.10.10.0	193.10.10.63
Second subnet	193.10.10.64	193.10.10.127
Third subnet	193.10.10.128	193.10.10.191
Fourth subnet	193.10.10.192	193.10.10.255

b. What is the subnet mask?

255. 255. 255. 192

c. What is the number of usable hosts per subnet?

62

44. Given network IP address 211.123.83.0 and assuming eight subnets are to be created, answer the following questions. The eight subnets include the network address and broadcast address.

a. What are the network address and the broadcast address for each subnet?

	Network Address	Broadcast Address
First subnet	211.123.83.0	211.123.83.31
Second subnet	211.123.83.32	211.123.83.63
Third subnet	211.123.83.64	211.123.83.95
Fourth subnet	211.123.83.96	211.123.83.127
Fifth subnet	211.123.83.128	211.123.83.159
Sixth subnet	211.123.83.160	211.123.83.191
Seventh subnet	211.123.83.192	211.123.83.223
Eighth subnet	211.123.83.224	211.123.83.255

b. What is the subnet mask?

255.255.255.224

c. What is the number of usable hosts per subnet?

30 (32)

45. Complete the following table, given Class C subnetting.

Number of Mask Bits	Subnet Mask	Number of Subnets	Number of Usable Hosts/Subnet
2	255.255.255.192	4	62
3	255.255.255.224	8	30
4	255.255.255.240	16	14
5	255.255.255.248	32	6
6	255.255.255.252	64	2

Section 6-6

46. Complete the following table.

128.123.0.0	B	/30	255.255.255.252	16384	2
135.45.0.0	B	/25	255.255.255.128	512	126
193.10.10.0	C	/28	255.255.255.240	16	14
211.123.83.0	C	/26	255.255.255.192	4	62
10.0.0.0	A	/13	255.248.0.0	32	524286
32.0.0.0	A	/20	255.255.240.0	4096	4094
204.204.5.0	C	/28	255.255.255.240	16	14
223.201.65.0	C	/27	255.255.255.224	8	30
156.35.0.0	B	/21	255.255.248.0	32	2046
116.0.0.0	A	/14	255.252.0.0	64	262142
145.23.0.0	B	/29	255.255.255.248	8192	6
199.12.1.0	C	/30	255.255.255.252	64	2
15.0.0.0	A	/29	255.255.255.248	2097152	6

47. What is the CIDR notation for network address 192.168.6.0 and subnet mask 255.255.254.0?

192.168.6.0/23

48. A CIDR block contains the subnets with the following IP addresses:

192.168.68.0/22

192.168.69.0/22

192.168.70.0/22

192.168.71.0/22

Are there any problems with this group of subnets in the CIDR block? Show your work.

There are no problems with the IP addresses. No boundary has been crossed.

192.168.68 .0

255.255.252.0

192.168.68 .0

128	64	32	16	8	4	2	1	
0	1	0	0	0	1	0	0	(68)
1	1	1	1	1	1	0	0	(252)
0	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**[68 subnet]**

192.168.69 .0

255.255.252.0

192.168.68 .0

128	64	32	16	8	4	2	1	
0	1	0	0	0	1	0	1	(69)
1	1	1	1	1	1	0	0	(252)
0	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**[68 subnet]**

192.168.70 .0

255.255.252.0

192.168.68 .0

128	64	32	16	8	4	2	1	
0	1	0	0	0	1	1	0	(70)
1	1	1	1	1	1	0	0	(252)
0	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**[68 subnet]**

192.168.71 .0

255.255.252.0

192.168.68 .0

128	64	32	16	8	4	2	1	
0	1	0	0	0	1	1	1	(71)
1	1	1	1	1	1	0	0	(252)
0	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**[68 subnet]**

Section 6-7

49. How many bits are in an IPv6 address?

    128 bits

50. In what format are IPv6 numbers written?

    Hexadecimal

51. Express the following IPv6 numbers using double-colon notation:

    a. 5355:4821:0000:0000:0000:1234:5678:FEDC

       5355:4821::1234:5678:FEDC

    b. 0000:0000:0000:1234:5678:FEDC:BA98:7654

       ::1234:5678:FEDC:BA98:7654

    c. 1234:5678:ABCD:EF12:0000:0000:1122:3344

       1234:5678:ABCD:EF12::1122:3344

52. Express the IPv4 IP address 192.168.12.5 in IPv6 form using dotted-decimal and double-colon format.

    ::192.168.12.5

53. Expand the IPv6 address from the following double-colon notation:

    1234:5678::AFBC

    1234:5678:0:0:0:0:0:AFBC

54. What is the 6to4 prefix?

    An address that enables IPv6 hosts to communicate over the IPv4 Internet

55. What is the purpose of a 6to4 relay router?

    A 6to4 relay router forwards 6to4 data traffic to other 6to4 routers on the Internet.

56. How many subnets do you get with a /56 CIDR in IPv6?

    256 IPv6 subnets

Critical Thinking

57. Your boss has read about IPv6 and wants to know whether the network you oversee is ready for the transition. Prepare a response, based on the networking and computer operating systems used in your facility.

    The students' answers should address the current status of IPv6 and the Internet. This is a dynamic situation, so the answers will vary. Students should check the following in their networks:

    - Is their operating software IPv6 compatible, and how do they know whether it is?

- Are the routers IPv6 compatible or upgradable?
- Is the ISP using IPv6?

58. Your ISP assigns your company a 206.206.155.0/24 CIDR block. Your company has four different networks:

    Network A: 50 users
    Network B: 26 users
    Network C: 12 users
    Network D: 10 users

    Your job is to create four subnets and allocate enough IP addresses for the users within the network. Document how you will do this.

    You can change the CIDR block to any private IP range, such as 172.16.1.0/24. Using the public IP range in this situation is more realistic, however, because the ISP only assigns a public IP CIDR.

    Several answers could satisfy the design criteria. Here are two of them:

    a. The following assignment will leave room to create more subnets if you need to add more networks:

       Network A: 206.206.155.0 255.255.255.192

       Network B: 206.206.155.64 255.255.255.224

       Network C: 206.206.155.96 255.255.255.240

       Network D: 206.206.155.112 255.255.255.240

    b. The following assignment will leave room for adding more users:

       Network A: 206.206.155.0 255.255.255.192

       Network B: 206.206.155.64 255.255.255.192

       Network C: 206.206.155.128 255.255.255.192

       Network D: 206.206.155.192 255.255.255.192

Certification Questions

59. The IP address 10.0.0.0 is a Class _____ address and, with the a CIDR of /13, has the subnet mask ____ with ____ subnets and ____ hosts/subnet.

    a. A, 255.248.0.0, 32, 524286
    b. A, 255.255.255.248. 2097150, 6
    c. A, 255.255.0.0, 62, 262142
    d. None of these answers are correct.

60. The IP address 156.35.0.0 is a Class _____ address and, with a CIDR of /21, has the subnet mask ____ with ____ subnets and ____ hosts/subnets.

    a. B, 255.255.255.252, 16382, 2
    b. B, 255,255,255,128, 510, 126
    c. B, 255.255.255.240, 14, 14
    d. None of these answers are correct.

61. The IP address 192.12.1.0 is a Class _____ address and, with a CIDR of block /30, has a subnet mask of ____ with ____ subnets and ____ hosts/subnet.

    a. C, 255.255.255.252, 64, 2
    b. C, 255.255.248.0, 30, 2046
    c. C, 255.255.255.240, 14, 14
    d. None of these answers are correct.

62. Which of the following are true of IPv4 addressing? (Select all that apply.)

    a. It is currently being used on the Internet.
    b. It uses four classes of IP addresses.
    c. It uses five classes of IP addresses.
    d. It is being replaced by IPv5.
    e. It is being replaced by IPv6.

63. What is the broadcast address for a host at 192.168.20.15 using the subnet mask 255.255.255.192?

    a. 192.168.20.63
    b. 192.168.20.0
    c. 192.168.20.127
    d. 192.168.20.255
    e. None of these answers are correct.

64. Given network IP address 192.168.12.0 and subnet mask 255.255.255.252, how many usable host IP addresses are provided?

    a. 2
    b. 4
    c. 8
    d. 16
    e. 0

65. A network with IP address 172.16.0.0 is divided into eight subnets. What are the network addresses for the subnets?

    a. 172.16.0.0, 172.16.32.0, 172.16.64.0, 172.16.96.0, 172.16.128.0, 172.16.160.0, 172.16.192.0, 172.16.224.0

    b. 172.16.0.0, 172.16.0.32, 172.16.0.64, 172.16.0.96, 172.16.0.128, 172.16.0.160, 172.16.0.192, 172.16.0.224

    c. 172.16.0.255, 172.16.32.255, 172.16.64.255, 172.16.96.255, 172.16.128.255, 172.16.160.255, 172.16.192.255, 172.16.224.255

    d. None of these answers are correct.

66. True or false: Well-known ports are reserved by ICANN and range from 1 to 23.

    False

67. True or false: Port numbers from 1024 to 49,151 are known as private ports.

    False

68. True or false: The network layer defines how data packets are routed in a network.

    True

This page intentionally left blank

7
CHAPTER

Introduction to Router Configuration

Chapter Outline

7-1 Introduction
7-2 Router Fundamentals
7-3 The Router's User EXEC Mode (**Router>**)
7-4 The Router's Privileged EXEC Mode (**Router#**)
7-5 Configuring the Network Interface: Auto-negotiation
7-6 Troubleshooting the Router Interface
Summary
Questions and Problems

Objectives

- Describe the purpose of a router
- Describe the purpose of a gateway
- Describe the steps (software and hardware) for connecting to a router's console port
- Describe the Cisco IOS command structure
- Define the function of the command-line interface
- Define the functional difference between a router's user and privileged EXEC modes
- Know how to enter basic router configuration modes
- Demonstrate that you can enable and disable certain router interfaces
- Describe what information is contained in the running configuration file

Key Terms

Cisco IOS
command-line interface (CLI)
CCNA
CCNP
CCIE
broadcast domain
flat network
routed network
layer 3 network
default gateway address
next hop address
subnet, NET
hostname
user EXEC mode
user mode
?
show flash
show version
router uptime
privileged mode
enable
Router#
configure terminal (**conf t**)
Router(config)#
Router(config-line)#
Router(config-if)#
no shutdown (**no shut**)
show ip interface brief (**sh ip int brief**)
DCE
DTE
auto-negotiation
fast link pulse (FLP)
half-duplex
keepalive packet
administratively down

Cisco IOS
Cisco Internet Operating System, the operating software used in all Cisco routers

Command-Line Interface (CLI)
A type of interface used for inputting commands and configuring devices such as routers

CCNA
Cisco Certified Network Associate

CCNP
Cisco Certified Network Professional

CCIE
Cisco Certified Internetwork Expert

The main objective of this chapter is to introduce the use of the **Cisco IOS** (Internetwork Operating System) software for configuring routers. Cisco IOS is the operating software used to configure all Cisco routers. It includes a **command-line interface (CLI)** for inputting instructions to configure the Cisco router interface. There are many choices for routers in the market; however, Cisco routers have set the standard. Also, Cisco certifications such as the Cisco Certified Network Associate (**CCNA**); the Cisco Certified Network Professional (**CCNP**); and the professional benchmark for internetworking expertise, the Cisco Certified Internetwork Expert (**CCIE**), test the candidate's ability to configure, troubleshoot, and analyze local area networks (LANs) that incorporate Cisco routers and switches.

7-1 INTRODUCTION

This chapter presents an introduction to routers. It first provides a review of router fundamentals and an introduction to the hardware and software needed to establish a router console connection. It also discusses concepts related to accessing a router's user and privileged modes. This chapter includes challenges that take advantage of the Net-Challenge software that is available from the book's companion website. (See the Introduction for information on how to access this site.) This software will help you test students' knowledge of router configuration.

Section 7-2, "Router Fundamentals," provides an overview of router fundamentals. It further examines some of the router concepts and terminology presented in Chapter 4, "Wireless Networking," including the following:

- Interconnecting LANs with routers
- Network segment
- Data flow through a routed network

Sections 7-3, "The Router's User EXEC Mode (**Router>**)," and 7-4, "The Router's Privileged EXEC Mode (**Router#**)," introduce the steps for accessing and configuring the router interface. These sections show how to work with the Cisco IOS command structure and how to access many of the configuration layers in Cisco IOS. Sections 7-3 and 7-4 also include router configuration challenges using the Net-Challenge software that is available from this book's companion website. (See the Introduction for information on how to access this site.) These challenges enable you to test your ability to access and program a router's interface. The simulator software was developed specifically for this text and emulates the experience of programming the interface of a Cisco router. The software emulates the console port connection, and although it doesn't emulate all the router programming modes or operational features, it does emulate the functions presented in this chapter.

Table 7-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 7-1 **Chapter 7 CompTIA Network+ Objectives**

Domain/ Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.2	Explain the characteristics of network topologies and network types.	7-2, 7-4
1.3	Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	7-5
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes.	7-2
1.5	Explain common ports and protocols, their application, and encrypted alternatives.	7-2, 7-4
1.7	Explain basic corporate and datacenter network architecture.	7-5
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	7-2, 7-3, 7-4
2.2	Compare and contrast routing technologies and bandwidth management concepts.	7-2, 7-4
2.3	Given a scenario, configure and deploy common Ethernet switching features.	7-2, 7-5
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	7-4, 7-6
3.2	Explain the purpose of organizational documents and policies.	7-3
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	7-2, 7-3
4.0	**Network Security**	
4.3	Given a scenario, apply network hardening techniques.	7-6
4.4	Compare and contrast remote access methods and security implications.	7-6
5.0	**Network Troubleshooting**	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	7-5, 7-6
5.3	Given a scenario, use the appropriate network software tools and commands.	7-3, 7-4
5.5	Given a scenario, troubleshoot general networking issues.	7-2

7-2 ROUTER FUNDAMENTALS

This section introduces broadcast domains and flat networks. Students should understand why it is not desirable to have multiple networks connected in one broadcast domain. This section also provides a review of IP data traffic flow and talks about gateways. It provides an example of subnets and how to determine the destination for a data packet.

This section further defines the function of a router in a network and describes how data packets travel through a layer 3 network. A layer 3 network uses IP addressing for routing data packets to the final destination. Delivery of data packets is made possible by the use of a destination MAC address, an IP address, network addresses, and routing tables. This section examines each of these concepts.

LANs are not necessarily restricted in size. A LAN can have 20 computers, 200 computers, or even more. Multiple LANs also can be interconnected to essentially create a single large LAN. For example, the first floor of a building could be set up as one LAN, the second floor as another LAN, and the third floor as another. The three LANs in the building could be interconnected into essentially one large LAN through the use of switches, with the switches interconnected as shown in Figure 7-1.

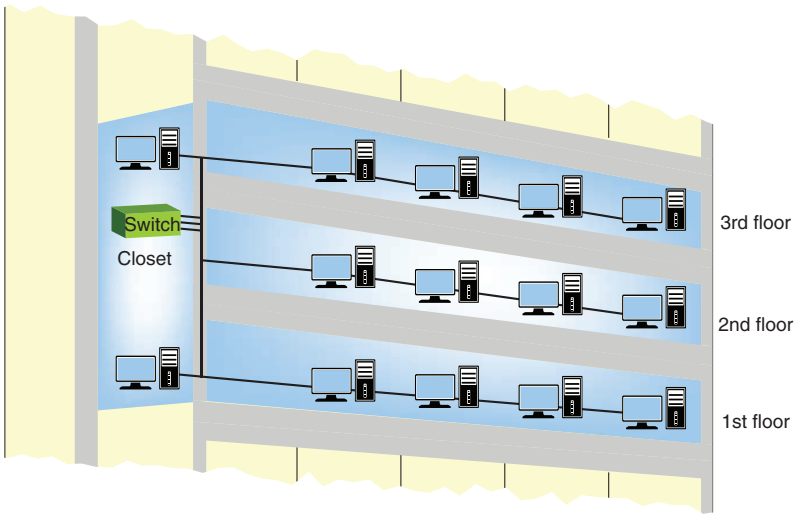


FIGURE 7-1 Three floors of a building interconnected using switches to form one large LAN.

Broadcast Domain
A portion of a network in which any broadcast sent out on the network is seen by all hosts

Is it problematic to interconnect LANs this way? As long as switches are being used to interconnect the computers, the interconnection of the LANs has minimal impact on network performance. This is true as long as there are not too many computers in the LAN. The number of computers in the LAN is an issue because layer 2 switches do not by default separate **broadcast domains**. This means that any broadcast sent out on the network (for example, the broadcast associated with an ARP request) will be sent to all computers in the LAN. Excessive broadcasts are a problem because each computer must process a broadcast to determine whether it needs to respond; this essentially slows down the computer and the network. Virtual LANs (VLANs) are now being used to interconnect LANs. This concept is examined in Chapter 8, "Introduction to Switch Configuration."

A network with multiple LANs interconnected at the layer 2 level is called a **flat network**. In a flat network, the LANs share the same broadcast domain. The use of a flat network should be avoided if possible for the simple reason that the network response time is greatly affected. Using layer 3 networks helps avoid flat networks, as discussed in the next section.

Flat Network
A network where the LANs share the same broadcast domain

Layer 3 Networks

In both the simple office-type LAN introduced in Chapter 1, "Introduction to Computer Networks," and the building LAN just discussed, the hosts are interconnected with a switch. The switch allows data to be exchanged within the LAN; however, data cannot be routed to other networks. Also, the broadcast domain of one LAN is not isolated from another LAN's broadcast domain. The solution for breaking up the broadcast domains and providing network routing is to incorporate routing hardware into the network design to create a **routed network**. A routed network uses layer 3 addressing for selecting routes to forward data packets, so a better name for this type of network is **layer 3 network**.

Routed Network
A network that uses layer 3 addressing for selecting routes to forward data packets

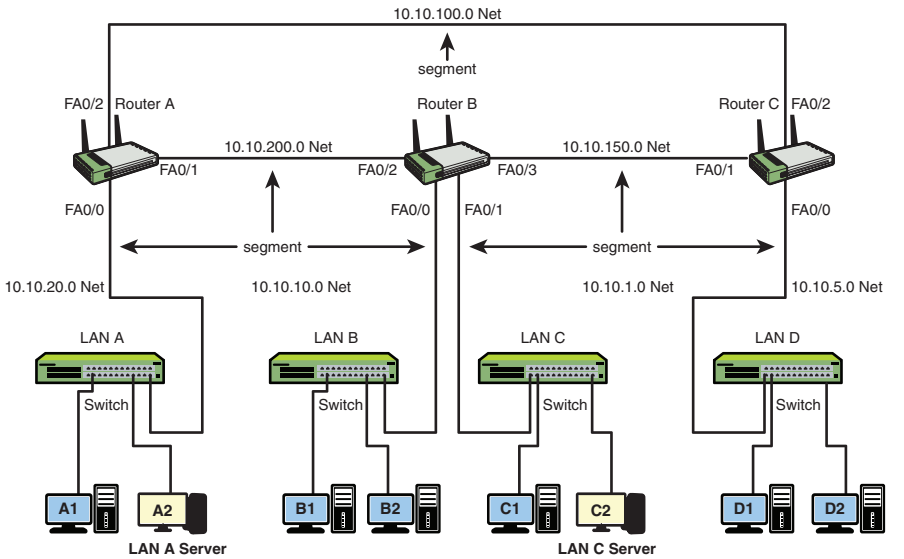
Layer 3 Network
Another name for a routed network

In layer 3 networks, routers and layer 3 switches are used to interconnect the LANs and other networks in order to isolate broadcast domains and enable hosts from different LANs and networks to exchange data. Data packet delivery is achieved by handing off data to adjacent routers until the packet reaches its final destination. This typically involves passing data packets through many routers and many networks. Figure 7-2 shows an example of a layer 3 network. This example has four LANs interconnected using three routers. The IP addresses for the networking devices are listed. How does information get from computer A1 in LAN A to computer C1 in LAN C? The following discussion describes the travel of the data packets.

Computer A1 (IP address 10.10.20.1) sends a data packet to computer C1 (IP address 10.10.1.1). Computer A1 uses the assigned subnet mask (255.255.255.0) to determine whether the destination IP address 10.10.1.1 is in the same subnet or network as itself. Applying the subnet mask to the destination address shows that the final destination of the data packet is the 10.10.1.0 network (10.10.1.0 NET). This is not the same subnet or network in which computer A1 resides (10.10.20.0 NET). Therefore, the data packet is forwarded to the **default gateway address** defined by the computer. The default gateway address is the IP address of a networking device (for example, a router) used to forward data that needs to exit the LAN. Figure 7-3 provides an example of setting a computer's default gateway address. The default gateway address for computer A1 is 10.10.20.250. This is the IP address of Router A's FastEthernet0/0 port. Figure 7-2 shows that Router A's FastEthernet FA0/0 port connects directly to the switch in LAN A.

Default Gateway Address
The IP address of the networking device used to forward data that needs to leave the LAN

Recall that the term *gateway* describes a networking device that enables data to enter and exit a LAN and that the gateway is where the host computers forward data packets that need to exit the LAN. In most networks, the gateway is typically a router or switch port address. An example of a gateway is provided in the block diagram shown in Figure 7-4. Keep in mind that the IP address of the gateway must be in the same subnet as the LAN that connects to the gateway, and this same gateway enables data traffic to enter and exit the LAN. An example of using the subnet mask to determine the destination network is provided in Example 7-1.



Router A Port Addresses (LAN A)		Router B Port Addresses (LAN B)		Router B Port Addresses (LAN C)		Router Port Addresses (LAN D)	
FastEthernet 0/0 (Gateway Address)	10.10.20.250	FastEthernet 0/0 (Gateway Address)	10.10.10.250	FastEthernet 0/1 (Gateway Address)	10.10.1.250	FastEthernet 0/0 (Gateway Address)	10.10.5.250
FastEthernet 0/1	10.10.200.1	FastEthernet 0/2	10.10.200.2	FastEthernet 0/2	10.10.200.2	FastEthernet 0/1	10.10.150.2
FastEthernet 0/2	10.10.100.1	FastEthernet 0/3	10.10.150.1	FastEthernet 0/3	10.10.150.1	FastEthernet 0/2	10.10.100.2
LAN A Computers		**LAN B Computers**		**LAN C Computers**		**LAN D Computers**	
Computer A1	10.10.20.1	Computer B1	10.10.10.1	Computer C1	10.10.1.1	Computer D1	10.10.5.1
Computer A2	10.10.20.2	Computer B2	10.10.10.2	Computer C2	10.10.1.2	Computer D2	10.10.5.2
Subnet Mask	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***

FIGURE 7-2 An example of a layer 3 network with routers interconnecting the LANs.

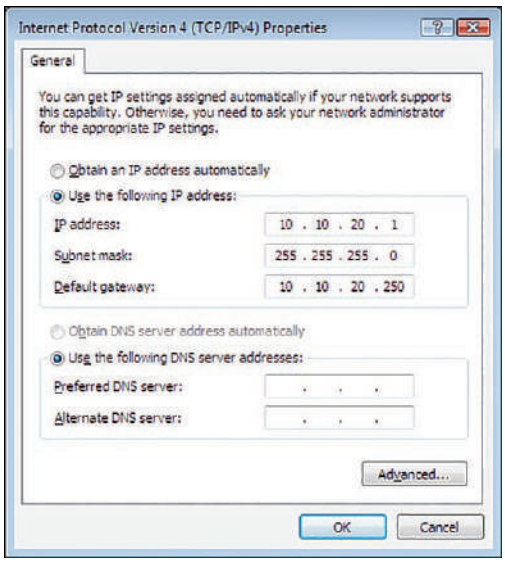


FIGURE 7-3 The TCP/IP dialog for setting the default gateway address for computer A1.

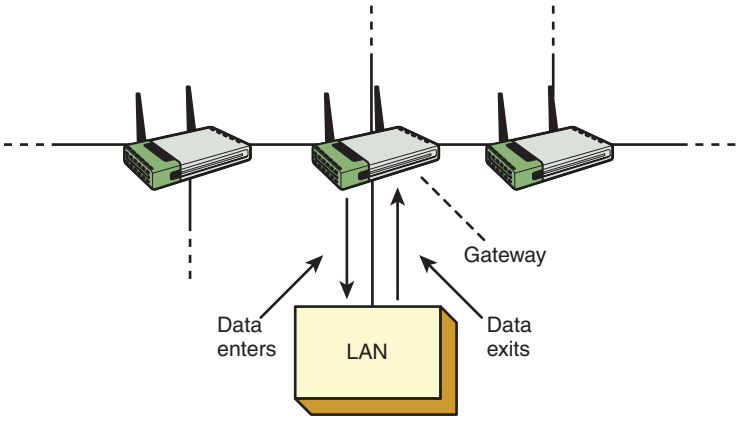


FIGURE 7-4 Data flow to and from the gateway.

Example 7-1

A computer host sends two data packets out on the network. The two packets have different IP destination addresses. Determine whether the data packets are to be forwarded to the default gateway or whether they should remain in the same LAN as the host. The source host IP address is 10.10.20.2, and the subnet mask 255.255.255.0 is being used. The destination IP addresses for the data packets are 10.10.1.1 and 10.10.20.3.

Solution

First, determine the network or subnet where the source host resides. This can be determined by ANDing the subnet mask with the source host IP address, as shown. (Chapter 6, "TCP/IP," discusses subnet masks and subnets, and you should review it if this concept is difficult to follow.) Remember that subnet masking is a binary AND operation. The decimal numbers are the equivalent of the 7-bit binary number. Here is an example:

255	1 1 1 1 1 1 1 1
20	0 0 0 1 0 1 0 0
10	0 0 0 0 1 0 1 0
2	0 0 0 0 0 0 1 0
Source IP address	10. 10. 20. 2
Subnet mask	255. 255. 255. 0
Subnet	10. 10. 20. 0

Therefore, the source host is in the 10.10.20.0 subnet (10.10.20.0 NET).

a. Determine the destination network for a data packet, given the following information:

Destination IP address	10. 10. 1. 1
Subnet mask	255.255.255. 0
Subnet	10. 10. 1. 0

Answer: The destination subnet address for Part a is 10.10.1.0. This is not in the same subnet as the 10.10.20.2 host (10.10.20.0 NET). Therefore, the data packet is forwarded to the default gateway.

b. Determine the destination network for a data packet, given the following information:

Destination IP address	10. 10. 20. 3
Subnet mask	255. 255. 255. 0
Subnet	10. 10. 20. 0

Answer: The destination subnet address for Part b is 10.10.20.0, which is the same subnet as the host. Therefore, the data packet remains in the 10.10.20.0 subnet.

Next Hop Address
The IP address of the next networking device that can be used to forward a data packet to its destination

The router examines the IP address of the data packet sent from the source computer to the gateway and selects a next hop address. The gateway examines the destination IP addresses of all data packets arriving at its interface. The router uses a routing table to determine a network data path and the next hop address. As noted previously, a *routing table* lists the possible networks that can be used to route the data packets. Alternative data paths are usually provided so that a new route can be selected and data delivery can be maintained if a network route is down. The **next hop address** is the IP address of the next networking device that can be used to forward a data packet to its destination.

For example, refer to Figure 7-2 and assume that a data packet is to be delivered from a host in LAN A to a destination address in LAN C. The data packet is forwarded to the LAN A gateway, which is the FastEthernet0/0 (FA0/0) port on Router A. The router examines the data packet and determines that the data can be sent to the host in LAN C via Router A's FastEthernet0/2 (FA0/2) interface over the 10.10.100.0 NET to Router C, then to Router B, and finally to LAN C. The routing table also shows that there is a route to LAN C via Router A's FastEthernet0/1 (FA0/1) interface over the 10.10.200.0 NET. The next hop from Router A's FastEthernet0/1 (FA0/1) interface is the FA0/2 FastEthernet interface on Router B. Which is the better route?

In terms of hops, data from LAN A will have to travel over two hops (Router C and Router B) to reach LAN C. The route to LAN C via Router B requires only one hop; therefore, Router A will select the 10.10.200.0 NET to route the data to LAN C because it involves fewer router hops. The IP address of the FastEthernet0/2 (FA0/2) port on Router B is the next hop address. In each case, the next hop address is the IP address of the next networking device. For example, if the data travels to LAN C via Router B, the next hop address from Router A is the IP address of the FastEthernet0/2 (FA0/2) port on Router B (10.10.200.2).

The MAC address is used to define the hardware address of the next hop in the network. When the next hop is defined, its MAC address is determined, and the data packet is relayed.

When the routes are fully configured, data packets can be exchanged between any LANs in the interconnected routed network. For example, data can be exchanged between any of the hosts in any of the LANs shown in Figure 7-2. Computer A2 in LAN A can exchange data with computer D1 in LAN D, and computer C1 in LAN C can exchange data with computer B2 in LAN B. This differs from the simple office LAN that has restricted data packet delivery: The data packets can be exchanged only within the LAN. Using IP addressing and routers enables the data to be delivered outside the LAN. Recall that a *segment* in a network defines the physical link between two internetworking devices (for example, router–hub, router–switch, or router–router). For example, in an interconnected network, a segment is a link between a router and another router. Another example is the segment that connects a router to a LAN via a hub or a switch. Each network segment has its own network address. For the small campus network shown in Figure 7-2, the network IP address for the segment connecting LAN A to the router is 10.10.20.0. All hosts connected to this segment must contain a 10.10.20.*x* address. For example, computer A1 is assigned the IP address 10.10.20.1.

The segment is sometimes called the **subnet**, or **NET**. These terms are associated with a network segment address, such as 10.10.20.0. In this case, the network is called the 10.10.20.0 NET. All hosts in the 10.10.20.0 NET have a 10.10.20.x IP address. The network addresses are used when configuring the routers and defining which networks are connected to the router. For example, the networks attached to Router A in Figure 7-2 are listed in Table 7-2.

Subnet, NET
A network segment

TABLE 7-2 **The Networks (Subnets) Attached to Router A in Figure 7-2**

Router Port	Subnet
FA0/0	10.10.20.0
FA0/1	10.10.200.0
FA0/2	10.10.100.0

The physical layer interface on a router provides a way to connect the router to other networking devices on the network. For example, the FastEthernet ports on the router are used to connect to other FastEthernet ports on other routers. Gigabit and 10 Gigabit Ethernet ports are also available on routers to connect to other high-speed Ethernet ports. (The sample network shown in Figure 7-2 includes only FastEthernet ports.) Routers also contain serial interfaces that are used to interconnect the router and the network to other serial communication devices. For example, connection to wide area networks (WANs) requires the use of a serial interface to connect to a communications carrier, such as T-Mobile, Verizon, or AT&T. The data speeds for the serial communication ports on routers can vary from slow (56Kbps) up to high-speed DS-3 data rates (47Mbps+), OC-3 (155Mbps), OC-12 (622Mbps), or even OC-192 (9953Mbps).

To provide a summary of the discussion on layer 3 networks, Figure 7-5 shows the components of a layer 3 network. The source host computer has an installed network interface card (NIC) and an assigned IP address and subnet mask.

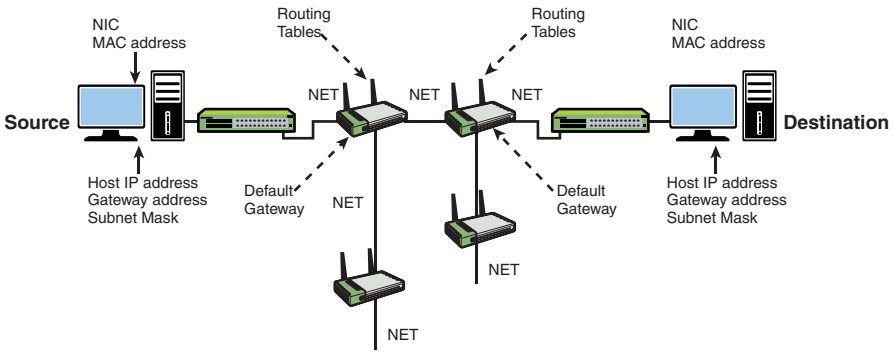


FIGURE 7-5 The components of a layer 3 network.

The subnet mask is used to determine whether the data should stay in the LAN or be forwarded to the default gateway provided by the router. The router uses its subnet mask to determine the destination network address. The destination network address is checked in the router's routing table to select the best route to the destination. The data is then forwarded to the next router, which is the next hop address. The next router examines the data packet, determines the destination network address, checks its routing table, and then forwards the data to the next hop. If the destination network is directly connected to the router, it issues an ARP request to determine the MAC address of the destination host. Final delivery is then accomplished by forwarding the data using the destination host computer's MAC address. Routing of the data through the networks occurs at layer 3, and the final delivery of data in the network occurs at layer 2.

Section 7-2 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.

This section discusses how routers are used to interconnect a network to other serial communication devices. For example, connection to WANs requires the use of a serial interface to connect to a communications carrier.

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

As discussed in this section, a broadcast domain is a portion of a network in which any broadcast sent out on the network is seen by all hosts.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

This section shows the TCP/IP dialog for setting the default gateway address for a computer.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

As discussed in this section, a segment in a network defines the physical link between two internetworking devices (for example, router–hub, router–switch, or router–router).

2.2 Compare and contrast routing technologies and bandwidth management concepts.

As discussed in this section, a layer 3 network uses IP addressing for routing data packets to the final destination. Delivery of data packets is made possible by the use of a destination MAC address, an IP address, network addresses, and routing tables.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

As discussed in this section, any broadcast sent out on the network (for example, the broadcast associated with an ARP request) will be sent to all computers in the LAN.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section introduces router configuration. Make sure you fully understand how to properly work with the command-line interface.

5.5 Given a scenario, troubleshoot general networking issues.

A router uses a routing table to determine a network data path and the next hop address. A routing table is a list of the possible networks that can be used to route data packets.

Test Your Knowledge

1. True or false: The purpose of a gateway is to allow data to enter and exit a LAN.

   True

2. What is a broadcast domain?

   a. A network where LANs share broadcasts
   b. A place to which networks forward data packets that need to leave the domain
   c. A portion of a network in which any broadcasts sent out on the network are seen by all hosts
   d. Another name for a routed network

3. What is a next hop address?

   a. Another name for the default gateway address
   b. The IP address of the next networking device that can be used to forward a data packet to its destination
   c. The IP address of the next networking device that can be used to forward a data packet to its source
   d. None of these answers are correct.

7-3 THE ROUTER'S USER EXEC MODE (ROUTER>)

This section introduces Cisco IOS, the software interface used to configure Cisco routers. The objective of this section is to acquaint students with the router prompt and the help command. This section also introduces the Net-Challenge software that comes with the text. This software has been developed specifically for the text to challenge students at multiple levels of router configuration. Selecting a challenge opens a check box for that challenge. The check boxes are reset if the window is closed. The Net-Challenge software has been used successfully in classes as a way to ensure that all students can demonstrate the ability to perform basic router configurations. Net-Challenge is especially useful when access to actual routers is limited.

The Net-Challenge software is not designed to run in a fully independent mode (for example, with no challenge selected); however, it makes available most router commands. Students should know how to use the **?** command to get help with router commands. The Net-Challenge software supports this command but displays only the commands available with the software. It also displays the recognized abbreviated commands.

This section introduces the use of Cisco Internetwork Operating System (Cisco IOS) for configuring Cisco routers. Cisco IOS, the standard interface software available on all Cisco routers, is regularly updated to provide improved configuration, management, and monitoring capabilities.

The Cisco IOS structure is fairly easy to navigate when you know a few basic commands. Cisco IOS uses a command-line interface (CLI) for inputting commands when configuring Cisco routers. This section explains some simple concepts, such as how to access the Help menu, how to use the **show** commands, and how to take advantage of configuration options. The text comes with the Net-Challenge software, which includes a router simulator specifically developed for this text. The simulator enables you to practice accessing various router modes and gain practice configuring a router for use in a network. The networking challenges presented in the text are available from this book's companion website for testing your knowledge (refer to the Introduction).

The User EXEC Mode

Hostname
The name assigned to a networking device

User EXEC Mode
A router mode that allows a user to check the router status

User Mode
Another term for user EXEC mode

After a console connection is made to a router, the first text you see on the terminal screen is **Router con0 is now available**. This text confirms that you have connected to the router's console port:

```
Router con0 is now available Press RETURN to get started! Router>
```

You are prompted to press Return to get started. Press **Return** (the **Enter** key on the keyboard) to connect to the router. The prompt **Router>** indicates that you have connected to a router with the **hostname** router, and the **>** symbol indicates that you have entered the **user EXEC mode** on the router. The user EXEC mode, also called the **user mode**, is the unsecured first level of entry you pass through when accessing a router's interface. It does not allow access to the router's configuration options. However, it does allow you to view some of the router parameters, such as

the version of the Cisco IOS software running on the machine, memory, flash, and the available commands.

One important point to keep in mind when connecting serially to a router is that the router's logging messages are displayed on the console terminal. These messages are useful when troubleshooting but can be annoying when they show up in the middle of entering configuration commands. Recommended practice dictates that you *not* enable the debug mode and configure the router at the same time due to the sheer number of logging messages you would receive.

You can view the commands that are recognized at the user level by entering **?** after the **Router>** prompt.**?** is the universal help command in Cisco IOS that allows you to view the available commands from any prompt. The following is an example of using the **?** command to display the available commands from the **Router>** prompt:

?
The help command, which can be used at any prompt in the command-line interface for the Cisco IOS software

```
Router> ?
Exec commands:
access-enable    Create a temporary Access-List entry
                 clear Reset functions
connect          Open a terminal connection disable Turn off
                 privileged commands
disconnect       Disconnect an existing network connection
enable           Turn on privileged commands
exit             Exit from the EXEC
help             Description of the interactive help system
lock             Lock the terminal
login            Log in as a particular user logout Exit from the EXEC
mrinfo           Request neighbor and version information from a
                 multicast router
mstat            Show statistics after multiple multicast traceroutes
mtrace           Trace reverse
multicast        path from destination to source
name-connection  Name an existing network connection
pad              Open a X.29 PAD connection ping Send echo messages
ppp              Start IETF Point-to-Point Protocol (PPP)
resume           Resume an active network connection
rlogin           Open an rlogin connection
set              Set system parameter (not config) show
Show             running system information
slip             Start Serial-line IP (SLIP)
systat           Display information about terminal lines
telnet           Open a telnet connection
terminal         Set terminal line parameters
traceroute       Trace route to destination
tunnel           Open a tunnel connection
where            List active connections
x28              Become an X.28 PAD
x3               Set X.3 parameters on PAD
```

It's obvious from this **Router>** help listing that the command options are quite extensive. It takes some time to master them all. This chapter introduces the fundamental commands required for navigating Cisco IOS and configuring the

router interface. In particular, this section concentrates on the commands and procedures for configuring the router's FastEthernet and serial ports.

Another way to display commands or features is to place a **?** after the command. A **?** can be used after any command from any prompt at the command-line interface in the Cisco IOS software. You can use **?** after the **show** command at the **Router>** prompt to see the available options in the user mode for the **show** command, as demonstrated here:

```
Router> show ?
backup          Backup status
clock           Display the system clock
dialer          Dialer parameters and statistics
flash           display information about flash: file system
history         Display the session command history
hosts           IP domain-name, lookup style, nameservers, and host
                table
location        Display the system location
modemcap        Show Modem Capabilities database
ppp             PPP parameters and statistics
rmon            rmon statistics
rtr             Response Time Reporter (RTR)
sessions        Information about Telnet connections
snmp            snmp statistics
tacacs          Shows tacacs + server statistics
terminal        Display terminal configuration parameters
traffic-shape   Traffic rate shaping configuration
users           Display information about terminal lines
version         System hardware and software status
```

show flash
A command that lists the details of a router's flash memory

show version
A command that lists the version of the Cisco IOS software running on the router

Two key options for **show** in the user (**Router>**) mode are **show flash** and **show version**. The **show flash** command lists the details of the router's flash memory, and **show version** lists the version of the Cisco IOS software running on the router. Examples of each are provided in the output samples that follow.

The show flash command displays the flash memory available and the amount of flash memory used. This command is typically used to verify whether sufficient memory is available to load a new version of the Cisco IOS software. In this example, IOS is already installed, the file length is 110493264 bytes, and the name of the file is c2900-universalk9-mz.SPA.157-3.M8.bin:

```
Router> show flash

-#- --length-- -----date/time------ path
1     110493264 Mar 10 2021 04:03:56 +00:00 c2900-universalk9-
mz.SPA.157-3.M8.bin
```

The following example of using **show version** indicates that the router is running version 15.7:

```
Router> show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version
 15.7(3)M8, RELEASE SOFTWARE (fc2)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Wed 09-Mar-21 19:23 by prod_rel_team
ROM: System Bootstrap, Version 15.0(1r)M16, RELEASE SOFTWARE (fc1)

Router uptime is 2 weeks, 3 days, 4 hours, 9 minutes
System returned to ROM by power-on
System image file is "flash0:c2900-universalk9-mz.SPA.157-3.M8.bin"
Last reload type: Normal Reload
Last reload reason: power-on

Cisco CISCO2901/K9 (revision 1.0) with 483328K/40960K bytes of memory.
Processor board ID FGL182420YZ
6 Gigabit Ethernet interfaces
1 terminal line
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)
```

Notice that the **show version** command also lists the **router uptime**—the amount of time that the router has been running. In this example, the router has been running 2 weeks, 3 days, 4 hours, and 9 minutes, and the output indicates that the system was restarted by power-on. This is a good place to check when trouble-shooting intermittent problems with a router. Recurring statements that the router was restarted by power-on could indicate that the router has an intermittent power supply problem or that the power to the router is intermittent. Another possibility is that someone is resetting the router. This is not common because access to a router is typically password protected.

Router Uptime
The amount of time a router has been running

Router Configuration Challenge: User EXEC Mode

For this challenge, you need to use the Net-Challenge software available from this book's companion website. Click on Net-ChallengeV5.exe to start the software, and the program opens on your desktop with the screen shown in Figure 7-6. The Net-Challenge software uses a three-router campus network scenario. The software allows you to configure each of the three routers and to configure the network interface for computers in the LANs attached to each router. You can connect to a router by clicking one of the three router buttons shown in Figure 7-6. Clicking a router button connects the selected router to a console session, thus enabling the simulated console terminal access to all three routers. The routers are marked with their default hostnames Router A, Router B, and Router C.

This challenge tests your ability to use router commands in the user EXEC mode. In the Net-Challenge software, click the **Select Challenge** button to open a list of challenges available with the software. Select the **User EXEC Mode** challenge. The check box window shown in Figure 7-7 appears. The tasks in each challenge will be checked as you complete them.

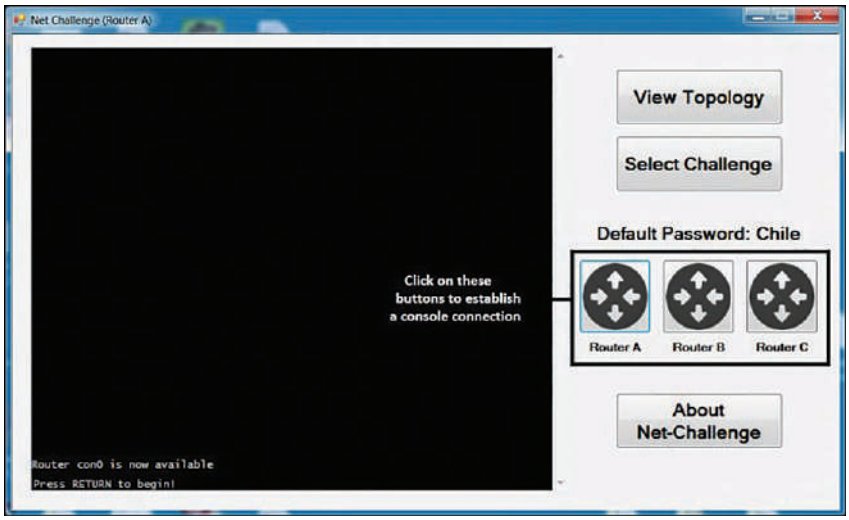


FIGURE 7-6 The Net-Challenge screen.

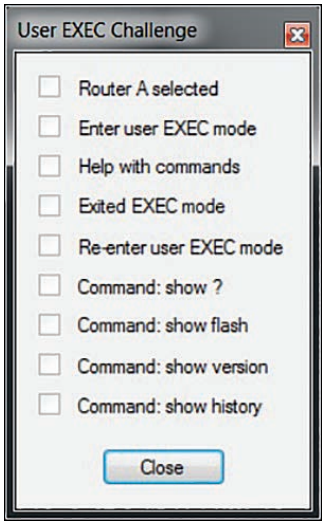


FIGURE 7-7 The check box window for the Net-Challenge software User EXEC Mode challenge.

To begin the User EXEC Mode challenge, follow these steps:

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 displays **Router>** when you are in the user EXEC mode.

3. Use the **?** command to see the available command options in the Net-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 commands and options available within the software. This chapter provides examples of what the full command and help options look like.)
4. Enter **exit** at the **Router>** prompt (**Router>exit**). You should now be back at the **Press RETURN** screen, shown in Figure 7-6.
5. Reenter user EXEC mode by pressing **Enter**.
6. Enter the command **show** at 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**. You should see text like that in Figure 7-8 displayed on the terminal screen.

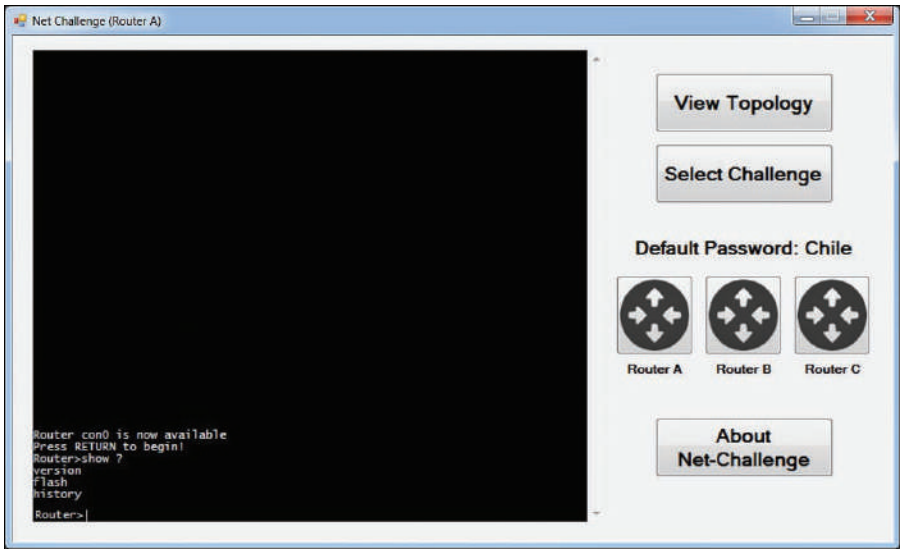


FIGURE 7-8 The display for step 6, using the **show** command.

7. Enter the command **show flash** at the **Router>** prompt. Describe the information displayed.
8. Enter the command **show version** at the **Router>** prompt. Describe the information displayed.
9. Enter the command **show history** at the **Router>** prompt. Describe the information displayed.

Section 7-3 Review

This section covers the following Network+ exam objectives.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section introduces Cisco IOS and explains the steps involved in establishing the router's console connection and operating in the user EXEC mode.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section introduces the use of the router's command line. Knowing how to navigate the CLI is extremely important.

5.3 Given a scenario, use the appropriate network software tools and commands.

This section introduces the use of the Net-Challenge software, which is available from this book's companion website. This software will help you improve your use of the command line on a router.

Test Your Knowledge

1. Which command can you use to see the uptime for a router?

   a. **show uptime**
   b. **sh uptime**
   c. **show time**
   d. **show version**

2. True or false: The prompt for a router's user EXEC mode is **router/>**.

   False

3. Which command can you use to view the details of a router's flash memory?

   a. **show mem**
   b. **show details**
   c. **show history**
   d. **show flash**

4. What is the help command in Cisco IOS?

   a. **?**
   b. **-help**
   c. **-h**
   d. **- help**

7-4 THE ROUTER'S PRIVILEGED EXEC MODE (ROUTER#)

This section describes basic router configuration tasks, such as how to enter a router's privileged EXEC mode and how to enter a router's configure terminal (**conf t**) mode. Students will learn how to configure a router's hostname, set up passwords, and configure the IP address for a router's Ethernet and serial interfaces. Students should understand the importance of using the **show ip interface brief** (**sh ip int brief**) command to verify the interface settings.

This section also demonstrates how to check whether a router's serial connection is DCE or DTE. Make sure students know how to check this before they make any real serial connections in the lab. This section concludes with a Net-Challenge exercise related to the router's privileged EXEC mode.

Configuring a router interface requires you to enter **privileged mode** on a router. Privileged mode (or privileged EXEC mode) allows full access for configuring the router interfaces and configuring a routing protocol. This section focuses on general configuration steps for a router and configuring a router's interfaces, FastEthernet, and serial ports. (Chapter 9, "Routing Protocols," discusses the configuration of routing protocols.)

Privileged Mode
A mode that enables configuration of router ports and routing features

```
Router> enable
Password:
Router#
```

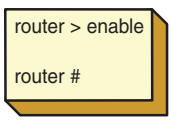
You enter privileged mode by using the command **enable** at the **Router>** prompt:

enable
A command used to enter a router's privileged mode

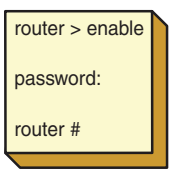
The **#** sign after the router name (**Router#**) indicates that you are in privileged EXEC mode.

Router#
The prompt for a router's privileged EXEC mode

Entry into the router's privileged mode is typically password protected. The exception to this is when a router has not been configured and a password has not been assigned to it. In this case, pressing **Enter** on the keyboard from the **Router>** prompt places you in the router's privileged mode (**Router#**). The two different options for entering the router's privileged mode are shown in Figure 7-9: (a) no password protection and (b) password required.



(a)



(b)

FIGURE 7-9 The options for entering the router's privileged EXEC mode: (a) no password and (b) password required.

It is important to use caution after entering the privileged mode on a router. It is easy to make mistakes, and incorrectly entered router configurations will adversely affect your network. Many options are available for configuring the router and the router's interfaces from the **Router#** prompt. This section presents the key options needed to configure the router.

Note

This text comes with the Net-Challenge router simulator (available at this book's companion website) to help you gain experience with router configuration. In fact, most of the router configuration commands presented in this chapter can be implemented using this router simulator.

configure terminal (conf t)
A command used to enter a router's terminal configuration mode

To use the commands presented in this section, you need to enter the router's terminal configuration mode. To enter the router's configuration mode, you can enter the command **configure terminal** at the **Router#** prompt:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Alternatively, you can enter the abbreviated version of the command, **conf t**:

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

As you can see in these examples, the prompt changes to **Router(config)#**. This indicates that the router is in terminal configuration mode.

The hostname Command

The generic name or the name of an unconfigured Cisco router is *router*, and the **hostname** command enables you to change the name to specifically identify the router. For example, valid hostname structures include RouterA, Router-A, and Router_A; however, Router A is not valid because hostnames cannot contain spaces. In addition, the word *router* does not have to be used in the hostname. The hostname can, for example, reflect the manner in which the router is being used. A router may serve as the network gateway for the LANs in a building; for example, for a building named Goddard, the router could be called *Goddard_gate*. This name tells the network administrator the location and purpose of the router.

In the privileged mode (**Router#**), enter the command **hostname [***router-name***]** and press **Enter** to set the hostname for the router to *router-name*. The following example demonstrates how the router's hostname is changed to **RouterA**:

```
Router(config)# hostname RouterA
RouterA#(config)
```

Notice the change in the router's name from the first line to the second line after the **hostname** command is entered

The enable secret Command

You configure password protection for privileged (enable) mode by using **enable secret**, as shown here:

1. Enter the router's configure terminal mode by entering **configure terminal** or **conf t** at the **Router#** prompt.
2. Enter the command **enable secret [***your-password***]** and press **Enter**.

The following is an example of the commands you use to enable password protection for privileged mode:

```
Router# conf t
Router(config)#
Router(config)# enable secret my-secret
```

This example sets the password for entering the router's privileged EXEC mode to **my-secret**. The password entered is automatically encrypted. The password for entering the router's privileged mode must now be entered to gain access to the mode. Cisco has 16 different privilege levels, defined using the numbers 0 to 15. When you do not specify a privilege level with the **enable secret** command, the privilege level defaults to the highest privilege level, which is 15.

Setting the Line Console Passwords

A router has three line connections through which a user can gain access to the router. The line connections available on a router can be displayed using the **line ?** command at the **Router(config)#** prompt. The available line connections are as follows:

Router(config)#
The prompt for a router's terminal configuration mode

- **aux:** Auxiliary line
- **console:** Primary terminal line (console port)
- **vty:** Virtual terminal (for a Telnet connection)

Console (primary terminal line) is the console port, *vty* is the virtual terminal used for Telnet and SSH connections, and *aux* is used to establish an external modem connection. The following steps demonstrate how to configure password protection for the console port and the virtual terminal:

1. Enter the command **line console 0** and then press **Enter**.
2. Enter the command **login** and then press **Enter**.
3. Type the command **password [***my-secret2***]**, where *my-secret2* is the console port password.

The following example shows how to use these commands to configure a console port:

```
Router(config)# line console 0
Router(config-line)# login
Router(config-line)# password [my-secret2]
```

Router (config-line)#
A prompt that indicates that you are in the router's line configuration mode

Note the change in the router prompt to **Router(config-line)#,** which indicates that you are in the router's line configuration mode.

You set password protection for the virtual terminal (line vty) from the router's configuration mode. You use the virtual terminal for entering the router via a Telnet connection:

1. Enter the command **line vty 0 4**. This places the router in the line configuration mode (config-line). The **0 4** represents the number of vty lines to which the configuration parameters that follow will be applied. The five virtual terminal connections are identified as 0, 1, 2, 3, and 4.
2. Enter the command **password [***my-secret3***]**, where *my-secret3* is the password for the virtual terminal connection.
3. Enter **login** and press **Enter**.

The following example shows how to use these commands to enable password protection for a virtual terminal:

```
Router(config)# line vty 0 4
Router(config-line)# password [my-secret3]
Router(config-line)# login
```

FastEthernet Interface Configuration

Routers can have Ethernet (10Mbps), Fast Ethernet (100Mbps), Gigabit Ethernet (1000Mbps), and 10 Gigabit Ethernet (10Gbps) interfaces. These routers can have multiple interfaces supporting 10/100/1000Mbps and 10Gbps connections, and the steps for configuring the different interfaces are basically the same. Each interface is assigned a number. For example, a router could have three FastEthernet interfaces identified as follows:

- FastEthernet0/0
- FastEthernet0/1
- FastEthernet0/2

The notation after FastEthernet indicates the interface card slot and port; for example, 0/0 indicates interface card slot 0 and port 0.

The following steps show how to configure a router's FastEthernet0/0 port (which can also be presented as fa0/0 or FA0/0):

1. In the router's configuration mode—that is, at the **Router(config)#** prompt—enter **interface fa0/0** and press **Enter**. This changes the router's prompt to **Router(config-if)#**, which indicates that you are in the router's interface configuration mode. The router keeps track of the interface you are configuring. The abbreviated command **int fa0/0** is used to access the FastEthernet0/0 interface. The router prompt still shows **Router(config-if)#**.
2. Enter the assigned IP address for the FastEthernet0/0 port—for example, **ip address 10.10.20.250 255.255.255.0**—and press **Enter**.
3. Enable the router interface by using the **no shutdown** (**no shut**) command.

Router(config-if)#
A prompt which indicates that you are in the router's interface configuration mode

no shutdown (no shut)
A command that enables a router's interface

The following example shows how to use these commands to configure a FastEthernet interface:

```
Router(config)# int fa0/0
Router(config-if)# ip address 10.10.20.250 255.255.255.0
Router(config-if)# no shut
2w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
```

Notice that the router prompts you that the line protocol on interface FastEthernet0/0 changed state to up. Repeat the previous steps for each of the FastEthernet interfaces. The command **show ip interface brief** (**sh ip int brief**) can be entered at the enable prompt (**Router#**) to verify the status of the router interfaces. The following is an example:

show ip interface brief (sh ip int brief)
A command used to verify the status of a router's interfaces

```
Router# sh ip int brief
Interface          IP-Address      OK?    Method    Status    Protocol
FastEthernet0      10.10.20.250    YES    manual    up        up
FastEthernet1      10.10.200.1     YES    manual    up        up
FastEthernet2      10.10.100.1     YES    manual    up        up
```

Serial Interface Configuration

A router's serial ports are used to interface to other serial communication devices. The serial communications link is often used in campus networks to connect to WANs or the Internet. To configure the serial port, you need to answer the following questions:

- What is the IP address of the interface?
- What is the subnet mask for the interface?
- Which interfaces are responsible for providing clocking?

A router's serial communication link has a **DCE** end and a **DTE** end. The serial cables on older routers are called *V.35* cables. Examples are shown in Figure 7-10. DCE stands for data communication equipment; DTE stands for data terminal equipment. The DTE interface on the V.35 cable is designed for connecting the router to a CSU/DSU and outside digital communication services. In regard to clocking, the

DCE
Data communications equipment, the serial interface responsible for clocking

DTE
Data terminal equipment, the serial interface designed for connecting to a CSU/DSU and outside digital communication services

serial interface defined to be the DCE is responsible for providing clocking. This section shows how to check to see whether your serial connection is DCE or DTE. Modern routers have a built-in CSU/DSU and use an RJ-45 cable to establish a WAN or Internet connection.



FIGURE 7-10 The (a) DCE and (b) DTE ends of V.35 serial cable (courtesy of StarTech.com).

You configure a serial interface by following these steps:

1. At the router's **Router(config)#** prompt, enter the command **int s0/0** to access the Serial0/0 interface. The router's prompt changes to **Router(config-if)#** to indicate that the interface configuration has been entered. Notice that this is the same prompt you see when configuring the FastEthernet interfaces.
2. Configure the IP address and subnet mask for the serial interface by entering the command **ip address 10.10.50.30 255.255.255.0**.

The following example shows how to use these commands to configure the Serial0/0 interface:

```
Router(config)# int s0/0
Router(config-if)# ip address 10.10.50.30 255.255.255.0
```

If this is a serial DCE connection, you must set the clock rate. The serial connection can have either a DCE or DTE end. Routers use RJ-45 and V.35 connections to connect to the serial interface. In the case of V.35 cables, the DCE end of the serial connection is the female end, and the DTE end of the cable is the male end (refer to Figure 7-10). There are three ways to check a cable to see whether the connection is DCE or DTE:

- Use the command **show controllers serial [***interface number***]** to get an abbreviated list of the displayed results for the **show controllers serial 0/0** command. The Serial0/0 interface is a V.35 DCE cable. This command should be used when you have an RJ-45 connection.
- A V.35 cable is typically labeled to indicate whether it is a DTE or DCE cable.
- Inspect the end of the V.35 cable to determine whether it is male (DTE) or female (DCE).

The customer is usually the DTE end, and the clock rate is set by the communications carrier. The exception to this is when a customer is setting up a back-to-back serial connection within the customer network. In this case, the customer sets the clock rate. The following example shows how to use the **show controllers** command for a DCE interface:

```
Router# sh controllers serial 0/0
HD unit 0,   idb    0xCF958,  driver structure at  0xD4DC8
Buffer size  1524    HD   unit 0, V.35  DCE  cable
cpb   0x21,  eda  0x4940,  cda  0x4800
```

The next example shows the results of using the command **show controllers serial [***interface number***]** for a DTE interface. This example shows the Serial0/1 interface being checked:

```
RouterA# sh controllers serial 0/1
HD unit 1, idb 0xD9050, driver structure at 0xDE4C0
buffer size 1524 HD unit 1, V.35 DTE cable
cpb 0x22, eda 0x30A0, cda 0x30B4
.
.
.
```

You set the clocking for the serial interface by using the **clock rate** command followed by a data rate. The clock rate for the serial interface on the router can be set for between 1200bps and 4Mbps. The following command sets the clock rate to 56000:

```
Router(config-if)# clockrate 56000
```

Next, you enable the serial interface by using the **no shut** command:

```
Router(config-if)# no shut
2w0d: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
2w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up
```

The router prompts the console port that interface Serial0/0 changed state to up. This command needs to be repeated for all the serial interfaces.

You can check the status of the serial interfaces by using the **sh ip int brief** command, as demonstrated here:

```
Router# sh ip int brief
Interface           IP-Address      OK?    Method Status Protocol
FastEthernet0       10.10.20.250    YES    manual   up     up
FastEthernet1       10.10.200.1     YES    manual   up     up
FastEthernet2       10.10.100.1     YES    manual   up     up
Serial0             10.10.128.1     YES    manual   up     up
Serial1             10.10.64.1      YES    manual   up     up
```

The configuration changes take effect right away, and it is important that you save them to the router as you go. These changes are made to the running configuration,

which is not saved in the router's nonvolatile random access memory (NVRAM). This means that when the router reboots, the configuration changes will be lost. To save the changes to the router's NVRAM to the startup configuration, use the **copy running-configuration startup-configuration** (or **copy run start** for short) command:

```
RouterA# copy run start
```

To verify the changes made and to view the running configuration, use the command **show running-configuration** (or **show run** for short). To view the saved configuration in NVRAM, use the command **show startup-configuration**:

```
RouterA# show run
RouterA# show startup-configuration
```

Router Configuration Challenge: Privileged EXEC Mode

For this challenge, you need to use the Net-Challenge software available from this book's companion website. Click the Net-ChallengeV5.exe file, and the program opens on your desktop (refer to Figure 7-6). The Net-Challenge software uses a three-router campus network scenario. You can view the topology for the network by clicking the **View Topology** button. Figure 7-11 shows the network topology used in the software. The software allows you to configure each of the three routers and to configure the network interface for computers in the LANs attached to each router. Clicking one of the router diagram symbols in the topology enables you to view the IP address for the router required for the configuration.

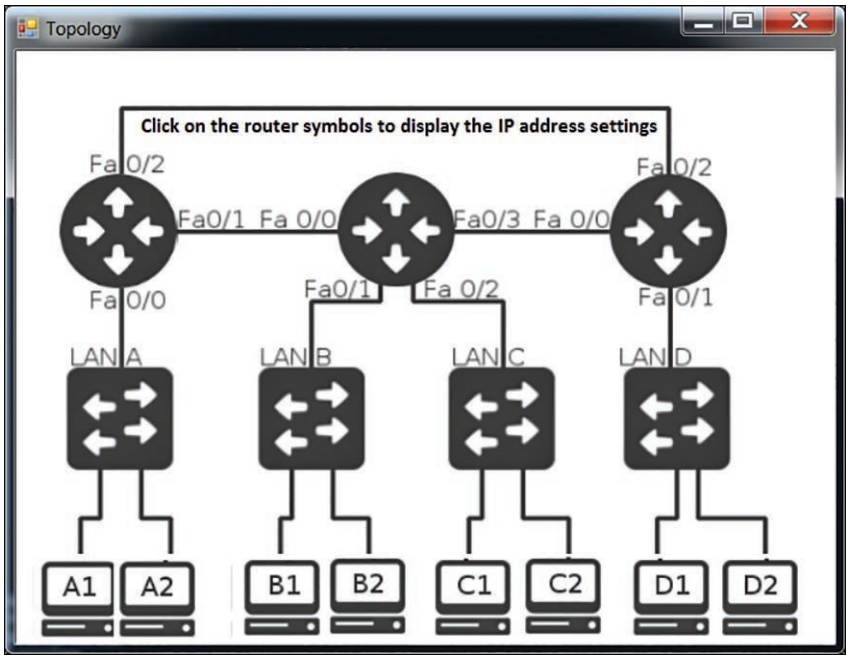


FIGURE 7-11 The network topology for Net-Challenge. The arrows indicate where to click to display the router IP address configurations.

You can connect to a router by clicking one of the three router buttons shown in Figure 7-8, earlier in this chapter. An arrow points to the buttons used to establish a console connection. Clicking a button connects the selected router to a terminal console session, enabling the simulated console terminal access to all three routers. The routers are marked with their default hostnames, Router A, Router B, and Router C.

This challenge tests your ability to use router commands in privileged EXEC mode, also called enable mode. In the Net-Challenge software, click the **Select Challenge** button to open a list of challenges available with the software. Select the **Privileged EXEC Mode** challenge to open the associated check box window. The tasks in each challenge will be checked as you complete them.

To begin the Privileged EXEC Mode challenge, follow these steps:

1. Make sure you are connected to Router A by clicking the appropriate selection button.
2. Demonstrate that you can enter the router's privileged EXEC mode. The router screen should display **Router#**. The password is **Chile**.
3. Place the router in terminal configuration mode [**Router(config)#**].
4. Use the **hostname** command to change the router's hostname to RouterA.
5. Set the enable secret for the router to **Chile**.
6. Set the vty password to **ConCarne**.
7. Configure the three FastEthernet interfaces on RouterA as follows:

```
FastEthernet0/0  (fa0/0)   10.10.20.250     255.255.255.0
FastEthernet0/1  (fa0/1)   10.10.200.1      255.255.255.0
FastEthernet0/2  (fa0/2)   10.10.100.1      255.255.255.0
```

8. Enable each of the router FastEthernet interfaces by using the **no shut** command.
9. Use the **sh ip interface brief** (or **sh ip int brief**) command to verify that the interfaces have been configured and are functioning. For this challenge, the interfaces on Router B and Router C have already been configured.
10. Configure the serial interfaces on the router. Serial0/0 is the DCE. Set the clock rate to 56000 and set the IP addresses and subnet masks as follows:

```
Serial 0/0   10.10.128.1   255.255.255.0
Serial 0/1   10.10.64.1    255.255.255.0
```

11. Use the **sh ip int brief** command to verify that the serial interfaces are properly configured. For this challenge, the interfaces on Router B and Router C have already been configured.
12. Use the **ping** command to verify that you have network connections for the following interfaces:

```
RouterA FA0/1 (10.10.200.1) to RouterB FA0/2 (10.10.200.2)
RouterA FA0/2 (10.10.100.1) to RouterC FA0/2 (10.10.100.2)
```

Section 7-4 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.

As discussed in this section, a CSU/DSU is used to establish a WAN or Internet connection.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

*The **telnet** command is still used, but because it isn't secure, other commands, such as **ssh**, are preferred.*

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section introduces routers and their various interfaces. Make sure you know about the DCE and DTE interfaces.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

This section introduces privileged EXEC mode, which allows full access for configuring the router interfaces and configuring a routing protocol.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

*When configuring a router, it is important that you save changes to the router as you go. These changes are made to the running configuration, which is not saved in the router's nonvolatile memory (NVRAM). This means that when the router reboots, the configuration changes will be lost. To save the changes to the router's NVRAM, use the **copy running-configuration startup-configuration** (or **copy run start** for short) command to save changes to the startup configuration.*

5.3 Given a scenario, use the appropriate network software tools and commands.

This section presents the command-line instructions available while in the router's privileged EXEC mode.

Test Your Knowledge

1. Which router interface is most commonly used to interconnect LANs to a campus network?

   a. Serial
   b. Parallel
   c. Console port
   d. Ethernet
   e. None of these answers are correct.

2. Serial interfaces on a router are typically used to ____.

   a. connect to console ports

   b. connect to communication carriers

   c. connect to auxiliary ports

   d. interconnect routers

3. True or false: The prompt for a router's terminal configuration mode is **router(config-term)#**.

   False

7-5 CONFIGURING THE NETWORK INTERFACE: AUTO-NEGOTIATION

This section examines how interconnected networking devices negotiate an operating speed. The steps for negotiation and the concepts of full- and half-duplex are all examined. This section also provides a summary of the advantages and disadvantages of the auto-negotiation protocol. Make sure students understand that auto-negotiation is not appropriate for every network application.

Most modern internetworking technologies (for example, hubs, switches, bridges, and routers) now incorporate the **auto-negotiation** protocol, which enables Ethernet equipment to automate many installation steps, including automatically configuring the operating speeds (for example, 10/100/1000Mbps) and the selection of full- or half-duplex operation for the data link. The auto-negotiation protocol is defined in the IEEE Ethernet standard 802.3x for Fast Ethernet.

Auto-negotiation
A protocol used by interconnected electronic devices to negotiate a link speed

The auto-negotiation protocol uses a **fast link pulse (FLP)** to carry the information between the ends of a data link. Figure 7-12 shows a data link. The data rate for the fast link pulses is 10Mbps, which is the same as for 10BASE-T. The link pulses were designed to operate over the limited bandwidth supported by CAT3 cabling. Therefore, even if a link is negotiated, there is no guarantee that the negotiated data rate will work over the link. Other tests on the cable link must be used to certify that the cable can carry the negotiated data link configuration (refer to Chapter 2, "Physical Layer Cabling: Twisted-Pair").

Fast Link Pulse (FLP)
A burst that carries configuration information between the ends of a data link

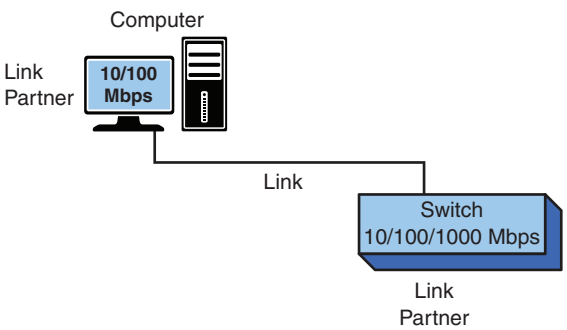


FIGURE 7-12 The two ends of a data link negotiating the operating parameters.

Auto-negotiation Steps

During auto-negotiation, each link partner shares or advertises its data link capabilities with the other link partner. The two link partners then use the advertised capabilities to establish the fastest possible data link rate for both links. In the example of the link partners shown in Figure 7-12, the computer advertises that its interface supports 10Mbps and 100Mbps. The switch advertises that it supports 10Mbps, 100Mbps, and 1000Mbps. The network interfaces on each link partner are set for auto-negotiation; therefore, the 100Mbps operating mode is selected. This is the fastest data rate that can be used in this data link. The data rate is limited by the 100Mbps capabilities of the computer's network interface.

You use the following commands to configure the speed auto-negotiation on Cisco routers and switches:

```
Router(config)# int GigabitEthernet0/0
Router(config-if)# speed auto
```

Keep in mind that both endpoints must be configured with the same auto-negotiation.

Note

Auto-negotiation is established when an Ethernet link is established. The link information is sent only one time, when the link is established. The negotiated link configuration remains until the link is broken or the interfaces are reconfigured.

Full-Duplex/Half-Duplex

Half-duplex
A mode in which a communications device can transmit or receive, but cannot do both at the same time

Modern network interfaces for computer networks are capable of running the data over the links in either full-duplex or half-duplex mode. As noted previously, *full-duplex* means that the communications device can transmit and receive at the same time. **Half-duplex** means the communications device can transmit or receive but cannot do both at the same time.

In full-duplex operation (10/100Mbps), the media must have separate transmit and receive data paths. This is provided for in UTP cable with pairs 1–2 (transmit) and pairs 3–6 (receive). Full-duplex with Gigabit and 10 Gigabit data rates requires the use of all four wire pairs (1–2, 3–6, 4–5, 7–8). According to the IEEE standards, Gigabit speed and above support only full-duplex. It is important to note that full-duplex mode in computer network links is only for point-to-point links. This means there can be only two end stations on a link. The CSMA/CD protocol is turned off; therefore, there can't be another networking device competing for use of the link.

An example of networking devices that can run full-duplex is computers connected to a switch. The switch can be configured to run full-duplex mode. In addition, each end station on the link must be configurable to run full-duplex mode.

In half-duplex operation, the link uses the CSMA/CD protocol. This means only one device talks at a time, and while the one device is talking, the other networking

devices "listen" to the network traffic. Figure 7-13 shows examples of networks configured for full- and half-duplex modes. In full-duplex operation [Figure 7-13(a)], CSMA/CD is turned off, and computers 1 and 2 and the switch are transmitting and receiving at the same time. In half-duplex mode [Figure 7-13(b)], CSMA/CD is turned on, computer 1 is transmitting, and computer 2 is "listening," or receiving the data transmission.

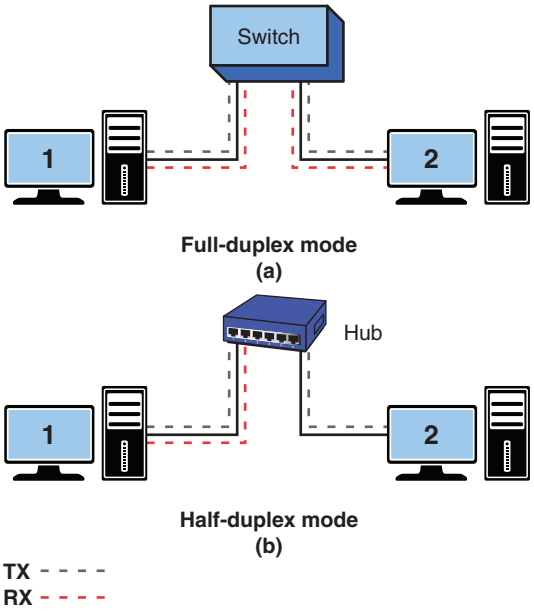


FIGURE 7-13 (a) Computer 1 transmits and receives at the same time; (b) computer 1 transmits, and others listen.

You use the following commands to configure duplex auto-negotiation on Cisco routers and switches:

```
Router(config)# int GigabitEthernet0/0
Router(config-if)# duplex auto
```

Figure 7-14 provides an example of the port management features available with a Cisco switch using the Cisco Network Assistant software. Figure 7-14(a) shows the settings for the speed. Figure 7-14(b) provides an example of setting the switch for auto (that is, auto-negotiate), half-duplex, and full-duplex.

It is very important to make sure both ends of the network are properly configured. If the speeds and half- and full-duplex modes are not properly specified, you can end up with a duplex speed mismatch and, as a result, a loss of the data link. Table 7-3 provides a summary of the advantages and disadvantages of the auto-negotiation protocol.

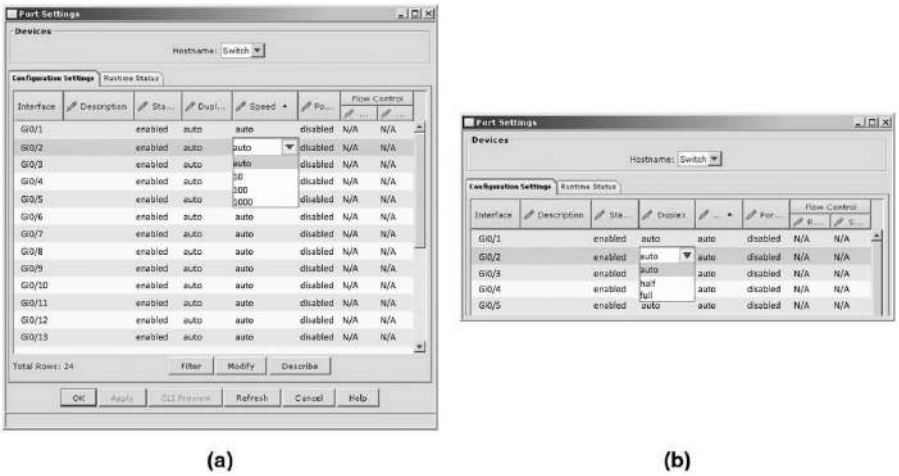


FIGURE 7-14 An example of the port management options available with a Cisco switch: (a) speed auto-negotiation option; (b) duplex auto option.

TABLE 7-3 **Advantages and Disadvantages of the Auto-negotiation Protocol**

Advantages	Disadvantages
Useful in LANs that have multiple users with multiple connection capabilities.	Not recommended for fixed data links such as the backbone in a network.
The auto-negotiation feature can maximize throughput on the data links.	A failed negotiation on a functioning link can cause a link failure.

Section 7-5 Review

This section covers the following Network+ exam objectives.

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

Most modern internetworking technologies (for example, hubs, switches, bridges, and routers) now incorporate the auto-negotiation protocol, which enables Ethernet equipment to automate many installation steps, including automatically configuring the operating speeds (for example, 10/100/1000Mbps) and the selection of full- or half-duplex operation for the data link.

1.7 Explain basic corporate and datacenter network architecture.

The auto-negotiation protocol is not recommended for fixed data links such as the backbone in a network.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

It is very important to make sure both ends of a network are properly configured. If the speeds and half-/full-duplex modes are not properly specified, then you may have a duplex speed mismatch and, as a result, a loss of the data link.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section mentions that the auto-negotiation feature can maximize throughput on data links.

Test Your Knowledge

1. Which of the following is a disadvantage of the auto-negotiation protocol?
   a. It is useful only in LANs that have multiple connection capabilities.
   b. A failed negotiation on a functioning link can cause a link failure.
   c. It should be used only in critical network data paths.
   d. It works at 10Mbps.
2. What does the fast link pulse do? (Select all that apply.)
   a. It carries configuration information between the ends of a data link.
   b. It is used in auto-negotiation.
   c. It uses a 100Mbps data rate.
   d. It uses a 1Mbps data rate.
3. Which of the following are advantages of auto-negotiation? (Select all that apply.)
   a. It is useful in LANs that have multiple users with multiple connection capabilities.
   b. It can maximize the data link throughput.
   c. It simplifies the backbone configuration.
   d. It simplifies LAN configuration.
   e. All of the answers are correct.

7-6 TROUBLESHOOTING THE ROUTER INTERFACE

This section presents the steps for using the **show ip interface brief** command and discusses the information displayed by this command. Make sure students fully understand the role of the status and protocol displays. This section also includes a discussion of the keepalive packet and how the protocol differs for Ethernet and serial connections.

This section examines one of the router commands most commonly used for troubleshooting and isolating problems that might be related to the router configuration and router interfaces: **show ip interface brief** (or **sh ip int brief**). Typically, a network administrator can use SSH to enter a router and establish a secure virtual terminal connection. The virtual terminal enables the administrator to connect to the router without physically plugging in to it. The virtual terminal connection looks the same as the console port connection. Remember that the virtual interface

is password protected, and only authorized users can access the router through this interface.

The **sh ip int brief** command enables you to check the status of the interfaces and verify that the interfaces are attached to another networking device. The command output provides a quick look at information about the interfaces and includes the following columns:

- **Interface:** Ethernet: 10Mbps, Fast Ethernet: 100Mbps, Gigabit Ethernet: 1000Mbps, or Serial: From 2500bps to 4Mbps and higher for high-speed serial interfaces.
- **IP-Address:** The IP address assigned to the interface.
- **OK?:** Whether the interface is functioning.
- **Method:** How the interface was brought up (for example, manually, via TFTP).
- **Status:** Current router status: **up**, **down**, or **administratively down**. (Displayed results differ for FastEthernet and the serial interfaces. For FastEthernet, the status **up** indicates that the FastEthernet interface has been administratively brought up.)
- **Protocol:** Protocol status **up** indicates that you are seeing the **keepalive packet**, which means the FastEthernet interface is connected to another networking device, such as a hub, switch, or router. Protocol status **down** indicates that the Ethernet port is not physically connected to another network device. This is not the same as the link integrity pulse that activates the link light. The link integrity pulse does not send a small Ethernet packet; a keepalive does send such a packet.

Keepalive Packet
A packet which indicates that the Ethernet interface is connected to another networking device, such as a hub, switch, or router

The following example demonstrates how to use the **sh ip int brief** command to check the status of the interfaces for different conditions, such as status down, status up/protocol down, and status/protocol down. You will learn how to interpret the results displayed by the **sh ip int brief** command, which is particularly important when you're troubleshooting a possible cable or link failure. When a FastEthernet interface cable is not attached or when the link is broken, the protocol shows **down**. If a serial interface cable is not attached or the link is broken, the status and the protocol both show **down**.

The following are text outputs from a Cisco router that demonstrate how the router status and protocol settings change based on the interface configuration and setup. The first output shows that the three Ethernet interfaces and two serial interfaces are properly configured. The status **up** means that the interface has been administratively turned on by the network administrator:

```
RouterA# sh ip int brief
Interface        IP-Address        OK     Method    Status    Protocol
FastEthernet0/0  10.10.20.250      YES    manual    up        up
FastEthernet0/1  10.10.200.1       YES    manual    up        up
FastEthernet0/2  10.10.100.1       YES    manual    up        up
Serial0/0        10.10.128.1       YES    manual    up        up
Serial0/1        10.10.64.1        YES    manual    up        up
```

The next example demonstrates that the router provides a prompt if the link between the router's FastEthernet0/0 interface and another networking device is lost. Within a few seconds of losing the link, the prompt shown appears:

```
2w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
```

The **sh ip int brief** command shows that the protocol for FastEthernet0/0 is **down**, and the status is still **up**, meaning the interface is still enabled but the router is not communicating with another networking device, such as a hub, switch, or router:

```
RouterA# sh ip int brief
Interface            IP-Address      OK?     Method   Status    Protocol
FastEthernet0/0      10.10.20.250    YES     manual   up        down
FastEthernet0/1      10.10.200.1     YES     manual   up        up
FastEthernet0/2      10.10.100.1     YES     manual   up        up
Serial0/0            10.10.128.1     YES     manual   up        up
Serial0/1            10.10.64.1      YES     manual   up        up
```

The protocol **down** condition for the FastEthernet interface, as viewed with the **sh ip int brief** command, indicates that there is a loss of communication between the router and a connected networking device. With a **down** condition, you might have to physically check the router's FastEthernet interface for a link light. In this example, a link light check on the router showed that there was not a link and, in fact, the RJ-45 plug connected to the router had come loose.

Reconnecting the RJ-45 cable reestablishes the link for the FastEthernet0/0 interface and the networking device. The router provides a prompt that the FastEthernet0/0 line protocol has changed state to **up**. The **sh ip int brief** command now shows the interface status is **up** and protocol is **up** for all the interfaces:

```
2w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
RouterA# sh ip int brief
Interface          IP-Address       OK?     Method   Status    Protocol
FastEthernet0/0    10.10.20.250     YES     manual   up        up
FastEthernet0/1    10.10.200.1      YES     manual   up        up
FastEthernet0/2    10.10.100.1      YES     manual   up        up
Serial0/0          10.10.128.1      YES     manual   up        up
Serial0/1          10.10.64.1       YES     manual   up        up
```

The router's serial ports behave differently from the FastEthernet interfaces, as shown with the following examples. The previous router text display using the **sh ip int brief** command shows that the Serial0/0 interface status is **up** and the protocol is **up**. If the serial link is lost or disconnected, the interface goes down, and a prompt is sent to the console screen, as shown earlier. The prompt advises the administrator that the Serial0/0 interface has changed state to **down**, and the line protocol for Serial0/0 is also **down**. The **sh ip int brief** command now shows that the status and line protocol for Serial0/0 are **down**:

```
2w0d: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down
2w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to down
```

```
RouterA# sh ip int brief

Interface          IP-Address      OK?    Method   Status      Protocol
FastEthernet0/0    10.10.20.250    YES    manual   up          up
FastEthernet0/1    10.10.200.1     YES    manual   up          up
FastEthernet0/2    10.10.100.1     YES    manual   up          up
Serial0/0          10.10.128.1     YES    manual   down        down
Serial1/1          10.10.64.1      YES    manual   up          up
```

Reestablishing the serial connection changes the status back to **up** and the protocol back to **up**, as shown here:

```
2w0d: %LINK-3-UPDOWN: Interface Serial0, changed state to up
2w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed
state to up
[Resuming connection 1 to 10.10.128.1 ... ]
RouterA# sh ip int brief
Interface          IP-Address      OK?    Method   Status      Protocol
FastEthernet0/0    10.10.20.250    YES    manual   up          up
FastEthernet0/1    10.10.200.1     YES    manual   up          up
FastEthernet0/2    10.10.100.1     YES    manual   up          up
Serial0/0          10.10.128.1     YES    manual   up          up
Serial10/1         10.10.64.1      YES    manual   up          up
```

Note that the prompt includes a statement that communication to 10.10.128.1 has been resumed. This is the IP address of the serial interface attached to the router's Serial0 interface.

There is also a physical method to troubleshoot the wiring of an Ethernet interface and a T1 serial interface; it involves using a loopback adapter. This type of adapter simply loops the transmit signal wires back into the system on the receive signal wires, which redirects the data being sent back into the system. The adapter can connect to the wall jack or the end of a network cable currently connected to an active piece of network equipment. If the wiring is good, the LED light of the interface lights up, and the interface status is **up**.

The following output shows that the Serial0 interface is **administratively down**:

```
RouterA# sh ip int brief
Interface       IP-Address   OK? Method Status                 Protocol
FastEthernet0/0 10.10.20.250 YES manual up                     up
FastEthernet0/1 10.10.200.1  YES manual up                     up
FastEthernet0/2 10.10.100.1  YES manual up                     up
Serial0/0       10.10.128.1  YES manual administratively down up
Serial0/1       10.10.64.1   YES manual up                     up
```

Administratively Down
An indication that the router interface has been shut off by an administrator

The term **administratively down** indicates that the router interface has been shut off by the administrator. Note the difference between the terms *down* and *administratively down*. Reissuing the command **no shut** for the Serial0/0 interface should correct the problem.

The command **show ip int brief** gives a summary view of the interface's status. To examine an interface in more detail, you would instead want to use the command **show interface** (or **sh int**). This command gives detailed information about all interfaces belonging to the router. The following output is part of the result from the command **sh int**:

```
RouterA# sh int
FastEthernet0/0 is up, line protocol is up
 Hardware is MV96340 Ethernet, address is 40f4.ecb9.1010 (bia 40f4.
 ecb9.1010)
 Internet address is 10.10.20.250/24
 MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
 reliability 255/255, txload 7/255, rxload 6/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Full-duplex, 100Mb/s, 100BaseTX/FX
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:00, output 00:00:00, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 2623000 bits/sec, 556 packets/sec
 5 minute output rate 2892000 bits/sec, 485 packets/sec
 48430288 packets input, 206222517 bytes
 Received 633291 broadcasts, 0 runts, 0 giants, 0 throttles
 2 input errors, 2 CRC, 0 frame, 0 overrun, 0 ignored
 0 watchdog
 0 input packets with dribble condition detected
 43353888 packets output, 2673132365 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 unknown protocol drops
 0 babbles, 0 late collision, 0 deferred
 0 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out
```

The **sh int** command shows the status of the interface FastEthernet0/0, and it also displays statistical information regarding the interface, such as input and output rate in bits per second and packets per second, broadcast packets, and error packets. Here, it shows that the interface received two input errors—both of which are CRC-type errors. This command is very useful when troubleshooting something beyond basic connectivity issues such as speed, performance, and throughput.

It is a best practice to always verify the router configuration. At the end of the output above, the status of the interface reflects how the router is programmed. When making changes to the router configuration, you make the changes to the running configuration. You can use the command **show running-config** (or **sh run**) to display the most current configuration of the router. The running configuration is stored in random access memory (RAM), which loses its content when the router is powered off. You can save the router configuration by issuing the command **copy running-config startup-config** (or **copy run start**). This saves the router

configuration to the startup configuration, which is stored in NVRAM. This type of memory does not lose its contents after the power down.

In this section, you have seen how to use the **show ip int brief** command to troubleshoot and isolate router interface problems. The status differs for the Ethernet and serial interfaces. This is an important concept and something you will encounter when working with routers.

Section 7-6 Review

This section covers the following Network+ exam objectives.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

*This section examines the use of the **show ip interface brief** command and how to interpret its results for both Ethernet and serial interface connections. This is a very important command for troubleshooting and isolating router problems.*

4.3 Given a scenario, apply network hardening techniques.

It is a best practice to verify the router configuration. The status of an interface reflects how the router is programmed.

4.4 Compare and contrast remote access methods and security implications.

This section examines the steps involved in establishing a secure virtual terminal connection to a router or a switch. This section also looks at connecting to a router's console port by using an SSH connection.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section mentions that there a physical method for troubleshooting the wiring of an Ethernet interface and a T1 serial interface: You can use a loopback adapter. If the wiring is good, the LED light of the interface lights up, and the interface status is up.

Test Your Knowledge

1. True or false: The purpose of the keepalive packet is to indicate that the Ethernet interface is connected to another networking device.

   True

2. True or false: When the **show ip interface brief** command shows **Yes** in the **OK?** column, this indicates that keepalive packets are being exchanged.

   False

SUMMARY

This chapter presents an overview of routers, a technique for establishing a console port connection, and the basic steps in configuring a router's interface. You should understand the difference between a router's user and privileged EXEC modes. Table 7-4 provides a list of the router prompts encountered in this chapter.

TABLE 7-4 **Router Prompts and Their Definitions**

Prompt	Definition
Router>	User EXEC mode
Router#	Privileged EXEC mode
Router(config)#	Configuration mode
Router(config-if)#	Interface configuration mode
Router(config-line)#	Line terminal configuration mode

You should understand and be able to demonstrate the steps involved in configuring Ethernet and serial interfaces. These concepts are used repeatedly in the following chapters. In this chapter, you have also learned about the router troubleshooting command **sh ip int brief**.

QUESTIONS AND PROBLEMS

Section 7-1

1. What is the command-line interface used for on a Cisco router?

   The command-line interface is used to configure a Cisco router. It allows you to enter commands into the router.

2. What does Cisco IOS stand for?

   Cisco IOS stands for Cisco Internet Operating System.

Section 7-2

3. Define broadcast domain.

   A broadcast domain is a portion of a network in which any broadcast sent out on the network is seen by all hosts.

4. What is a flat network?

   A flat network is a network where the LANs share the same broadcast domain.

5. What is a layer 3 network?

   A layer 3 network uses layer 3 addressing to select routes to forward data packets.

6. What is the purpose of a gateway?

   A gateway is a networking device that enables data to enter and exit a LAN.

7. Where is the default gateway address assigned in Windows?

   In the TCP/IP menu.

8. A computer with host IP address 10.10.5.1 sends a data packet with destination IP address 10.10.5.2. Subnet mask 255.255.255.0 is being used. Determine whether the packet stays in the LAN or is sent to the gateway. Show your work.

   The data stays in the LAN.

   10. 10. 5. 1

   255. 255. 255. 0

   10. 10. 5. 0

   10. 10. 5. 2

   255. 255. 255. 0

   10. 10. 5. 0

9. Repeat problem 8 with the destination IP address for the data packet as 10.5.10.2 and the subnet mask the same. Show your work.

   The data does not stay in the same subnet, so it is sent to the gateway.

   10. 10. 5. 1

   255. 255. 255. 0

   10. 10. 5. 0

   10. 5. 10. 2

   255. 255. 255. 0

   10. 5. 10. 0

10. Repeat problem 9 with the subnet mask changed to 255.0.0.0. Show your work.

    10.10.5.1 and 10.5.10.2 are both in the same subnet; therefore, the data packet stays in the LAN. The work can be shown by ANDing the IP addresses with the Subnet Mask, 255.0.0.0.

    10. 10. 5 .1

    255. 0. 0. 0

    10. 0. 0. 0

    10. 5. 10. 2

    255. 0. 0. 0

    10. 0. 0. 0

11. Repeat problem 9 with the subnet mask changed to 255.255.0.0. Show your work.

    10.10.5.1 and 10.5.10.2 are not in the same subnet; therefore, the data packet is sent to the gateway.

    10. 10. 5. 1

    255. 255. 0. 0

    10. 10. 0. 0

    10. 5. 10. 2

    255. 255. 0. 0

    10. 5. 0. 0

12. The IP address for computer C2 is 10.10.1.2. The IP address for computer B1 is 10.10.10.1. Subnet mask 255.255.0.0 is being used. Are the computers in the same network? Does the data packet stay in the LAN? Show your work.

    The computers are in the same LAN; therefore, the data packet stays in the LAN.

    10. 10. 1. 2

    255. 255. 0. 0

    (C2) 10. 10. 0. 0

    10. 10. 10. 1

    255. 255. 0. 0

    (B1) 10. 10. 0. 0

13. Determine the router hop count from LAN A to LAN D in the network shown in Figure 7-15 for the route with the fewest hops.

    Router A > Router E > Router D; 2 hops

    Router A > Router B > Router E > Router D; 3 hops

14. List all the possible routes from LAN B to LAN D in the network shown in Figure 7-15.

    Router B > Router C > Router B > Router E > Router D

    Router B > Router E > Router D

    Router B > Router A > Router E > Router D

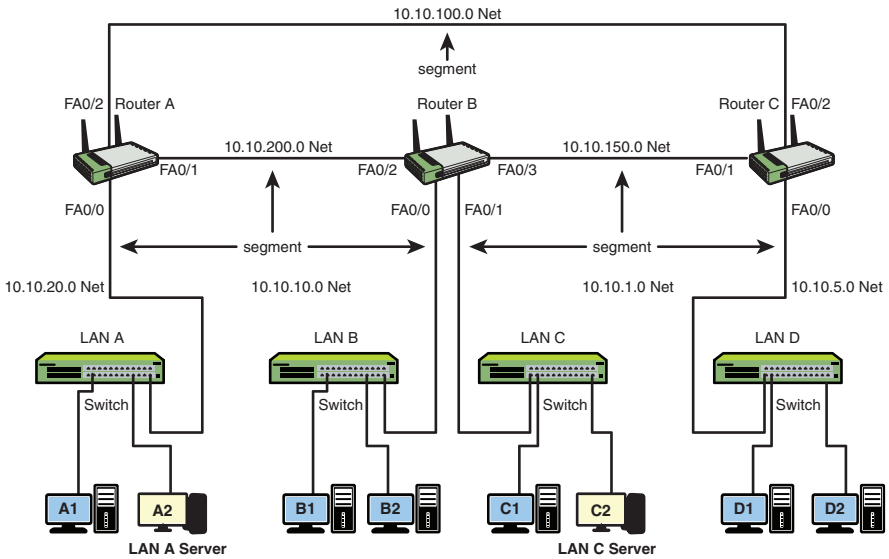
15. List the subnets attached to Router B in Figure 7-15.

    10.10.200.0 NET

    10.10.150.0 NET

    10.10.10.0 NET

    10.10.1.0 NET



Router A Port Addresses (LAN A)	
FastEthernet 0/0 (Gateway Address)	10.10.20.250
FastEthernet 0/1	10.10.200.1
FastEthernet 0/2	10.10.100.1
LAN A Computers	
Computer A1	10.10.20.1
Computer A2	10.10.20.2
Subnet Mask	***255.255.255.0***

Router B Port Addresses (LAN B)	
FastEthernet 0/0 (Gateway Address)	10.10.10.250
FastEthernet 0/2	10.10.200.2
FastEthernet 0/3	10.10.150.1
LAN B Computers	
Computer B1	10.10.10.1
Computer B2	10.10.10.2
Subnet Mask	***255.255.255.0***

Router B Port Addresses (LAN C)	
FastEthernet 0/1 (Gateway Address)	10.10.1.250
FastEthernet 0/2	10.10.200.2
FastEthernet 0/3	10.10.150.1
LAN C Computers	
Computer C1	10.10.1.1
Computer C2	10.10.1.2
Subnet Mask	***255.255.255.0***

Router Port Addresses (LAN D)	
FastEthernet 0/0 (Gateway Address)	10.10.5.250
FastEthernet 0/1	10.10.150.2
FastEthernet 0/2	10.10.100.2
LAN D Computers	
Computer D1	10.10.5.1
Computer D2	10.10.5.2
Subnet Mask	***255.255.255.0***

FIGURE 7-15 Network topology for problems 13–18.

16. List the subnets attached to Router C in Figure 7-15.

    10.10.100.0 NET

    10.10.150.0. NET

    10.10.5.0 NET

17. What is the next hop address for the FastEthernet port 1 on Router A in Figure 7-15?

    Router B, FA0/2, 10.10.200.2

18. What is the next hop address for the FastEthernet port 2 on Router C in Figure 7-15?

    Router A, FA0/2, 10.10.200.1

Section 7-3

19. What command is used to determine the version of IOS running on a Cisco router? Show the prompt and the command.

    Router > show version

20. What is the help command in Cisco IOS?

    ?

21. What command can be used to see the uptime for a router?

    show version

22. What command is used to verify that there is sufficient memory available to load a new version of the Cisco IOS software?

    show flash

23. What is the router prompt for user EXEC mode?

    Router>

24. If you enter **exit** from the **Router>** prompt, where does it place you?

    Back at the "Press RETURN" screen

Section 7-4

25. What is the router prompt for privileged EXEC mode?

    Router#

26. What command is used to enter a router's privileged mode?

    To enter a router's privileged mode, you use the **enable** command and the appropriate password.

27. What command is used to change a router's hostname to **Tech-router**?

    hostname Tech-router

28. What command is used to enter a router's terminal configuration mode?

    configure terminal (or **conf t**)

29. What is the router prompt for terminal configuration mode?

    Router(config)#

30. What is the command for setting password protection for privileged mode if the password is **Tech**?

    enable secret Tech

31. What does the command **line vty 0 4** mean?

    - **line:** Places the router in line configuration mode
    - **vty:** Virtual terminal
    - **0 4:** The number of vty lines to which the configuration parameters that follow will be applied. The five virtual terminal connections are identified as 0, 1, 2, 3, and 4.

32. List the commands used to configure and enable a FastEthernet0/1 router interface with IP address 10.10.20.250 and subnet mask 255.255.0.0.

    conf t

    int fa0/1

    ip address 10.10.20.250 255.255.0.0

    no shut

33. What is the most efficient command for viewing the router interface status and protocol?

    show ip interface brief (or **sh ip int brief**) is the best option. There are other commands, but this is the best choice.

34. Is clocking of a router's serial interface set by the DCE or the DTE?

    DCE

35. What are the three ways to see if a router's serial port is a DCE or DTE end?

    1. Inspect the ends of the V.35 cable. DCE is female.
    2. Check the label of the V.35 cable.
    3. Use the **show controllers serial** (*interface name*) command.

36. What command is used to set the data speed on a router's serial port to 56Kbps?

    clock rate 56000

37. What is the router prompt for interface configuration mode?

    Router(config-if)#

Section 7-5

38. What is the purpose of the fast link pulse?

    It carries the configuration information between the ends of a data link.

39. Define full-duplex.

    Full-duplex means that a communications device can transmit and receive at the same time.

40. Define half-duplex.

    Half-duplex means that a communication device can transmit and receive but not at the same time.

41. Which of the following is a disadvantage of the auto-negotiation protocol?

    a. It is useful only in LANs that have multiple connection capabilities.
    b. A failed negotiation on a functioning link can cause a link failure.
    c. It's recommended for use in critical network data paths.
    d. It works at 10Mbps.

Section 7-6

42. What is the purpose of a keepalive packet?

    It indicates that the Ethernet interface is connected to another networking device.

43. The **sh ip interface brief** command indicates that the protocol for a FastEthernet interface is **down**. What does this mean?

    It indicates that there is a loss of communications between the router and a connected networking device.

44. In a serial interface, what is the difference between the status **down** and the status **administratively down**?

    status **down** means the link has been lost or disconnected.

    status **administratively down** means the interface has been shut down.

45. What command should be used to look at collision errors?

    show interface

Critical Thinking

46. What does the command **line vty 0 1** mean?

    0 1 represents the number of vty lines to which the configuration parameters that follow will be applied. The two virtual terminal connections are identified as 0 and 1.

47. How can you check to see if the FastEthernet interface on a router is connected to the FastEthernet interface on another networking device?

    1. Check the link lights.
    2. Use the **sh ip int brief** command to check the interface status and protocol. You know there is a network connection if Protocol is **up**.

48. You suspect that a router's LAN gateway is down. Describe how you would troubleshoot the problem.

    1. Ping the gateway IP address.
    2. Check the link lights.
    3. Use the **sh ip int brief** command to determine whether the interface is configured and the interface is up.

49. Can the following configurations be accomplished on Router A? Explain your answers.

    a.
    ```
    interface FastEthernet 0/0
    IP address 10.1.0.5 255.255.255.252

    interface FastEthernet 1/0
    IP address 10.1.0.5 255.255.255.252
    ```

    No. The IP addresses are the same on both interfaces, and IP address duplication is not allowed.

b.
```
interface FastEthernet 0/0
IP address 10.1.0.5 255.255.255.252

interface FastEthernet 1/0
IP address 10.1.0.6 255.255.255.252
```

No. The IP addresses are in the same subnet.

c.
```
interface FastEthernet 0/0
IP address 10.1.0.4 255.255.255.252

interface FastEthernet 1/0
IP address 10.1.0.5 255.255.255.252
```

No. The IP address on interface FastEthernet0/0 is a network number, but the network number cannot be used as the interface IP address.

d.
```
interface FastEthernet 0/0
IP address 10.1.0.5 255.255.255.252

interface FastEthernet 1/0
IP address 10.1.0.9 255.255.255.252
```

Yes. The interface IP addresses are on different subnets.

Certification Questions

50. Which of the following is the most efficient command to use to view the router's interface status and protocol status?

    a. **sh int brief**
    b. **show interface brief**
    c. **show ip interface brief**
    d. **show status**

51. The designation fa0/0 indicates ____.

    a. FastEthernet interface 0/0
    b. external port 0/0
    c. exit port 0/0
    d. FastEthernet input port 0/0
    e. FastEthernet output port 0/0

52. The IP address of the networking device used for the default gateway must ____.

    a. be in the same subnet as the LAN
    b. use subnet mask 255.255.255.0
    c. use CIDR block /22
    d. None of these answers are correct.

53. What is the command for setting password protection for privileged mode if the password is **tech**?

    a. **enable tech**
    b. **enable secret tech**
    c. **enabling secret tech**
    d. **enabling tech**

54. True or false: Clocking for the serial port on a router occurs at the DTE end.

    False

55. True or false: These are the three ways to see if your router's serial port is a DTE or the DCE:

    - Inspect the ends of the V.35 cable; DCE is male.
    - Check the label on the V.35 cable.
    - Use the **show serial [***interface name***]** command.

    False

56. True or false: The following is the sequence of commands and prompts used to change the hostname of a router to **Network**:

```
router> enable
router# enable
router# conf t
router# hostname Network
Network#
```

    False

57. True or false: The router prompt for the interface configuration mode on a Cisco router is **Router(config-if)#**.

    True

58. True or false: The following are the settings for the console serial communication port on a Cisco router:

    Bits per seconds: 9600

    Data bits: 8

    Parity: none

    Stop bits: 1

    Flow control: none

    True

59. The command **sh ip int brief** is executed from what prompt?

    a. **Router(config)**
    b. **Router(config-if)#**
    c. **Router#**
    d. **Router(config)#**

This page intentionally left blank

8
CHAPTER

Introduction to Switch Configuration

Chapter Outline

8-1 Introduction
8-2 Introduction to VLANs
8-3 Introduction to Switch Configuration
8-4 Spanning Tree Protocol
8-5 Power over Ethernet
8-6 Troubleshooting the Switch Interface
Summary
Questions and Problems

Objectives

- Be able to identify and describe the three types of VLANs
- Discuss two ways of establishing VLAN membership
- Understand how to use commands to configure a network switch
- Be able to explain the steps for configuring a static VLAN
- Explain the purpose of Spanning Tree Protocol
- Discuss the purpose of the five Spanning Tree Protocol states
- Discuss the advantages of using Power over Ethernet
- Understand best practices for managing switch security

Key Terms

VLAN (virtual LAN)
port-based VLAN
tag-based VLAN
protocol-based VLAN
static VLAN
dynamic VLAN
configure terminal (**conf t**)
switch#
Switch(config)#
Switch(config-line)#
Spanning Tree Protocol (STP)
bridge protocol data unit (BPDU)
configuration BPDU
topology change notification (TCN)
topology change notification acknowledgment (TCA)
Power over Ethernet (PoE)
PD
PSE
endpoint PSE
midspan (midpoint) PSE
resistive power discovery
PoE+

8-1 INTRODUCTION

This chapter introduces switch VLANs, switch configuration, and Spanning Tree Protocol. It also introduces Simple Network Management Protocol (SNMP) and Power over Ethernet (PoE).

This chapter examines the computer networking issues that arise when configuring a network switch and presents the commands for configuring a network switch. Section 8-2, "Introduction to VLANs," provides an introduction to virtual local area networks (VLANs). The section begins with an overview of the three types of VLANs followed by a discussion of the two ways to establish VLAN membership. Section 8-3, "Introduction to Switch Configuration," describes the basics of configuring a Cisco switch and describes how to configure a static VLAN. Section 8-4, "Spanning Tree Protocol," examines Spanning Tree Protocol (STP), which is a link management protocol that prevents looping and also controls data flow over possible redundant data paths. Section 8-5, "Power over Ethernet," provides an overview of Power over Ethernet (PoE) and the benefits of implementing this technology in a network. Section 8-6, "Troubleshooting the Switch Interface," introduces the switch commands **show interface status** and **show mac address-table** (or **show mac-address-table**) for layer 2 switch troubleshooting.

Table 8-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 8-1 **Chapter 8 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.3	Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	8-5
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes.	8-2
1.5	Explain common ports and protocols, their application, and encrypted alternatives.	8-3
1.6	Explain the use and purpose of network services.	8-2, 8-6
1.7	Explain basic corporate and datacenter network architecture.	8-6
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	8-2, 8-3, 8-4, 8-5

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
2.3	Given a scenario, configure and deploy common Ethernet switching features.	8-2, 8-3, 8-4, 8-5, 8-6
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	8-5, 8-6
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	8-3, 8-4
5.0	**Network Troubleshooting**	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	8-2, 8-4, 8-5, 8-6
5.3	Given a scenario, use the appropriate network software tools and commands.	8-3
5.5	Given a scenario, troubleshoot general networking issues.	8-2, 8-4

8-2 INTRODUCTION TO VLANS

This section introduces VLANs, which are a very important concept in computer networks. It examines the three types of VLANs—port-based, tag-based, and protocol-based VLANs—and it also examines static and dynamic VLANs.

This section provides an overview of VLANs, which are an important networking concept in modern computer networks. This section discusses port-based, tag-based, and protocol-based VLANs, and it also examines static and dynamic VLANs.

Virtual LANs

A switch can be configured to work with a **VLAN (virtual LAN)**, which is a group of host computers and servers configured as if they are in the same LAN, even if they reside across routers in separate LANs. The advantage of using VLANs is that a network administrator can group computers and servers in the same VLAN based on the organizational group (for example, Sales, Engineering), geographic location (for example, first floor, second floor), or the network purpose (for example, office network, voice over IP phone network, utility network). This grouping is possible even if the computers and servers are not on the same physical segment or even in the same building.

VLAN (Virtual LAN)
A group of host computers and servers that are configured as if they are in the same LAN, even if they reside across routers in separate LANs

There are three types of VLANs: port-based VLANs, tag-based VLANs, and protocol-based VLANs.

In a **port-based VLAN**, the host computers connected to specific ports on a switch are assigned to a specific VLAN. For example, say that the computers connected to switch ports 2, 3, and 4 are assigned to the Sales VLAN, VLAN 2, while the computers connected to switch ports 6, 7, and 8 are assigned to the Engineering VLAN, VLAN 3, as shown in Figure 8-1. The switch will be configured as a

Port-Based VLAN
A VLAN in which host computers connected to specific ports on a switch are assigned to a specific VLAN

port-based VLAN so that ports 2, 3, and 4 are assigned to the Sales VLAN, while ports 6, 7, and 8 belong to the Engineering VLAN. The devices assigned to the same VLAN will share broadcasts for that LAN; however, computers that are connected to ports not assigned to the VLAN will not share the broadcasts. For example, the computers in VLAN 2 (Sales) share the same broadcast domain, and computers in VLAN 3 (Engineering) share a different broadcast domain.

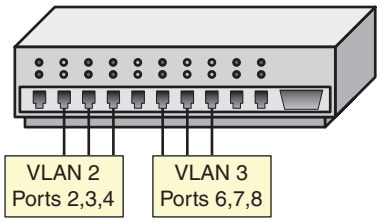


FIGURE 8-1 An example of grouping for port-based VLANs.

Tag-Based VLAN
A VLAN in which the VLAN ID is based on 802.1Q

In **tag-based VLANs**, a tag is added to the Ethernet frames. This tag contains the VLAN ID that is used to indicate that a frame belongs to a specific VLAN. The addition of the VLAN ID is based on the 802.1Q specification. An advantage of an 802.1Q VLAN is that it helps contain broadcast and multicast data traffic, which helps minimize data congestion and improve throughput. This specification also provides guidelines for a switch port to belong to more than one VLAN. In addition, a tag-based VLAN can help provide better security by logically isolating and grouping users.

Protocol-Based VLAN
A VLAN in which connection to ports is based on the protocol being used

In **protocol-based VLANs**, the data traffic is connected to specific ports based on the type of protocol being used. If the protocol doesn't match any of the VLANs, a packet is dropped when it enters the switch. For example, an IP network could be set up for the Engineering VLAN on ports 6, 7, and 8 and a network for the Sales VLAN on ports 2, 3, and 4. The advantage of this is that the data traffic for the two networks is separated.

There are two approaches to assigning VLAN membership:

Static VLAN
A port-based VLAN, with assignments created when ports are assigned to a specific VLAN

Dynamic VLAN
A VLAN in which ports are assigned based on either the computer's MAC address or the username of the client logged on to the computer

- **Static VLAN:** This is basically a port-based VLAN. The assignments are created when ports are assigned to a specific VLAN.
- **Dynamic VLAN:** Ports are assigned to a VLAN based on either the computer's MAC address or the username of the client logged on to the computer. This means the system has been previously configured with the VLAN assignments for the computer or the username. The advantage of this is that the username and/or the computer can move to a different location, and VLAN membership is retained.

Let's explore a scenario in which the Sales team and the Engineering team are spread out in two different buildings. Each building has its own network switch, and both switches are connected via one physical link. Therefore, both VLANs must be available in both buildings. In a scenario like this, not only is it necessary to have the same Sales VLAN running on both building switches, it is also important

to have members of the same VLAN able to communicate with each other across buildings and to adhere to the same VLAN restrictions. In order to accomplish this, the very same 802.1Q protocol used in tag-based VLANs can be used for VLAN tagging. *VLAN tagging* is a technique deployed on a switch interface to carry Ethernet frames of multiple VLANs. The interface must connect to another switch port, router port, or network device that understands VLAN tagging, and both sides must agree on the VLAN tagging protocol. A switch interface or port configured to carry multiple VLANs is often referred to as a *trunk port*. Frames that are marked with the VLAN tags are routed to the correct VLAN at the other end of the trunk line. The ports between the switch and the customer are considered untagged, which means the Ethernet packets are normal and do not contain any tags. However, a trunk port between the two switches that has tagged packets (tagging) knows which customer VLAN the packet should be delivered to.

Having multiple VLANs and multiple switches on a network can increase administrative overhead in configuring and maintaining the correct VLANs in all the switches on the network. VLAN Trunking Protocol (VTP) is Cisco's proprietary protocol for managing and propagating the VLAN definitions to all of the VTP-capable switches. With VTP, a new VLAN can be defined on a VTP server, and then the VLAN information gets propagated to every switch on the network.

Section 8-2 Review

This section covers the following Network+ exam objectives.

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

As discussed in this section, an advantage of an 802.1Q VLAN is that it helps contain broadcast and multicast data traffic, which helps minimize data congestion and improve throughput.

1.6 Explain the use and purpose of network services.

A VLAN (virtual LAN) is a group of host computers and servers that are configured as if they are in the same LAN even if they reside across routers in separate LANs.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section introduces port-based, tag-based, and protocol-based VLANs. It also discusses the VLAN ID, which is based on the 802.1Q specification. In a tag-based VLAN, a tag containing the VLAN ID is added to the Ethernet frame.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

An advantage of an 802.1Q VLAN is that helps contain broadcast and multicast data traffic, which helps minimize data congestion and improve throughput. This specification also provides guidelines for a switch port to belong to more than one VLAN. In addition, a tag-based VLAN can help provide better security by logically isolating and grouping users.

5.5 Given a scenario, troubleshoot general networking issues.

This section discusses dynamic VLANs, in which ports are assigned to a VLAN based on either the computer's MAC address or the username of the client logged on to the computer. This means the system has been previously configured with the VLAN assignments for the computer or the username. The advantage of this is that the username and/or the computer can move to a different location, and VLAN membership is retained.

Test Your Knowledge

1. What are the three types of VLANs? (Select three.)
   a. Port-based VLAN
   b. Tag-based VLAN
   c. Pd-based VLAN
   d. Protocol-based VLAN
   e. Label-based VLAN
   f. Routing-based VLAN
2. A static VLAN is basically which of the following?
   a. Seldom used
   b. A MAC VLAN
   c. A port-based VLAN
   d. None of these answers are correct.

8-3 INTRODUCTION TO SWITCH CONFIGURATION

This section provides an introduction to switch configuration. Students will notice many similarities between switch commands and the router commands. However, there are some distinct differences, such as the commands required for configuring a static VLAN. You should have students use the static VLAN configuration that comes with the Net-Challenge software.

This section examines the basics of configuring a Cisco switch. The commands for switch configuration are similar to those for router configuration. To configure a switch, you must first establish a console connection and enter privileged mode on the switch. The procedure for establishing a console connection to a switch is the same as for a router. (Refer to Section 5-5, "The Console Port Connection," for the steps for establishing a console connection.) The privileged EXEC mode (also called the enable mode) allows full access for configuring the switch ports and establishing a VLAN. This section focuses on general configuration steps for a switch and examines MAC address information and IP address configuration of VLANs.

You enter privileged mode by using the command **enable** at the **Switch>** prompt, as shown here:

```
Switch> enable
Password:
Switch#
```

The **#** sign after the switch name indicates that you are in privileged EXEC mode.

Entry into the switch's privileged mode is typically password protected. The exception to this is when a switch has not been configured and a password has not been assigned to it. In this case, pressing **Enter** on the keyboard at the **Switch>** prompt promotes the user to privileged mode (**Switch#**) without requiring a password.

Note

It is important to use caution after entering privileged mode on a switch. It is easy to make mistakes, and incorrectly entered switch configurations adversely affect the network. This text comes with the Net-Challenge software, which you can download from the textbook companion website to help you gain experience with switch configuration. (See the Introduction for information on how to access this site.) In fact, most of the switch configuration commands presented in this section can be implemented in the Net-Challenge switch simulator.

Hostname

The commands examined in this section require you to enter a switch's terminal configuration mode. To enter a switch's configuration mode, enter the command **configure terminal** (abbreviated **conf t**) at the **switch#** prompt like this:

configure terminal (conf t)
A command to enter a switch's terminal configuration mode

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
```

or like this:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
```

Note that the prompt changes to **switch(config)#**. This indicates that the switch is in terminal configuration mode.

Let's examine a switch configuration option that enables the user to assign a hostname to a switch. The generic name or the name of an unconfigured Cisco switch is **switch**, and the **hostname** command enables you to change the name to specifically identify the switch. For example, valid hostname structures include switchA, switch-A, and switch_A, but switch A is not valid because switch hostnames may not have any spaces. The word *switch* does not have to be used in a hostname.

In privileged mode (that is, at the **switch#** prompt), enter the command **hostname [***switch-name***]** and press **Enter** to set the hostname for the switch to *switch-name*. The following example shows how to change a switch's hostname to SwitchA:

```
switch(config)# hostname SwitchA
SwitchA#
```

Notice that the switch's name changes from switch to SwitchA after the **hostname** command is entered.

Enable Secret

switch#
The prompt for a switch's privileged EXEC mode

You configure password protection for privileged EXEC mode (sometimes known as enable mode) by setting the enable secret. To do so, you need to enter the switch's configure terminal mode by entering **configure terminal** or **conf t** at the **switch#** prompt and then enter the command **enable secret [***your-password***]** and press **Enter**:

```
SwitchA# conf t
SwitchA(config)#
SwitchA(config)# enable secret my-secret
```

This example sets the password for entering the switch's privileged EXEC mode to **my-secret**. The password for entering the switch's privileged mode must now be entered to gain access to the mode.

Setting the Line Console Passwords

Switch(config)#
The prompt for a switch's terminal configuration mode

A switch has two line connections through which a user can gain access to the switch. The line connections available on a switch can be displayed by using the **line ?** command at the **Switch(config)#** prompt. Two line connections are typically available:

- **console:** Primary terminal line (the console port)
- **vty:** Virtual terminal for Telnet connections

The following steps demonstrate how to configure password protection for the console port and the virtual terminal:

1. Enter the command **line console 0** and press **Enter**.
2. Enter the command **login** and press **Enter**.
3. Enter the command **password my-secret2**, where **my-secret2** is the console port password.

Here is what the command line looks like when you follow these steps:

```
SwitchA(config)# line console 0
SwitchA(config-line)# login
SwitchA(config-line)# password my-secret2
```

Note the change in the switch prompt to **Switch(config-line)#**, which indicates that you are in the switch's line configuration mode.

Switch(config-line)#
A prompt which indicates that you are in the switch's line configuration mode

Password protection for the virtual terminal (line vty) is set from the switch's configuration mode. You use the virtual terminal to enter a switch via a Telnet connection:

1. Enter the command **line vty 0 15**. This places the switch in line configuration mode (config-line). The **0 15** indicates that 16 virtual terminal connections (0, 1, 2, 3, 4,…15) can be made simultaneously.
2. Enter **login**, press **Enter**, and enter the command **password my-secret3**, where **my-secret3** is the password for the virtual terminal connection:
   - `SwitchA(config)# line vty 0 4`
   - `SwitchA(config-line)# password my-secret3`
   - `SwitchA(config-line)# login`
3. Set layer 3 access to the switch by using the following command sequence:
   - `SwitchA(config)# interface VLAN 1`
   - `SwitchA(config-if)# ip address 172.16.32.2 255.255.255.0`
   - `SwitchA(config-if)# no shutdown`

Note that the IP address is being set for VLAN 1. The interface for the switch is also enabled at this point with the **no shutdown** command.

Configuring an IP address on a router's interface enables a layer 3 routed network. In addition, the interface IP address becomes a gateway address of that network, as described in Chapter 7, "Introduction to Router Configuration." However, it is not the same on layer 2 switches. When configuring an IP address on a VLAN interface such as this, you merely assign an IP address to a switch. So, a switch can communicate with other network devices on the same VLAN and vice versa. This is an important addition to the switch for management purposes because it enables networking staff to connect remotely and configure the switch. The IP VLAN interface does not perform any routing functions when running as a layer 2 switch. As a matter of fact, the IP VLAN interface is not required for a switch to start forwarding packets and perform its other layer 2 functions.

The configuration settings entered on the VLAN 1 interface can be viewed by entering the following command:

```
SwitchA# show interface VLAN 1
```

For the interface VLAN to be up, at least one switch port in the VLAN must be up or have a physical link. You can verify the status of a switch port by entering the following command:

```
SwitchA# show interface Fastethernet0/1
```

To see the statuses of all the switch ports, including their speed, duplex, and VLAN, use the following command:

```
SwitchA# show interfaces status
Port    Name          Status      Vlan    Duplex    Speed    Type
Fa0/1                 connected   1       a-full    a-100    10/100BaseTX
Fa0/1                 connected   1       a-full    a-100    10/100BaseTX
Fa0/2                 connected   1       a-full    a-100    10/100BaseTX
Fa0/3                 connected   1       a-full    a-100    10/100BaseTX
Fa0/4                 connected   1       a-full    a-100    10/100BaseTX
Fa0/5                 connected   1       a-full    a-100    10/100BaseTX
Fa0/6                 connected   1       a-full    a-100    10/100BaseTX
```

You can view the running configuration for a switch by using the **show running-config** command. To display the startup configuration, use the **show startup-config** command. To copy the running-configuration file to NVRAM, use the **copy running-config startup-config** command.

As you can see, there is a lot of similarity between switch configuration and router configuration at the command-line interface. However, the major differences are apparent when configuring a VLAN. The next section describes how to configure a static VLAN.

Static VLAN Configuration

This section demonstrates the steps for configuring a static VLAN. It uses an example that shows how to define the ports for VLAN 2 (Sales) and VLAN 3 (Engineering). VLAN memberships must be defined for the required ports.

The first step in configuring a VLAN is to establish a terminal connection to the switch by using the Cisco console cable. The console connection is used to perform the initial configurations needed to use the Cisco Network Assistant software:

1. Connect the console cable to your workstation and switch.
2. Open the HyperTerminal software on your workstation.
3. Make a HyperTerminal connection to the switch, just as you would do with a router. After you have made a HyperTerminal connection to the switch, the switch's initial prompt should appear as **Switch>**.
4. At the initial prompt, type **enable** or **en**. The prompt should change to **Switch#**, allowing you to enter privileged mode for the switch.
5. Next, type **configure terminal** or **conf t**. The prompt should change to **Switch(config)#**, which means you are in the global configuration mode of the switch.
6. Now type **interface Vlan1** or **int Vlan1**. The prompt should now change to **Switch(config-if)#**, and you can make changes to VLAN 1's interface.

7. Enter **ip address 192.168.1.1 255.255.255.0** to change the switch's IP address to 192.168.1.1.
8. Type **no shut** in order to keep VLAN 1 up and active.

You have now set the IP address of the switch to 192.168.1.1. Notice that the subnet mask is set to 255.255.255.0, which places the switch in the 192.168.1.0 network. The IP address is set for VLAN 1 because this is the default administrative VLAN for the switch, and it can never be removed. The workstation should be connected to port 1 on the switch, and the computer's IP address should be configured to 192.168 1.2. This places the computer in the same network defined for the VLAN 1 interface. At this point, you can use the **ping** command to verify network connectivity from the computer to the switch.

The next step is to use the **show vlan** command to verify which ports have been defined for the switch. By default, all ports are assigned to VLAN 1, as demonstrated in the following example:

```
Switch# show vlan
VLAN          Name            Status        Ports
1             default         active        Fa0/1, Fa0/2, Fa3/3, Fa0/4
                                            Fa0/5, FA0/6, Fa0/7, Fa0/8
                                            Fa0/9, Fa0/10
```

This shows that all the FastEthernet interfaces are currently assigned to VLAN 1.

Next, you will create two additional VLANs: one for Sales and one for Engineering.

The following example of configuring a VLAN requires you to enter configuration mode on the switch. In this case, the Sales and Engineering VLANs are being created:

```
SwitchA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)# vlan 2
SwitchA (config-vlan)# name Sales
Switch(config)# vlan 3
Switch(config-vlan)# name Engineering
```

The next step is to verify that the new VLANs have been created:

```
Switch(config-vlan)# exit
Switch(config)# exit
Switch# show vlan
VLAN          Name            Status        Ports
1             default         active        Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                            Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                            Fa0/9, Fa0/10
2             Sales           active
3             Engineering     active
```

Next, you need to assign ports to the newly created VLANs. To do this, you need to enter configuration mode and assign each FastEthernet interface (port) to the proper VLAN. This example shows FastEthernet interface 0/2 being assigned to VLAN 2:

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# int fa 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

The next step is to verify that FastEthernet0/2 has been assigned to the Sales VLAN (VLAN 2). To do this, you use the **show vlan brief** command, which displays only the interfaces assigned to each VLAN:

```
Switch# show vlan brief

VLAN         Name             Status         Ports
1            default          active         Fa0/1, Fa0/3, Fa0/4, Fa0/5
                                             Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                             Fa0/10
2            Sales            active         Fa0/2
```

Next, you assign ports 3 and 4 to the Sales VLAN (VLAN 2) and ports 6, 7, and 8 to the Engineering VLAN (VLAN 3). Then you can verify the port assignments by using the **show vlan** command, as shown here:

```
Switch# show vlan
VLAN         Name             Status        Ports
1            default          active        Fa0/1, Fa0/5, Fa0/9, Fa0/10
2            Sales            active        Fa0/2, Fa0/3, Fa0/4
3            Engineering      active        Fa0/6, Fa0/7, Fa0/8
```

You can look specifically at the assignments for only one of the VLANs by entering the command **show vlan name** <*vlan-name*>, where *vlan-name* is the (case-sensitive) name assigned to the VLAN:

```
Switch# sh vlan name Engineering

VLAN         Name             Status        Ports
3            Engineering      active        Fa0/6, Fa0/7, Fa0/8
```

Alternatively, you can use the number of the VLAN instead of using the name, by using the command **sh vlan id** <*vlan#*>:

```
Switch# show vlan id 3
VLAN         Name             Status        Ports
3            Engineering      active        Fa0/6, Fa0/7, Fa0/8
```

You can view the overall configuration of a switch by using the **show running-config** (or **sh run**) command, as shown in the following example, which displays only part of the configuration:

```
Switch# sh run - -
Building configuration...Current configuration : 1411 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
ip subnet-zero
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
interface FastEthernet0/1
!-
 interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
 . .
 . .
 . .
 . .
interface FastEthernet0/5
!
interface FastEthernet0/6
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
 no ip route-cache
!
ip http server
!
line con 0
line vty 0 15
 login
end
```

The running configuration for the switch shows that the FastEthernet interfaces have been assigned to the proper VLANs. In addition, you can see that an IP address has been assigned to the default VLAN 1.

A voice VLAN is a special VLAN designated for IP phones. In a voice VLAN, voice over IP (VoIP) features such as power and quality of service are part of the port configuration. Voice VLANs have become very common, and there is a special command for configuring a switch port as a voice VLAN. For example, you can add the following command to the port configurations to enable voice VLAN 219 on that port:

```
Switch# switchport voice vlan 219
```

VLAN SUBINTERFACES

As discussed earlier in this chapter, each VLAN is its own broadcast domain. It cannot forward traffic across its VLAN boundaries. However, it is almost impractical in today's applications for a VLAN not to be able to communicate beyond itself. To enable communications among VLANs, InterVLAN *routing* is required.

The most logical solution for routing traffic between different VLANs is to introduce or create a layer 3 routed network between them. One traditional way is to connect each VLAN to a router interface. Then, each router interface is configured as a different layer 3 network. This enables VLANs to communicate and pass traffic via the layer 3 IP network. For a few VLANs, this does not present an issue, but for a large number of VLANs, it could create problems. Every VLAN requires a physical connection to a router port. Router ports are expensive, and requiring physical connections can be costly as the number of VLANs increases and more physical links are required. A more common and popular design is to implement a *router on a stick* design, which eliminates the need to connect a link from each VLAN to a router port and instead uses a trunk or 802.1Q port. A single trunk port is connected to a router, and it passes the tagged VLAN traffic to the router as shown in Figure 8-2.

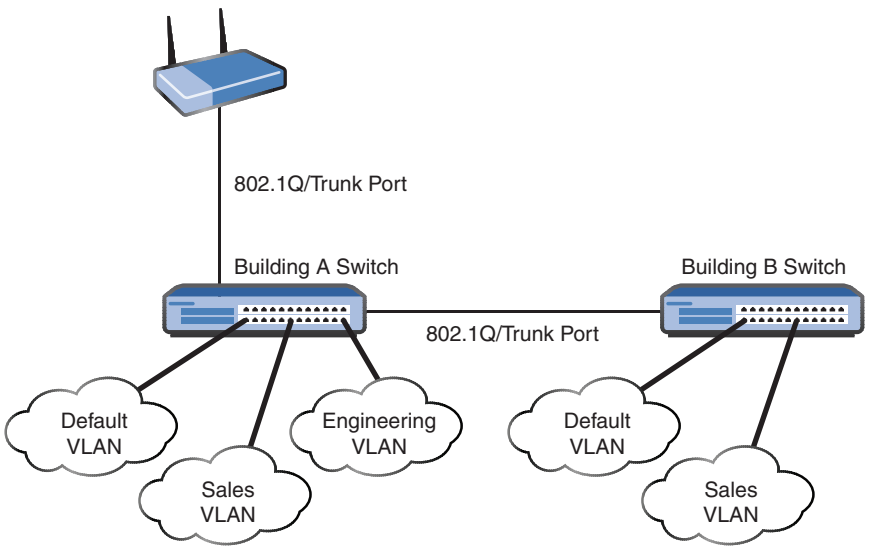


FIGURE 8-2 Router on a stick topology.

This design requires that the router be configured to accept the tagged VLANs. A layer 3 network is then assigned to each VLAN coming to the router. The following example demonstrates how to configure a Cisco router for 802.1Q inter-VLAN routing:

```
Router(config)# interface FastEthernet0/0
Router(config-if)# no ip address
Router(config-if)# interface FastEthernet0/0.1
Router(config-if)# description Default VLAN
Router(config-subif)# encapsulation dot1Q 1
Router(config-subif)# ip address 172.16.10.1 255.255.255.0

Router(config-subif)# interface FastEthernet0/0.2
Router(config-if)# description Sales VLAN
Router(config-subif)# encapsulation dot1Q 2
Router(config-subif)# ip address 172.16.20.1 255.255.255.0

Router(config-subif)# interface FastEthernet0/0.3
Router(config-if)# description Engineering VLAN
Router(config-subif)# encapsulation dot1Q 3
Router(config-subif)# ip address 172.16.30.1 255.255.255.0
```

To accommodate the VLANs, subinterfaces are created under the router interface at which the switch trunk port is terminated. A subinterface is a virtual interface that is indicated with a dot followed by the subinterface number (for example, for **FastEthernet0/0.1 FastEthernet0/0.2** and **FastEthernet0/0.3**).

For ease of programming, it is recommended to keep the subinterface number the same as the VLAN ID. Recall that in our earlier example, the default VLAN is 1, the Sales VLAN is 2, and the Engineering VLAN is 3. The next step is to define the VLAN tagging encapsulation. In this case, it is dot1q, which essentially is 802.1Q. With the encapsulation, the appropriate VLAN ID is specified. Next, the IP address is assigned by creating a routed layer 3 network for a VLAN.

In this section you have seen the steps for creating a static VLAN. You saw how to create the Sales and Engineering VLANs and assign specific ports on the switch to the respective VLANs. Unassigned ports remained as part of the default VLAN, VLAN 1.

Networking Challenge: Switch Configuration

Use the Net-Challenge simulator software provided at the text's companion website to demonstrate that you can perform basic switch and static VLAN configuration. Connect to the website and open the Net-Challenge folder and click **Net-ChallengeV6.exe**. When the software is running, click the **Select Challenge** button to open the Select Challenge drop-down menu. Select **Introduction to Switch Configuration** to open a check box that can be used to verify that you have completed all the tasks. Then follow these steps:

1. Enter privileged EXEC mode on the switch (using the password **Chile**).
2. Enter the switch's configuration mode, **Router(config)**.
3. Set the hostname of the switch to switch-A.

4. Configure the VLAN 1 interface with the following IP address and subnet mask:
    - **IP address:** 10.10.20.250
    - **Subnet mask:** 255.255.255.0
5. Enable the VLAN 1 interface.
6. Use the appropriate command to display the current VLAN settings for the switch.
7. Create another VLAN, VLAN 2, named Sales.
8. Verify that a new Sales VLAN has been created.
9. Issue the command to enter interface configuration mode for the fa0/2 interface.
10. Enter the sequence of commands that are used to assign the interface fa0/2 to the Sales VLAN.
11. Enter the command that enables you to display the interface assigned to each VLAN.
12. Enter the command that enables you to specifically view the assignments for the Sales VLAN.
13. Issue the command that allows you to view the switch's running configuration.

Section 8-3 Review

This section covers the following Network+ exam objectives.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

A switch has two line connections through which a user can gain access to the switch. The line connections available on a switch can be displayed by using the ***line ?*** *command at the* ***Switch(config)#*** *prompt. The following line connections are typically available:*

- **console:** Primary terminal line (the console port)
- **vty:** Virtual terminal for Telnet connections

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section presents the basics of configuring a Cisco switch. You should have noticed the similarities and distinct differences between router and switch IOS commands. Spend time working through the Net-Challenge exercises, which will help you remember the commands.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

To see the statuses of all the switch ports, including their speed, duplex, and VLAN, use the following command:

```
SwitchA# show interfaces status
```

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section examines the basics of configuring a Cisco switch. The commands for switch configuration are similar to those for a router. To configure a switch, you must first establish a console connection and enter privileged mode on the switch. The procedure for establishing a console connection to a switch is the same as for a router.

5.3 Given a scenario, use the appropriate network software tools and commands.

This section mentions that the console (primary terminal line) is the console port, and vty is the virtual terminal used for Telnet connections.

Test Your Knowledge

1. Which of the following is used to look specifically at the assignments for the Administrator VLAN?

   a. `Switch(config)# sh vlan name Administrator`

   b. `Switch(vlan)# sh vlan name Administrator`

   c. `Switch# sh vlan name Administrator`

   d. `Switch# sh vlan Administrator`

2. Which of the following command sequences is used to set password protection for the console port?

   a.
   ```
   SwitchA(config)# line console 0
   SwitchA(config-line)# login
   SwitchA(config-line)# password my-secret2
   ```

   b.
   ```
   SwitchA# line console 0
   SwitchA(config-line)# login
   SwitchA(config-line)# password my-secret2
   ```

   c.
   ```
   SwitchA# line console 0
   SwitchA# login
   SwitchA# password my-secret2
   ```

   d.
   ```
   SwitchA(config)# line console 0
   SwitchA(config)# login
   SwitchA(config)# password my-secret2
   ```

8-4 SPANNING TREE PROTOCOL

This section examines the Spanning Tree Protocol link management protocol. It is important that students understand the purpose of the bridge protocol data unit and the process of electing a root bridge. Students should also understand the five Spanning Tree Protocol states.

Spanning Tree Protocol (STP)
A link management protocol that prevents looping and controls data flow over possibly redundant data paths

This section examines **Spanning Tree Protocol (STP)**, which is a link management protocol that prevents switching loops and controls data flow over possibly redundant data paths. Looping is bad for Ethernet networks because it means duplicate packets are sent over redundant paths. A switch should send packets over only one path. Spanning Tree Protocol is used to ensure that only one data path is selected. Spanning Tree Protocol also forces one of the redundant data paths into a standby mode by placing the path in a blocked state.

Bridge Protocol Data Unit (BPDU)
A message unit that switches use to share information with other switches that are participating in Spanning Tree Protocol

Switches that are participating in Spanning Tree Protocol use **bridge protocol data units (BPDUs)** to exchange information with other switches. Switches use BPDUs for the following:

- To elect a root switch for the spanning tree network topology
- To remove redundant data paths
- To calculate the shortest distance to a root switch
- To select a port from each switch as the best path to the root switch
- To select ports that are part of Spanning Tree Protocol

A switch assumes that it is the root switch until the BPDUs are exchanged and a root switch is elected. The switch with the lowest MAC address is elected as the root switch. The following example shows a switch with the MAC address 0030194A6940 issuing a data packet as the start of the bidding process to see which switch will be elected as the root switch:

```
BPDU Config BID=0030194A6940 PID=0x801B
```

Configuration BPDU
A BPDU that switches use to elect the root switch

Topology Change Notification (TCN)
A packet used to indicate that there has been a change in the switch network topology

Topology Change Notification Acknowledgment (TCA)
An acknowledgment from another switch that the TCN has been received

In this case, **Config** indicates that this is a **configuration BPDU**, which the switches use to elect the root switch. Two other types of packets that can come from the switch are the **topology change notification (TCN)**, which is used to indicate that there has been a change in the switch network topology, and the **topology change notification acknowledgment (TCA)**, which is an acknowledgment from another switch that the TCN has been received.

Figure 8-3 shows an example of the contents of a BPDU. It shows that the Root ID MAC address is 0030194A6940. The BPDUs are exchanged at regular intervals and are used to keep the switches notified of any changes in the network topology. The default notification interval, which is 2 seconds, is called the hello time.

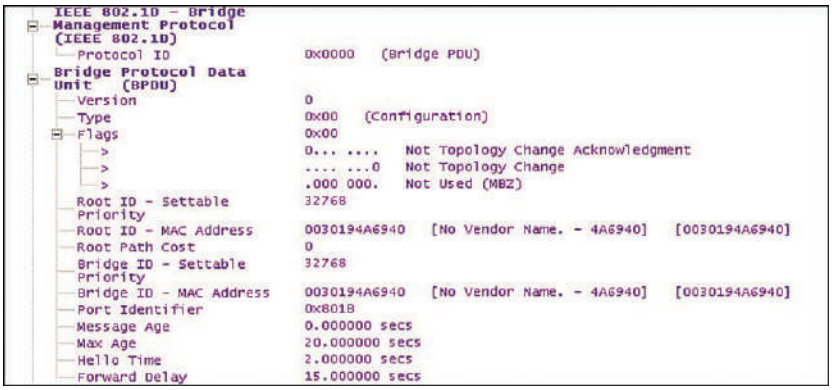


FIGURE 8-3 An example of BPDU packet information.

A switch does not begin to forward data packets immediately when a networking device is connected to a port. Instead, there is a delay during which the switch begins to process the BPDUs to determine the topology of the switch network. This is called the forward delay. Figure 8-3 shows a forward delay of 15 seconds, which is the default value set by the root switch. During the delay period, the switch goes through the listening and learning states.

Spanning Tree Protocol has five states:

- **Blocking state:** In this state, the switch is not sending data out the ports. However, the switch is receiving and monitoring the BPDUs. This state is used to prevent any possible switching loops.
- **Listening state:** BPDUs are being processed.
- **Learning state:** The switch is learning source MAC addresses from the received data packets and will add the addresses to the MAC address table.
- **Forwarding state:** The switch is sending and receiving data packets. The BPDUs are still being monitored for any possible changes in the switch network.
- **Disabled:** This setting is available for the network administrator to manually disable the port. This is not part of Spanning Tree Protocol but rather a function available on a switch.

Spanning Tree Protocol has been a standard feature in all layer 2 switches for many years. Many improvements have been made to the original STP. For example, Rapid Spanning Tree Protocol (RSTP) reduces the convergence time to less than 10 seconds. RSTP proactively monitors switch ports for status change and allows a port to safely transition to the forwarding state. RSTP is also backward compatible with STP switches. Multiple Spanning Tree Protocol (MSTP) is VLAN aware, thus allowing each VLAN to have its own MST instance (MSTI). This enables load balancing of network traffic across redundant links so that each of the links in a network can be used by at least one MSTI. There are also other improved

proprietary spanning tree protocols. For example, Cisco developed Per-VLAN Spanning Tree (PVST) and PVST+, and Juniper developed VLAN Spanning Tree Protocol (VSTP).

Spanning Tree Protocol can also be used to create network redundancy. When there are redundant paths in a network, Spanning Tree Protocol prevents loops by ensuring that only one data path is used. Spanning Tree Protocol forces the other redundant links into standby mode by placing the links in blocking state. When the primary link becomes unavailable, Spanning Tree Protocol recalculates its topology and then starts forwarding via another redundant link.

Another technique that can be used to provide redundancy is link aggregation, sometimes called port aggregation. This technique uses Link Aggregation Control Protocol (LACP), which allows for multiple physical ports on an Ethernet switch to be bundled as one single logical channel. This increases bandwidth capacity, and it also creates redundancy if a member port in the link aggregation group fails. LACP is a standard protocol supported by most network switches, and PAgP (Port Aggregation Protocol) is a Cisco-proprietary protocol that performs a similar function to create a port bonding, which Cisco calls EtherChannel. A common limitation of link aggregation is that all member ports must have identical speed and duplex.

Section 8-4 Review

This section covers the following Network+ exam objectives.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

As discussed in this section, Multiple Spanning Tree Protocol (MSTP) is VLAN aware, thus allowing each VLAN to have its own MST instance (MSTI). This enables load balancing of network traffic across redundant links so that each of the links in a network can be used by at least one MSTI.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section describes the learning state, in which a switch is learning source MAC addresses from the received data packets and adds the addresses to the MAC address table.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

Multiple Spanning Tree Protocol (MSTP) is VLAN aware, thus allowing each VLAN to have its own MSTI. This enables load balancing of network traffic across redundant links so that each of the links in a network can be used by at least one MSTI.

5.5 Given a scenario, troubleshoot general networking issues.

This section examines STP, which is a link management protocol that prevents switching loops and controls data flow over possibly redundant data paths.

Test Your Knowledge

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

8-5 POWER OVER ETHERNET

One of the challenges a network administrator faces as a campus network grows is making sure that electrical power is available for the networking devices (for example, switches, wireless access points, and IP phones). It is not always practical or affordable to run electrical power to all the places networking devices are needed. This challenge can be met with Power over Ethernet (PoE). Students need to be aware of this technology.

One of the challenges a network administrator faces as a campus network grows is making sure that electrical power is available for the networking devices (for example, switches, wireless access points, and IP phones). It is not always practical or affordable to run electrical power to all the places where networking devices are needed. This challenge can be met with **Power over Ethernet (PoE)**. The Power over Ethernet standard (IEEE 802.3af) was approved in 2003 for networks running 10BASE-T, 100BASE-T, and 1000BASE-T technologies. PoE is a standardized technology that can be used to supply power over existing CAT5 or better network cabling to networking devices.

Power over Ethernet (PoE)
A technology developed to supply power over CAT5 or better network cabling

PoE offers the following benefits:

- It is not necessary to run external power to all networking devices.
- Power and data run over one cable.

- Monitoring of power management can be done via SNMP.
- Networking devices can be moved easily.

As defined by IEEE 802.3af, PoE provides 15.4 watts per port to Ethernet devices and uses a 48-volt system.

PD
Powered device

PSE
Power sourcing equipment

Two pieces of networking hardware are defined for PoE: **powered device (PD)** and **power sourcing equipment (PSE)**. The three main functions provided by the PSE are as follows:

- Detecting a PD
- Supplying power to the PD
- Monitoring the power supply

Endpoint PSE
A PoE switch such as the source port on an Ethernet switch that connects to the PD

Midspan (Midpoint) PSE
A PoE switch that is used to provide power to a PD when a powered Ethernet port is not available

The two types of PSE are the **endpoint PSE** and the **midspan (midpoint) PSE**. These types of network switches are usually referred to as *PoE switches*. Besides being PSEs, they provide typical switching functions. They are not meant to replace layer 2 switches because they are more expensive. These switches are used extensively in VoIP environments to power IP phones. The VoIP endpoint is the final destination of a voice call. It can be a physical device or server or even a software application.

One useful command for checking the power status of the switch ports is **show power inline**, demonstrated here:

```
SwitchA# sh power inline
Module     Available (Watts)      Used (Watts)      Remaining (Watts)
1          740.0                  0.0               740.0
Interface   Admin    Oper    Power (Watts)   Device   Class   Max
Gi1/0/1     auto     off     0.0             n/a      n/a     30.0
Gi1/0/2     auto     off     0.0             n/a      n/a     30.0
Gi1/0/3     auto     off     0.0             n/a      n/a     30.0
Gi1/0/4     auto     off     0.0             n/a      n/a     30.0
Gi1/0/5     auto     off     0.0             n/a      n/a     30.0
Gi1/0/6     auto     off     0.0             n/a      n/a     30.0
```

An example of an endpoint PSE is the source port on an Ethernet switch that connects, via a cable, to a PD. The power to the PD can be delivered in two ways: over the active data pairs (for example, 1–2/3–6) or via pairs 4–5/7–8, as demonstrated in Figure 8-4. Both types of power delivery can be used for 10BASE-T, 100BASE-T, and 1000BASE-T. The most common power delivery is over pairs 1–2/3–6, as shown in Figure 8-4(a).

A midspan, or midpoint, PSE is used to provide power to a PD when a powered Ethernet port is not available. This setup requires the use of a power injector and typically uses pairs 4–5/7–8, and this does not support 1000BASE-T connections.

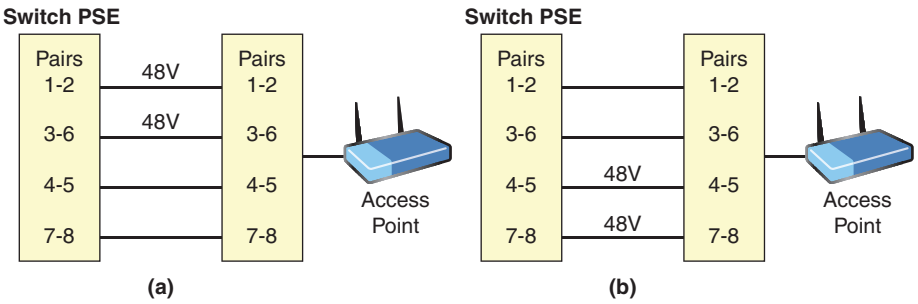


FIGURE 8-4 The two ways to deliver power to a PD: (a) pairs 1–2/3–6 and (b) 4–5/7–8.

The PD is the device that actually receives power, such as a wireless access point or an IP phone. There are four classes of PDs:

- **Class 0:** 0.44 to 12.95 watts
- **Class 1:** 0.44 to 3.84 watts
- **Class 2:** 3.84 to 6.49 watts
- **Class 3:** 6.49 to 12.95 watts

A PSE "discovers" PDs by sending discovery signals on active and inactive Ethernet ports. The discovery process (called **resistive power discovery**) involves looking for devices that support PoE. Valid PDs have a 25kΩ resistor connected between the transmit and receive pairs. Before full power is delivered to the PD, two low-voltage discovery signals are sent out to verify whether a compatible PoE device is attached. The second of the two signals is a slightly higher voltage than the first, but neither is large enough to damage an incompatible device. If the PSE detects a compatible PD, the full 48 volts is applied to all ports that have compatible PDs connected.

Resistive Power Discovery
The process of looking for devices that support PoE and have a 25kΩ resistor connected between the transmit and receive pairs

There are a limited number of problems with PoE, as long as the devices support IEEE 802.3af. In cases where vendor-proprietary PoE equipment is being used, the PSEs and PDs must be compatible. Also, a network administrator must be aware of how many PDs are connected to the PSE and must ensure that the total power requirements for the PDs do not exceed the PSE limit. For example, a network could have 10 access points and 25 IP phones, all requiring PoE connections. If the total number of devices requiring power exceeds the power output for a PSE, some PDs may not be powered up or may not operate properly.

A newer version of Power over Ethernet, called **PoE+**, defined by the IEEE 802.3at standard, was announced in 2009. Much like 802.3af PoE, PoE+ uses two pairs of twisted-pair cable to deliver power. PoE+ provides the following features:

PoE+
A newer version of PoE, based on IEEE 802.3at

- It can supply up to 30 watts of power to the PD.
- It supports both 802.3af (PoE) and 802.3at (PoE+) PDs.
- It supports midspan PSEs for 1000BASE-T.

- It supports 10GBASE-T.
- It operates over CAT5 and higher cabling.

The latest PoE standard, 802.3bt (ratified in 2018), is known as PoE++. This standard defines two type of PoE:

- Type 3 PoE can supply up to 60 watts of power to the PD.
- Type 4 PoE can supply up to 100 watts of power to the PD.

The POE++ standard uses all four pairs of twisted-pair cable to deliver power and provides the following features:

- It is fully backward compatible with both 802.3af (PoE) and 802.3at (PoE+) PDs.
- It supports 10GBASE-T.
- It operates with CAT5 and higher cabling.

Section 8-5 Review

This section covers the following Network+ exam objectives.

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

The Power over Ethernet standard (IEEE 802.3af) was approved in 2003 for networks running 10BASE-T, 100BASE-T, and 1000BASE-T technologies. It provides a standardized technology that can be used to supply power over existing CAT5 or better network cabling to networking devices.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section introduces PoE switches. Besides being PSEs, they provide typical switching functions. They are not meant to replace layer 2 switches because they are more expensive. These switches are used extensively in the VoIP environment to power IP phones.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

It is not always practical or affordable to run electrical power to every place networking devices are needed. This challenge can be met with Power over Ethernet (PoE). The PoE standard (IEEE 802.3af) was approved in 2003 for networks running 10BASE-T, 100BASE-T, and 1000BASE-T technologies. It provides a standardized technology that can be used to supply power over existing CAT5 or better network cabling to networking devices.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

One of the challenges a network administrator faces as a campus network grows is making sure electrical power is available for the networking devices (for example, switches, wireless access points, and IP phones).

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section describes the power provided by PoE standards:

- **IEEE 802.3af (PoE):** 15.4 watts per port to PDs
- **IEEE 802.3at (PoE+):** 30 watts per port to PDs
- **IEEE 802.3bt (PoE++):** 60–100 watts per port to PDs

Test Your Knowledge

1. Which of the following is an advantage of running Power over Ethernet?
   a. It is not necessary to run external power to all networking devices.
   b. PoE improves data throughput.
   c. PoE works with all networking devices, regardless of manufacturer.
   d. It allows you to run power and data over one cable.
2. How is a PD discovered, and which device discovers it?
   a. A PD is discovered through resistor power discovery by an ESE.
   b. A PD is discovered through PoE discovery by a PSE.
   c. A PD is discovered through resistive power discovery by a PSE.
   d. A PD is discovered through PoE discovery by an ESE.

8-6 TROUBLESHOOTING THE SWITCH INTERFACE

This section introduces the switch commands **show interface status** and **show mac address-table** (**show mac-address-table**) for layer 2 switch troubleshooting. It also examines the output of these commands. Be sure to emphasize that many of the commands used on routers can also be used on switches. When working with a layer 2 switch, students should be reminded to think in terms of layer 2 of the OSI model.

This section examines how to troubleshoot switches. The router troubleshooting concepts from Chapter 7 also apply to switch troubleshooting. Much as when troubleshooting a router, you should verify the switch configuration to ensure that it is correct and verify the switch interfaces to make sure they are up and operating in the right mode. Many router commands can also be used for switches. On Cisco routers and switches, commands such as **show running-config** are universal. This

command, for example, is used to display the currently running configuration of the network device.

Before you begin using commands to troubleshoot problems, remember to look at the most rudimentary way to troubleshoot connectivity issues: Be sure to check the physical connections—cables, physical equipment, and network connection LED status indicators. This type of troubleshooting is fondly referred to as "checking the blinking lights."

The **show ip int brief** command, which can be used to check the status of the interfaces on a router, can also be used on a switch. The output of this command shows the statuses of the physical interfaces as well as the VLAN interfaces, if any are configured. The following example shows that VLAN1 is configured, and it is up and operational:

```
SwitchA# sh ip int brief
Interface          IP-Address      OK?     Method     Status     Protocol
Vlan1              10.123.124.2    YES     NVRAM      up         up
FastEthernet0/1    unassigned      YES     unset      up         up
FastEthernet0/2    unassigned      YES     unset      up         up
FastEthernet0/3    unassigned      YES     unset      up         up
FastEthernet0/4    unassigned      YES     unset      up         up
FastEthernet0/5    unassigned      YES     unset      down       down
```

You might find that the command **show ip int brief** does not offer enough layer 2 or layer 1 information. In such cases, you can use another useful command for displaying the statuses of the switch interfaces: **show interface status** (or **sh int status**). This command provides the following switch port information:

- **Port:** The type of interface: Ethernet (10Mbps), Fast Ethernet (100Mbps), or Gigabit Ethernet (1000Mbps)
- **Name:** A description of the interface, if it is configured
- **Status:** Can be either **connect** (which indicates that the interface is physically connected to another network device) or **notconnect** (which indicates that the switch port has no physical link to an active network device)
- **Vlan:** The VLAN ID, which indicates the VLAN port membership
- **Duplex:** The duplexing mode of the connection, which can be **a-full** (auto-negotiation full-duplex), **a-half** (auto-negotiation half-duplex), **full** (manual full-duplex), or **half** (manual half-duplex)
- **Speed:** The speed at which the connection is negotiated or configured, which can be **a-1000** (auto-negotiation 1Gbps), **a-100** (auto-negotiation 100Mbps), **a-10** (auto-negotiation 10Mbps), **1000** (manual 1Gbps), **100** (manual 100Mbps), or **10** (manual 10Mbps)
- **Type:** The physical connection type of the interface, which can be **100BaseTX** (100Mbps copper), **1000BaseTX** (1Gbps copper), **100BaseFX** (100Mbps fiber), **1000BaseSX** (1Gbps multimode fiber), or **1000BaseLX** (1Gbps single-mode fiber)

The following example shows output from a Cisco switch:

```
SwitchA# sh interface status
Port      Name         Status       Vlan   Duplex    Speed     Type
Gi0/1     Main feed    connected    1      a-full    a-1000    1000BaseLX
Gi0/2     BuildingA    connected    2      a-full    a-1000    1000BaseSX
Gi0/3     BuildingB    connected    2      a-full    a-1000    1000BaseSX
Gi0/4     BuildingC    connected    1      a-full    a-1000    1000BaseSX
Gi0/5                  notconnect   1      auto      auto      unknown
Gi0/6                  notconnect   1      auto      auto      unknown
```

This output shows the status of GigabitEthernet interfaces 0/1 to 0/6, where only Gi0/1–Gi0/4 have connections. All the ports are configured to be auto-negotiated. All the active ports are connected at 1Gbps full-duplex. The physical connection on GigabitEthernet0/1 is **1000BaseLX**, which indicates a single-mode fiber-type connection; the rest of the active ports are using multimode fiber-type connectors (**1000BaseSX**). GigabitEthernet0/1 and GigabitEthernet0/4 are configured to be members of VLAN 1, and GigabitEthernet0/2 and GigabitEthernet0/3 are members of VLAN2. Because GigabitEthernet0/5 and GigabitEthernet0/6 are not used, their statuses are shown as **notconnect**, and their types are **unknown**. The output shows that these two ports are configured to be auto-negotiated, and they are configured to be members of VLAN 1.

Note

It is very important to pay attention to VLAN port assignments as they report the configured VLAN membership of each switch port. A computer can be connected to a switch port and the interface status can be connected, but the computer may still be unable to access the network. This could be a result of a VLAN mismatch, where the computer is connected to the incorrect VLAN. This is a very common issue for network administrators.

The duplex and speed are good information when you're troubleshooting performance issues. When the reported duplex or speed does not match what the NIC is using, the result is performance degradation due to collisions and packet drops. Most NICs are typically left to auto-negotiate their speed and duplex. If auto-negotiation is configured at the switch interface and at the device NIC, then it will be no problem because auto-negotiation will do its job and find the proper speed and duplex. Issues arise when one end is configured to use auto-negotiation and the other end is not or when both ends are configured for manual duplex and speed and their settings do not match. It is a good fundamental troubleshooting practice to make sure the duplex and speed of the connection are matched at both ends.

When a network device is connected to an available port and the physical link is successful, messages are displayed on the switch console. The following example shows the messages displayed for GigabitEthernet0/5, indicating that the interface has successfully linked with an active network device:

```
2w0d: %LINK-3-UPDOWN: Interface GigabitEthernet 0/5, changed state to up
2w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet
 0/5,

changed state to up
```

For a detailed view of a particular switch port, you can use the command **sh int [*Interface_ID*]**, as shown in this example:

```
SwitchA# sh int GigabitEthernet1/0/2
GigabitEthernet1/0/2 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 6c9c.ed9f.4402
 (bia 6c9c.ed9f.4402)
  Description: reserved for Data
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
 43088
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 68000 bits/sec, 35 packets/sec
     25857744 packets input, 15164000519 bytes, 0 no buffer
     Received 149779 broadcasts (144381 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 144381 multicast, 0 pause input
     0 input packets with dribble condition detected
     104281005 packets output, 31296767730 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

This is a very useful command for troubleshooting as it provides status details as well as interface errors or alerts. These errors are good indications of possible connection issues between the switch port and the end device, especially if the errors keep incrementing. Table 8-2 describes some notable errors.

TABLE 8-2 **Some of the Errors Displayed with the sh int [*Interface_ID*] Command**

Error	Description
Input errors	The accumulative counter of all input errors that have occurred
CRC	CRC (cyclic redundancy checksum) errors that occur when there is an FCS (frame check sequence) mismatch between the sender and the switch, causing an incoming Ethernet frame to be discarded

Error	Description
Giants	An illegal Ethernet frame size that exceeds the maximum Ethernet frame size (typically more than 1518 bytes)
Runts	An illegal Ethernet frame size that is very small (smaller than 64 bytes)
Collisions	The number of collisions detected

Unlike a router, a switch is an OSI layer 2 device that operates by storing and forwarding MAC addresses. Also, a switch generally services more directly connected network devices than does a router. More populated switch ports mean more network clients, which makes troubleshooting more difficult. So it is very important to know how to isolate network devices. Being able to tell to which switch port a particular network device is connected comes in handy. On a Cisco switch, the switch command **show mac-address-table** (or the command **show mac address-table** on a newer switch) can be used to display the MAC address table of the switch, as shown here:

```
SwitchA# sh mac address-table
VLAN    Mac Addre          Type         Ports
All     0100.0ccc.cccc     STATIC       CPU
All     0100.0ccc.cccd     STATIC       CPU
All     0180.c200.0000     STATIC       CPU
All     0180.c200.0001     STATIC       CPU
All     0180.c200.0002     STATIC       CPU
All     0180.c200.0003     STATIC       CPU
All     0180.c200.0004     STATIC       CPU
All     0180.c200.0005     STATIC       CPU
All     0180.c200.0006     STATIC       CPU
All     0180.c200.0007     STATIC       CPU
All     0180.c200.0008     STATIC       CPU
All     0180.c200.0009     STATIC       CPU
All     0180.c200.000a     STATIC       CPU
All     0180.c200.000b     STATIC       CPU
All     0180.c200.000c     STATIC       CPU
All     0180.c200.000d     STATIC       CPU
All     0180.c200.000e     STATIC       CPU
All     0180.c200.000f     STATIC       CPU
All     0180.c200.0010     STATIC       CPU
All     ffff.ffff.ffff     STATIC       CPU
1       0003.ba53.164d     DYNAMIC      Gi1/0/9
1       0006.5bf7.6e9a     DYNAMIC      Gi1/0/8
1       000c.0c01.4711     DYNAMIC      Gi1/0/11
1       000f.1f64.978b     DYNAMIC      Gi1/0/13
1       000f.1f64.979f     DYNAMIC      Gi1/0/14
1       0013.210b.20c8     DYNAMIC      Gi1/0/10
1       0013.211d.6475     DYNAMIC      Gi1/0/5
1       0016.3e09.39e7     DYNAMIC      Gi1/0/7
1       0016.3e32.3198     DYNAMIC      Gi1/0/7
```

```
1      0017.0850.17f0    DYNAMIC      Gi1/0/6
1      001e.c9b5.1dd2    DYNAMIC      Gi1/0/3
1      001e.c9b5.1e4f    DYNAMIC      Gi1/0/4
1      0050.8bc2.5471    DYNAMIC      Gi1/0/12
1      0060.2e00.529b    DYNAMIC      Gi1/0/1
1      02d0.6819.1854    DYNAMIC      Gi1/0/2

Total Mac Addresses for this criterion: 35
```

A network administrator can use this command to map a network device to a switch port by using its MAC address. The connected device's MAC address is a dynamic type because it is not stationary or specific to a switch port. When a device moves from one switch port to another, the switch relearns the MAC address's new location. The switch deletes its old MAC entry and updates its database with the new MAC entry mapping. The static MAC addresses shown previously are those assigned to the switch interfaces. These MAC addresses do not change.

A common task for a network technician is to verify the uptime for a switch to help identify potential problems with switches that might be intermittently resetting. This is the command for viewing the switch uptime:

```
switch# show version
```

It is important to check the uptime in order to see if a switch has been rebooting. Rebooting problems can be due to power fluctuations or switch problems. In either case, a network technician needs to know how to identify such a problem and propose a solution. The following is sample output from the **show version** command, which shows that SwitchA has been up for 1 year, 5 weeks, 8 hours, and 24 minutes:

```
ROM: Bootstrap program is Alpha board boot loader
BOOTLDR: C2960S Boot Loader (C2960S-HBOOT-M) Version 12.2(55r)SE,
RELEASE SOFTWARE (fc1)
SwitchA uptime is 1 year, 5 weeks, 8 hours, 24 minutes
System returned to ROM by power-on
System restarted at 06:11:00 MDT Sat Jul 12 2014
System image file is "flash:/c2960s-universalk9-mz.122-
55.SE7/c2960s-universalk9-mz.122-55.SE7.bin"
```

Section 8-6 Review

This section covers the following Network+ exam objectives.

1.6 Explain the use and purpose of network services.

*This section talks about the importance of being able to tell to which switch port a particular network device is connected. On a Cisco switch, the switch command **show mac-address-table** (or the command **show mac address-table** on a newer switch) can be used to display the MAC address table of the switch.*

1.7 Explain basic corporate and datacenter network architecture.

*The command **show interface status** (or **sh int status**) outputs switch port information such as the physical connection type—for example, 100Mbps copper or 1Gbps multimode fiber (**1000BaseSX**) or 1Gbps single-mode fiber (**1000BaseLX**).*

2.3 Given a scenario, configure and deploy common Ethernet switching features.

*This section presents an example of using the switch command **show mac-address-table** (or the command **show mac address-table** on a newer switch) to display the MAC address table of the switch. This is a very useful troubleshooting tool that a network administrator can use to map a network device to a switch port by using its MAC address.*

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

*This section examines the use of the **show ip interface brief** and **show interface status** commands and how to interpret their output for a switch.*

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This reminds you to look at the most rudimentary way to troubleshoot connectivity issues: Be sure to check the physical connections—cables, physical equipment, and network connection LED status indicators. This type of troubleshooting is fondly referred to as "checking the blinking lights."

Test Your Knowledge

1. True or false: Unlike a router, a switch is an OSI layer 2 device that operates by storing and forwarding MAC addresses.

   True

2. On a switch, static MAC addresses are best characterized by which of the following?

   a. They are dynamic and change as the device changes interface ports.

   b. They are assigned to a specific interface and do not change.

   c. They are not stationary for a switch port.

   d. All of these answers are correct.

SUMMARY

This chapter presents the fundamentals of VLANs and switch configuration. It also introduces Spanning Tree Protocol and the process of selecting a root bridge. It also covers the operation of Power over Ethernet. You should understand the following concepts presented in this chapter:

- The three types of VLANs
- The basics of switch configuration and static VLAN configuration
- Spanning Tree Protocol
- The operation of PoE and PoE+
- Best practices for switch configuration

QUESTIONS AND PROBLEMS

Section 8-2

1. What is a VLAN?

   A VLAN is a group of host computers and servers that are configured as if they are in the same LAN even if they reside across routers in separate LANs.

2. List the three types of VLANs.

   Port-based, tag-based, and protocol-based

3. When a port is not assigned to any VLAN, is it still a member of a VLAN?

   Yes. It becomes a member of a default VLAN, which is VLAN 1.

4. What is an advantage of using VLANs?

   A network administrator can group computers and servers in the same VLAN, based on the organizational group, even if the computers and servers are not on the same physical segment or even in the same building.

5. What is a port-based VLAN?

   A port-based VLAN is a VLAN in which the host computers connected to specific ports on a switch are assigned to a specific VLAN.

6. What is a tag-based VLAN?

   A tag-based VLAN adds a tag to the Ethernet frames that contains the VLAN ID that is used to indicate that a frame belongs to a specific VLAN.

7. What is a protocol-based VLAN?

   A protocol-based VLAN forwards traffic through ports based on the protocol being used.

8. What is a VLAN ID?

   A VLAN ID indicates that a frame belongs to a specific VLAN.

9. What are the two approaches for assigning VLAN membership? Explain the function of each.

   A static VLAN is basically a port-based VLAN 2. With a dynamic VLAN, ports are assigned to a VLAN based on either the computer's MAC address or the username of the client logged on to the computer.

Section 8-3

10. What is the purpose of the enable secret for a switch?

    It provides password protection for the privileged (enable) mode.

11. What commands would you use to assign the IP address 192.168.20.5 to VLAN 1?

```
SwitchA(config)# interface VLAN 1
SwitchA(config-if)# ip address 172.16.32.2 255.255.255.0
SwitchA(config-if)# no shutdown
```

12. What switch command would you use to display the interfaces assigned to a VLAN?

```
SwitchA# show interface VLAN
```

13. What is the purpose of a VLAN database?

    A VLAN database stores information on which interfaces are assigned to which VLANs.

14. List the commands used to create VLAN 5 and name this VLAN Marketing-group.

```
SwitchA# configure terminal
SwitchA(config)# vlan 5
SwitchA(config-vlan)# name Marketing-group
```

15. List the commands used to assign FA0/5 to the Marketing-group VLAN (VLAN 5). Show the switch prompts.

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# int fa 0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 5
Switch(config-if)# end
```

16. What command is used to display the port assignments for the Software-Development VLAN? List both the prompt and the command.

```
Switch# show vlan name Software-Development
```

17. List the commands used to configure the IP address for the default interface VLAN 1. The IP address should be set to 10.10.20.1 with subnet mask 255.255.255.0.

```
Switch# configure terminal
Switch(config)# interface Vlan1
Switch(config-if)# ip address 10.10.20.1 255.255.255.0.
```

Section 8-4

18. What is the purpose of Spanning Tree Protocol?

    It is a link management protocol that prevents looping and controls data flow over possibly redundant data paths.

19. What is a BPDU, and what is its purpose?

    A bridge protocol data unit (BPDU) is a message unit that switches use to share information with other switches that are participating in Spanning Tree Protocol. Switches use BPDUs for the following:

    - Electing a root switch for the spanning tree network topology
    - Removing redundant data paths
    - Calculating the shortest distance to a root switch.
    - Selecting a port from each switch as the best path to the root switch
    - Selecting ports that are part of Spanning Tree Protocol

20. Discuss how a root switch is elected.

    A switch assumes that it is the root switch until BPDUs are exchanged and a root switch is elected. The switch with the lowest MAC address is elected as the root switch.

21. What are the five STP protocol states?

    Blocking

    Listening

    Learning

    Forwarding

    Disabled

22. A BPDU data packet shows that the hello time is 2.0 seconds. What information does this provide?

    This indicates how often the BPDUs are being exchanged.

23. A BPDU data packet lists the forward delay as 15 seconds. What information does this provide?

    The switch will not begin to forward data packets when a networking device is connected to a port. Instead, during this 15-second delay, the switch begins

to process the BPDUs to determine the topology of the switch network. This is called the forward delay. During the delay period, the switch goes through the listening and learning states.

Section 8-5

24. What are the two types of devices defined by PoE?

    Powered device (PD) and power sourcing equipment (PSE)

25. What should you check if you are installing a Power over Ethernet connection using computer equipment from two different manufacturers?

    The PSEs and PDs must be compatible.

26. List four benefits of Power over Ethernet.

    - It is not necessary to run external power to all networking devices.
    - You can run power and data over one cable.
    - You can monitor power management via SNMP.
    - It is easy to move networking devices.

27. What is resistive power discovery, and how does it work?

    Resistive power discovery basically looks for devices that support PoE. Valid PDs have a 25kΩ resistor connected between the transmit and receive pairs. Before full power is delivered to the PD, two low-voltage discovery signals are sent to verify that a compatible PoE device is attached. The second of the two signals is a slightly higher voltage than the first, but neither is large enough to damage an incompatible device. If the PSE detects a compatible PD, the full 48 volts is applied to all ports that have compatible PDs connected.

28. Which wire pairs are used in PoE?

    The power to the PD can be delivered in two ways: over the active data pairs 1–2 and 3–6 or via pairs 4–5 and 7–8.

29. How much power can a Class 0 PD PoE device source?

    0.44–12.95 watts

30. What are the benefits of PoE+?

    - It supports both 802.3af (PoE) and 802.3at (PoE+) PDs.
    - It supports midspan PSEs for 10000BASE-T.
    - It supports a minimum of 30 watts of power for the PD.
    - It supports for 10GBASE-T.
    - It operates over CAT5 and higher cabling.

Section 8-6

31. How does the **show ip interface brief** command differ for a switch and a router?

    Basically, the results of this command are the same for router and switch interfaces.

32. What does the following information indicate if the **show interfaces status** command is entered on a switch?

    ```
    Gi0/2        notconnect   1      auto   auto unknown
    ```

    This indicates that the switch port has no physical link to an active network device.

33. The **show interface status** command is entered on a switch. What does it mean if the switch interface's status shows **connect**?

    In the output of this command, **connect** indicates that the interface is physically connected to another network device.

34. What command is used to display the MAC address of a switch port?

    show mac address-table or **show mac-address-table**

35. If the command **show ip int brief** shows the interface status **administratively down** and the protocol status **down**, what will be the status of the port reported by the command **show int status**?

    disabled

Critical Thinking

36. Your supervisor asks you if a layer 2 switch could be used in the core of the campus network. Prepare a response to your supervisor. Be sure to justify your recommendation.

    Yes, a layer 2 switch can be used, and the advantage is cost.

37. A 10Gbps data link is to be set up between building A and building B in a campus network. Does it matter if the link is fiber or microwave or some other medium? Explain your answer.

    The best choice in this case is fiber because this media can easily support the required 10Gbps data rate. However, this assumes that you can run the fiber from building A to building B. You could also use a microwave system because this technology will support 10Gbps data rates. The 802.11 wireless technologies are not yet a viable solution for such a case because 10Gbps is a theoretical bandwidth that 802.11ax can achieve but is not available in the real world. UTP is also not a viable choice here because this technology is limited to 100-meter lengths.

38. You've just configured an IP VLAN interface on a switch, and the interface is not up. How do you troubleshoot the issue?

    First, make sure to do a **no shutdown** on the VLAN interface. Then be sure there is at least an active switch port assigned to the VLAN.

Certification Questions

39. You are a network administration and have been asked to create a VLAN called Administrator. What command do you use on a Cisco switch to create the Administrator VLAN as VLAN 2?

    a.
    ```
    SwitchA# vlan
    Switch# vlan 2 name Administrator
    ```

    b.
    ```
    SwitchA# vlan
    Switch(data)# vlan 2 name Administrator
    ```

    c.
    ```
    SwitchA(config)# vlan 2
    Switch(config-vlan)# name Administrator
    ```

    d.
    ```
    SwitchA# vlan database
    Switch(vlan)# vlan name Administrator
    ```

40. You are configuring a switch so that a specific port on the switch is assigned to VLAN 3. What command do you use to assign FastEthernet port 0/4 to VLAN 3 on a Cisco switch?

    a.
    ```
    Switch(config)# int fa 0/4
    Switch(config-if)# switchport mode access
    Switch(config-if)# switchport access vlan 3
    ```

    b.
    ```
    Switch(config)# int fa 0/4
    Switch(config-if)# switchport mode access
    Switch(config-if)# switchport access 3
    ```

    c.
    ```
    Switch(config)# int fa 0/4
    Switch(config)# switchport mode access
    Switch(config-if)# switchport access vlan 3
    ```

    d.
    ```
    Switch(config)# int fa 0/4
    Switch(config-if)# switchport mode access 3
    Switch(config-if)# switchport access vlan
    ```

41. You are cabling a UTP connection to a switch that will also be used for supplying power via Power over Ethernet. The power to the PoE devices is provided using which of the following pairs? (Select all that apply.)

    a. 1–3 and 4–6
    b. 1–6 and 5–8
    c. 1–2 and 3–6
    d. 4–5 and 7–8

42. The source port of an Ethernet switch that connects to a PD is an example of which of the following?

    a. A midpoint PSE
    b. An endpoint PSE
    c. A start PSE
    d. None of these answers are correct.

43. Switches use bridge protocol data units for which of the following? (Select all that apply.)

    a. To select ports that are part of STP
    b. To calculate the longest distance to a root switch
    c. To elect a root switch for the spanning tree network topology
    d. To remove redundant data paths

44. What is the purpose of a VLAN?

    a. A VLAN is a group of host computers and servers that are configured as if they are not in the same LAN even if they reside across routers.
    b. A VLAN is a group of host computers and servers that are configured as if they are in the same LAN even if they reside across routers.
    c. A VLAN is a group of host computers and servers that are configured as if they are in the same LAN even if they reside across switches.
    d. A VLAN is a group of host computers and servers that are configured as if they are not in the same LAN even if they reside across switches.

45. Your supervisor asks you to create a port-based VLAN to support the development group. Specifically, you are being asked to do which of the following?

    a. Use the 802.1Q protocol for VLAN assignment.
    b. Assign specific ports on a switch to a specific VLAN.
    c. Specify which protocols control port assignment.
    d. Specify which ports will share broadcasts.

46. A network administrator is configuring a VLAN named Development. Which of the following shows how to create this VLAN?

a.
```
SwitchA vlan database
Switch(vlan)# vlan 2 name Development
VLAN 2 modified:
  Name: Sales
```

b.
```
SwitchA(config)# vlan 2
 Switch(config-vlan)# name Development
```

c.
```
SwitchA# vlan
 Switch(int-vlan)# vlan 2 name Development
 VLAN 2 modified:
   Name: Sales
```

d.
```
SwitchA# vlan
  Switch(config-vlan)# vlan 2 name Development
  VLAN 2 modified:
    Name: Sales
```

47. A network administrator sees that the following data packet has been sent: **BPDU Config BID=0030194A6940 PID=0x801B**. What is the purpose of this data packet?

a. This BPDU indicates the peripheral interface device (**PID=0x801B**) requesting a data packet.

b. This BPDU indicates the peripheral interface device (**PID=0x801B**) requesting to send a data packet.

c. **Config** indicates that this is a configuration BPDU, which is used by the switches to elect the root switch.

d. **Config** indicates that this is a static BPDU, which is configured by the user that connects to the root bridge.

9
CHAPTER

Routing Protocols

Chapter Outline

9-1 Introduction
9-2 Static Routing
9-3 Dynamic Routing Protocols
9-4 Distance Vector Protocols
9-5 Configuring RIP and RIPv2
9-6 Link State Protocols
9-7 Configuring the Open Shortest Path First (OSPF) Routing Protocol
9-8 Advanced Distance Vector Routing Protocol: Configuring Enhanced Interior Gateway Routing Protocol (EIGRP)
9-9 Internet Routing with Border Gateway Protocol (BGP)
9-10 IPv6 Routing
Summary
Questions and Problems

Objectives

- Describe the difference between static and dynamic routing protocols
- Describe the difference between distance vector and link state protocols
- Know how to configure a basic setup for a static routing protocol
- Understand the relative amount of traffic generated by each protocol
- Understand the basics of the OSPF, IS-IS, and EIGRP routing protocols
- Know how to configure a basic setup for the RIP and RIPv2 routing protocols
- Know how to configure a basic setup for the OSPF, EIGRP, and BGP routing protocols
- Examine how to apply various routing protocols to IPv6

Key Terms

static route
netstat -r
route print
loopback
ip route
variable-length subnet masking (VLSM)
show ip route (sh ip route)
routing table code S
routing table code C
gateway of last resort
show ip route static (sh ip route static)
show running-config (sh run)
show startup-config (sh start)
copy running-configuration startup-configuration (copy run start)
write memory (wr m)
dynamic routing protocol
administrative distance
distance vector protocol
RIP
RIPv2
routing loop
advertise
class network address
classful addressing
contiguous network
show ip protocol (sh ip protocol)
link state protocol
OSPF
IETF
link state advertisement (LSA)
hello packets
areas
backbone
variable-length subnet mask
route flapping
IS-IS
NET
router ospf [*process id***]**
network number
wildcard bits
area 0
EIGRP
RIPng
[*rip_tag*]
OSPFv3
BGP

This chapter introduces routing protocols, which provide a standardized format for route management, including selecting routes, sharing route status with neighbor routers, and calculating alternative routes if the best path route is down. The focus of this chapter is on the use of routing protocols in a campus network environment.

9-1 INTRODUCTION

This chapter introduces routing, including both static and dynamic routing protocols. The discussion of dynamic routing protocols covers the distance vector protocol RIP, the link state protocols OSPF and IS-IS, the advanced distance vector protocol EIGRP, and the path-vector routing protocol BGP. This chapter includes a section on configuring RIP and RIPv2, as well as a RIPv2 network configuration challenge using the Net-Challenge software provided at the companion website. (See the Introduction for information on how to access this site.)

The routing types presented in this chapter include the static routing protocols RIPv2, OSPF, EIGRP, and BGP. This chapter includes several networking challenges you can complete by using the Net-Challenge software, which is downloadable from the textbook's companion website. (See the Introduction for information on how to access this site.) These challenges enable you to test your ability to configure static, RIPv2, OSPF, and EIGRP routing on a virtual router.

Section 9-2, "Static Routing," includes examples of how to configure static routes and view the routes in a routing table. It includes a discussion of when and where static protocols are used and also when and why it is not advantageous to use a static routing protocol. Section 9-3, "Dynamic Routing Protocols," presents an overview of dynamic protocols, which are divided into two types: distance vector and link state. Distance vector protocols are introduced in Section 9-4, "Distance Vector Protocols." The steps for configuring the distance vector protocols RIP and RIPv2 are presented in Section 9-5, "Configuring RIP and RIPv2." A discussion of link state protocols is presented in Section 9-6, "Link State Protocols." The steps for configuring the OSPF routing protocol are presented in Section 9-7, "Configuring the Open Shortest Path First (OSPF) Routing Protocol." Section 9-8, "Advanced Distance Vector Routing Protocol: Configuring Enhanced Interior Gateway Routing Protocol (EIGRP)," provides an introduction to configuring the EIGRP routing protocol. Section 9-9, "Internet Routing with Border Gateway Protocol (BGP)," examines Internet routing using the BGP routing protocol.

Section 9-10, "IPv6 Routing," demonstrates that the routing protocols for IPv6 work the same way as the routing protocols with IPv4.

Table 9-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 9-1 **Chapter 9 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes.	9-2, 9-5, 9-6, 9-8, 9-10
1.5	Explain common ports and protocols, their application, and encrypted alternatives.	9-2, 9-5
1.6	Explain the use and purpose of network services.	9-3
1.8	Summarize cloud concepts and connectivity options.	9-9
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	9-2, 9-3, 9-4
2.2	Compare and contrast routing technologies and bandwidth management concepts.	9-2, 9-3, 9-4, 9-5, 9-6, 9-7, 9-8, 9-9, 9-10
2.3	Given a scenario, configure and deploy common Ethernet switching features.	9-8
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	9-2, 9-3, 9-6, 9-7, 9-10
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	9-2, 9-3
4.0	**Network Security**	
4.1	Explain common security concepts.	9-5
5.0	**Network Troubleshooting**	
5.1	Explain the network troubleshooting methodology.	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	9-3, 9-4, 9-5
5.3	Given a scenario, use the appropriate network software tools and commands.	9-7
5.5	Given a scenario, troubleshoot general networking issues.	9-2, 9-3, 9-4, 9-5, 9-7, 9-9

9-2 STATIC ROUTING

This section examines the use of static routes in computer networking. The first example explains the static routes defined by a computer, including the default gateway and loopback address. Students should understand how to configure a computer's default gateway address and how to use the loopback address 127.0.0.1 to verify the network interface. Figure 9-2 shows how to display a computer's static routes.

The section concludes with the steps for configuring a static route on a router. It introduces the router commands **sh ip int brief**, **sh ip route**, and **sh run**, which students will use often when configuring routers. This section includes a Net-Challenge exercise that focuses on configuring static routes for the three-router campus network shown in Figure 9-3.

The objective of this section is to demonstrate how data packets are routed in a network using a static routing protocol. It presents techniques for configuring static

Static Route
A data traffic route that has been manually entered into either a router's or a computer's routing table

routes so that data packets can be forwarded. A **static route** is a list of IP addresses to which data traffic can be forwarded that has been manually entered into either a router's or a computer's routing table. A static route is specified in a PC in terms of the computer's default gateway, and routers sometimes use a static route when specifying where the network data traffic is to be forwarded.

The static route most commonly used in a host computer is the default gateway, or default route. The *default gateway* specifies where the data traffic is to be sent when the destination address for the data is not in the same LAN or is unknown. If you don't have a route specified for a subnet in your network or if you have a missing route, the default route is used. For example, if your PC is on the 10.10.0.0 network and wants to send data to 100.100.20.1, the data is sent to the default gateway, as specified by the TCP/IP setup on the PC. Figure 9-1a shows an example of setting the host computer's default gateway for Windows, and Figure 9-1b shows an example of setting the host computer's default gateway for macOS. In this example, the default gateway IP address is 10.10.20.250, with a subnet mask of 255.255.255.0 for the computer in LAN A with IP address 10.10.20.1.

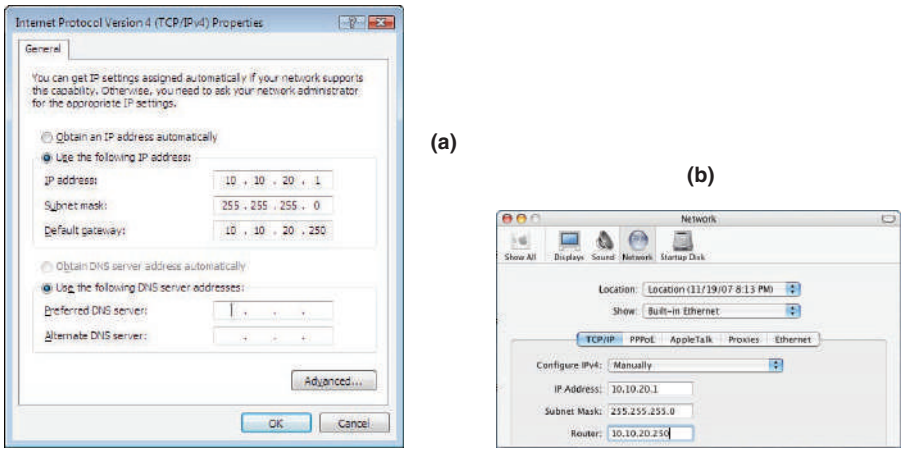


FIGURE 9-1 Setting the default gateway address or default static route on a host computer (PC and macOS).

netstat -r
A command used to obtain the routing table for a host PC computer

route print
A command used to obtain the routing table for a host PC computer

The routing tables for the host PC can be obtained by entering the command **netstat -r** at the PC's command prompt and from the macOS terminal screen. Figure 9-2(a) shows an example. The command **route print** can also be used to view the active routes from the host PC, as shown in Figure 9-2(b).

The default route is specified in the routing table by a 0.0.0.0 network address entry with subnet mask 0.0.0.0. The gateway address 10.10.20.250 is the IP address of the FastEthernet port of the router connected to the LAN. The IP address 10.10.20.1 for the interface is the IP address for the host computer's network interface card (NIC). The network destination 10.10.20.0 is returned to the computer's NIC at IP address 10.10.20.1. The gateway for the network destination 10.10.20.1 is

127.0.0.1, which is a **loopback** to the host computer. A loopback means the data is routed directly back to the source. In this case, the source is the computer's NIC. The loopback can be used to check whether the network interface is working; if it is, pinging IP address 127.0.0.1 generates a reply. In IPv6, the IPv6 loopback address is 0000:0000:0000:0000:0000:0000:0000:0001, which can be simplified to ::1.

Loopback
A mechanism by which data is routed directly back to the source

What about setting static routes for a router in a small campus network? Let's examine how data packets travel from one LAN to another in the three-router campus network shown in Figure 9-3. Specifically, how is information sent from a host computer in LAN A (10.10.20.0 subnet) to a host computer in LAN B (10.10.10.0 subnet)? The data packets must travel from LAN A to the RouterA gateway (FA0/0 interface), from RouterA to RouterB via the 10.10.200.0 subnet, and then to LAN B via the RouterB gateway (FA0/0 interface). A physical communications link must be established between the routers, and a routing protocol must be defined for RouterA and RouterB before data packets can be exchanged. The physical connection is typically CAT6 or higher UTP or fiber.

```
C:\netstat -r

Route Table
---------------------------------------------------------------------------
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 b0 d0 25 bf 48 ...... 3Com 3C920 Integrated Fast Ethernet Controller
3C905C-TX Compatible) - Packet Scheduler Miniport
---------------------------------------------------------------------------
---------------------------------------------------------------------------
Active Routes:
Network Destination           Netmask          Gateway       Interface  Metric
          0.0.0.0           0.0.0.0    10.10.20.250    10.10.20.1        20
       10.10.20.0     255.255.255.0      10.10.20.1    10.10.20.1        20
       10.10.20.1   255.255.255.255       127.0.0.1     127.0.0.1        20
   10.255.255.255   255.255.255.255      10.10.20.1    10.10.20.1        20
        127.0.0.0         255.0.0.0       127.0.0.1     127.0.0.1         1
        224.0.0.0         240.0.0.0      10.10.20.1    10.10.20.1        20
  255.255.255.255   255.255.255.255      10.10.20.1    10.10.20.1         1
Default Gateway:         10.10.20.250
---------------------------------------------------------------------------
Persistent Routes:
  None
```

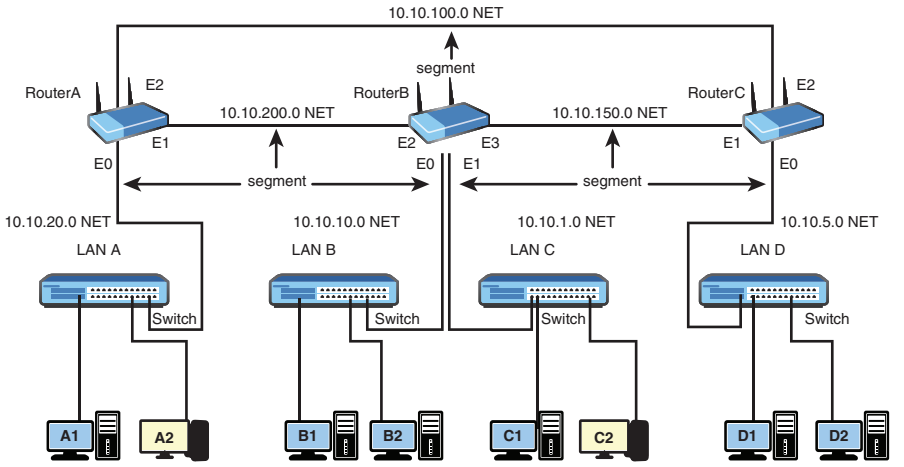
(a)

```
C:\route print
---------------------------------------------------------------------------
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 b0 d0 25 bf 48 ...... 3Com 3C920 Integrated Fast Ethernet Controller
3C905C-TX Compatible) - Packet Scheduler Miniport
---------------------------------------------------------------------------
---------------------------------------------------------------------------
Active Routes:
Network Destination           Netmask          Gateway       Interface  Metric
          0.0.0.0           0.0.0.0    10.10.20.250    10.10.20.1        20
       10.10.20.0     255.255.255.0      10.10.20.1    10.10.20.1        20
       10.10.20.1   255.255.255.255       127.0.0.1     127.0.0.1        20
   10.255.255.255   255.255.255.255      10.10.20.1    10.10.20.1        20
        127.0.0.0         255.0.0.0       127.0.0.1     127.0.0.1         1
        224.0.0.0         240.0.0.0      10.10.20.1    10.10.20.1        20
  255.255.255.255   255.255.255.255      10.10.20.1    10.10.20.1         1
Default Gateway:         10.10.20.250
---------------------------------------------------------------------------
Persistent Routes:
  None
```

(b)

FIGURE 9-2 (a) A host computer's static route listing, obtained by using the **netstat -r** command; (b) a host computer's static route listing, obtained by using the **route print** command.

A simplified network can be used to demonstrate what is required to develop static routes in a multiple-router network. For this example, let's use two routers from the campus network. The two routers, RouterA and RouterB, connect to LAN A and LAN B, as shown in Figure 9-4. This simplified network will be used to describe how data packets travel from LAN A to RouterA to RouterB to LAN B and what is required to define the static routes.



RouterA Port Addresses (LAN A)	
Ethernet 0 (Gateway Address)	10.10.20.250
Ethernet 1	10.10.200.1
Ethernet 2	10.10.100.1
LAN A Computers	
Computer A1	10.10.20.1
Computer A2	10.10.20.2
Subnet Mask	***255.255.255.0***

RouterB Port Addresses (LAN B)	
Ethernet 0 (Gateway Address)	10.10.10.250
Ethernet 2	10.10.200.2
Ethernet 3	10.10.150.1
LAN B Computers	
Computer B1	10.10.10.1
Computer B2	10.10.10.2
Subnet Mask	***255.255.255.0***

RouterB Port Addresses (LAN C)	
Ethernet 1 (Gateway Address)	10.10.1.250
Ethernet 2	10.10.200.2
Ethernet 3	10.10.150.1
LAN C Computers	
Computer C1	10.10.1.1
Computer C2	10.10.1.2
Subnet Mask	***255.255.255.0***

RouterC Port Addresses (LAN D)	
Ethernet 0 (Gateway Address)	10.10.5.250
Ethernet 1	10.10.150.2
Ethernet 2	10.10.100.2
LAN D Computers	
Computer D1	10.10.5.1
Computer D2	10.10.5.2
Subnet Mask	***255.255.255.0***

FIGURE 9-3 A three-router campus network.

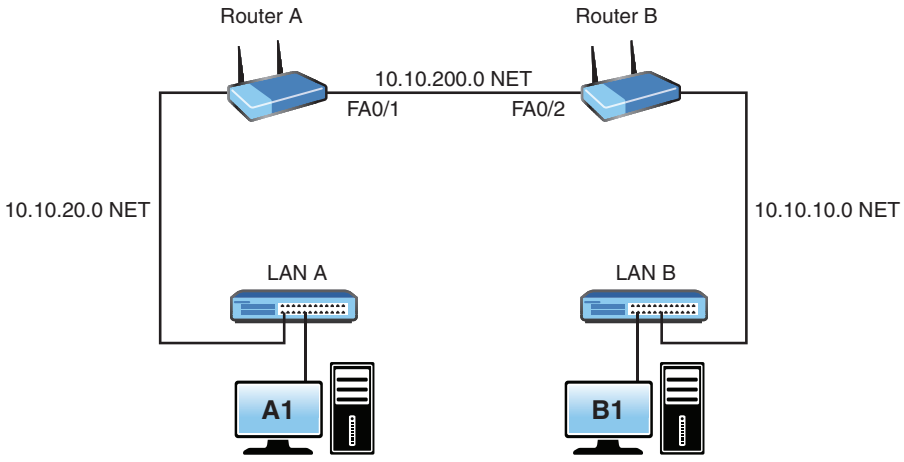


FIGURE 9-4 A simplified two-router network.

The data packets pass through three subnets (indicated by *NET*) when traveling from LAN A to LAN B. The IP subnets for the networks are as follows:

10.10.20.0 NET: LAN A
10.10.200.0 NET: RouterA connection to RouterB
10.10.10.0 NET: LAN B

In this network, there are only two routers, and RouterA is directly connected to RouterB. This means that the only route between the routers is via the 10.10.200.0 NET, which is the connection between RouterA and RouterB. The static route information is entered from the router's configure terminal prompt **(config)#**, using the **ip route** command, which has the following syntax:

ip route
The router configuration command for manually setting the next hop IP address

```
Router(config)# ip route [destination] [subnet mask] [next hop]
```

where *destination* is the network's destination IP address (NET), *subnet mask* is what has been defined for the subnets, and *next hop* is the IP address of the next router's interface in the link. The command for routing the data to the 10.10.10.0 subnet is as follows:

```
RouterA(config)# ip route 10.10.10.0 255.255.255.0 10.10.200.2
```

The following configuration information is entered into RouterA:

- **Destination subnet IP address:** 10.10.10.0
- **Subnet mask:** 255.255.255.0
- **Next hop IP address:** 10.10.200.2

The next hop IP address is the IP address of the Ethernet2 port on RouterB. Now the router knows how to deliver data packets from host computers in the 10.10.20.0 NET (LAN A) to destination computers in the 10.10.10.0 NET (LAN B).

Note

Each static route can use a different subnet mask. This is accomplished using **variable-length subnet masking (VLSM)**. For example, one static route could have subnet mask 255.255.255.0 and another could have subnet mask 255.255.255.252.

Variable-Length Subnet Masking (VLSM)
A process in which routes can be configured using different subnet masks

You can verify the routing address entry into the routing table by entering the command **show ip route (sh ip route)** from the router's **(config)#** prompt, as shown in this example:

show ip route (sh ip route)
The command that displays the routes and the routing address entry into the routing table

```
RouterA# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S 10.10.10.0/24 [1/0] via 10.10.200.2
C 10.10.200.0/24 is directly connected, FastEthernet0/1
L 10.10.200.1/32 is directly connected, FastEthernet0/1
```

The static route configured on RouterA only dictates how the 10.10.10.0 network should be routed from RouterA's perspective—and that is in the outgoing, or egress, direction only. This does not influence how the returned traffic will come back to RouterA. Routing is bidirectional; therefore, when a route is configured at one end, the reverse has to be configured at the other end.

What about data traffic flow from the 10.10.10.0 NET (LAN B) to the 10.10.20.0 NET (LAN A)? Once again, the data packets pass through three subnets (indicated by NET) when traveling from LAN B to LAN A. The IP addresses for the subnets are as follows:

10.10.10.0 NET: LAN B
10.10.200.0 NET: RouterB connection to RouterA
10.10.20.0 NET: LAN A

In this scenario, LAN B connects directly to RouterB, and the only route to LAN A from RouterB is via the 10.10.200.0 NET, which is the connection between Routers B and A. The destination network IP address is 10.10.20.0. The command input to RouterB for routing the data to the 10.10.20.0 subnet is as follows:

```
RouterB(config)# ip route 10.10.20.0 255.255.255.0 10.10.200.1
```

The following information is entered into the router:

- **Destination subnet IP address:** 10.10.20.0
- **Subnet mask:** 255.255.255.0
- **Next hop IP address:** 10.10.200.1

The next hop IP address is the IP address of the FastEthernet0/1 port on RouterA. Now a static route has been configured on RouterB to route data packets from host computers in the 10.10.10.0 NET (LAN B) to destination computers in the 10.10.20.0 NET (LAN A). The entries into RouterB's routing table can be confirmed by using the command **sh ip route** at the **Router#** prompt, as shown here:

```
RouterB# sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S 10.10.20.0/24 [1/0] via 10.10.200.1
C 10.10.200.0/24 is directly connected, FastEthernet0/2
L 10.10.200.2/32 is directly connected, FastEthernet0/2
```

The **sh ip route** command lists a table of codes first, followed by the routes. This output above shows a static route (**S**) 10.10.20.0 via 10.10.200.1, which indicates that a static route to the destination 10.10.20.0 subnet can be reached via the next hop address 10.10.200.1. The **C** indicates that the 10.10.200.0 network is directly connected to the FastEthernet0/2 port.

routing table code S
The router code for a static route

routing table code C
The router code for specifying a directly connected network

This simplified network has only one route; therefore, the entries for the static routes using the **sh ip route** command are limited but were required for each router. Static routes are sometimes used when configuring the routers for routing in a small network. Static routing is not the best choice, as you will learn, but it can be suitable in a small network (for example, a two-router network). It can be suitable for situations in which there is only one route to the destination, such as in a wide area network (WAN) or an Internet feed. This concept is examined in Chapter 9-9.

What about using static routes in the three-router campus network shown in Figure 9-3? A computer in LAN A (10.10.20.0 NET) sends data to a computer in LAN B (10.10.10.0 NET). This is the same requirement specified in the two-router network example. Once again, a static route must be entered into RouterA's routing table, telling the router how to forward data to the 10.10.10.0 NET. However, in this example, there are two possible choices for a data packet to travel to the 10.10.10.0 NET from RouterA. The IP addresses for the two possible next hops are 10.10.200.2 and 10.10.100.2. These are the router commands:

```
RouterA(config)# ip route 10.10.10.0 255.255.255.0 10.10.200.2
RouterA(config)# ip route 10.10.10.0 255.255.255.0 10.10.100.2
```

What about sending information from LAN A to LAN C or to LAN D? This requires four additional **ip route** entries into the router's routing table, as shown here:

```
RouterA(config)# ip route 10.10.1.0 255.255.255.0 10.10.200.2
RouterA(config)# ip route 10.10.1.0 255.255.255.0 10.10.100.2
RouterA(config)# ip route 10.10.5.0 255.255.255.0 10.10.200.2
RouterA(config)# ip route 10.10.5.0 255.255.255.0 10.10.100.2
```

But wait! You aren't done. You must enter return static routes for all the LANs back to LAN A and then enter the static routes for the other three LANs. For trouble-shooting purposes, you want to be able to ping all the Ethernet interfaces on the subnets, so you need to add static IP routes to each subnet (NET). For example,

when defining a route to the 10.10.150.0 NET, the following are the static IP route entries:

```
RouterA(config)# ip route 10.10.150.0 255.255.255.0 10.10.200.2
RouterA(config)# ip route 10.10.150.0 255.255.255.0 10.10.100.2
```

This means that many static route entries must be made for the routes in this network to be completely defined. This requires a lot of time, and if routes change in the network, new static entries must be made and old static routes must be deleted. The problem with using a static routing protocol in a network is the amount of maintenance required by the network administrator to keep the route selections up to date in a large network. Say that a network connection uses five router hops. The entries for the static routes on each router are numerous, and if the routes change, the routing tables in all routers must be manually updated to account for the data path changes.

When static routes are used, the network administrator in essence becomes the routing protocol. In other words, the network administrator makes all the decisions regarding data traffic routing. This requires the administrator to know all network data routes, set up the routes to each subnet, and be constantly aware of any route changes. In contrast, dynamic routing protocols communicate routing information between the routers to determine the best route to use to forward the data packets. The concept of a dynamic routing protocol is introduced in Section 9-3.

Gateway of Last Resort

Gateway of Last Resort
The IP address of the router in a network to which data packets with unknown routes should be forwarded

One of the most important applications for a static route is for configuring the gateway of last resort on a router. The **gateway of last resort** is the IP address of the router in a network where data packets with unknown routes should be forwarded. The purpose of this is to configure a route for data packets that do not have a destination route configured in the routing table. In this case, a default route can be configured that instructs the router to forward the data packet(s) with an unknown route to another router. This is the command for doing this:

```
ip route 0.0.0.0 0.0.0.0 [next hop address]
```

If this static route has not been configured, the router displays the following message when the **show ip route** command is entered:

```
Gateway of last resort is not set
```

This means the router does not know how to route a data packet with a destination IP address that differs from the routes stored in the routing table. Without the gateway of last resort, a router drops any data packets with destination networks that are not in its routing table.

Configuring Static Routes

This section describes how to configure static routes on a Cisco router. The topology used here is the three-router campus network shown in Figure 9-3. This demonstration is for configuring the static routes for RouterA only.

The first step is to connect to the router via a console or virtual terminal connection. Next, enter the privileged EXEC mode, as shown here:

```
Router con0 is now available Press RETURN to get started!
RouterA>en
RouterA#
```

Next, enter the configure terminal mode on the router (**RouterA(config)#**), using the **configure terminal** (**conf t**) command. Before configuring the static routes, make sure the interfaces are configured. The FastEthernet0/1 interface is configured with the assigned IP address 10.10.200.1 and the subnet mask 255.255.255.0, and the FastEthernet0/2 interface is assigned the 10.10.100.1 IP address and subnet mask 255.255.255.0. Use the **no shut** command to enable the FastEthernet ports. The following example shows these commands in use:

```
RouterA# conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)# int fa0/1
RouterA(config-if)# ip address 10.10.200.1 255.255.255.0
RouterA(config-if)# no shut
00:19:07: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state
to up
RouterA(config)# int fa0/2
RouterA(config-if)# ip address 10.10.100.1 255.255.255.0
RouterA(config-if)# no shut
00:21:05: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state
to up
```

Notice that the FastEthernet0/1 and FastEthernet0/2 interfaces change state to **up** after the **no shut** command is issued. It is a good idea to verify the interface status by using the **show ip interface brief** (**sh ip int brief**) command, as follows:

```
RouterA# sh ip int brief
00:22:18: %SYS-5-CONFIG_I: Configured from console
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 10.10.200.1 YES manual up down
FastEthernet0/2 10.10.100.1 YES manual up down
```

The status for both FastEthernet ports indicates that they are **up**; however, **down** indicates that no physical connection is established between the routers. You can fix this problem of the protocol being down by reestablishing the physical connection between the routers.

The static routes are entered using the **ip route** command after the interfaces are configured. You don't have to enter all routes at once, but all routes must be properly entered for the network to work. To keep the following example brief, only the routes to the 10.10.10.0 NET are listed:

```
RouterA(config)# ip route 10.10.10.0 255.255.255.0 10.10.200.2
RouterA(config)# ip route 10.10.10.0 255.255.255.0 10.10.100.2
```

show ip route static (sh ip route static)
The command that limits the routes displayed to only static ones

There are two places to verify whether static routes are properly configured. First, verify that the routes are in the routing table by using either the **show ip route** command or the **show ip route static (sh ip route static)** command. Adding the word **static** after **show ip route** limits the routes displayed to only those that are **static**. Note that with the **show ip route** command, the routes are displayed only if the line protocol is **up**. The following is an example:

```
RouterA# sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
S 10.10.10.0/24 [1/0] via 10.10.200.2
S 10.10.10.0/24 [1/0] via 10.10.100.2
C 10.10.200.0/24 is directly connected, FastEthernet0/1
L 10.10.200.1/32 is directly connected, FastEthernet0/1
C 10.10.100.0/24 is directly connected, FastEthernet0/2
L 10.10.100.1/32 is directly connected, FastEthernet0/2
```

This is the command for showing only the static routes:

```
RouterA# sh ip route static
```

show running-config (sh run)
The command that displays the router's running configuration

The other place to check the routing configuration is by examining the router's running configuration file by using the command **show running-config (sh run)**, as shown here:

```
RouterA# sh run
Using 519 out of 32762 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
ip subnet-zero
!
interface FastEthernet0/1
ip address 10.10.200.1 255.255.255.0
```

```
no ip directed-broadcast no keepalive
!
interface FastEthernet0/2
ip address 10.10.100.1 255.255.255.0
no ip directed-broadcast no keepalive
!
ip classless
ip route 10.10.10.0 255.255.255.0 10.10.200.2
ip route 10.10.10.0 255.255.255.0 10.10.100.2
!
line con 0
transport input none line aux 0
line vty 0 4
!
end
```

This command displays the current configuration of the router, but it does not show what is currently saved in the router's nonvolatile memory (NVRAM). The command **show startup-config (sh start)** displays the router's configuration saved in NVRAM. After the configuration is saved, the show run and show config commands should both present the same result for the configuration.

show startup-config (sh start)
The command that displays the router's startup configuration

It is important to save your configuration changes to the router as you go. You can save changes to the router configuration by using the **copy running-configuration startup-configuration (copy run start)** command or **write memory (wr m)**, as follows:

```
RouterA# copy run start
RouterA# wr m
```

copy running-configuration startup-configuration (copy run start)
The command for copying the running configuration to the startup configuration

write memory (wr m)
The command that saves configuration changes to memory

Using write memory is the same as issuing the **copy run start** command, which is the command most commonly used for saving configuration.

Table 9-2 describes a number of the commands used for configuring static routes.

TABLE 9-2 **Commands Used to Configure Static Routing**

Command	Description
ip route	Specifies the destination IP address, the subnet mask, and the next hop IP address
show ip route	Displays the IP routes listed in the routing table
show ip route static	Displays only the static IP routes listed in the routing table
show running-configuration	Displays the router's running configuration
show startup-configuration	Displays the router's saved configuration in NVRAM
write memory	Copies the current router changes to memory (NVRAM)
copy run start	Copies the current router changes to memory (NVRAM)

Networking Challenge: Static Routes

Use the Net-Challenge software included with the text's companion website to demonstrate that you can configure static routes for a router. Select the **Static Routes** challenge and use the software to demonstrate that you can complete the following tasks.

This challenge requires you to configure the static routes for RouterA. Do the following:

1. Click the **RouterA** button and press **Enter** to get started.
2. Configure the IP address, subnet mask, and default gateway address for computerA1 in LAN A (10.10.20.250). To do so, click the **computerA1** icon in the LAN topology to bring up the TCP/IP Properties menu. Click **OK** on the menu and press **Enter** to see the check.
3. Enter the privileged EXEC mode using the password **Chile**.
4. Configure the IP addresses for the FastEthernet0/0 and FastEthernet0/1 ports. (*Note:* Click the **RouterA** symbol in the topology to display the IP address and subnet mask for the router.)
5. Use the **no shut** command to enable both FastEthernet ports.
6. Use the **show ip int brief** command to view the current interface status.
7. Use the **ip route** command to configure two routes to the 10.10.10.0 subnet (NET). (*Note:* Click the **RouterB** and **RouterC** symbols in the network topology to display the IP addresses for the router interfaces.) (Use subnet mask 255.255.255.0.)
8. Use the **show ip route** command to view whether the routes are entered into the router's routing table.
9. Use the **show run** command to verify whether the static routes are listed in the router's running configuration.

Section 9-2 Review

This section covers the following Network+ exam objectives.

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

This section presents the concept of a loopback, which means the data is routed directly back to the source.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

Figure 9-1 shows the TCP/IP setup menu on a PC.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section presents documentation of a three-router campus network that lists the interface IP addresses, the assigned subnet masks, and the gateway address.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

*This section demonstrates how static routes are entered using the **ip route** command.*

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

*This section mentions that the command for copying the running configuration to the startup configuration is **write memory** (**wr m**).*

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

*In this section, notice that the interfaces change state to **up** after the **no shut** command is issued.*

5.5 Given a scenario, troubleshoot general networking issues.

*This section presents examples using both the **netstat -r** and **route print** commands. The routing tables for the host PC computer can be obtained by entering the command **netstat -r** at the PC's command prompt and from the macOS terminal screen.*

Test Your Knowledge

1. The default gateway specifies which of the following?
   a. Where the data is to be sent when the source address for the data is not in the same subnet or is unknown
   b. Where the data is to be sent when the destination address for the data is in the same subnet or is unknown
   c. Where the data is to be sent when the destination address for the data is not in the same subnet or is unknown
   d. Where the data is to be routed when the source and the destination addresses for the data are not in the same subnet or are unknown
   e. None of these answers are correct.
2. Which of the following is the generic command for configuring a static route?
   a. router(config) **ip route** [*destination*] [*subnet mask*] [*next hop ip address*]
   b. router(config-static)# **ip route** [*destination*] [*subnet mask*] [*next hop ip address*]
   c. router(config)# **router static** router(config)# **ip route** [*destination*] [*subnet mask*] [*next hop ip address*]
   d. router(config)# **ip route** [*destination ip address*] [*subnet mask*] [*next hop ip address*]
   e. router(config)# **ip route** [*next hop ip address*] [*subnet mask*] [*destination ip address*]

9-3 DYNAMIC ROUTING PROTOCOLS

This section introduces the key features of and issues associated with dynamic routing protocols. Many new routing protocol terms are introduced. Make sure students clearly understand these terms. Distance vector protocol and link state protocols are introduced at the end of this section.

As you learned in Section 9-2, the time required for entering and maintaining static routes can be problematic. Therefore, static routing protocols are of limited use for campuswide network routing. However, they are essential when configuring the default route (gateway of last resort) on routers. Static routes are used in situations such as configuring small networks with few routes.

Dynamic Routing Protocol
A protocol that dynamically updates a routing table to account for loss of or changes in routes or changes in data traffic

This section introduces an improvement over static routing: the use of **dynamic routing protocols**, which enable a router's routing tables to be dynamically updated to account for losses of or changes in routes or changes in data traffic. The routers update their routing tables using information obtained from adjacent routers. A dynamic routing protocol is responsible for managing the exchange of routing information between the routers, and the choice of protocol defines how the routing information is exchanged and used.

Dynamic routing protocols are responsible for four primary features:

- What information is exchanged between routers
- When updated routing information is exchanged
- Steps for reacting to changes in the network
- Criteria for establishing the best route selection

Four key issues are associated with dynamic routing protocols:

- **Path determination:** This is a procedure in the protocol that is used to determine the best route.
- **Metric:** A metric is a numeric measure assigned to a route that can be used to rank routes from best to worst; the smaller the number, the better.
- **Convergence:** Convergence occurs when a router obtains a clear view of the routes in a network. The time it takes for the router to obtain a clear view is called the *convergence time*.
- **Load balancing:** Load balancing is a procedure in a protocol that enables routers to use any of the multiple data paths available from multiple routers to reach the destination. The purpose of load balancing is to distribute data traffic across multiple links or routers, thereby improving the reliability of a route.

Examples of route metrics are as follows:

- **Hop count:** The number of routers the data packet must pass through to reach the destination network.
- **Reliability:** A measure of the reliability of the link, typically in terms of the number of errors.
- **Bandwidth:** The data capacity of the networking link. For example, a 1000Mbps link has greater data capacity than a 100Mbps or 10Mbps Ethernet link.
- **Delay:** The time it takes for a data packet to travel from source to destination.
- **Cost:** A value assigned by a routing protocol or a network administrator to a link or an interface. Typically, the value is based on the referenced bandwidth.
- **Load:** The network activity on a link or router.
- **Ticks:** The measured delay time in terms of clock ticks, where each tick is approximately 55 milliseconds (1/18 second).
- **Latency:** A measure of how much time it takes for a data packet to get from the input into a network to its output. Latency results in poor throughput in a computer network and should be minimized.

There are two types of internal dynamic routing protocols: distance vector and link state. These protocols are briefly introduced in Sections 9-4 and 9-6. Another concept related to metrics is **administrative distance**, which enables routing protocols to select the best path when more than one path is available. For example, say that there are two network routes: One is an OSPF route, and the other is an EIGRP route. If the OSPF route has an administrative distance of 110, and the EIGRP route has an administrative distance of 90, the EIGRP route will be selected as the preferred route. Table 9-3 provides a short list of administrative distances for common routing protocols.

Administrative Distance
A feature used by routers to select the best path when more than one path is available

TABLE 9-3 **Administrative Distances for Common Routing Protocols**

Routing Protocol	Default Distance Values
Connected	0
Static	1
BGP	20
EIGRP	90
OSPF	110
RIP	120

Section 9-3 Review

This section covers the following Network+ exam objectives.

1.6 Explain the use and purpose of network services.

This section looks at load balancing. The purpose of a load balancer is to distribute data traffic across routes and servers, thereby improving the reliability of a route or a server.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section introduces dynamic routing protocols that enable a router's routing tables to be dynamically updated to account for loss or changes in routes or changes in data traffic.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

This section introduces four key issues that are associated with dynamic routing protocols: path determination, metric, convergence, and load balancing.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section introduces various routing metrics, including hop count, bandwidth, cost, latency, and administrative distance. Understanding these metrics is important when planning routing for a network.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section introduces load balancing, which is a procedure in a protocol that enables routers to use any of the multiple data paths available from multiple routers to reach the destination. The purpose of load balancing is to distribute data traffic across multiple links or routers, thereby improving the reliability of a route.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section introduces latency, which results in poor throughput in a computer network and should be minimized.

5.5 Given a scenario, troubleshoot general networking issues.

This section discusses dynamic routing protocols, which enable a router's routing tables to be dynamically updated to account for loss of or changes in routes or changes in data traffic.

Test Your Knowledge

1. What is a metric?
   a. A numeric measure assigned to a route that is used to rank routes from best to worst; the larger the number, the better
   b. A numeric measure assigned to a route that is used to rank routes from best to worst; the smaller the number, the better
   c. A numeric measure assigned to a route that is used to rank routes from best to worst; a number equal to 100 indicates the best route
   d. A numeric measure assigned to a route that is used to rank routes from best to worst; the number indicates the ticks
2. What is hop count?
   a. A value typically assigned by a network administrator that takes into account bandwidth and expense
   b. The number of routing devices a data packet must pass through to reach the destination network
   c. The data capacity of the networking link; a 1000Mbps link has greater data capacity than a 100Mbps or a 10Mbps Ethernet link
   d. The measured delay time in terms of clock ticks, where each tick is approximately 55 milliseconds (1⁄18 second)

9-4 DISTANCE VECTOR PROTOCOLS

This section examines distance vector protocols. It is important for students to understand that these types of protocols send their entire routing table to neighboring or adjacent routers. The neighbor routers then update their routing tables. Students should understand that this takes processing time, and the exchange of routing table information consumes network bandwidth. The dynamic routing protocol RIP is classified as a distance vector protocol, and it uses router hop count as the metric. It is important that students understand hop count and how to determine the hop count.

A **distance vector protocol** is a routing algorithm that periodically sends the entire routing table to its neighboring or adjacent router. When the neighboring router receives the table, it assigns a distance vector number to each route. The distance vector number is typically specified by some metric, such as hop count.

Distance Vector Protocol
A routing algorithm that periodically sends the entire routing table to its neighboring or adjacent router

With a distance vector protocol, the router first determines its neighbors or adjacent routers. All the connected routes have a distance or hop count of 0, as illustrated in Figure 9-5. Routers use the hop count metric to determine the best route for forwarding a data packet. Figure 9-6 provides an example of determining the hop count to a destination subnet.

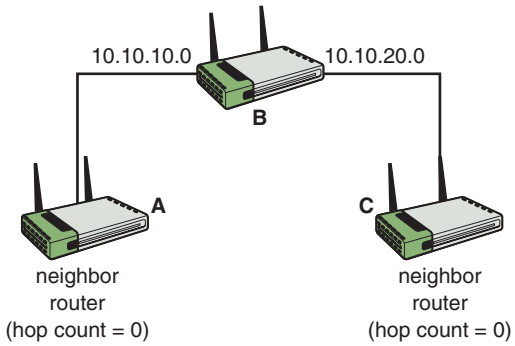
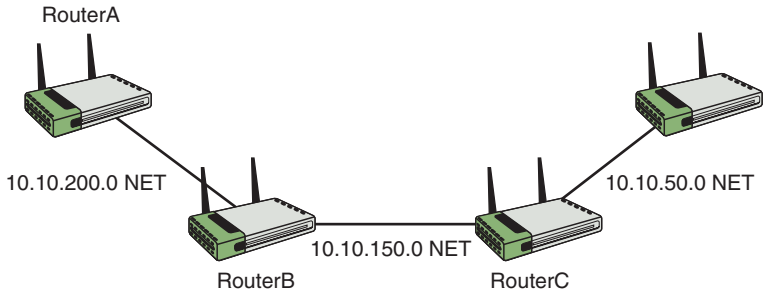


FIGURE 9-5 An example of router neighbors (hop count = 0).



Hop Count

From:	To:	Hop Count
RouterA	10.10.200.0	0
RouterA	10.10.150.0	1
RouterA	010.10.50.0	2

FIGURE 9-6 An example of determining the router hops.

The hop counts from RouterA to the 10.10.200.0, 10.10.150.0, and 10.10.50.0 subnets are as follows:

From	To	Hop Count
RouterA	10.10.200.0	0
RouterA	10.10.150.0	1
RouterA	10.10.50.0	2

With a distance vector protocol, each router determines its neighbors, builds its list of neighboring routers, and sends its routing table to its neighbors. The neighboring routers update their routing table based on the received information. When this is complete, each router's routing table provides a list of known routes within the network.

Routing Information Protocol (**RIP**) is a dynamic routing protocol, which means the routers periodically exchange routes. RIP is classified as a distance vector protocol, and it uses router hop count as the metric. RIP permits a maximum of 15 hops to prevent **routing loops**. A routing loop occurs when a router forwards packets back to the router that sent them, as graphically shown in Figure 9-7. RIP and other distance vector routing protocols send the entire routing table to neighbor routers at regular intervals. Sometimes the routing tables can be quite large, and the transfer can consume network bandwidth. This is of great concern in networks with limited bandwidth (also called throughput) because the periodic exchange can lead to slowdowns in data traffic. The default time interval for RIP for exchanging routing tables is 30 seconds. This results in slow route convergence, and if multiple routers are sharing RIP routes, the convergence time is even longer.

RIP
Routing Information Protocol

Routing Loop
A situation in which data is forwarded back to the router that sent the data packets

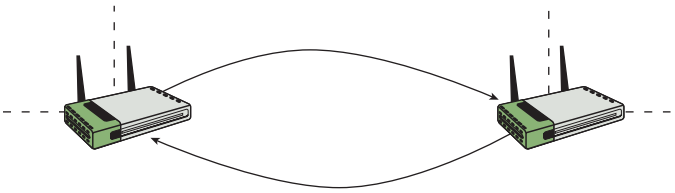


FIGURE 9-7 An example of data packet travel in a routing loop. Note that the packets never leave the routes between the two routers.

RIP is a relatively simple-to-configure routing protocol. However, RIP is good only for very small networks; it is not suited for networks that need fast convergence. RIP is a standards-based protocol, not a proprietary protocol, which means the use of RIP is not limited to certain equipment manufacturers. Section 9-5 examines the procedures for configuring a router to use the RIP and RIPv2 dynamic routing protocols.

Section 9-4 Review

This section covers the following Network+ exam objectives.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section introduces the concept of distance vector protocols.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

*This section discusses Routing Information Protocol (***RIP***), which is a dynamic routing protocol, which means the routers periodically exchange routes. RIP is classified as a distance vector protocol, and it uses router hop count as the metric.*

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section says that sometimes the routing tables can be quite large, and the transfer can consume network bandwidth. This is of great concern

in networks with limited bandwidth (also called throughput) because the periodic exchange can lead to slowdowns in data traffic.

5.5 Given a scenario, troubleshoot general networking issues.
This section states that RIP permits a maximum of 15 hops to prevent **routing loops**. *A routing loop occurs when a router forwards packets back to the router that sent them, as graphically shown in Figure 9-7.*

Test Your Knowledge

1. RIP is classified as which of the following?
   a. Distance vector protocol
   b. Dynamic routing protocol
   c. Link state protocol
   d. Both a and c
   e. Both a and b
   f. Both b and c
2. When does a routing loop occur?
   a. When the cost of a route is too low
   b. When the cost of a route is too high
   c. When a router forwards packets back to the router that sent them
   d. When static routing is used

9-5 CONFIGURING RIP AND RIPV2

The RIP dynamic routing protocol is easy to configure, and students will find that it is useful in small networks. This section examines the concept of sharing route information or advertising a route. Students will use this concept throughout the rest of this chapter. This section introduces the steps for configuring RIP, including the basic commands used, such as **router rip**, **network A.B.C.D**, **show ip protocol**, **copy running-config startup-config**, and **show startup-config**. This section also includes a description of the information displayed when the **show running-config** command is entered. Many students ask what certain output means, such as **ip subnet-zero**. This section explains only a small portion of the possible output displayed with **sh run**, but it provides a good start for students. The section concludes with a Net-Challenge exercise for configuring RIPv2. This challenge verifies that students can use the router commands presented in this section. A good task is to have the students complete the exercise in class.

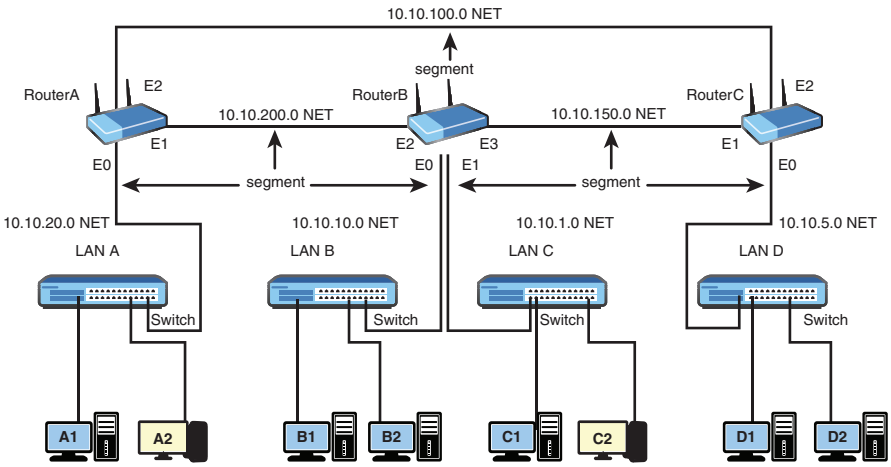
Advertise
To share route information

You enable the RIP routing protocol on a router by entering the command **router rip** at the **Router(config)#** prompt in privileged EXEC mode. Next, **network** statements are required to declare which networks will be advertised by the RIP routing protocol. To **advertise** the network means to share the routing table containing

the network with neighbors. The **network** command requires the use of a **class network address** (Class A, Class B, Class C) after the **network** command. This is called **classful addressing**. A class network address, or classful address, is the network portion of an address for a particular class of network. For example, LAN A in the campus network in Figure 9-8 is on the 10.10.20.0 NET. This is a Class A network, and the network portion of the address is 10.0.0.0. The structure of the **network** command is **network [***network address***]**, where *network address* is the network where RIP is to be advertised; therefore, the command with RIP is **network 10.0.0.0**.

Class Network Address
The network portion of an IP address, based on the class of the network

Classful Addressing
Addressing that requires the network portion of a particular network address



RouterA Port Addresses (LAN A)	
Ethernet 0 (Gateway Address)	10.10.20.250
Ethernet 1	10.10.200.1
Ethernet 2	10.10.100.1
LAN A Computers	
Computer A1	10.10.20.1
Computer A2	10.10.20.2
Subnet Mask	***255.255.255.0***

RouterB Port Addresses (LAN B)	
Ethernet 0 (Gateway Address)	10.10.10.250
Ethernet 2	10.10.200.2
Ethernet 3	10.10.150.1
LAN B Computers	
Computer B1	10.10.10.1
Computer B2	10.10.10.2
Subnet Mask	***255.255.255.0***

RouterB Port Addresses (LAN C)	
Ethernet 1 (Gateway Address)	10.10.1.250
Ethernet 2	10.10.200.2
Ethernet 3	10.10.150.1
LAN C Computers	
Computer C1	10.10.1.1
Computer C2	10.10.1.2
Subnet Mask	***255.255.255.0***

RouterC Port Addresses (LAN D)	
Ethernet 0 (Gateway Address)	10.10.5.250
Ethernet 1	10.10.150.2
Ethernet 2	10.10.100.2
LAN D Computers	
Computer D1	10.10.5.1
Computer D2	10.10.5.2
Subnet Mask	***255.255.255.0***

FIGURE 9-8 Multiple LANs in a campus network.

This section explains how to initialize RIP and how to set the networks attached to the router. After these commands are entered, any interfaces that are part of the 10.0.0.0 network will run the RIP routing protocol. Note that subnets or subnet masks are not specified with the RIP **network** command because the class network address is used, and all IP addresses in the network (for example, 10.0.0.0) are enabled to use RIP. To configure RIP, you will need to enter the privileged EXEC mode. Then at the (config)# prompt, enter the command "router rip" and enter the specific network which will be running the RIP protocol as shown below.

```
Router(config)# router rip
Router(config-router)# network 10.0.0.0
```

RIP can be used only in **contiguous networks**, which means the networks and routes must have the same class network address. The router addresses for the

Contiguous Networks
Networks and routes that have the same class network address

network connecting the routers must be the same class as the LAN connected to the router (see Figure 9-9). LAN A and LAN B have a 10.#.#.# address (also called a *10 network* address). The network address connecting the two routers must also be a 10 network address. The IP address for the network connecting the two routers in Figure 9-9(a) is 10.10.200.0. This is a 10 network address. The network shown in Figure 9-9(b) uses the IP address 192.168.10.0 for the network connecting the two routers. This address is in the 192.168.10.0 network and is not part of the 10.0.0.0 network; therefore, the 192.168.10.0 address is not suitable for use with RIP.

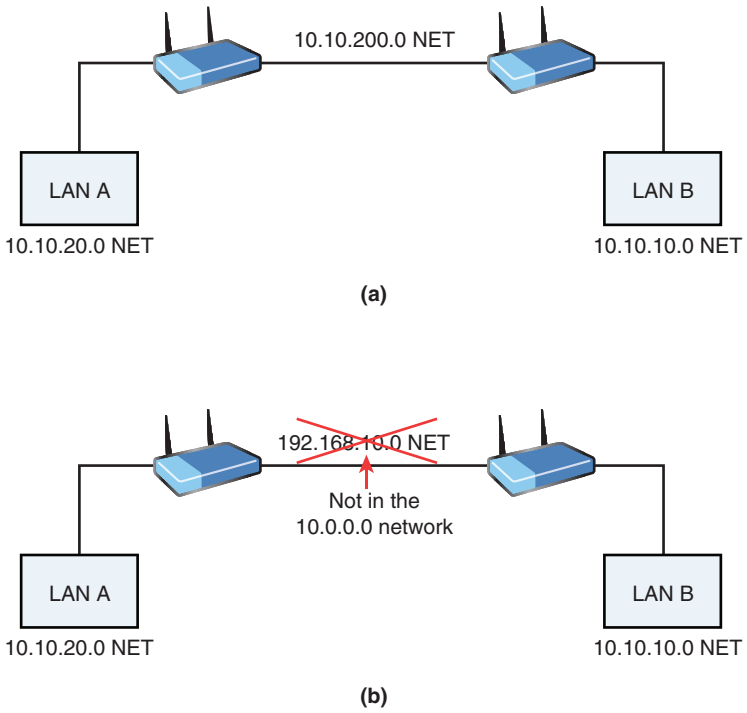


FIGURE 9-9 An example of (a) a contiguous network and (b) a discontiguous network.

Configuring Routes with RIP

The first step in configuring a router for RIP is to set up the interfaces, which involves assigning an IP address and a subnet mask to the interface by using the command **ip address** *A.B.C.D. subnet-mask*. Next, you enable the interface by using the **no shut** command. The following example shows how to configure the FastEthernet0/0 and FastEthernet 0/1 interfaces on RouterA in the campus network shown in Figure 9-9:

```
Router con0 is now available
Press RETURN to get started.
RouterA> en
Password:
RouterA# conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)# int fa0/0
```

```
RouterA(config-if)# ip address 10.10.20.250 255.255.255.0
RouterA(config-if)# no shut
00:59:03: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1, changed state to up Router(config)# int fa0/1
RouterA(config-if)# ip address 10.10.200.1 255.255.255.0
RouterA(config-if)# no shut
00:59:03: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1, changed state to up
```

Next, you enter the router's configuration mode and input the command **router rip** to use RIP as the routing protocol and then specify the network that uses RIP for routing, as shown here:

```
RouterA(config)# router rip
RouterA(config-router)# network 10.0.0.0
```

The command **router rip** enables the RIP routing protocol, and the command **network 10.0.0.0** instructs the router to use RIP on the 10 network. Remember that RIP requires the use of a class network address (for example, 10.0.0.0). Notice that the **router rip** command places the router in the router configuration mode, as shown in the prompt (**RouterA(config)#**). This indicates that the router is in the state for specifying the networks using RIP.

It's a good idea to periodically check that the router interfaces are properly configured. To do this, you can use the command **show ip interface brief** (**sh ip int brief**). This is an important troubleshooting command when you're trying to figure out why a router is not working. Use this command to check whether the IP address has been assigned to the interface and to check the status and protocol settings. In this case, the FastEthernet0/1 port has been assigned the IP address 10.10.200.1, the status is **up**, and the protocol is **up**. You can see here that the FastEthernet0/2 port for RouterA has not been configured, the status is **administratively down**, and the protocol is **down**:

```
RouterA# sh ip int brief
Interface IP-Address OK? Method Status Protocol
FastEthernet 0/0 10.10.20.250 YES manual up up
FastEthernet 0/1 10.10.200.1 YES manual up up
FastEthernet 0/2 unassigned YES unset administratively down down
```

The command **show ip protocol (sh ip protocol)** is used to display the routing protocols running on a router, as shown here:

show ip protocol (sh ip protocol)
The command that displays the routing protocols running on the router

```
RouterA# sh ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 5 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is Incoming update
filter list for all interfaces is Redistributing: rip
Default version control: send version 1, receive any version
Interface Send Recv Key-chain
FastEthernet0/0 1 1 2
FastEthernet0/1 1 1 2
```

```
FastEthernet0/2 0 0 0
Routing for Networks:
10.0.0.0
Routing Information Sources:
Gateway Distance Last Update
10.10.200.2 120 00:00:14
Distance: (default is 120)
```

This command displays protocol information only after the routing protocol has been enabled and the network addresses are specified. Notice that there are no values specified for the FastEthernet0/0 and FastEthernet0/2 ports. Neither of these interfaces has been configured. The **show ip protocol** command also shows that router updates are being sent every 30 seconds and indicates that the next update is due in 5 seconds.

The routes configured for the router can be displayed by using the **show ip route** (**sh ip route**) command, as shown here:

```
RouterA# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * candidate default
U - per-user static route, o - ODR T - traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 1 subnets
C 10.10.20.0 is directly connected, FastEthernet0/0
C 10.10.200.0 is directly connected, FastEthernet0/1
```

In this example, the FastEthernet 0/0 and FastEthernet0/1 ports for RouterA have been configured and are displayed as connected networks. This routing table shows the connected networks, but RIP (**R**) is not enabled for any networks. Why? At this point, RIP has been enabled only on RouterA in the campus network. RouterB and RouterC also need to have RIP enabled. Use the commands **router rip** and **network** to enable RIP on RouterB. RIP is next configured on RouterB, and the updated routing table for RouterA is provided:

```
Router# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * candidate default
U - per-user static route, o - ODR T - traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 5 subnets
R 10.10.1.0 [120/1] via 10.10.200.2, 00:00:05, FastEthernet0/1
R 10.10.10.0 [120/1] via 10.10.200.2, 00:00:05, FastEthernet0/1
```

```
C 10.10.20.0 is directly connected, FastEthernet0/0
C 10.10.200.0 is directly connected, FastEthernet0/1
```

Now, the networks (10.10.10.0 and 10.10.1.0) from LAN B and LAN C, respectively, are shown in this routing table. RouterA learns these network routes via its FastEthernet0/1 port from the IP address 10.10.200.2, which is the FastEthernet0/2 interface of RouterB.

You can verify the settings in the running configuration file by using the **sh run** command. (Recall that this is the abbreviated version of **show running-configuration**.) The configuration list should show that the interfaces have been assigned an IP address and that RIP has been configured. Table 9-4 provides some commented output from the **sh run** command.

TABLE 9-4 **sh run Command Output**

Output	Comments
RouterA# **sh run**	**sh run** command
Building configuration	Assembling the data file
!	! is used for spaces or comments
version 12.0	Displays the Cisco IOS version
service timestamps debug uptime	Displays time in debug mode since last reboot
service timestamps log uptime	Records time in syslog since last reboot
no service password-encryption	The enable (line 14) and vty (line 42) passwords, which appear as plaintext
hostname RouterA	The name of the router
enable secret 5 $1$6EWO$kWlakDz89zac.koh/pyG4.	The encrypted enable secret
enable password Salsa	The enable password
ip subnet-zero	Enables subnet zero routing
interface FastEthernet0/0 ip address 10.10.20.0 255.255.255.0 no ip directed-broadcast	FastEthernet0/0 settings
interface FastEthernet0/1 ip address 10.10.200.1 255.255.255.0 no ip directed-broadcast no mop enabled	FastEthernet0/1 settings
interface FastEthernet0/2 ip address 10.10.100.1 255.255.255.0 no ip directed-broadcast no mop enabled	FastEthernet0/2 settings
router rip	Enables RIP
network 10.0.0.0	Specifies a network class address
ip classless	Enables classless routing
line con 0	Console terminal settings
transport input none	Disables all forms of remote access
line aux 0	AUX terminal settings
line vty 0 4	Virtual terminal settings for telnet and SSH
password ConCarne	VTY password
!	Login
end	

Notice that the IP addresses for FA0/0, FA0/1, and FA0/2 have been configured. Also note that RIP has been configured for the router. The **sh run** command displays the router's running configuration. The **copy run start** command must be entered to save to NVRAM the changes made to the router's configuration.

RIP, introduced in 1988, is among the oldest protocols. It has a number of limitations that make it inefficient in handling a lot of newer IP features, including the following:

- **RIP is a classful routing-only protocol:** It therefore does not support VLSM and CIDR. This prevents it from being the routing protocol of choice for dealing with different-sized subnets in a network.
- **RIP does not support router authentication:** This means routers are vulnerable to exploits.
- **RIP has a hop count limit of 15:** With RIP, a destination that is more than 15 hops away is considered unreachable.
- **RIP uses hop count as a metric:** RIP determines the best route by counting the number of hops to reach the destination. A lower hop count wins over a higher hop count. This is a disadvantage when dealing with different bandwidths between hops. RIP does not take into consideration whether a higher hop count route might have higher bandwidth. Therefore, it might take the lower-bandwidth route.

The following example demonstrates one of RIP's limitations. In this example, the subnet mask of the LAN C network is changed to 255.255.255.128. To accomplish this task, the FastEthernet0/1 interface for RouterB needs to be reconfigured as follows:

```
RouterB# conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)# int fa0/1
RouterB(config-if)# ip address 10.10.1.250 255.255.255.128
```

RIP does not support VLSM, so what will happen to the newly reconfigured subnet? The network 10.10.1.0 will not be advertised by RIP. The route for network 10.10.1.0 is not displayed in the routing table of RouterA, as shown in the output of the command **sh ip route**:

```
RouterA# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * candidate default
U - per-user static route, o - ODR T - traffic engineered route
```

```
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 5 subnets
R 10.10.10.0 [120/1] via 10.10.200.2, 00:00:05, FastEthernet0/1
C 10.10.20.0 is directly connected, FastEthernet0/0
C 10.10.200.0 is directly connected, FastEthernet0/1
```

To address some of RIP's limitations, the second version of RIP, RIP version 2 (RIPv2), was developed in 1993. The original version of RIP is now sometimes called RIP version 1 (RIPv1). RIPv2 is not quite a redesign of RIPv1; rather, it can be thought of as an enhanced version of RIPv1. RIPv2 works basically just like RIPv1, but it introduced new features, such as support for VLSM and CIDR, router authentication, next hop specification, route tags, and multicasting. However, it still cannot resolve the hop count and metric decision limitations of RIPv1.

Configuring Routes with RIPv2

The steps needed to configure RIPv2 are almost exactly the same as for configuring RIPv1. The only difference is that the version must be specified in the **router rip** configuration. The following example shows how to start with the RIP configuration from earlier in this chapter and enter the router's configuration mode (**Router(config)#**) and input the command **router rip** to use the RIP routing protocol. The next step is to configure RIPv2 to be used with the command **version 2**. (If you don't specify the version, RIPv1 is used by default.) This is what these two steps look like:

```
RouterA(config)# router rip
RouterA(config-router)# version 2
```

To verify that RIPv2 is the routing protocol, you use the **sh ip protocol** command. Notice the line **Default version control**, which confirms that RIPv2 is being sent as well as being received by RouterA. The rest of the information shown is similar to the protocol result with RIPv1, as you can see here:

```
RouterA# sh ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 17 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive version 2
Interface Send Recv Triggered RIP Key-chain
FastEthernet0/0 2 2
FastEthernet0/1 2 2
FastEthernet0/2 2 2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
10.0.0.0
```

```
Routing Information Sources:
Gateway Distance Last Update
10.10.200.2 120 00:00:20
Distance: (default is 120)
```

Now let's reexamine the earlier demonstration of the RIPv1 limitation in which VLSM was being used, and the subnet mask for the network 10.10.1.0 was changed to 255.255.255.128. This resulted in the network no longer showing up in the routing table. The command **version 2** needs to be applied under **router rip** on RouterB. With RIPv2 enabled, the command **sh ip route** is reissued at RouterA. This time, the routing table shows that the LAN C network 10.10.1.128/25 is being displayed, even though it has a different-sized subnet than the others:

```
RouterA# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * candidate default
U - per-user static route, o - ODR
T - traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 5 subnets
R 10.10.10.0 [120/1] via 10.10.200.2, 00:00:05, FastEthernet0/1
C 10.10.20.0 is directly connected, FastEthernet0/0
R 10.10.1.128/25 [120/1] via 10.10.200.2, 00:00:15, FastEthernet0/1
C 10.10.200.0 is directly connected, FastEthernet0/1
```

Networking Challenge: RIPv2

Use the Net-Challenge router simulator software to demonstrate that you can configure RIP for RouterA in the campus LAN. (*Note:* The campus LAN is shown in Figure 9-8 and is displayed on the computer screen after the software is started and you click on **View Topology**.) In Net-Challenge, click the **Select Challenge** button to open the Select Challenge drop-down menu. Select **RIP V2** to open a check box list that can be used to verify that you have completed all the tasks. Then follow these steps:

1. Enter privileged EXEC mode on the router using the password **Chile**.
2. Enter router configuration mode, **Router(config)**.
3. Configure the FastEthernet0/0 interface as follows:
   - **IP address:** 10.10.20.250
   - **Subnet mask:** 255.255.255.0
4. Enable the FA0/0 interface.

5. Configure the FastEthernet0/1 interface as follows:
    - **IP address:** 10.10.200.1
    - **Subnet mask:** 255.255.255.0
6. Enable the FA0/1 interface.
7. Configure the FastEthernet0/2 interface as follows:
    - **IP address:** 10.10.100.1
    - **Subnet mask:** 255.255.255.0
8. Enable the FA0/2 interface.
9. Enable RIPv2.
    a. Specify that RIPv2 is to be used.
    b. Use the **network** command to specify the class network address to be used by RIP (10.0.0.0).
    c. Use the **sh ip int brief** command to check the interface status.
    d. Use the **sh ip protocol** command to see whether RIP is running.
    e. Use the **show ip** route command to verify whether the three FastEthernet ports are connected to the router.
    f. Display the contents of the **running configuration** file. Verify that RIP is enabled and the proper network address is specified.
    g. Copy the router's running configuration to the startup configuration.
    h. Display the contents of the startup configuration.

Section 9-5 Review

This section covers the following Network+ exam objectives.

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

*In this section, it states that the **ip classless** command enables classless routing.*

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

*This section says that **line vty 0 4** indicates the virtual terminal settings for Telnet and SSH.*

2.2 Compare and contrast routing technologies and bandwidth management concepts.

*This section states that to verify the routing protocol, you use the **sh ip protocol** command.*

4.1 Explain common security concepts.

This section mentions that RIP does not support router authentication, which means routers are vulnerable to exploits.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

RIP, introduced in 1988, is among the oldest protocols. A number of limitations make it inefficient at handling a lot of newer IP features.

5.5 Given a scenario, troubleshoot general networking issues.

It's a good idea to periodically check that the router interfaces are properly configured. To do this, you can use the command ***show ip interface brief*** *(****sh ip int brief****) to check whether the IP address has been assigned to the interface and to check the status and protocol settings.*

Test Your Knowledge

1. What Cisco router IOS command is used to specify the RIP routing protocol?
   a. router(config) **router rip**
   b. router# **router rip**
   c. router(config)# **router rip protocol**
   d. router(config)# **router rip**

2. Which command is used to display the routing protocols currently running on a router?
   a. router# show ip protocol
   b. router# **show protocol**
   c. router(config)# **show ip protocol**
   d. router# (config) **show ip protocol**

9-6 LINK STATE PROTOCOLS

This section examines link state protocols. It is important that students understand that link state advertisements are exchanged only if routes change. This is a distinct advantage over dynamic routing protocols. Make sure students understand why. Students should also understand the purpose of the hello packets and how they are used to verify that links are still communicating.

Link State Protocol
A type of protocol that establishes a relationship with a neighboring router and uses route advertisements to build routing tables

A **link state protocol** establishes a relationship with a neighboring router. The routers exchange link state advertisements to update neighbors regarding route status. The link state advertisements are sent only if there is a change or loss in the network routes and the link state protocols converge to route selection quickly. This is a distinct advantage over distance vector protocols, which exchange updated

routing tables at fixed intervals and are slow to converge. In fact, link state routing protocols are replacing distance vector protocols. Link state protocols are also called *shortest path first protocols,* based on the algorithm developed by E. W. Dijkstra. Link state protocols use hello packets to verify that communication is established with neighbor routers.

The key issues related to link state protocols are summarized as follows:

- They find neighbors/adjacencies.
- They use route advertisements to build the routing table.
- They send hello packets.
- They send updates when routing changes.

Open Shortest Path First (**OSPF**) is a dynamic link state routing protocol. It was developed by the Interior Gateway Protocol (IGP) working group for the Internet Engineering Task Force (**IETF**) specifically for use in TCP/IP networks. OSPF is an open (that is, not proprietary) protocol that is supported by many vendors. The main advantages of OSPF are rapid convergence and very low bandwidth consumption. When a network is completely *converged*, all the routers in the network agree on the best routes. After the initial flooding of routes in the form of **link state advertisements (LSAs)**, OSPF sends route updates only when there is a change in the network. Every time LSAs are sent, each router must recalculate the routing table.

OSPF
Open Shortest Path First, a dynamic link state routing protocol that is supported by many vendors

IETF
Internet Engineering Task Force

Link State Advertisement (LSA)
An announcement of updated link state information when routes change

Link state protocols have a distinct advantage over RIP. Recall that RIP exchanges the entire routing table at fixed intervals—every 30 seconds. Also, with RIP, the routing table update is propagated through the network at regular intervals, and therefore the convergence to final routes is slow. With OSPF, an LSA is sent as soon as the loss of a route has been detected. The loss is immediately reported to neighbor routers, and new routes are calculated much more quickly than with RIP.

OSPF sends small **hello packets** at regular intervals to adjacent routers to verify that the link between two routers is active and the routers are communicating. If a router fails to respond to a "Hello," it is assumed that the link—or possibly the router—is down.

Hello Packets
Packets used with the OSPF protocol to verify that links are still communicating

OSPF uses the concept of **areas** to partition a large network into smaller networks. The advantage of this is that the routers have to calculate routes only for their area. If a route goes down in a given area, only the routers in that area have to calculate new routes. Any number between 0 and 4294967295 ($2^{32} - 1$) can be used; however, area 0 is reserved for the root area, which is the **backbone** of the network. The backbone is the primary path for data traffic to and from destinations and sources in the campus network. All areas must connect to area 0, and area 0 cannot be split. You can also express the area numbers in IP notation—for example, area 0 could be 0.0.0.0—or you can specify an area as 192.168.25.0 or in subnet notation. Hence there is a need for a large upper area number. That is, ($2^{32} - 1$) = 255.255.255.255 when converted to a decimal number.

Areas
Smaller OSPF networks partitioned from a large OSPF network

Backbone
The primary path for data traffic to and from destinations and sources in a campus network

Variable-Length Subnet Mask
Different-sized subnet masks that better fits the needs of a network, thereby minimizing the waste of IP addresses when interconnecting subnets

OSPF allows the use of **variable-length subnet masks**, which enable different-size subnets in the network to better meet the needs of the network and more efficiently use the network's limited IP address space. For example, point-to-point inter-router links don't need a large block of addresses assigned to them. Figure 9-10 shows an example of an inter-router link.

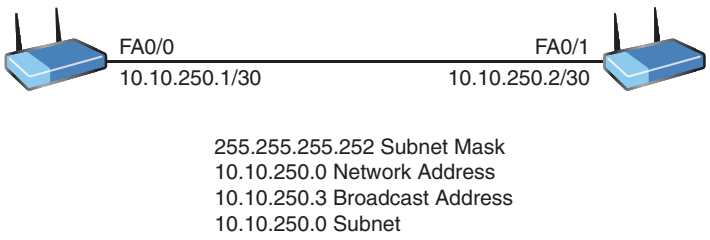


FIGURE 9-10 An inter-router link subnetted to provide for two host IP addresses

A subnet of size 4 is sufficient for the inter-router link that includes the IP addresses for the router interfaces, the network address, and the broadcast address. The subnet mask 255.255.255.252 meets this requirement of a subnet size 4 and is permissible in OSPF. This subnet mask provides for the addressing of the two host addresses (the router interfaces on each end) and the network and broadcast addresses, which provides the total subnet size 4. (Refer to Chapter 6, "TCP/IP," to review subnet masking, if needed.) This is an important advantage of OSPF because using variable-length subnet masks minimizes the waste of IP addresses when interconnecting subnets. Table 9-5 summarizes the advantages and disadvantages of OSPF.

TABLE 9-5 **Advantages and Disadvantages of OSPF**

Advantages	Disadvantages
Not proprietary; available for use by all vendors.	Can be very complicated to implement.
Link state changes are immediately reported, which enables rapid convergence.	Is process intensive due to routing table calculations.
Consumes very little network bandwidth.	Intermittent routes that are going up and down create excessive LSA updates; this is called **route flapping**.
Uses VLSM.	
Uses areas to partition the network into smaller networks, minimizing the number of route calculations.	

Route Flapping
A situation in which intermittent routes go up and down, creating excessive LSA updates

IS-IS
Intermediate System-to-Intermediate System, a link state protocol used in many service provider core networks

Another link state protocol is Intermediate System-to-Intermediate System (**IS-IS**), which was developed by the Digital Equipment Corporation for its DECnet phase V. Later, it was adopted by the International Organization for Standardization (ISO),

around the same time that the IETF was developing OSPF. The term *intermediate system* refers to a router. Even though IS-IS is not as well-known as OSPF, it is still in use (primarily in service provider core networks).

There are many similarities between IS-IS and OSPF:

- They are both link state protocols that use the Dijkstra algorithm.
- They are both classless protocols, which means they support VLSM.
- They both use hello packets to form and maintain adjacencies, and they both use the areas concept.

However, there is a difference in the way the areas are defined. In IS-IS, there are two hierarchical topology areas: level 1 (intra-area) and level 2 (inter-area). A router can either be a level 1 (L1) router, a level 2 (L2) router, or both (L1/L2). L1 routers are analogous to OSPF non-backbone routers, L2 routers are analogous to OSPF backbone routers, and L1/L2 routers are analogous to OSPF area border routers (ABRs). However, unlike OSPF ABRs, L1/L2 routers do not advertise routes from L2 routers to L1 routers. The packets from different areas can only be routed through the L1/L2 routers. Essentially, L1/L2 routers are default gateways to L1 routers. Another big difference is that the IS-IS backbone area can be segmented. Unlike the backbone area in OSPF, all routers in area 0 must be connected; the IS-IS L2 routers do not need to be connected directly together.

IS-IS was originally designed as part of the Open System Interconnection (OSI) network layer service called Connectionless Network Service (CLNS). IS-IS was designed to work on the same network layer as IP; therefore, IS-IS does not require IP in order to function. It was later adapted to work with IP. Hence, it is sometimes referred to as *integrated* IS-IS. In IS-IS, every router uses the Network Entity Title (**NET**) to define its process. The NET address is unique to each router, and it is composed of the following, in hexadecimal format:

NET
In IS-IS, the Network Entity Title, an address that is unique to each router

- The area ID in IS-IS is analogous to the OSPF area number, and it is used by L2 routers.
- The system ID is analogous to the OSPF router ID, and it is used by L1 routers.
- The network service access point selector (NSEL) identifies the network service type.

A NET address can look intimidating due to its long hexadecimal format, but it is easy to understand when you work from right to left. For example, in the NET address 49.0001.0014.a909.5201.00, the last 1 byte from the right is NSEL, which is always set to 00 on a router. The next 6 bytes separated into 3 groups of 2 bytes are the system ID, which is 0014.a909.5201 in this example. This is always unique and is typically represented as the MAC address of the router. The rest of the numbers to the left of the system ID are the area ID, which is 49.0001. The area ID has a variable length, but its first number must be at least 1 byte long.

Section 9-6 Review

This section covers the following Network+ exam objectives.

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

Figure 9-10 shows an inter-router link subnetted to provide for two host IP addresses, a network address, and a broadcast address.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

This section examines link state protocols. It is important to understand that link state advertisements are exchanged only if routes change. This is a distinct advantage over dynamic routing protocols.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section discusses how a link state protocol establishes a relationship with a neighboring router. The routers exchange link state advertisements to update neighbors regarding route status. The link state advertisements are sent only if there is a change or loss in the network routes and the link state protocols converge to route selection quickly.

Test Your Knowledge

1. Which of the following are key features of link state protocols? (Select all that apply.)
   a. Finding neighbors/adjacencies
   b. Sending hello packets
   c. Sending updates when routing changes
   d. Minimizing route flapping
2. What is the purpose of a hello packet?
   a. It is used to partition a large network into smaller networks.
   b. It verifies that the link between two routers is active and the routers are communicating.
   c. It enables VLSM.
   d. It is assigned to a protocol or route to declare its reliability.

9-7 CONFIGURING THE OPEN SHORTEST PATH FIRST (OSPF) ROUTING PROTOCOL

This section introduces the steps for configuring the OSPF routing protocol. Have students experiment by using the Net-Challenge software. This will give them a better understanding of steps and commands required to configure OSPF.

This section describes how to configure OSPF on a router. The first example is for configuring the three routers in the campus LAN shown in Figure 9-11. The routers will be configured to run OSPF on each of the router's three Ethernet interfaces. The example begins with configuring RouterA, which must first be placed in the router's configuration mode (**Router(config)#**), as shown here:

```
RouterA# conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#
```

The next step is to enter the information about the IP address for each of the Ethernet interfaces. The IP addresses for RouterA are as follows:

- **FastEthernet0/0:** 10.10.20.250
- **FastEthernet0/1:** 10.10.200.1
- **FastEthernet0/2:** 10.10.100.1

Subnet mask 255.255.255.0 is assigned to each of the FastEthernet interfaces. After the FastEthernet interfaces are configured, you verify the configuration settings by using the **sh ip int brief** command, as shown here:

```
RouterA# sh ip int brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.10.20.250 YES manual up up
FastEthernet0/1 10.10.200.1 YES manual up down
FastEthernet0/2 10.10.100.1 YES manual up down
```

Make sure the status for each FastEthernet interface is **up**. This indicates that the interface is turned on, and an Ethernet networking device is connected. The protocol shows **down** until the Ethernet cable is connected and the connecting interface is enabled. In this example, the connecting interfaces to FA0/1 and FA0/2 are not enabled and therefore show the status **down**.

router ospf [*process id*]
The command used to enable OSPF routing

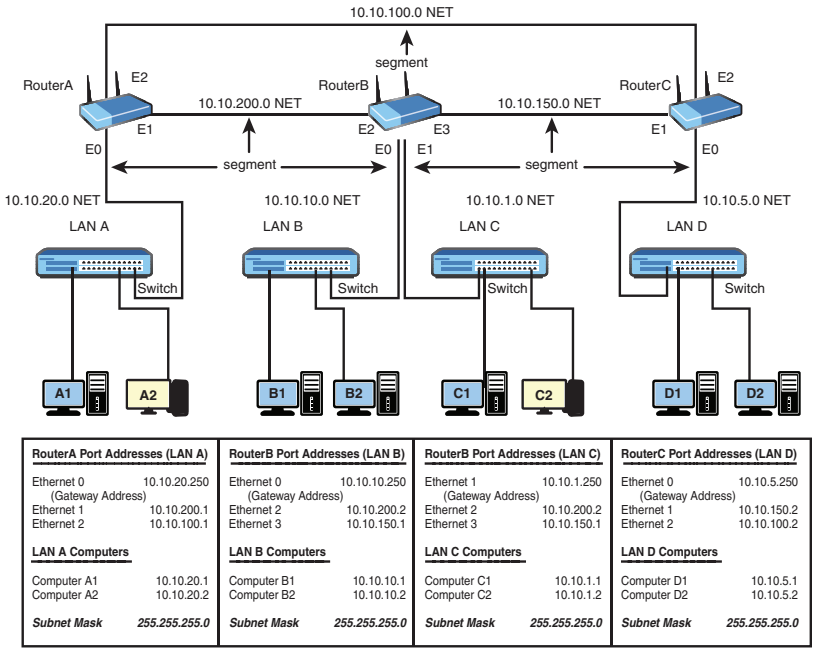
Next, you use the command **router ospf [*process id*]** to enable OSPF routing. In this case, the command **router ospf 100** is entered, where **100** is the *process ID number*, which must be the same on each router in order for OSPF to exchange routes. The process ID number is selected by the network administrator and is not used for routing outside the network. It is customary to use the same process ID throughout a network for ease of management, but it is not required. Entering the **router ospf 100** command places the router at the **RouterA(config-router)#** prompt:

```
RouterA(config)# router ospf 100
RouterA(config-router)#
```

The next step is to define the network running OSPF by entering the **network** command followed by the IP address of the interface, the OSPF wildcard bits, and

then an area number. The following example shows each step and lists the results of entering a question mark as the command is entered:

```
RouterA(config-router)# network ?
A.B.C.D Network number
```



RouterA Port Addresses (LAN A)		RouterB Port Addresses (LAN B)		RouterB Port Addresses (LAN C)		RouterC Port Addresses (LAN D)	
Ethernet 0 (Gateway Address)	10.10.20.250	Ethernet 0 (Gateway Address)	10.10.10.250	Ethernet 1 (Gateway Address)	10.10.1.250	Ethernet 0 (Gateway Address)	10.10.5.250
Ethernet 1	10.10.200.1	Ethernet 2	10.10.200.2	Ethernet 2	10.10.200.2	Ethernet 1	10.10.150.2
Ethernet 2	10.10.100.1	Ethernet 3	10.10.150.1	Ethernet 3	10.10.150.1	Ethernet 2	10.10.100.2
LAN A Computers		**LAN B Computers**		**LAN C Computers**		**LAN D Computers**	
Computer A1	10.10.20.1	Computer B1	10.10.10.1	Computer C1	10.10.1.1	Computer D1	10.10.5.1
Computer A2	10.10.20.2	Computer B2	10.10.10.2	Computer C2	10.10.1.2	Computer D2	10.10.5.2
Subnet Mask	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***

FIGURE 9-11 A three-router campus LAN.

Network Number
Another name for the IP subnet

When you enter the command **network ?**, the router prompts you to enter the **network number** or network address of the interface. In this example, *A.B.C.D* is the network address for the FastEthernet0/0 interface, which has the IP address 10.10.20.250 with subnet mask 255.255.255.0. Therefore, the network address is 10.10.20.0.

Wildcard Bits
The inverse mask bits used to match network IP addresses to interface IP addresses

Next, you enter **network 10.10.20.0 ?**, and you are prompted to enter the OSPF wildcard bits in the form *A.B.C.D*. The **wildcard bits**, also called the *inverse mask bits,* are used to match the network IP addresses (in *A.B.C.D* format) to interface IP addresses. If there is a match, the subnet on the interface is advertised on OSPF, and OSPF packets are sent out the interface. A 0 wildcard bit is used to indicate a "must" match. A 255 is a "don't care"—hence the name *inverse mask*.

Area 0
In OSPF, the root area, or backbone, for a network

The last entry when defining an OSPF route is for the area. Remember that areas are used to partition a large network into smaller networks. **Area 0** is the root area, or backbone, for the network. All other areas must connect to area 0. Area 0 cannot be split. Other area numbers are specified by the network administrator.

Next, the router command **network 10.10.20.0 0.0.0.255 area 0** is entered. The wildcard bits indicate that any interface with address 10.10.20.x must run OSPF on the interface and will be assigned to area 0 (the network backbone). The following example shows these commands entered:

```
RouterA(config-router)# network 10.10.20.0 ? A.B.C.D OSPF wildcard bits
RouterA(config-router)# network 10.10.20.0 0.0.0.255 ?
```

```
area Set the OSPF area ID
RouterA(config-router)# network 10.10.20.0 0.0.0.255 area 0
```

The following example shows the three OSPF network entries needed to configure OSPF routing for RouterA:

```
RouterA(config-router)# network 10.10.20.0 0.0.0.255 area 0
RouterA(config-router)# network 10.10.200.0 0.0.0.255 area 0
RouterA(config-router)# network 10.10.100.0 0.0.0.255 area 0
```

Note that the RouterA interface to LAN A (10.10.20.250 NET) is listed when configuring OSPF. This is used in OSPF to advertise the LAN to the other routers. Also note that the network has been assigned to area 0 (the backbone). The command **sh ip int brief** is used to check the status of the interfaces:

```
RouterA# show int brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.10.20.250 YES NVRAM up up
FastEthernet0/1 10.10.200.1 YES manual up down
FastEthernet0/2 10.10.100.1 YES manual up down
```

The text protocol **down** indicates that either the cable to the interface is unplugged or the interface is shut down. This problem with the protocol being **down** is fixed by reestablishing the physical connection between the routers.

The next step is to configure RouterB. First, you configure the four FastEthernet interfaces on RouterB. Next, you set the OSPF routing protocol for RouterB. Unlike with RouterA, you can use one command-line instruction to configure RouterB to run OSPF on all four of its interfaces instead of specifying each network address command. This is done with a subnet mask or wildcard in OSPF. You enter RouterB's configuration mode by using the **configure terminal** command. Then you enter the command **router ospf 100**. Note that the same process ID number, **100**, is used. The next step is to enter **network 10.0.0.0 0.255.255.255 area 0**. This command tells the router that any address that starts with 10 belongs to area 0 on RouterB. The following example shows these commands entered:

```
RouterB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)# router ospf 100
RouterB(config-router)# network 10.0.0.0 0.255.255.255 area 0
```

Next, you verify that the interfaces are properly configured by using the **sh ip int brief** command, as shown here:

```
RouterB# sh ip int brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.10.10.250 YES manual up up
FastEthernet0/1 10.10.1.250 YES manual up up
FastEthernet0/2 10.10.200.2 YES manual up up
FastEthernet0/3 10.10.150.1 YES manual up down
```

The FastEthernet0/3 interface shows the protocol as **down** because the connecting interface is shut down on RouterC.

The next step is to configure RouterC. You set the OSPF routing protocol for RouterC by using the command **router OSPF 100** followed by **network 10.0.0.0. 0.255.255.255 area 0**, as shown here:

```
RouterC(config)# router ospf 100
RouterC(config-router)# network 10.0.0.0 0.255.255.255 area 0
```

Then you check the interfaces on RouterC by using the **sh ip int brief** command, as shown here:

```
RouterC# sh ip int brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.10.5.250 YES manual up up
FastEthernet0/1 10.10.150.2 YES manual up up
FastEthernet0/2 10.10.100.2 YES manual up up
```

Notice that the protocol shows as **up** for all interfaces. This is because all interfaces are connected and enabled.

The following is a partial listing of the running configuration file on RouterA, which shows the router OSPF network configuration:

```
router ospf 100
 network 10.10.200.1 0.0.0.0 area 0 network 10.10.20.250 0.0.0.0
area 0
 network 10.10.100.1 0.0.0.0 area 0
```

Similar information appears on RouterB and RouterC.

Next, you check the routing table for RouterA by using the command **show ip route**, as shown here:

```
RouterA# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O 10.10.5.0/24 [110/74] via 10.10.100.2, 00:03:28, FastEthernet0/2
O 10.10.10.0/24 [110/74] via 10.10.200.2, 00:03:28, FastEthernet0/1
O 10.10.1.0/24 [110/74] via 10.10.200.2, 00:03:28, FastEthernet0/1
C 10.10.20.0/24 is directly connected, FastEthernet0/0
L 10.10.20.250/32 is directly connected, FastEthernet0/0
C 10.10.100.0/24 is directly connected, FastEthernet0/2
L 10.10.100.1/32 is directly connected, FastEthernet0/2
O 10.10.150.0/24 [110/128] via 10.10.200.2, 00:03:28, FastEthernet0/1
```

```
[110/128] via 10.10.100.2, 00:03:28, FastEthernet0/2
C 10.10.200.0/24 is directly connected, FastEthernet0/1
L 10.10.200.1/32 is directly connected, FastEthernet0/1
```

The routing table indicates that there are seven subnets in the campus network shown in Figure 9-11. **O** indicates the subnets running OSPF, and **C** indicates the subnets directly connected to the router.

A command used to display only the OSPF routes is **show ip route ospf**. The following are the results of running this command from RouterA:

```
RouterA# show ip route ospf
10.0.0.0/24 is subnetted, 6 subnets
O 10.10.5.0 [110/74] via 10.10.100.2, 00:10:03, FastEthernet0/2
O 10.10.10.0 [110/74] via 10.10.200.2, 00:10:03, FastEthernet0/1
O 10.10.150.0 [110/128] via 10.10.200.2, 00:10:03, FastEthernet0/1
[110/128] via 10.10.100.2, 00:10:03, FastEthernet0/2
```

Another command that is used for displaying protocol information for a router is **sh ip protocol**. The following are the results of entering this command for RouterA:

```
RouterA# show ip protocol
Routing Protocol is "ospf 100" Sending updates every 0 seconds
Invalid after 0 seconds, hold down 0, flushed after 0
Outgoing update filter list for all interfaces is Incoming update
filter list for all interfaces is Redistributing: ospf 100
Routing for Networks:
10.10.20.250/32
10.10.100.1/32
10.10.200.1/32
Routing Information Sources:
Gateway Distance Last Update
10.10.100.1 110 00:06:01
10.10.200.2 110 00:06:01
Distance: (default is 110)
```

Networking Challenge: OSPF

Use the Net-Challenge simulator software to demonstrate that you can configure OSPF for RouterB in the campus LAN shown in Figure 9-11 and displayed on the computer screen when the software is started. In Net-Challenge, click the **Select Router Challenge** button to open the Select Router Challenge drop-down menu and then select **OSPF** to open a check box list that can be used to verify that you have completed all the tasks. Then follow these steps:

1. Enter privileged EXEC mode on the router.
2. Enter the router's terminal configuration mode, **Router(config) #**.
3. Set the hostname to **RouterA**.

4. Configure the FastEthernet0/0 interface as follows:
    - **IP address:** 10.10.20.250
    - **Subnet mask:** 255.255.255.0
5. Enable the FA0/0 interface.
6. Configure the FastEthernet0/1 interface as follows:
    - **IP address:** 10.10.200.1
    - **Subnet mask:** 255.255.255.0
7. Enable the FA0/1 interface.
8. Configure the FastEthernet0/2 interface as follows:
    - **IP address:** 10.10.100.1
    - **Subnet mask:** 255.255.255.0
9. Enable the FA0/2 interface.
10. Enable OSPF with network number **100**.
11. Use a single command-line instruction to configure RouterA to run OSPF on all three of the FastEthernet interfaces. (Use area **100**.)
12. Use the **sh ip int brief** command to check the interface status.
13. Use the **sh ip protocol** command to see whether OSPF is running on RouterA.
14. Use the **sh ip route** command to verify that the three FastEthernet ports are connected to RouterA.
15. Use the **sh run** command to view the running configuration file on RouterA. Verify that OSPF is enabled and the proper network address is specified.

Section 9-7 Review

This section covers the following Network+ exam objectives.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

This section introduces the technique for configuring OSPF routing.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

*This section demonstrates how to verify that the interfaces are properly configured by using the **sh ip int brief** command*

5.3 Given a scenario, use the appropriate network software tools and commands.

This section introduces the steps for configuring the OSPF routing protocol.

5.5 Given a scenario, troubleshoot general networking issues.

*This section demonstrates how to use the **show ip int brief** command to check the interface status.*

Test Your Knowledge

1. What command is used to enable OSPF routing?
   a. **[*router ospf*]**
   b. **router - ospf**
   c. **router ospf [*process id*]**
   d. **router [*process id*] ospf**
2. The command **show ip routing** is issued. Which of the following indicates OSPF routes?
   a. **D**
   b. **S**
   c. **R**
   d. **O**

9-8 ADVANCED DISTANCE VECTOR PROTOCOL: CONFIGURING ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (EIGRP)

This section introduces the advanced distance vector (hybrid) routing protocol EIGRP. EIGRP is a Cisco-proprietary protocol that supports variable-length subnetting, uses hello packets to verify that neighbor routers are communicating, and exchanges routing tables only if there is a change in routes.

This section introduces Enhanced Interior Gateway Routing Protocol (**EIGRP**), which is an enhanced version of Interior Gateway Routing Protocol (IGRP). EIGRP is a Cisco-proprietary protocol and is often called an advanced distance vector routing protocol because it incorporates the best of the distance vector and link state algorithms.

EIGRP
Enhanced Interior Gateway Routing Protocol, a Cisco-proprietary protocol that incorporates the best of the distance vector and link state algorithms

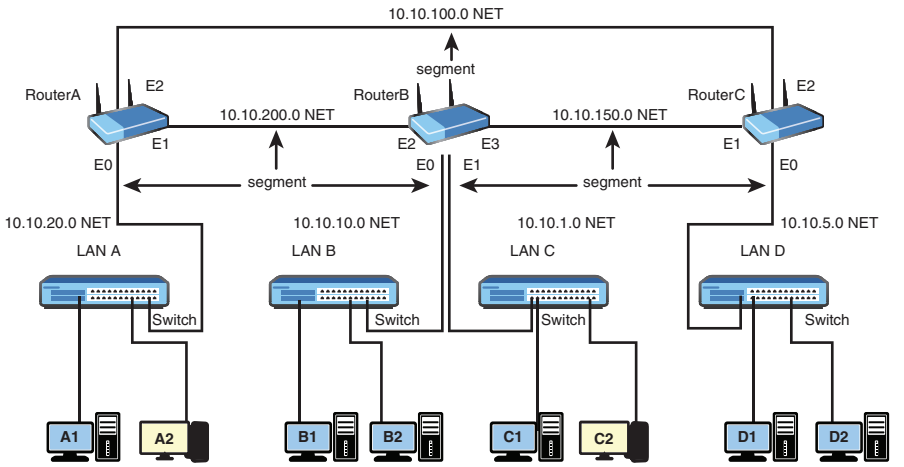
EIGRP allows the use of VLSM, which is beneficial when you're trying to conserve IP addresses. EIGRP also uses hello packets to verify that a link from one router to another is still active. The routing table updates are exchanged when there is a change in the network. In other words, the routers don't exchange unnecessary information unless a route changes. This helps conserve the limited bandwidth of the network data link. When route information is exchanged, EIGRP quickly converges to the new route selection.

EIGRP has four components:

- **Neighbor Discovery/Recovery:** EIGRP learns about other routers on directly attached networks and can also discover whether neighbor routers are unreachable. This discovery is accomplished by periodically sending hello packets to verify that a neighbor router is functioning.
- **Reliable Transport Protocol:** EIGRP can guarantee delivery of EIGRP packets to neighbor routers. Both unicast and multicast packet transmission are supported.
- **DUAL Finite State Machine:** EIGRP tracks all routes advertised by its neighbors and performs route computation to obtain loop-free routing.
- **Protocol-dependent modules:** These modules handle network layer protocol-specific requirements. For example, the IP-EIGRP module is responsible for extracting information from the EIGRP packets and passing that information to DUAL. DUAL uses the information to make routing decisions, and IP-EIGRP then redistributes the learned routes.

Configuring Routes with EIGRP

This section describes how to configure EIGRP on a router. The first example is for configuring RouterA in the campus LAN shown in Figure 9-12.



RouterA Port Addresses (LAN A)	
Ethernet 0 (Gateway Address)	10.10.20.250
Ethernet 1	10.10.200.1
Ethernet 2	10.10.100.1
LAN A Computers	
Computer A1	10.10.20.1
Computer A2	10.10.20.2
Subnet Mask	***255.255.255.0***

RouterB Port Addresses (LAN B)	
Ethernet 0 (Gateway Address)	10.10.10.250
Ethernet 2	10.10.200.2
Ethernet 3	10.10.150.1
LAN B Computers	
Computer B1	10.10.10.1
Computer B2	10.10.10.2
Subnet Mask	***255.255.255.0***

RouterB Port Addresses (LAN C)	
Ethernet 1 (Gateway Address)	10.10.1.250
Ethernet 2	10.10.200.2
Ethernet 3	10.10.150.1
LAN C Computers	
Computer C1	10.10.1.1
Computer C2	10.10.1.2
Subnet Mask	***255.255.255.0***

RouterC Port Addresses (LAN D)	
Ethernet 0 (Gateway Address)	10.10.5.250
Ethernet 1	10.10.150.2
Ethernet 2	10.10.100.2
LAN D Computers	
Computer D1	10.10.5.1
Computer D2	10.10.5.2
Subnet Mask	***255.255.255.0***

FIGURE 9-12 A three-router campus LAN.

In this section you will configure the three routers in the campus LAN shown in Figure 9-12 to run EIGRP. The first step is to configure the interfaces on each of the three routers. The IP addresses and the subnet masks for the router interfaces are as follows:

RouterA:

```
FA0/0 10.10.20.250 255.255.255.0
FA0/1 10.10.200.1 255.255.255.0
FA0/2 10.10.100.1 255.255.255.0
```

RouterB:

```
FA0/0 10.10.10.250 255.255.255.0
FA0/1 10.10.1.250 255.255.255.0
FA0/2 10.10.200.2 255.255.255.0
FA0/3 10.10.150.1 255.255.255.0
```

RouterC:

```
FA0/0 10.10.5.250 255.255.255.0
FA0/1 10.10.150.2 255.255.255.0
FA0/2 10.10.100.2 255.255.255.0
```

After the router interfaces are configured, you configure the EIGRP routing protocol for RouterA. You use the **configure terminal** command to enter the router's configuration mode and then enter the command **router eigrp [***AS number***]**. The AS number is the same as that for the EIGRP routing protocol, and any AS number can be used. The router uses the AS numbers to determine which routers share routing tables. Only routers with the same ASN share routing updates. In this case, you can use the command **router eigrp 150**. The prompt changes to **(config-router)**, and you enter a command to set the network to run EIGRP—in this example, **network 10.0.0.0**:

```
RouterA(config)# router eigrp 150
RouterA(config-router)# network 10.0.0.0
```

Much as with RIP, a classful network statement such as 10.0.0.0 can be specified as a network state in EIGRP. This instructs the router to run EIGRP on any of the router's interfaces that have an IP address that begins with 10. A different network command will be used on RouterB to show how the command can be used to specify a limited IP address range.

You enter the command **show ip protocol** to verify that the EIGRP routing protocol is enabled on RouterA:

```
RouterA# show ip protocol
Routing Protocol is "eigrp 150"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1 1, K2 0, K3 1, K4 0, K5 0
```

```
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 150
Automatic network summarization is in effect
Routing for Networks:
10.0.0.0
Routing Information Sources:
Gateway Distance Last Update
10.10.200.2 90 00:00:09
Distance: internal 90 external 170
```

This example shows that the routing protocol is **eigrp 150** and indicates that it has been 9 seconds since the last update to the routing table. In EIGRP, updates to the routing table are made when there are changes in the network.

Another useful command is **show ip route**:

```
RouterA# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C 10.10.20.0/24 is directly connected, FastEthernet0/0
L 10.10.20.250/32 is directly connected, FastEthernet0/0
C 10.10.200.0/24 is directly connected, FastEthernet0/1
L 10.10.200.1/32 is directly connected, FastEthernet0/1
C 10.10.100.0/24 is directly connected, FastEthernet0/2
L 10.10.100.1/32 is directly connected, FastEthernet0/2
```

In this case, the router does not show any EIGRP routes to the subnets in the network because EIGRP has not been configured on RouterB or RouterC.

Next, you enter the command **show ip int brief**, as shown here, and you see that the status and protocols for the Ethernet interfaces are **up**:

```
RouterA# show ip int brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 10.10.20.250 YES NVRAM up up
FastEthernet0/1 10.10.200.1 YES manual up up
FastEthernet0/2 10.10.100.1 YES manual up up
```

They show as **up** as long as there are network connections to the interfaces.

Next, you use the **show run** command to view the contents of the router's running configuration file. The following is the part of the configuration file that shows the entries for EIGRP:

```
! router eigrp 150
 network 10.0.0.0
!
```

Notice that these entries are the same as the commands entered earlier in configuring EIGRP.

The next step is to configure RouterB. To do so, you enter the configuration mode (**(config)#**) for RouterB and use the command **router eigrp 150**. Remember that 150 is the ASN, which is the same number used when configuring RouterA. For EIGRP routers to establish a neighbor adjacency, the ASN must be the same. The next command, **network 10.10.0.0 0.0.255.255**, sets the network that is running EIGRP. Much as with OSPF, you can use a variable-length subnet mask by specifying a different subnet mask with wildcard bits or inverse mask bits. This means that on RouterB, all interfaces with a 10.10.*x.x* address will run EIGRP. In this case, all interfaces on RouterB have a 10.10.*x.x* address and will run EIGRP. The following example shows these commands in use:

```
RouterB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)# router eigrp 150
RouterB(config-router)# network 10.10.0.0 0.0.255.255
```

Next, you use the command **show ip protocol** to verify that EIGRP is running on RouterB. The following output shows that **eigrp 150** is running on RouterB, and it has been 27 seconds since the last update to the routing table:

```
RouterB# sh ip protocol
Routing Protocol is "eigrp 150"
Outgoing update filter list for all interfaces is Incoming update
filter list for all interfaces is Default networks flagged in outgoing
updates Default networks accepted from incoming updates EIGRP metric
weight K1 1, K2 0, K3 1, K4 0, K5 0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 150
Automatic network summarization is in effect
Routing for Networks:
10.0.0.0/16
Routing Information Sources:
Gateway Distance Last Update
10.10.200.1 90 00:00:27
Distance: internal 90 external 170
```

The **show ip route** command for RouterB shows that six routes are on RouterB, and there are EIGRP routes to the 10.10.20.0 and 10.10.100.0 subnets:

```
RouterB# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C 10.10.1.0/24 is directly connected, FastEthernet0/1
L 10.10.1.250/32 is directly connected, FastEthernet0/1
C 10.10.10.0/24 is directly connected, FastEthernet0/0
C 10.10.10.250/32 is directly connected, FastEthernet0/0
D 10.10.20.0/24 [90/2195456] via 10.10.200.1, 00:00:09,
FastEthernet0/2
D 10.10.100.0/24 [90/2681856] via 10.10.200.1, 00:00:09,
FastEthernet0/2
C 10.10.150.0/24 is directly connected, FastEthernet0/3
L 10.10.150.1/32 is directly connected, FastEthernet0/3
C 10.10.200.0/24 is directly connected, FastEthernet0/2
L 10.10.200.2/32 is directly connected, FastEthernet0/2
```

The code for the EIGRP routes is **D**. Remember that the **C** code is for the subnets directly connected to the router.

A check of the IP routes on RouterA shows that RouterA and RouterB are exchanging routes with each other. RouterA now shows six subnets. Once again, **D** indicates the EIGRP routes, and **C** indicates the directly connected subnets:

```
RouterA# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
D 10.10.1.0/24 [90/2195456] via 10.10.200.2, 00:00:50, FastEthernet0/1
```

```
D 10.10.10.0/24 [90/2195456] via 10.10.200.2, 00:00:50,
FastEthernet0/1
C 10.10.20.0/24 is directly connected, FastEthernet0/0
L 10.10.20.250/32 is directly connected, FastEthernet0/0
C 10.10.100.0/24 is directly connected, FastEthernet0/2
L 10.10.100.1/32 is directly connected, FastEthernet0/2
D 10.10.150.0/24 [90/2681856] via 10.10.200.2, 00:00:50,
FastEthernet0/1
C 10.10.200.0/24 is directly connected, FastEthernet0/1
L 10.10.200.1/32 is directly connected, FastEthernet0/1
```

The last step is to configure EIGRP for RouterC by using the **router eigrp 150** command. You use the command **network 10.10.0.0** to instruct the router to assign EIGRP to all interfaces that are under the 10.10.0.0 network:

```
RouterC(config)# router eigrp 150
RouterC(config-router)# network 10.10.0.0
```

In this case, all interfaces on RouterC have a 10.10.*x.x* address and therefore will run EIGRP.

Next, you use the **sh ip route** command to display the IP routes for RouterC:

```
RouterC# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C 10.10.5.0/24 is directly connected, FastEthernet0/0
L 10.10.5.250/32 is directly connected, FastEthernet0/0
D 10.10.10.0/24 [90/2195456] via 10.10.150.1, 00:00:01,
FastEthernet0/1
D 10.10.1.0/24 [90/2195456] via 10.10.150.1, 00:00:01, FastEthernet0/1
D 10.10.20.0/24 [90/2195456] via 10.10.100.1, 00:00:01,
FastEthernet0/2
C 10.10.100.0/24 is directly connected, FastEthernet0/2
L 10.10.100.2/32 is directly connected, FastEthernet0/2
C 10.10.150.0/24 is directly connected, FastEthernet0/1
L 10.10.150.2/32 is directly connected, FastEthernet0/1
D 10.10.200.0/24 [90/2681856] via 10.10.150.1, 00:00:01,
FastEthernet0/1
[90/2681856] via 10.10.100.1, 00:00:01, FastEthernet0/2
```

RouterC shows seven subnets. In fact, there are seven subnets in the campus LAN shown in Figure 9-12. The setup for running EIGRP on the campus LAN is now complete.

Networking Challenge: EIGRP

Use the Net-Challenge software to demonstrate that you can configure EIGRP for RouterA in the campus LAN shown in Figure 9-12 and displayed on the computer screen when the software is started. EIGRP has already been configured for RouterB and RouterC. In Net-Challenge, click the **Select Router Challenge** button to open the Select Router Challenge drop-down menu and select **EIGRP** to open a check box list that can be used to verify that you have completed all the tasks. Then follow these steps:

1. Enter privileged EXEC mode on the router.
2. Enter the router configuration mode, **Router(config)**.
3. Set the hostname to **RouterA**.
4. Configure the FastEthernet0/0 interface as follows:
   - **IP address:** 10.10.20.250
   - **Subnet mask:** 255.255.255.0
5. Enable the FA0/0 interface.
6. Configure the FastEthernet0/1 interface as follows:
   - **IP address:** 10.10.200.1
   - **Subnet mask:** 255.255.255.0
7. Enable the FA0/1 interface.
8. Configure the FastEthernet0/2 interface as follows:
   - **IP address:** 10.10.100.1
   - **Subnet mask:** 255.255.255.0
9. Enable the FA0/2 interface.
10. Enable EIGRP with ASN **200**.
11. Enter the **network** command to enable EIGRP on the router.
12. Use the **show ip int brief** command to check the interface status.
13. Use the **show ip protocol** command to see whether EIGRP is running on RouterA.
14. Use the **show ip route** command to verify that the three FastEthernet ports are connected to RouterA.
15. Use the **show run** command to view the running configuration file on RouterA. Verify that EIGRP is enabled and the proper network address is specified.

Section 9-8 Review

This section covers the following Network+ exam objectives.

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

This section mentions Reliable Transport Protocol, which enables EIGRP to guarantee delivery of EIGRP packets to neighbor routers. Both unicast and multicast packet transmission are supported.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

This section introduces the advanced distance vector routing protocol EIGRP. This protocol incorporates the best of distance vector and link state algorithms.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section mentions the Neighbor Discovery/Recovery process, in which EIGRP learns about other routers on directly attached networks and can also discover whether neighbor routers are unreachable.

Test Your Knowledge

1. EIGRP is classified as which of the following?
   a. Link state protocol
   b. Distance vector protocol
   c. Advanced distance vector routing protocol
   d. All of these answers are correct.
2. When is route information with EIGRP routes exchanged?
   a. Every 90 seconds
   b. Every 300 seconds
   c. When there is a change in the network
   d. When IP addresses are reconfigured

9-9 INTERNET ROUTING WITH BORDER GATEWAY PROTOCOL (BGP)

The objective of this section is to examine Internet routing using the BGP routing protocol. Students might need to review the concept of routing protocols. If a customer has more than one Internet connection, BGP is used for Internet routing. Make sure students understand the concepts multihomed customer and stubby area.

This section examines routing issues for WAN and Internet routing. WAN connections typically link remote sites and branch offices to a main network. Internet connections are usually between an Internet service provider (ISP) and its customers. Typically, the ISP and its customers do not use routing protocols such as OSPF for the Internet connection because these protocols do not scale well to this type of implementation. Instead, the two main routing options that are used for making the Internet connection to the ISP are static routes and Border Gateway Protocol (BGP).

Static routes are implemented in the same fashion as discussed in Section 9-2. Static routes are used only when the customer has a single Internet connection. If the customer is multihomed—that is, if the customer has more than one Internet connection—BGP is used. The most current version of BGP is version 4.

BGP is considered an external routing protocol and is designed for routing between separate organizational networks. The BGP term for such a network is *autonomous system* (*AS*). An AS is assigned an *AS number* (*ASN*) by the same organization that assigns IP addresses in North America, ARIN. An ASN is used with BGP to distinguish separate networks and to prevent routing loops. A set of ASNs are reserved for private use. These numbers, 64512 through 65535, are not to be propagated to the Internet. It is a best practice for an ISP to remove all of the private ASs before advertising BGP routes. The public ASNs are within the range 1 to 64511. The configurations in this section use private ASNs.

Each router participating in BGP must manually make a peering with its BGP neighbor. *Peering* is an agreement made for the exchange of data traffic between large and small ISPs or, as in this case, between a router and its neighbor router. The agreement on peering is how different networks are joined to form the Internet. BGP uses TCP as its transport protocol to establish peering and to exchange messages and routes. The network administrator configuring the Internet connection must know the remote IP address and ASN to make this peering. An AS path is created when a network is connected.

Configuring BGP

This section demonstrates how to configure a router to run BGP for connecting to an ISP. First, the ISP router must be configured. The ISP in this example has been assigned the ASN 65000. (*Note:* This is actually a private ASN. In practice, an ISP is assigned a public ASN.) The ASN is used when entering the command for BGP. In this example, the command **router bgp 65000** is entered, and the command **network 10.20.20.0 mask 255.255.255.0** follows, to instruct the router to advertise the 10.20.20.0/24 network to its BGP peers:

```
Router-ISP(config)# router bgp 65000
Router-ISP(config-router)# network 10.20.20.0 mask 255.255.255.0
```

There are three ways to originate network prefixes or network routes in BGP:

- Via the network statement, as shown in this example
- Using the **aggregate-address** command to combine contiguous network prefixes
- Using the **redistribute** command to redistribute IGP routes into BGP

The next command is for specifying the IP address of the BGP neighbor. This is the IP address of the interface on the customer's router (RouterB) that is directly connected to the ISP router. The format for the command is **neighbor [***ip address***] remote ASN [***neighbor's ASN***]**. The last command is for entering a description of the entries. The comment **neighbor 192.168.1.2 description Customer BGP** is used to document the router configuration for the neighbor IP address for the customer and that the routing protocol is BGP:

```
Router-ISP(config-router)# neighbor 192.168.1.2 remote-as 65001
Router-ISP(config-router)# neighbor 192.168.1.2 description Customer
B BGP
```

The next example demonstrates the steps for configuring the customer's router (RouterB). The customer has been assigned the ASN 65001. In this example, the command **router bgp 65001** is entered:

```
RouterB(config)# router bgp 65001
```

The 10.10.10.0/24 network is a network for CustomerB. The command **network 10.10.10.0 mask 255.255.255.0** follows:

```
RouterB(config-router)# network 10.10.10.0 mask 255.255.255.0
```

The next command is for specifying the IP address of the BGP neighbor:

```
RouterB(config-router)# neighbor 192.168.1.1 remote-as 65000
```

This is the IP address of the interface on the ISP's router. The last command, **neighbor 192.168.1.1 descr ISP BGP**, identifies the neighbor IP address (the ISP) and comments that the routing protocol is BGP:

```
RouterB(config-router)# neighbor 192.168.1.1 descr ISP BGP
```

To verify that the routers are connected via BGP, you can use the command **sh ip bgp sum** to see whether the routers are exchanging routes:

```
RouterB# sh ip bgp sum
BGP router identifier 192.168.1.2, local AS number 65001
BGP table version is 1, main routing table version 1
1 network entries using 101 bytes of memory
1 path entries using 48 bytes of memory
1 BGP path attribute entries using 60 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
```

```
BGP using 209 total bytes of memory
BGP activity 17/16 prefixes, 17/16 paths, scan interval 60 secs
Neighbor        V    AS         MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
192.168.1.1     4 65000   41       34        0       0    0
00:00:21   1
```

You can use the **sh ip route** command to display BGP routes received from the neighbor:

```
RouterB# sh ip route
Codes: C  connected, S  static, I  IGRP, R  RIP, M  mobile, B  BGP D
EIGRP, EX  EIGRP external, O  OSPF, IA  OSPF inter area
N1  OSPF NSSA external type 1, N2  OSPF NSSA external type 2
E1  OSPF external type 1, E2  OSPF external type 2, E  EGP
i  IS-IS, L1  IS-IS level-1, L2  IS-IS level-2, *  candidate default
U  per-user static route, o  ODR T  traffic engineered route
Gateway of last resort is not set
     10.0.0.0/24 is subnetted, 2 subnets
B       10.20.20.0 [20/0] via 192.168.1.1, 00:03:56
C       10.10.10.0 is directly connected, FastEthernet0/0
192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, serial0/1
```

This example shows that network 10.20.20.0 is a BGP(B) route advertised via 192.168.1.1. The 192.168.1.0 network is directly attached to the ISP's router.

Section 9-9 Review

This section covers the following Network+ exam objectives.

1.8 Summarize cloud concepts and connectivity options.

This section presents the concept of privates ASNs.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

This section examines Internet routing with BGP.

5.5 Given a scenario, troubleshoot general networking issues.

This section mentions that the ASN in BGP is used to distinguish separate networks and to prevent routing loops.

Test Your Knowledge

1. A multihomed customer has which of the following?
   a. A single Internet connection
   b. More than one Internet connection
   c. Static routes
   d. None of these answers are correct.

2. BGP is considered to be which of the following?

   a. An external routing protocol
   b. An internal routing protocol
   c. Used for routing between the same network
   d. Outdated

9-10 IPV6 ROUTING

This section takes a look at the concept of IPv6 routing with RIP, OSPF, EIGRP, and BGP. The routing protocols for IPv6 work the same way as the routing protocols for IPv4. Have students review IPv6 addressing concepts (refer to Chapter 6) before starting this section of the chapter.

When you interconnect IPv6 networks, you need a routing protocol. IPv6 supports static, RIP, OSPF, EIGRP, and BGP routing, as well as other routing protocols. Most of these protocols had to be revised to be able to deal with IPv6 addresses. However, the routing protocols for IPv6 work the same way as the routing protocols for IPv4. In fact, they still maintain the same routing principles. The following sections demonstrate how to configure IPv6 static, RIP, OSPF, EIGRP, and BGP routing.

IPv6 Static Routing

The techniques for configuring static routing with IPv6 are almost the same as the techniques for configuring static routing with IPv4. With IPv4, you can specify the next hop IP address or/and the exit interface. With IPv6, there is an extra feature: With IPb6, the next hop IP address can be either the link-local address or the global address. The following examples show how to configure an IPv6 static route using these three different methods:

```
Router# conf t
Router(config)# ipv6 route 2001:0db8:BEEF::/32 FA1/0
Router(config)# ipv6 route 2001:0db8:BEEF::/32 FA1/0 fe80::2
Router(config)# ipv6 route 2001:0db8:BEEF::/32 2001:0db8:FEED::1
Router(config)#
```

The first static route shows that the route to the network 2001:0db8:BEEF::/32 is configured via interface FastEthernet1/0. The second static route gives an option of the link-local next hop address, which is specified with the **fe80** prefix. The third static entry shows a route to the network that points to the global IPv6 address 2001:0db8:FEED::1.

RIP for IPv6

RIP routing using IPv6 requires the use of a RIP version called Routing Information Protocol Next Generation (**RIPng**). RIPng has the same basic features as RIPv2. For example, it is a distance vector protocol, and there is a maximum hop

RIPng
Routing Information Protocol Next Generation, a protocol used for RIP routing using IPv6

limitation. However, RIPng has been updated to use IPv6 for transport. Also, RIPng uses the IPv6 multicast address FF02::9 for all RIP updates.

Configuring RIPng on Cisco routers is simple. The biggest difference between configuring RIPv2 and RIPng on Cisco routers is that RIPng must be configured on a per-network-link or per-interface basis rather than on a per-network basis, as is the case with RIPv2. The following examples demonstrate how to enable RIPng and how to configure RIPng on a Cisco router interface:

```
Router# conf t
Router(config)#
Router(config)# ipv6 router rip RIP100
Router(config)#
Router(config)# int Gig3/1
Router(config-if)# ipv6 rip RIP100 enable
```

[*rip_tag*]
A tag that is used to identify the RIP process

The command **ipv6 router rip** [*rip_tag*], where **[rip_tag]** is a tag that identifies the RIP process, enables RIPng on Cisco routers. For example, you can enable RIPng on the GigabitEthernet3/1 interface with the command **ipv6 rip** [*rip_tag*] **enable**. The same command is used to enable other RIP interfaces. In contrast, when configuring RIPv2, the network statement needs to be issued for every RIP network.

OSPF for IPv6

The current OSPF version used in IPv4 is OSPFv2. Most OSPF information relies heavily on the IP number—for example, the router ID and the link state ID. In order to support IPv6, the OSPF routing protocol has been significantly revamped. The new OSPF version for IPv6 is **OSPFv3**. The basic foundation of OSPF remains intact. For example, OSPFv3 is still a link state routing protocol. However, OSPFv3 uses the IPv6 link-local multicast addresses FF02::5 for all OSPF routers running in the same network.

OSPFv3
Open Shortest Path First version 3, the new OSPF version for IPv6

OSPFv3 is now enabled on a per-link basis rather than on a per-network basis on Cisco routers. (This is similar to the changes in RIPng.) OSPFv3 identifies which networks are attached to the link and propagates them into the OSPF area. The following examples demonstrate how to enable OSPFv3 and how to configure OSPFv3 on a Cisco router interface:

```
Router# conf t
Router(config)#
Router(config)# ipv6  router ospf 99
Router(config-rt)# router-id 9.9.9.9
Router(config)#
Router(config)# int Gig3/1
Router(config-if)# ipv6 ospf 99 area 0.0.0.0
```

The command **ipv6 router ospf** [*process_id*] enables OSPFv3 on Cisco routers. **router-id** is needed to establish OSPF adjacency in the IPv6 environment. OSPFv3 is enabled on the GigabitEthernet3/1 interface with the command **ipv6 ospf** [*process_id*] **area** [*area_id*]. The same command is used to enable other OSPF

interfaces. The router in this example is configured to be area 0, which is the backbone (area 0.0.0.0).

EIGRP for IPv6

EIGRP is inherently a multiprotocol routing protocol. It was designed to support non-IP protocols such as IPX and AppleTalk, and it supports both IPv4 and IPv6. EIGRP for IPv6 uses the IPv6 link-local multicast addresses FF02::A for all EIGRP hello packets and updates.

EIGRP for IPv6 is configured over a network link, so there is no need to configure a network statement, as with EIGRP for IPv4. The following examples demonstrate how to enable EIGRP for IPv6 and how to configure it on a Cisco router interface:

```
Router# conf t
Router(config)#
Router(config)# ipv6 router eigrp 999
Router(config-rtr)# eigrp router-id 9.9.9.9
Router(config-rtr)# no shut
Router(config)# int Gig3/1
Router(config-if)# ipv6 eigrp 999
```

The command **ipv6 router eigrp** [*as_number*] enables EIGRP on Cisco routers. Much as with OSPF, **eigrp router-id** is needed. EIGRP for IPv6 is in shutdown mode by default. The command **no shut** is issued to ensure that EIGRP is enabled. Next, EIGRP for IPv6 is enabled on the GigabitEthernet3/1 interface with the command **ipv6 eigrp** [*as_number*]. The network link is now part of the EIGRP routing network.

BGP for IPv6

Internet routing—with both IPv4 and IPv6—is dominated by the BGP routing protocol. The current version of BGP that is used by IPv4 is BGP4. The multiprotocol BGP extensions, or BGP4+, allows BGP4 to be used for IPv6. BGP4+ for IPv6 supports the same features and functionality as IPv4 BGP and also provides additional support for the IPv6 address family and the IPv6 address for the BGP next hop.

The steps to configure IPv6 BGP on Cisco routers are similar to the steps used with IPv4. The first step is to configure the interface on the router that will run IPv6. The next hop IPv6 address or its IPv6 BGP peer must be reachable by the router. You configure the router BGP process by issuing the command **router bgp** [*AS_Number*]. (This is not required if a BGP process already exists for IPv4, since the same BGP process will be used.)

You use the **no bgp default ipv4-unicast** command to allow protocols other than IPv4 to be activated within multiprotocol BGP (BGP4+). By default, only the IPv4 unicast is enabled. Next, you specify an IPv6 peer by using the command **neighbor** [*IPv6_address*] **remote as** [*AS_Number*]. With BGP4+, you specify a protocol by using the command **address-family**, which indicates that IPv6 is selected. Specifically, for IPv6, you use the command **address-family ipv6**.

Within the address family group, the BGP peering with the neighbor can be established using the command **neighbor [***IPv6_address***] activate**. Also, inside the same group, you must specify the IPv6 networks that will be advertised to the peer with the command **network [***IPv6_network***]**. The following example shows a sample configuration of the IPv6 section of a Cisco router:

```
router bgp 65203
 no bgp default ipv4-unicast
 neighbor 2001:DB8:1:128::2 remote-as 65200
 neighbor 2001:DB8:1:128::2 description ISP
!
 address-family ipv6
  neighbor 2001:DB8:1:128::2 activate
  neighbor 2001:DB8:1:128::2 soft-reconfiguration inbound
  network 2001:D00::/32
 exit-address-family
!
```

This section shows how to configure static, RIP, OSPF, EIGRP, and BGP routing for IPv6. As you have seen, the steps are very similar to those for configuring routing for IPv4.

Section 9-10 Review

This section covers the following Network+ exam objectives.

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

This section looks at IPv6 routing with RIP, OSPF, EIGRP, and BGP. The routing protocols for IPv6 work the same way as the routing protocols with IPv4. In fact, they still maintain the same routing principles.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

This section presents the techniques for configuring static routing with IPv6. These techniques are almost the same as the techniques used with IPv4. However, in IPv4, you can specify the next hop IP address or/and the exit interface.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section states that OSPFv3 is a link state routing protocol, but it uses the IPv6 link-local multicast addresses FF02::5 for all OSPF routers running in the same network.

Test Your Knowledge

1. Which of the following types of routing does IPv6 support?
   a. Static
   b. RIP
   c. OSPF
   d. EIGRP routing
   e. All of these answers are correct.
2. What does the following command do?

```
Router(config)# ipv6 route 2001:0db8:BEEF::/32 FA1/0
```

   a. This is the IPv6 command for configuring a RIP route.
   b. This is the IPv6 command for configuring an OSPF route.
   c. This is the IPv6 command for configuring a static route.
   d. This is the IPv6 command for configuring an EIGRP route.
3. Which of the following commands is used to route EIGRP?
   a. Router(config)# **ipv6 eigrp route 999**
   b. Router(config)# **ipv6 router eigrp 999**
   c. Router(config) **ipv6 router eigrp 999**
   d. Router(config) **ipv6 route eigrp 999**

SUMMARY

This chapter shows how to configure static and dynamic routing protocols. No matter what type of routing protocol is used, you must remember that routing is a bidirectional communication. When configuring a network route on a router, the reverse route has to be configured at the corresponding router. At the most basic level, all the routers involved in routing must use the same routing protocol in order to communicate and exchange routing information.

The networking challenges in this chapter provide opportunities to test your configuration skills prior to actually configuring a real router. You should be able to configure and verify operation of static, RIP, RIPv2, OSPF, and EIGRP routing for both IPv4 and IPv6.

QUESTIONS AND PROBLEMS

Section 9-2

1. What is a routing table?

   A list of IP addresses to which data traffic can be forwarded

2. What is the most common static route used in a host computer?

   The default gateway

3. What command is used to view a PC's routing table?

   netstat -r or **route print**

4. What is meant by a 0.0.0.0 network address entry with subnet mask 0.0.0.0 in a PC's routing table?

   It is the gateway of last resort for any IP address and any subnet mask.

5. What is the 127.0.0.1 IP address, and what is it used for?

   It is the loopback, which loops data directly back to the source.

6. What is the router command to configure a static route from LAN A to LAN B for the network shown in Figure 9-13?

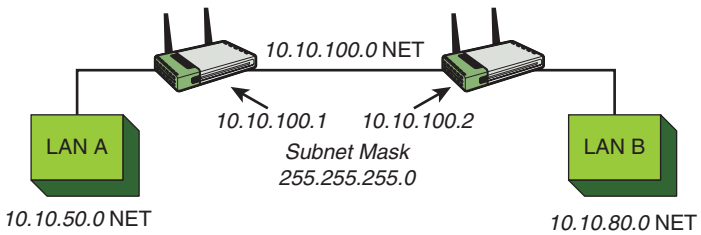


FIGURE 9-13 The network for question 6.

ip route 10.10.80.0 255.255.255.0 10.10.100.2

7. What is the difference between a router's running configuration and startup configuration?

   The startup configuration is stored in NVRAM, whereas the running configuration file is temporary.

8. What router command is used to view the routes entered in a router's routing table?

   show ip route

9. What router command is used to configure a static route for a router?

   ip route [*destination*] [*subnet mask*] [*next hop*]

10. List two static routes for routing data from LAN A to LAN C in the network shown in Figure 9-14, assuming the subnet mask 255.255.255.0.

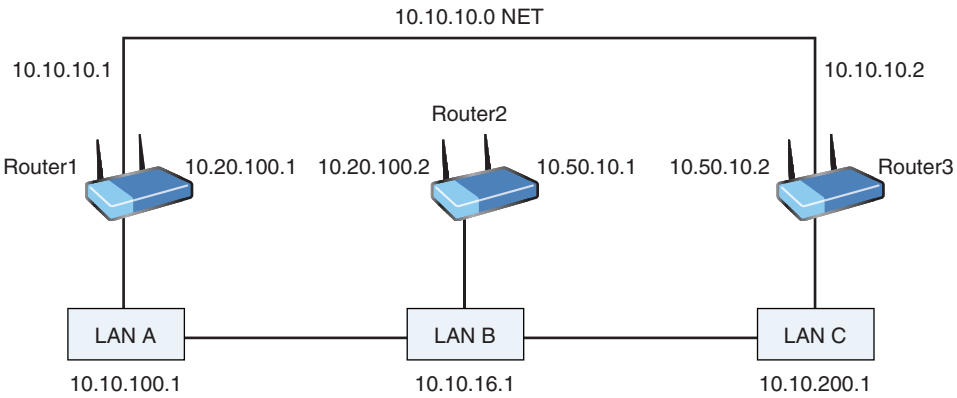


FIGURE 9-14 The network for questions 10 through 13.

   ip route 10.10.200.0 255.255.255.0 10.10.10.2

   ip route 10.10.200.0 255.255.255.0 10.20.100.2

11. List two static routes to route data from LAN B to LAN C in the network shown in Figure 9-14, assuming the subnet mask 255.255.255.0.

   ip route 10.10.200.0 255.255.255.0 10.50.10.2

   ip route 10.10.200.0 255.255.255.0 10.20.100.1

12. Which of the following are suitable subnet masks for use in configuring static routes for the network shown in Figure 9-14?

   a. 255.255.0.0
   b. 255.0.0.0
   c. 255.255.255.224
   d. All of these answers are correct.

13. A static route is configured to route data from LAN A to LAN B on Router1 in Figure 9-14. Which of the following are appropriate static routes to achieve this goal? (Select all that apply.)

    a. ip route 10.10.16.0 255.255.255.255 10.20.100.2

    b. ip route 10.10.16.0 255.255.255.0 10.20.100.2

    c. ip route 10.10.16.0 255.255.255.255 10.10.10.2

    d. ip route 10.10.16.0 255.255.255.0 10.10.10.2

Section 9-3

14. What is the difference between a *static* routing protocol and a *dynamic* routing protocol?

    Static means fixed routes. Dynamic means routing tables are dynamically updated to account for loss or changes in routes.

15. What are the four key issues in dynamic routing protocols?

    Path determination, metric, convergence, load balancing

16. Define *hop count*.

    The number of routers a data packet must pass through to reach the destination

17. Which of the following is *not* a metric used in dynamic routing protocols?

    a. Hop count

    b. Cost

    c. Runs

    d. Ticks

18. Determine the hop count for Router2 to subnet B in Figure 9-15.

    Subnet B is connected to Router2; therefore, the hop count is 0.

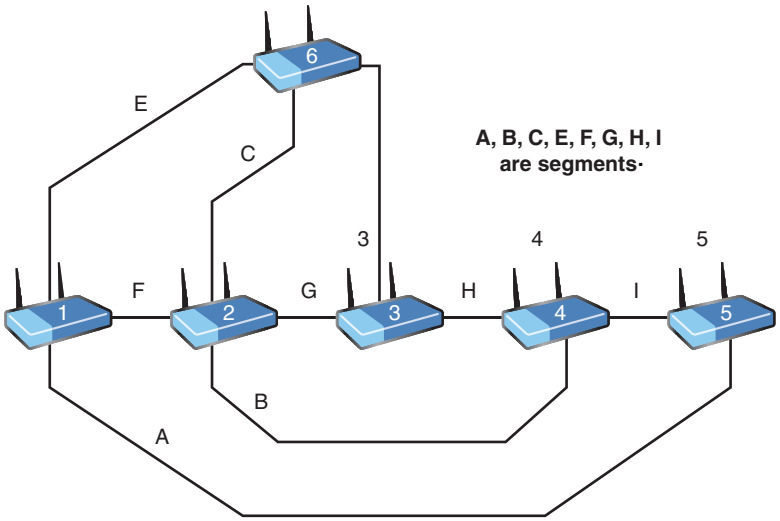


FIGURE 9-15 The network for questions 18 through 20.

19. For the network shown in Figure 9-15, what is the hop count from Router5 to subnet G?

    Hop count = 2

20. For the network shown in Figure 9-15, what is the hop count from Router3 to subnet A?

    Hop count = 2

21. What do link state protocols issue to update neighbor routers regarding route status?

    a. Hop status
    b. Link state advertisements
    c. Hello packets
    d. Adjacencies

22. Which of the following is a key feature of link state protocols?

    a. Sending updates every 90 seconds
    b. Sending update when routing changes
    c. Using link lights to establish adjacencies
    d. Using a hop count metric to determine the best route to a destination

Section 9-4

23. Define *routing loops*.

    A situation in which data is forwarded back to the router that sent the data packets

24. Which of the following is an example of a classful address?

    a. 10.10.0.0
    b. 172.0.0.0
    c. 10.1.0.0
    d. 10.0.0.0

25. All connected routes from a router have a distance, or hop count, of what value?

    0

26. In a distance vector protocol, the neighboring routers update their routing table based on what received information?

    a. The cost of each route
    b. The list of neighboring routers
    c. The hop count of each router
    d. All of these answers are correct.

27. RIP permits a maximum of 15 hops to prevent what?

    a. Routing metrics
    b. Router table exchanges
    c. Bandwidth issues
    d. Routing loops

Section 9-5

28. What is the router command to enable the RIP routing protocol on a router?

    a. config router RIP
    b. router rip
    c. rip 10.0.0.0
    d. network 10.0.0.0

29. What does it mean to *advertise* a network?

    It means the routing table containing the network is shared with the neighbor routers.

30. What commands do you use to enable RIP on an interface with IP address 192.168.10.250?

    router rip

    network 192.168.10.0

31. You use the command **show ip protocol** on a router to do which of the following?

    a. Display the routing protocol that can run on the router
    b. Display the IP address of the routers running IP
    c. Display the routing protocols running on the router
    d. None of these answers are correct.

32. The command **show ip interface brief** is used on a router to do which of the following?

    a. Check the current configuration of the interfaces
    b. Check the assigned IP addresses for the interface
    c. Check the status of the interfaces
    d. All these answers are correct.
    e. None of these answers are correct.

33. The command **show ip route** is used on a router to do which of the following? (Select all that apply.)

    a. Set a static route
    b. Configure a static route
    c. Display the configured routes on a router
    d. Display how often routing updates are sent

34. What command do you use to display a router's current running configuration?

    a. **show running-config**
    b. **show routing**
    c. **show interface**
    d. **show controller**

35. True or false: The network shown in Figure 9-16 is an example of a contiguous network.

    False

Section 9-6

36. Which of the following are true of OSPF? (Select all that apply.)

    a. It stands for Open Shortest Path First.
    b. It is an open protocol.
    c. It was developed specifically for TCP/IP networks.
    d. It was developed specifically for IPX networks.
    e. It is a distance vector protocol.

f. It is a dynamic routing protocol.

g. It is a link state protocol.

h. It consumes a lot of bandwidth.

37. In OSPF, route updates are sent in the form of which of the following?

a. Link state advertisements

b. Routing table exchanges every 30 seconds

c. Routing table exchanges every 90 seconds

d. IETF packets

38. The OSPF routing protocol uses which of the following to verify that a link between two routers is active and the routers are communicating?

a. LSAs

b. Hello packets

c. ARP messages

d. **ping**

39. Which of the following best defines how areas are used with OSPF?

a. Areas are not used.

b. Areas are used to partition a large network into small networks.

c. Areas are used to combine small networks into one large network.

d. Areas are an inefficient use of bandwidth.

40. Which of the following best characterizes variable-length subnet masks?

a. They minimize wasted IP address space when interconnecting subnets.

b. They are not recommended in modern computer networks.

c. They reduce the number of bits required in a subnet mask from 32 to 24.

d. They are used for classful addressing.

41. Which of the following is *not* an advantage of OSPF?

a. It is very easy to implement.

b. It uses VLSM.

c. Link state changes are immediately reported.

d. It is not a proprietary protocol.

42. Define *route flapping*.

A situation in which intermittent routes go up and down, creating excessive LSA updates

Section 9-7

43. Which of the following is true of VLSM?

    a. It minimizes wasted IP address space when interconnecting subnets.
    b. It is not recommended in modern computer networks.
    c. It reduces the number of bits required in a subnet mask from 32 to 24.
    d. It is the same as classful addressing.

44. Which of the following is the command syntax for enabling OSPF routing on a router?

    a. **router ospf**
    b. **router ospf** [*area*]
    c. **routing protocol ospf**
    d. **router ospf** [*number*]

45. What is another name for wildcard bits?

    a. OSPF pass-through bits
    b. Area 0 selection bits
    c. Inverse mask bits
    d. Route selection bits

46. Area 0 is ____.

    a. used to hide data packets
    b. the root, or backbone, for a network
    c. the home of inverse mask bits
    d. the home of route selection bits

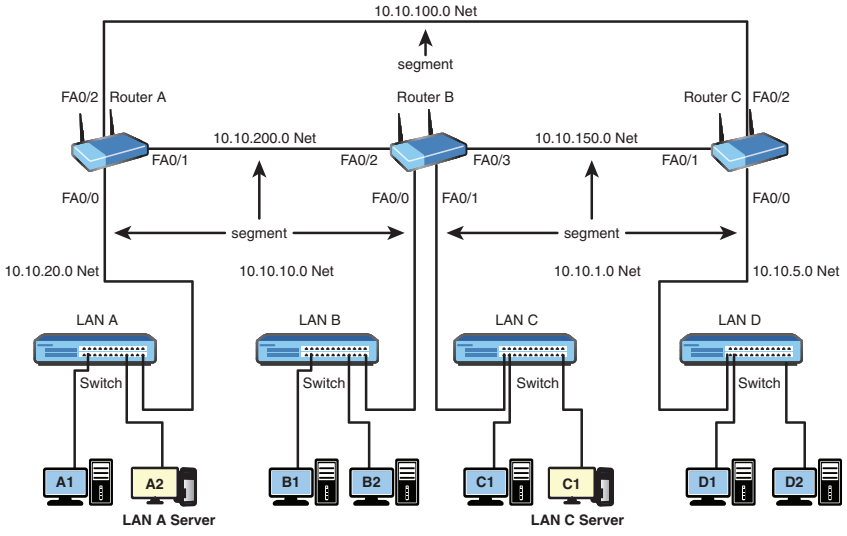
47. Assuming that OSPF has been enabled, which of the following is *not* used for configuring a route to run over OSPF?

    a. **network 10.10.20.0 0.0.0.127 area 0**
    b. **network 10.10.20.1 0.0.0.255 area 0**
    c. **network 10.0.0.0 0.0.255.255**
    d. **network 10.10.100.1 0.0.0.0 area 0**

48. The command **show ip route ospf** ____.

    a. is not valid with OSPF
    b. displays only IP routes
    c. displays only OSPF routes
    d. enables OSPF routing

49. The command **sh ip route** is entered on RouterB in the campus LAN shown in Figure 9-16. The LAN has been fully configured to run OSPF. How many OSPF subnets are running on the network? Identify the connected C and OSPF O subnets.



Router A Port Addresses (LAN A)	
FastEthernet 0/0 (Gateway Address)	10.10.20.250
FastEthernet 0/1	10.10.200.1
FastEthernet 0/2	10.10.100.1
LAN A Computers	
Computer A1	10.10.20.1
Computer A2	10.10.20.2
Subnet Mask	***255.255.255.0***

Router B Port Addresses (LAN B)	
FastEthernet 0/0 (Gateway Address)	10.10.10.250
FastEthernet 0/2	10.10.200.2
FastEthernet 0/3	10.10.150.1
LAN B Computers	
Computer B1	10.10.10.1
Computer B2	10.10.10.2
Subnet Mask	***255.255.255.0***

Router B Port Addresses (LAN C)	
FastEthernet 0/1 (Gateway Address)	10.10.1.250
FastEthernet 0/2	10.10.200.2
FastEthernet 0/3	10.10.150.1
LAN C Computers	
Computer C1	10.10.1.1
Computer C2	10.10.1.2
Subnet Mask	***255.255.255.0***

Router Port Addresses (LAN D)	
FastEthernet 0/0 (Gateway Address)	10.10.5.250
FastEthernet 0/1	10.10.150.2
FastEthernet 0/2	10.10.100.2
LAN D Computers	
Computer D1	10.10.5.1
Computer D2	10.10.5.2
Subnet Mask	***255.255.255.0***

FIGURE 9-16 Network topology for questions 49 and 50.

Seven subnets are running on the network.

The following output shows the connected C and OSPF O subnets:

```
RouterB# sh ip route
Codes: L - local, C - connected, S - static,
R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
```

```
ia - IS-IS inter area, * - candidate default,
U - per-user
static route
o - ODR, P - periodic downloaded static route,
H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is 10.10.200.1 to network 0.0.0.0
10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
O 10.10.5.0/24 [110/74] via 10.10.150.2, 01:15:22,
FastEthernet0/3
C 10.10.10.0/24 is directly connected, FastEthernet0/0
L 10.10.10.250/32 is directly connected, FastEthernet0/0
C 10.10.1.0/24 is directly connected, FastEthernet0/1
L 10.10.1.250/32 is directly connected, FastEthernet0/1
O 10.10.20.0/24 [110/74] via 10.10.200.1, 01:15:22,
FastEthernet0/2
O 10.10.100.0/24 [110/128] via 10.10.200.1, 01:15:22,
FastEthernet0/2
[110/128] via 10.10.150.2, 01:15:22, FastEthernet0/3
C 10.10.150.0/24 is directly connected, FastEthernet0/3
L 10.10.150.1/32 is directly connected, FastEthernet0/3
C 10.10.200.0/24 is directly connected, FastEthernet0/2
L 10.10.200.2/32 is directly connected, FastEthernet0/2
S* 0.0.0.0/0 [1/0] via 10.10.200.1
```

50. The **sh ip route** command is entered on Router C in the campus LAN shown in Figure 9-16. The LAN has been fully configured to run OSPF. How many OSPF subnets are running on the network? Identify the connected C and OSPF O subnets.

    Seven subnets are running on the network.

    The following output shows the connected C and OSPF O subnets:

```
RouterC# sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
ia - IS-IS inter area, * - candidate default, U - per-user
static route
```

```
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C 10.10.5.0/24 is directly connected, FastEthernet0/0
L 10.10.5.250/32 is directly connected, FastEthernet0/0
O 10.10.10.0/24 [110/74] via 10.10.150.1, 01:16:06,
FastEthernet0/1
O 10.10.1.0/24 [110/74] via 10.10.150.1, 01:16:06,
FastEthernet0/1
O 10.10.20.0/24 [110/74] via 10.10.100.1, 01:16:06,
FastEthernet0/2
C 10.10.100.0/24 is directly connected, FastEthernet0/2
L 10.10.100.2/32 is directly connected, FastEthernet0/2
C 10.10.150.0/24 is directly connected, FastEthernet0/1
L 10.10.150.2/32 is directly connected, FastEthernet0/1
O 10.10.200.0/24 [110/128] via 10.10.100.1, 01:16:06,
FastEthernet0/2
[110/128] via 10.10.150.1, 01:16:06,
FastEthernet0/1
```

Section 9-8

51. What does *EIGRP* stand for?

    a. Enhanced Interior Routing Protocol
    b. Enhanced Interior Gateway Routing Protocol
    c. Enhanced Internet Gateway Routing Protocol
    d. None of these answers are correct.

52. Why is it beneficial to use VLSM?

    It helps conserve IP addresses.

53. What do routing protocols use to verify that a link from one router to another is active?

    Hello packets

54. What are the four components of EIGRP?

    Neighbor Discovery/Recovery, Reliable Transport Protocol, DUAL Finite State Machine, protocol-dependent modules

55. When are routing tables exchanged with EIGRP?

    Routing tables are exchanged when routes change.

56. What is the command for enabling EIGRP on a router?

    a. **router igrp [***as_number***]**
    b. **router eigrp**
    c. **router eigrp [***as_number***]**
    d. **router eigrp enable**

57. The command network 10.10.0.0 is entered on a router after EIGRP has been enabled. What does this mean?

    It means all interfaces on the router that have a 10.*x.x.x* address will participate in EIGRP.

58. What router command verifies whether EIGRP is running on a router?

    a. **show run**
    b. **show ip int brief**
    c. **show history**
    d. **show ip protocol**

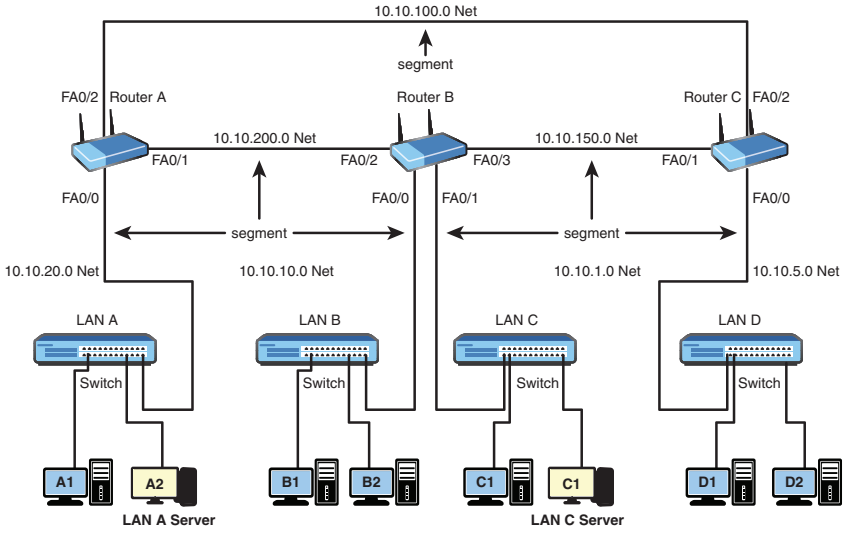
59. What router command shows how many subnets are configured?

    a. **show run**
    b. **show ip int brief**
    c. **show list**
    d. **show ip route**

60. What router command shows whether a router is exchanging routes?

    a. **show run**
    b. **show ip int brief**
    c. **show list**
    d. **show ip route**

61. The **sh ip route** command is entered on Router A in the campus LAN shown in Figure 9-17. The LAN has been fully configured to run EIGRP. How many EIGRP subnets are running on the network? Identify the connected C and EIGRP D subnets.



Router A Port Addresses (LAN A)	
FastEthernet 0/0 (Gateway Address)	10.10.20.250
FastEthernet 0/1	10.10.200.1
FastEthernet 0/2	10.10.100.1
LAN A Computers	
Computer A1	10.10.20.1
Computer A2	10.10.20.2
Subnet Mask	***255.255.255.0***

Router B Port Addresses (LAN B)	
FastEthernet 0/0 (Gateway Address)	10.10.10.250
FastEthernet 0/2	10.10.200.2
FastEthernet 0/3	10.10.150.1
LAN B Computers	
Computer B1	10.10.10.1
Computer B2	10.10.10.2
Subnet Mask	***255.255.255.0***

Router B Port Addresses (LAN C)	
FastEthernet 0/1 (Gateway Address)	10.10.1.250
FastEthernet 0/2	10.10.200.2
FastEthernet 0/3	10.10.150.1
LAN C Computers	
Computer C1	10.10.1.1
Computer C2	10.10.1.2
Subnet Mask	***255.255.255.0***

Router Port Addresses (LAN D)	
FastEthernet 0/0 (Gateway Address)	10.10.5.250
FastEthernet 0/1	10.10.150.2
FastEthernet 0/2	10.10.100.2
LAN D Computers	
Computer D1	10.10.5.1
Computer D2	10.10.5.2
Subnet Mask	***255.255.255.0***

FIGURE 9-17 Network topology for questions 61 and 62.

Seven subnets are running on the network.

The following output shows the connected C and EIGRP D subnets:

```
RouterA# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
default
U - per-user static route, o - ODR
T - traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 7 subnets
```

```
D 10.10.5.0 [90/2195456] via 10.10.100.2, 00:01:39, Serial0
D 10.10.10.0 [90/2195456] via 10.10.200.2, 00:01:38, Serial1
D 10.10.1.0 [90/2195456] via 10.10.200.2, 00:01:38, Serial1
C 10.10.20.0 is directly connected, Ethernet0
C 10.10.100.0 is directly connected, Serial0
D 10.10.150.0 [90/2681856] via 10.10.200.2, 00:01:39, Serial1
[90/2681856] via 10.10.100.2, 00:01:39, Serial0
C 10.10.200.0 is directly connected, Serial1
```

62. The **sh ip route** command is entered on RouterB in the campus LAN shown in Figure 9-17. The LAN has been fully configured to run EIGRP. How many EIGRP subnets are running on the network? Identify the connected C and EIGRP D subnets.

    Seven subnets are running on the network.

    The following output shows the connected C and EIGRP D subnets:

```
RouterB# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
default
U - per-user static route, o - ODR
T - traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 7 subnets
D 10.10.5.0 [90/2195456] via 10.10.150.2, 00:01:03, Ethernet3
C 10.10.10.0 is directly connected, Ethernet0
C 10.10.1.0 is directly connected, Ethernet1
D 10.10.20.0 [90/2195456] via 10.10.200.1, 00:01:02, Ethernet2
D 10.10.100.0 [90/2681856] via 10.10.200.1, 00:01:03, Ethernet2
[90/2681856] via 10.10.150.2, 00:01:03, Ethernet3
C 10.10.150.0 is directly connected, Ethernet3
C 10.10.200.0 is directly connected, Ethernet2
```

Section 9-9

63. What is the purpose of a wide area network connection?

    To link remote sites and branch offices to the main network.

64. What routing protocol is the easiest one to use for WAN links? What if there are multiple connections to the remote sites?

    Static routes are the easiest; in the case of multiple connections to the remote sites, a dynamic routing protocol such as OSPF or EIGRP should be used.

65. Define the following terms:

    a. Stubby area

    A stubby area is an area of a network that does not accept routes from the Internet.

    b. Totally stubby area

    A totally stubby area only uses a default route to reach destinations external to the autonomous system.

66. A multihomed customer has which of the following?

    a. A single Internet connection

    b. More than one Internet connection

    c. Static routes

    d. None of these answers are correct.

67. BGP is considered to be which of the following?

    a. An external routing protocol

    b. Used for routing between the same networks

    c. Used for routing between switches and routers on the same networks

    d. Outdated

68. Each router participating in BGP must manually make a peering with its BGP neighbor. What is peering?

    Peering is an agreement made for the exchange of data traffic between large and small ISPs or, as in this case, between a router and its neighbor router.

69. What are three ways to originate network prefixes or network routes in BGP? (Select three.)

    a. Via the network statement

    b. Using the **aggregate-address** command to combine contiguous network prefixes

    c. Using the **route all** command to connect to neighbors

    d. Using the **redistribute** command to redistribute IGP routes into BGP

70. Which of the following could be used for specifying the IP address of the BGP neighbor?

    a. RouterB(config-router)# **neighbor 192.168.1.1 remote-as 65000**

    b. RouterB(config)# **neighbor 192.168.1.1 remote-as 65000**

    c. RouterB(config-router)# **neighbor 192.168.1.1 remote 65000**

71. What command can be used to verify that routers are connected via BGP?

    sh ip bgp sum

72. What command is used to show BGP routes?

    sh ip route

Section 9-10

73. What does the following command show?

    ```
    Router(config)# ipv6 route 2001:0db8:ABCD::/32 FA0/0
    ```

    This command configures a static route to the network 2001:0db8:ABCD::/32 via the FA0/0 interface.

74. What command would you use to create a static route for 2001:0db8:1234::/32 that points to the global network 2001:0db8:ABCD::1?

    ```
    Router(config)# ipv6 route 2001:0db8:1234::/32 2001:0db8:ABCD::1
    ```

75. Show the command to create an IPv6 static route for 2001:0db8:1234::/32 from the FA0/0 interface that gives the link-local next hop address, specified with the fe80::1 prefix.

    ```
    Router(config)# ipv6 route 2001:0db8:1234::/32 FA0/0 fe80::1
    ```

76. What does RIPng stand for, and what is it used for?

    RIPng stands for Routing Information Protocol Next Generation, and it is required to support IPv6 routing.

77. What is the multicast address for RIPng?

    RIPng uses the IPv6 multicast address FF02::9 for all RIP updates.

78. What command enables RIPng on Cisco routers?

    ipv6 router rip [*rip_tag*]

79. What is the purpose of [*rip-tag*]?

    It is used to identify the RIP process.

80. What version of OSPF is used with IPv6?

    OSPFv3 is used with IPv6.

81. What are the IPv6 link-local multicast addresses for all OSPF?

    FF02::5 is used for all OSPF routers.

82. What command is used to configure OSPF routing for IPv6, using process ID 50?

    ```
    Router(config)# ipv6 router ospf 50
    ```

83. What does the following command do?

    ```
    Router(config-if)# ipv6 ospf 50 area 0.0.0.0
    ```

    It configures the router to be area 0, the backbone (area 0.0.0.0).

84. What is the IPv6 link-local multicast addresses for EIGRP? What is the link-local address used for in IPv6?

    The link-local multicast address for EIGRP is FF02::A. It is used for all EIGRP hello packets and updates.

85. What is the command for enabling EIGRP for IPv6, with AS 100 specified?

```
Router(config)# ipv6 router eigrp 100
```

Critical Thinking

86. Say that you are configuring a router connection to a remote network. What protocol would you select if there is only one network route to the remote network? Explain why you selected the protocol.

    Static routing is the best choice because there is only one route.

87. You are configuring the routing protocols for a small network. Which routing protocol would you select, and why?

    There are many suitable answers to this question. The decision should be based on economics, available networking staff, network equipment, and many other possible issues.

Certification Questions

88. Which subnets are connected to Router4 in Figure 9-15?

    a. A, G, D
    b. F, G, H, I
    c. H, I, B
    d. G, G, H

89. Which router command displays the number of subnets configured?

    a. **show run**
    b. **show ip int brief**
    c. **show list**
    d. **show ip route**

90. The command **show ip protocol** is used to do which of the following?

    a. Display the routing protocols that can run on the router
    b. Display the IP addresses of the routers running an IP protocol
    c. Display the routing protocols running on the router
    d. None of these answers are correct.

91. The command **show ip route** is used on a router to do what?

    a. Set a static route
    b. Configure a static route
    c. Display the configured routes
    d. Display how often routing updates are sent

92. Which router command displays the configured routes on a router?

    a. **show running-config**
    b. **show ip int brief**
    c. **show list**
    d. **show ip route**

93. What command is used to display a router's current running configuration?

    a. **show running-config**
    b. **show routing**
    c. **show interface**
    d. **show controller**
    e. **show config**

94. What is the router command for displaying the startup configuration?

    a. **show running-config**
    b. **show flash**
    c. **show history**
    d. **show startup-config**

95. What is the router command for enabling the RIP routing protocol on a router?

    a. **config router RIP**
    b. **router rip**
    c. **router rip [***area***]**
    d. **router rip [***AS number***]**

96. RIP is classified as which of the following? (Select two.)

    a. Distance vector protocol
    b. Dynamic routing protocol
    c. Link state protocol
    d. Multivendor protocol

97. True or false: All subnets connected to Router3 in the network shown in Figure 9-14 are:

    10.10.10.0

    10.50.10.0

    10.10.200.0

    True

98. True or false: Route flapping means intermediate routers are going up and down, creating excessive LSA updates.

    True

99. True or false: A computer with IP address 10.10.5.1 sends a data packet with destination IP address 10.10.5.20 using subnet mask 255.255.255.0. The packet stays in the LAN.

    True

100. True or false: A computer with IP address 10.10.5.1 sends a data packet with destination IP address 10.5.10.10 and subnet mask 255.0.0.0. The packet stays in the LAN.

    True

101. A router has three network routes to a destination. The routing protocols used for the paths are OSPF, EIGRP, and RIP. Based on administrative distance, what is the routing protocol with the smallest default distance value?

    EIGRP

This page intentionally left blank

10
CHAPTER

Managing the Network Infrastructure

Chapter Outline

10-1 Introduction
10-2 Domain Name and IP Address Assignment
10-3 IP Address Management with DHCP
10-4 Scaling a Network with NAT and PAT
10-5 Domain Name System (DNS)
10-6 Network Management Protocols
10-7 Analyzing Network Traffic
10-8 Network Analyzer: Wireshark
10-9 Analyzing Computer Networks: FTP Data Packets
10-10 Troubleshooting IP Networks
Summary
Questions and Problems

Objectives

- Describe the purpose of a remote access server
- Describe Metro Ethernet and Carrier Ethernet and related services types
- Describe the purpose of DHCP and DNS network services
- Discuss Internet routing with BGP
- Describe Internet data traffic

Key Terms

wide area network (WAN)
IANA
gTLD
ccTLD
.int
in-addr.arpa
RIR
AS
ICANN
ARIN
domain registrar
BOOTP
DHCP
lease time
DHCP Discover
DHCP Offer
DHCP Request
DHCP ACK
DHCP Relay
ipconfig /release
ipconfig /renew
APIPA
unicast
ip helper
MT Discover
MT Offer
MT Request
MT ACK
SOHO
NOC
NAT
PAT
DNS
forward DNS lookup (forward lookup)
reverse DNS lookup (reverse lookup)
TLD
country domain
root DNS servers
RR
nslookup and **dig**
SOA
A record (Address record)
PTR record (Pointer record)
CNAME record (Canonical Name record)
NS record (Name Server record)
MX record (Mail Exchange record)
TXT record (Text record)
SPF
DKIM
SRV record (Service record)
AAAA record (Quad-A record)
IPAM (IP address management)
SNMP (SNMPv1)
management information base (MIB)
SNMPv2
SNMPv3
outbound data traffic
inbound data traffic
Wireshark
Address Resolution Protocol (ARP)

Key Terms continued

ARP reply
echo request
FTP
SFTP
BYOD
IoT
smart device
bottom-to-top (or bottom-up) approach
top-to-bottom (or top-down) approach
divide-and-conquer approach
spot-the-difference approach
DHCP snooping

Wide Area Network (WAN)
A network that uses the telecommunications network to interconnect sites that are geographically distributed throughout a region, a country, or the world

This chapter examines concepts and technologies related to establishing **wide area network (WAN)** connections. WANs use the telecommunications network to interconnect sites that are geographically distributed throughout a region, a country, or even the world. Connections can include extensions of the campus LAN to remote members of the network. For example, the corporate office for a company could be located in one part of a state, and the engineering, manufacturing, and sales sites could be at different locations in the state. Figure 10-1 shows an example of a WAN, with connections for the Internet, a Frame Relay network, a virtual private network (VPN), and remote client access through a remote access server.

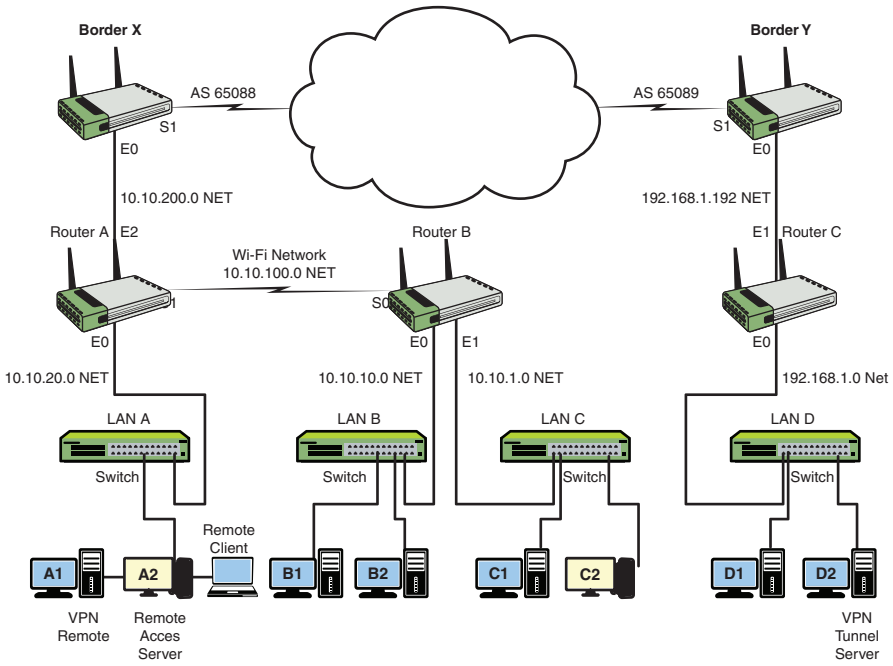


FIGURE 10-1 An example of a wide area network.

10-1 INTRODUCTION

Section 10-2, "Domain Name and IP Address Assignment," provides an introduction to configuring and managing the network infrastructure. This section also reviews the functions of IANA, which has been set up to be in charge of domain name management, number resources management, and protocol assignments. This section also looks at ARIN, which also assigns IP addresses.

Section 10-3, "IP Address Management with DHCP," examines how point-to-point dial-in connections are established using a phone modem, cable modem, Digital Subscriber Line (DSL) service, and other technologies.

Section 10-4, "Scaling a Network with NAT and PAT," describes the use of Ethernet as a WAN connection; this technology is called Metro Ethernet or Carrier Ethernet. Section 10-5, "Domain Name System (DNS)," provides a look at both the DHCP and DNS network services. Section 10-6, "Network Management Protocols," provides an overview of issues related to WAN routing and examines BGP, which is used for routing Internet data traffic. Section 10-7, "Analyzing Network Traffic," includes an example of using a network protocol analyzer to examine Internet data traffic entering and exiting a campus LAN. Section 10-8, "Network Analyzer: Wireshark," examines the use of the Wireshark network analyzer, which is a very important tool for managing traffic. Sections 10-9, "Analyzing Computer Networks: FTP Data Packets," explores the data packet contents of an FTP data transfer. The chapter concludes with Section 10-10, "Troubleshooting IP Networks," which looks at techniques and issues involved in troubleshooting modern computer networks.

Table 10-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 10-1 **Chapter 10 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.1	Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.	10-7
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes.	10-3, 10-4
1.5	Explain common ports and protocols, their application, and encrypted alternatives.	10-2, 10-3, 10-5, 10-8, 10-9
1.6	Explain the use and purpose of network services.	10-3, 10-5
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	10-8

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	10-6
4.0	**Network Security**	
4.3	Given a scenario, apply network hardening techniques.	10-10
5.0	**Network Troubleshooting**	
5.1	Explain the network troubleshooting methodology.	10-9, 10-10
5.3	Given a scenario, use the appropriate network software tools and commands.	10-6, 10-7, 10-8, 10-9, 10-10
5.5	Given a scenario, troubleshoot general networking issues.	10-10

10-2 DOMAIN NAME AND IP ADDRESS ASSIGNMENT

This section examines issues related to configuring and managing the network infrastructure. It introduces the steps required to obtain a domain name for a network and the steps required to get IP addresses assigned to the network.

IANA
Internet Assigned Numbers Authority, an organization that governs IP address assignment and Internet domain names

This section looks at configuring and managing the network infrastructure. The general population uses two key elements when accessing websites on the Internet: the Internet name of the website and the public IP address of that site. These two elements go hand in hand. People generally connect to Internet services via Internet hostnames (for example, www.example.com), but behind the scenes, the Internet name is translated to a public IP address. Both the IP address assignment and the Internet domain name are governed at the highest level by the Internet Assigned Numbers Authority (**IANA**).

gTLD
A generic (g) top-level domain

ccTLDs
A country-code (cc) top-level domain

.int
An intergovernmental domain registry

in-addr.arpa
The reverse DNS lookup for IPv4 addresses on the Internet

IANA, which is one of the Internet's oldest organizations, was set up to be in charge of the Internet management authorities or registration authorities. IANA has three primary functions:

- **Domain name management:** IANA manages the DNS root zone for the generic (g) top-level domains (**gTLDs**), such as .com, .net, .org, and .info, and country-code (cc) top-level domains (**ccTLDs**), such as .us, .uk, and .au. IANA maintains the **.int** (intergovernmental) domain registries, which are exclusive registrations for intergovernmental treaty organizations, such as United Nations (un.int) and NATO (nato.int). IANA maintains the .arpa domain registries, which include the in-addr.arpa domain. **in-addr.arpa** is the reverse DNS lookup for IPv4 addresses on the Internet. IANA also maintains the Repository of IDN (Internationalized Domain Name) Practices, which is known as the *language table registry*. This repository allows for domain name registration containing international characters (for example, müller.info).

- **Number resources management:** IANA coordinates the global pool of IP addresses, which include both IPv4 and IPv6 addresses. To coordinate the global effort of IP address allocation more effectively, IANA delegates the allocation to the regional Internet registries (**RIR**), each of which is responsible for a different area. The five RIRs accounting for the different regions of the world are as follows:
  - **AfriNIC:** Africa Region
  - **APNIC:** Asia/Pacific Region
  - **ARIN:** North America Region
  - **LACNIC:** Latin America and some Caribbean Islands
  - **RIPE NCC:** Europe, the Middle East, and Central Asia

  IANA is also responsible for allocation of **AS** (autonomous system) numbers, which are used with BGP to route Internet traffic. ASNs are allocated to the RIRs in the same manner as IP addresses.

RIR
Regional Internet registry, one of five organizations that are responsible for IP address allocation

AS
Autonomous system

- **Protocol assignment:** IANA is also responsible for maintaining the registries of protocol names and numbers used on the Internet today. IANA manages these protocol numbering systems in conjunction with standards bodies.

Today, IANA is working with support from the Internet Corporation for Assigned Names and Numbers (**ICANN**). IANA and ICANN do not directly allocate IP address space or register domain names for the general public. In North America, IP addresses are assigned by the American Registry for Internet Numbers (**ARIN**; https://www.arin.net). ARIN assigns IP address space to Internet service providers (ISPs) and end users that qualify by being large enough to merit a block of addresses.

When ARIN allocates a block of addresses to an ISP, the ISP then issues addresses to its customers. For example, an ISP called Telco might have a large block of IP addresses and issue one of them to a user. ARIN also assigns blocks of IP addresses to local ISPs that have large numbers of users.

ARIN also assigns end users' IP addresses. Once again, an end user must qualify to receive a block of addresses from ARIN, which usually means the end user must be large. For example, many universities and large businesses can receive blocks of IP addresses from ARIN. However, most end users get their IP addresses from an ISP (such as a telco) or have IP addresses assigned dynamically when they connect to the ISP.

ICANN
Internet Corporation for Assigned Names and Numbers

ARIN
American Registry for Internet Numbers, the North American organization that assigns IP addresses to ISPs and end users that are large enough to merit blocks of addresses

Today, available IPv4 address space is limited, and it is expected to be totally depleted within a few years. As a result, it has become increasingly difficult to acquire IPv4 space from ARIN. In fact, it is nearly impossible to acquire Class B IP space today. It is possible to buy a pool of IP addresses from an ISP, but the larger the IP range, the more expensive it is. There is good news, however: There are abundant IPv6 addresses available, and it is much easier to acquire IPv6 address space than to acquire IPv4 space. There is a big push by the Internet community to transition to IPv6.

Domain Registrar
An organization that has control over the granting of domains within certain top-level domains

An Internet hostname is a subset of an Internet domain name. For example, www.example.com is a web server for the domain example.com. The Internet domain name is the identity of the organization. The first step in obtaining an Internet domain name is to find a domain name registrar. The **domain registrar** has control over the granting of domains within certain top-level domains (TLDs). IANA and ICANN do not directly register domain names for the general public. ICANN delegates the TLD registry to other companies or organizations. A couple of the most notable TLD registrars are Educause, which is an organization operating the .edu TLD, and Verisign, which is a company authorized to operate the TLDs .com and .net. Verisign delegates the responsibilities further to other domain registrars, such as networksolutions.com, godaddy.com, and tucows.com.

An Internet domain can be purchased from any of these registrars. When you visit a registrar's website, you can input a domain name to have the registrar check whether that domain name is available. If the domain name is available, you are prompted to complete an application for the domain name and enter the DNS servers that are to be used to host the domain. The DNS servers will be assigned IP addresses and names. When the network's DNS servers are placed online, the root servers will point to the network's DNS servers. Those DNS servers then become the authoritative DNS servers for the domain.

The registration for both the IP address and the Internet domain name can be verified using the whois protocol in a Linux environment. The whois protocol queries databases that store user registration information for an Internet domain name and IP space. The whois information includes ownership information such as the point of contact. There are many whois servers that are accessible via a web interface, and all of them derive from the simple UNIX command **whois**, which is still available today. The following example shows the result of entering the **whois** command at a UNIX prompt for the domain example.com:

```
[admin@noc ~]$ whois example.com
Domain Name: EXAMPLE.COM
   Registry Domain ID: 2336799_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.iana.org
   Registrar URL: http://res-dom.iana.org
   Updated Date: 2020-08-14T07:02:37Z
   Creation Date: 1995-08-14T04:00:00Z
   Registry Expiry Date: 2021-08-13T04:00:00Z
   Registrar: RESERVED-Internet Assigned Numbers Authority
   Registrar IANA ID: 376
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: clientDeleteProhibited
https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited
https://icann.org/epp#clientUpdateProhibited
   Name Server: A.IANA-SERVERS.NET
   Name Server: B.IANA-SERVERS.NET

>>> Last update of whois database: 2021-05-24T03:59:37Z <<<
```

Section 10-2 Review

This section covers the following Network+ exam objective.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

This section introduces the Domain Name System (DNS).

Test Your Knowledge

1. The IP address assignment and the Internet domain name are governed at the highest level by what agency?

   IANA (Internet Assigned Numbers Authority)

2. What are the three functions of IANA?

   Domain name management, number resources management, and protocol assignment

10-3 IP ADDRESS MANAGEMENT WITH DHCP

This section examines the use of DHCP for assigning IP addresses in a network. It is important to ensure that students understand the purpose of a DHCP relay. This section examines DHCP packets to give students a better understanding of DHCP.

This section also reviews the hierarchy of DNS to help students understand how a name is translated to an IP address. This section looks at the top-level domain, the root servers, and the purpose of the A record. It also examines the steps for incorporating DNS service into a campus network.

An IP address is one of the most basic pieces of information needed for a computer to communicate on a network. An IP address can be either configured manually or assigned dynamically. In the manual process, a network administrator assigns an IP address to a user computer. Then either the administrator or the user has to configure the computer's network settings with the assigned IP address along with other network parameters, such as the subnet mask, default gateway, domain name, and domain name servers. This can be a tedious process, especially when it involves multiple machines.

BOOTP
Bootstrap Protocol, a protocol that enables a computer to discover its own IP address

The IP address assignment process can be automated to some extent by using a program called **BOOTP**. BOOTP, which stands for *Bootstrap Protocol*, enables a computer to discover its own IP address. When a client requests an IP address, it is assigned to the Ethernet address (MAC address) based on the BOOTP record. In this case, the IP and MAC addresses have a one-to-one relationship.

DHCP
Dynamic Host Configuration Protocol, a protocol that assigns a pool of IP addresses to requesting clients

Dynamic Host Configuration Protocol (**DHCP**) simplifies the steps for IP assignment even further. DHCP's function is to assign a pool of IP addresses to requesting clients. DHCP is a superset of BOOTP and runs on the same port numbers. In this process, DHCP requests an IP address from the DHCP server. The DHCP server retrieves an available IP address from a pool dedicated to the subnet of the

Lease Time
The amount of time that a client can hold an IP address

requesting client. The IP address is passed to the client, and the server specifies a length of time that the client can hold the address. This is called the **lease time**. This feature keeps an unused computer from unnecessarily tying up an IP address.

When a computer is configured to obtain an IP address automatically or to use the DHCP option, the process of requesting an IP address with DHCP is as follows:

DHCP Discover
A broadcast message that is sent to all computers in a LAN

DHCP Offer
A message sent by a DHCP server listening on the LAN takes the DHCP Discover message, retrieves an available IP address from the address pool, and sends the address to the client. This includes the lease time and other necessary network parameters, such as subnet mask, default gateway, and domain name server

DHCP Request
A message sent by a DHCP client to formally request and confirm the offered IP address with the server

DHCP ACK
A unicast packet sent back to a DHCP client with the same IP address information

1. The client boots up and sends out a **DHCP Discover** message. This is a broadcast, meaning that the message is sent to all computers in the LAN.
2. A DHCP server listening on the LAN takes the DHCP Discover message, retrieves an available IP address from the address pool, and sends the address to the client via a **DHCP Offer** message. The server sends the IP address, and the server sends the lease time and other necessary network parameters, such as subnet mask, default gateway, and domain name server.
3. The client receives the DHCP Offer message from the server and agrees to use the lease. It replies back to the server with a **DHCP Request** to formally request and confirm the offered IP with the server.
4. The server receives the DHCP Request message and sends back a **DHCP ACK** message, which is a unicast packet acknowledging the request of the IP address information.
5. The client applies the IP address and its network settings to the computer, and it is ready to make network connections.

Figure 10-2 provides an example of this process.

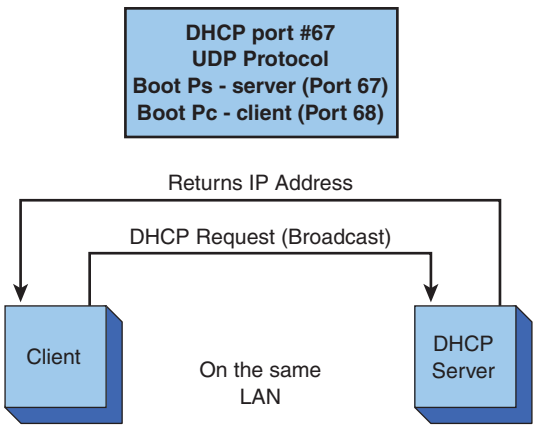


FIGURE 10-2 An example of a DHCP server and client in the same LAN.

ipconfig /release
A command used to release the current IP address

ipconfig /renew
A command used to initiate the DHCP process

When a computer boots up, its network software automatically engages in a DHCP process. This process can also be invoked by using the command line. In Windows, the command **ipconfig /release** can be used to release the current IP address, and the command **ipconfig /renew** can be used to initiate the DHCP process. But what happens if the DHCP server is not available? In a situation where a DHCP server

isn't available, the Windows operating system can automatically self-configure its IP address and subnet mask, through a process called Automatic Private IP Addressing (**APIPA**). APIPA uses the Class B IP address space 169.254.0.0/16, which ranges from 169.254.0.0 to 169.254.255.255. In addition, you can use an IP reservation to assign to a networking device an IP address that never changes.

APIPA
Automatic Private IP Addressing

What if a DHCP server is on the other side of the router (for example, not in the same LAN)? Remember that routers don't pass broadcast addresses, so the DHCP broadcast is not forwarded. This situation requires that a DHCP relay be used, as shown in Figure 10-3. The DHCP relay sits on the same LAN as the client. It listens for DHCP requests and then takes the broadcast packet and issues a packet to the network DHCP server. **Unicast** means that the packet is issued a fixed destination and therefore is not a broadcast packet. The DHCP relay puts its LAN address in the DHCP field so the DHCP server knows what subnet the request is coming from and can properly assign an IP address. The DHCP server retrieves an available IP address for the subnet and sends the address to the DHCP relay, which forwards it to the client.

Unicast
A transmission in which a packet has a fixed destination

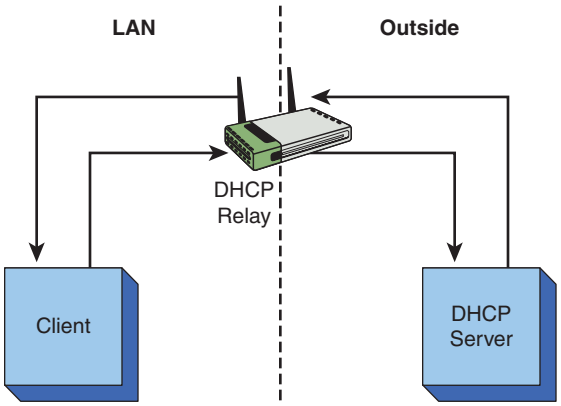


FIGURE 10-3 An example requiring the use of a DHCP relay.

A Cisco router has a DHCP relay built in to its operating system. **ip helper** is the router command you use to enable the DHCP relay:

ip helper
A router command that is used to enable a router's DHCP relay function

```
Router(config-if)# ip helper [ip address of the DHCP server]
```

Notice that this command is issued from the interface that connects to the LAN. In fact, this command can also be used to forward other User Datagram Protocol (UDP) protocols—such as TACACS, DNS, and NetBIOS—to a designated server.

DHCP is a UDP protocol and uses port 68 for the BOOTP client and port 67 for the BOOTP server. (Remember that BOOTP and DHCP use the same port numbers.) The BOOTP client is the user requesting the DHCP service. The BOOTP server is the DHCP server. The following section describes how these services are used in a DHCP request, where the DHCP proxy on the router listens for the packets that are going to DHCP or BOOTP port numbers.

The DHCP Data Packets

This section discusses the TCP packets transferred during a DHCP request. The examples in this section use the network setup shown in Figure 10-3. The data traffic in this example contains only the data packets seen by the client computer. Figure 10-4 shows the result of using a protocol analyzer to capture the data packets. In this example, Packet 10 is a DHCP request with message type discover (**MT Discover**). This is also called the DHCP Discover packet. The destination for the packet is a broadcast. The message source has MAC address Dell 09B956 and IP address 0.0.0.0. The IP address is shown in the middle panel, and *0.0.0.0* indicates that an IP address has not been assigned to the computer. The source and destination ports are shown in the third panel in Figure 10-4. The source port is 68, which is for the Bootstrap Protocol client (the computer requesting the IP address). The destination port is 67, the Bootstrap Protocol server (the DHCP server).

MT Discover
Message type discover, a DHCP Discover packet

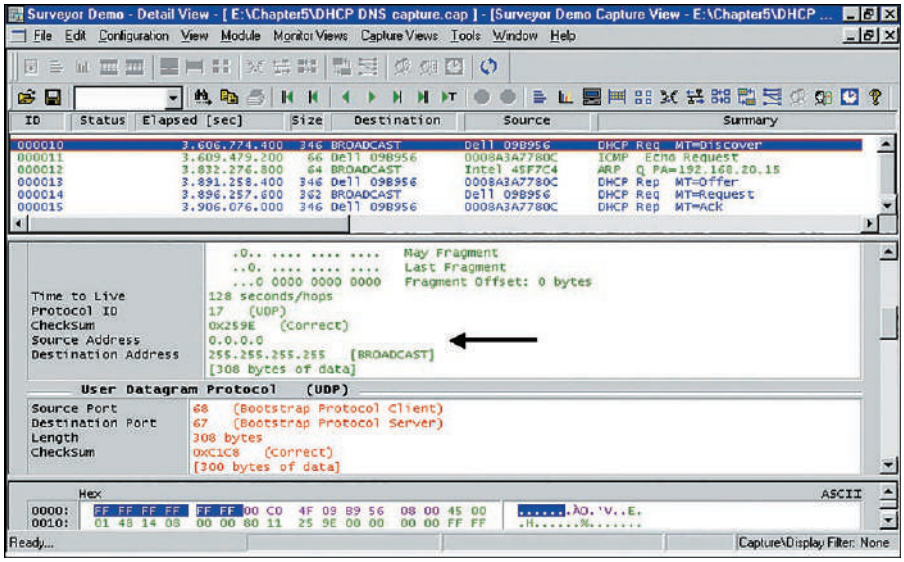


FIGURE 10-4 Captured DHCP packets.

MT Offer
Message type offer, a DHCP offer packet

MT Request
Message type request, a DHCP request packet

MT ACK
Message type acknowledgment, a DHCP ACK packet

Packet 13 is a reply from the DHCP server, an offer of the IP address to the client. This is called the DHCP Offer packet (**MT Offer**). This packet contains the domain name, the domain name server, the default gateway, and other network information the client may need to connect to the network. Packet 14 has message type **MT Request**. This packet is sent from the client back to the server that has been selected to provide the DHCP service. (Note that it is possible for a campus LAN to have more than one DHCP server answering the DHCP request.) The packet is sent through the DHCP relay to the DHCP server. This means the client is accepting the IP address offer. Packet 15 is message type acknowledgment (**MT ACK**). This message indicates that the DHCP server is acknowledging the client's acceptance of the IP address from the DHCP server. The client computer now has an IP address assigned to it.

DHCP Deployment

SOHO
Small office/home office

In a small office/home office (**SOHO**) environment, the network is typically small, and only one router is needed. In this kind of network, a router performs simple routing functions, acts as a gateway to the outside world, and manages IP assignment via DHCP. Most network routers are capable of running DHCP service, so it makes sense and is most cost-effective to deploy DHCP service at the router. The following example shows a Cisco router being configured to provide DHCP service:

```
RouterA# conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#
RouterA(config)# ip dhcp pool dhcp1pool
RouterA(dhcp-config)# network 172.20.224.0 255.255.255.0
```

The DHCP pool is configured with the command **ip dhcp** [*pool_name*]. Then, an IP network is defined as the IP address allocation pool. In this case, the IP addresses from 172.20.224.0 to 172.20.224.255 have been set aside for the address pool.

When the basic DHCP pool is set up, it is time to associate other network settings to it. The following example shows how to define the DNS server, domain name, and gateway to the DHCP pool:

```
RouterA(dhcp-config)# dns-server 172.20.224.8
RouterA(dhcp-config)# domain-name et477.com
RouterA(dhcp-config)# default-router 172.20.224.1
```

The subnet mask is already defined as part of the network.

Even though an entire Class C network is being configured for the DHCP network, a portion of it might be reserved for something else, like static IP machines and servers. The command **ip dhcp [***excluded-address***]** is used to exclude some IP addresses (called an *exclusion range*) from being allocated to the DHCP devices. In this example, the IP addresses from 172.20.224.0 to 172.20.224.20 are excluded, leaving the rest of network addresses available for DHCP allocation use:

```
RouterA(config)# ip dhcp excluded-address 172.20.224.0 172.20.224.20
```

To show the available leases, you use the command **show ip dhcp pool**:

```
RouterA# show ip dhcp pool
Pool dhcp1pool :
 Utilization mark (high/low): 100 / 0
 Subnet size (first/next): 0 / 0
 Total addresses: 254
 Leased addresses: 5
 Pending event : none
 1 subnet is currently in the pool:
 Current index IP address range Leased addresses
172.20.224.132   172.20.224.1 - 172.20.224.254    5
```

In larger and more complex environments where there are multiple networks and multiple routers, deploying DHCP service at the routers is not as simple. Having

NOC
Network operations center

to manage a different DHCP service for each network on multiple routers can be tedious, time-consuming, and inefficient. Such environments tend to use centralized DHCP service. This setup offers centralized management, which scales better and is easier to support. A typical setup involves running a DHCP service program on a centralized server. With centralized DHCP service, the IP address assignment is typically tracked by the network administrator or the network operations center (**NOC**). The tracking information can include more than the IP and MAC addresses; it can also include the user information. The information can be kept in a central log file or in the database so that the administrator can troubleshoot network problems. For example, a machine could be causing network problems possibly due to hacked or corrupted software. The NOC needs to be able to track down the network problem(s). The NOC database holds the MAC address, the IP address, and the name of the person who uses the computer.

In a large environment, DHCP pools are usually planned and preallocated. IP addresses are assigned by the NOC based on where the subnet for the computer is located. The subnet could be in a building, on a floor of a building, in a department, and so on. The subnets are created by network administrators based on the expected number of users (hosts) in a subnet (refer to Chapter 6, "TCP/IP"). For example, the 192.168.12.0 network shown in Figure 10-5 has been partitioned into four subnets. Table 10-2 shows the network addresses for each of the subnets. Any computer in subnet B is assigned one of the 62 IP addresses in the range 192.168.12.65 to 192.168.12.126.

Note

Remember that the first IP address in the subnet is reserved for the network address, and the last is reserved for the broadcast address.

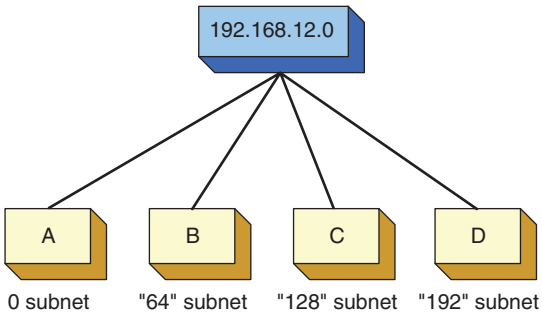


FIGURE 10-5 IP assignment of computers in a network's subnet.

TABLE 10-2 **Subnet Addresses for the Subnets Shown in Figure 10-5**

Subnet	Network Address	Broadcast Address
A	192.168.12.0	192.168.12.63
B	192.168.12.64	192.168.12.127
C	192.168.12.128	192.168.12.191
D	192.168.12.192	192.168.12.255

In a DHCP environment, a computer gets reassigned an IP address every time it reboots or renews its IP lease. There is no guarantee that it will have the same IP address as before. So, there is a common DHCP feature on most routers and DHCP servers called DHCP reservations or MAC address reservations, which reserves specific IP addresses for certain reserved MAC addresses. This guarantees that a device with a reserved MAC addresses will acquire the same IP address from the DHCP server every time. Of course, the same effect can also be accomplished by using a static IP address.

Section 10-3 Review

This section covers the following Network+ exam objectives.

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

This section introduces the concept of unicasts.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

This section examines the function of a DHCP server.

1.6 Explain the use and purpose of network services.

This section introduces lease time.

Test Your Knowledge

1. What is the purpose of BOOTP?

   It enables a computer to discover its own IP address.

2. What is lease time relative to IP addresses?

   The amount of time that a client can hold an IP address.

10-4 SCALING A NETWORK WITH NAT AND PAT

This section provides an overview of NAT and PAT. It introduces concepts such as static and dynamic NAT, local and global addresses, and NAT overload. This section describes the steps for configuring NAT and the use of the command **show ip nat translation**.

Today, there are more network devices than there are IP addresses available. Most institutions have to use private IP addresses in their networks. These private IP addresses cannot communicate with outside, or Internet, hosts because private IP addresses are not routable on the Internet. In order for these devices to communicate on the Internet, private IP addresses must be translated to public IP addresses using techniques like Network Address Translation and Port Address Translation.

Network Address Translation (NAT) is a technique used to translate an internal private IP address to a public IP address before a packet leaves a local network and moves into a public network. NAT is typically implemented and deployed at

Network Address Translation (NAT)
A technique used to translate an internal private IP address to a public IP address

the router facing the outside network. NAT provides a one-to-one translation of a private IP address to a public IP address. This means that, for every connection made to the outside world, there must be a public IP address available. The public IP address is relinquished when it is no longer used or when the NAT timeout occurs. In addition to being used as a way to communicate to the outside world, NAT can be used to hide the internal IP infrastructure of a network.

Port Address Translation (PAT)
A technique that translates many IP addresses into a single public IP address or a handful of public IP addresses

To address the limitations of NAT, **Port Address Translation (PAT)** was developed. PAT is sometimes referred to as *many-to-one NAT* or *NAT overload* because of its capability to translate many IP addresses with a single public IP address or a handful of public IP addresses. PAT accomplishes this by using the TCP/UDP ports. The PAT process tracks a port number for the connection. The router stores the IP address and port number in a NAT lookup table. The port number differentiates the computer that is establishing a connection to the Internet because the router uses the same public IP address for all computers. This port number is used when a data packet is returned to the home network. The port number identifies the computer that established the Internet connection, and the router can deliver the data packet to the correct computer.

For example, if computer 1 establishes a connection to a website on the Internet, the data packets from the website are sent back to computer 1 using the network's routable public IP address. This first step enables the data packet to be routed back to the home network. Next, the router uses the NAT lookup table and port number to translate the destination for the data packet back to the computer 1 private IP address and original port number, which might be different. Table 10-3 shows an example of a PAT table for a router. The router translates the private IP addresses to the public routable IP address assigned by the ISP. In addition, the router tracks a port number with the public IP address to identify the computer. For example, the computer with the private IP address 10.0.0.1 is assigned the public IP address 12.0.0.1:2000, where 2000 is the port number tracked by the router.

Note

The term NAT is used more commonly than PAT and, most times, it covers PAT.

TABLE 10-3 **Example of a Router's PAT Table**

Inside IP Address	Inside Port	Outside IP Address	Outside Port
10.0.0.1	2000	12.0.0.1	2000
10.0.0.2	3000	12.0.0.1	3000
10.0.0.2	30001	12.0.0.1	4000
10.0.0.3	3000	12.0.0.1	6000

Section 10-4 Review

This section covers the following Network+ exam objective.

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

This section describes NAT and PAT.

Test Your Knowledge

1. What does NAT stand for, and what does it do?

   NAT stands for Network Address Translation, which is a technique used to translate an internal private IP address to a public IP address.

2. What does PAT stand for, and what does it do?

   PAT stands for Port Address Translation (PAT). Its function is to translate many IP addresses with a single public IP address or a handful of public IP addresses.

10-5 DOMAIN NAME SYSTEM (DNS)

This section examines DNS, which runs on UDP and TCP port 53. There is a lot of information in this section, and students may have trouble comprehending various concepts such as record types.

This section examines the DNS services typically available in a campus network. **DNS**, which stands for the Domain Name System, translates a human-readable name to an IP address or an IP address to a domain name. The translation of a name to an IP address is called a **forward DNS lookup (forward lookup)**, and the translation of an IP address to a domain name is called a **reverse DNS lookup (reverse lookup)**. DNS runs on UDP and TCP port 53.

The DNS hierarchy is a tree hierarchy. It starts with the root, then the top-level domains (**TLDs**), and then subdomains. Root DNS servers are well-known IP addresses that have been programmed into DNS servers. When DNS is installed on a server, the root DNS server's IP addresses are automatically configured in DNS. The campus DNS server queries the root DNS servers to try to find TLD DNS servers. The next hierarchical level from the root is the TLD, such as .com, .net, .org, .edu, .mil, .gov, .us, .ca, .info, .biz, or .tv.

Country domains are also TLDs and are usually defined by two letters, such as .us (United States) and .ca (Canada). The primary DNS server for a country domain has to exist in that country; for example, the .us primary domain server is located in the United States. Figure 10-6 shows the top-level domains and their relationships to the subdomains and **root DNS servers**.

DNS
Domain Name System, the Internet's system for translating human-readable names to IP addresses and vice versa

Forward DNS Lookup (Forward Lookup)
Translation of a name to an IP address

Reverse DNS Lookup (Reverse Lookup)
Translation of an IP address to a name

TLD
Top-level domain

Country Domain
Usually two letters, such as .us (United States) or .ca (Canada), that indicate the domain server for a country

Root DNS Servers
A group of servers that use well-known IP addresses that have been programmed into DNS servers

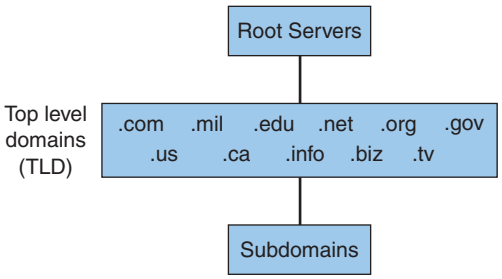


FIGURE 10-6 The DNS tree hierarchy.

By having a tree hierarchy structure, DNS operates in a delegation mode, starting from the root and moving to subtree levels. This way, each level only has to maintain the information of the next level. With this structure, the root DNS servers only know of the TLD DNS servers, to which they can delegate the top-level domain queries. The root DNS servers do not know of domains such as www.example.com. A root DNS server delegates a query to a next-level authoritative server, which repeats the delegation to the next level until it reaches the final server that can authoritatively give the answer www.example.com. The DNS server that is authorized and configured to answer DNS queries for a particular domain or zone is called an authoritative DNS server.

For example, say that a computer in Network-A wants to know the IP address for the server at Network-B.edu (that is, www.network-b.edu). The following steps occur:

1. The computer sends a DNS query to the Network-A DNS server. Typically, the host knows the IP addresses of the primary and secondary DNS servers, through either static input or dynamic assignment.
2. The Network-A DNS server does not have the answer and queries other DNS servers on behalf of the client; this process is known as a *recursive lookup*. In this case, the Network-A DNS server would query one of the root DNS servers and would receive the IP addresses of the DNS servers for the .edu top-level domain.
3. The Network-A DNS server sends a query to one of the .edu TLD DNS servers for www.network-b.edu and receives the IP addresses of the authoritative DNS servers for the www.network-b.edu domain. This process of querying a delegated DNS server is known as an *iterative lookup*.
4. The Network-A DNS server sends a query to one of the www.network-b.edu DNS servers, which is the authoritative DNS server for www.network-b.edu, and it receives the DNS answer or authoritative answer of the IP address for www.network-b.edu.
5. The Network-A DNS server tells the computer the IP address.

A DNS server keeps a cache of recent queries so that this multiple-step process of obtaining an IP address does not have to be repeated unnecessarily. With DNS

caching, the next time any computer in Network-A is asking for www.network-b.edu, the Network-A DNS server can provide the answer without having to fetch the answer through the delegation process.

DNS Resource Records

As mentioned earlier in this section, an authoritative name server is a name server that is authorized and configured to answer DNS queries for a particular domain or zone. The authoritative name server is in charge of managing the information about that zone or domain. Information about the domain and its hosts and services is defined by resource records (**RR**). Each zone contains resource records that define or describe its domain, its subdomains and its host information. The terms *domain* and *zone* are often used interchangeably. These resource records can be found by using either the **dig** command in Linux or **nslookup** command in Windows.

RR
Resource record is a DNS record that is used to define or describe a domain, its subdomains or its host information

nslookup and dig
Commands that query the specified DNS server and retrieve the requested records associated with the domain name provided

The Start of Authority (**SOA**) record is a mandatory RR for a zone. It marks the start of the zone and provides technical details about the zone, such as the zone name, the primary authoritative name server, the email address of the domain administrator, the serial number of the domain, the TTL (Time to Live) of the domain, and refresh, retry, and expiration times for the secondary name server. The following example uses the **nslookup** command to find the SOA record of the domain example.com:

```
C:\nslookup -query=SOA example.com
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
example.com
        primary name server = dns1.icann.org
        responsible mail addr = hostmaster.icann.org
        serial  = 2011063168
        refresh = 7200 (2 hours)
        retry   = 3600 (1 hour)
        expire  = 1209600 (14 days)
        default TTL = 3600 (1 hour)
```

SOA
Start of Authority, a mandatory resource record for a zone that marks the start of the zone and provides the technical details of the zone

nslookup is available by default on Windows, macOS, and Linux. **dig** is available on macOS and Linux but is not available by default on Windows.

The **A record (Address record)** is the most common record in DNS. It is a hostname mapping to an IP address. For example, the host1 entry in domain network-B.edu is an A record. The A record is used by a DNS server at the parent company for Network-B to convert the name host1.network-B.edu to an IP address. The following example uses the **nslookup** command to find the A record of the host www.example.com:

A Record (Address Record)
The most common record in DNS, which maps a hostname to an IP address

```
C:\nslookup  www.example.com
Server:  192.168.1.1
Address:  192.168.1.1#53

Non-authoritative answer:
Name: www.example.com
Address: 192.0.43.10
```

Note

www.example.com is known as a fully qualified domain name (FQDN) because it consists of a hostname and the complete domain name.

PTR Record (Pointer Record)
A record that maps an IP address to a hostname

A **PTR record (Pointer record)** is the reverse of an A record: It maps an IP address to a hostname. It is sometimes referred to as a reverse record. The following example uses the **nslookup** command to find the PTR record or the reverse record of the IP address given for www.example.com:

```
C:\nslookup -query=PTR 192.0.43.10
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
10.43.0.192.in-addr.arpa name = 43-10.any.icann.org.
```

In this example, the answer is not exactly the reverse hostname that you would expect. You would think that the name result would be the reciprocal to the previous example, which is www.example.com. In this case, the name listed is 43-10.any.icann.org instead. This result has to do with how the Internet domain name is registered and how the IP address is acquired. As you have learned, Internet domain names can come from different sources. An Internet domain name is generally purchased from a domain registrar, and the IP address has to be allocated by ARIN (in North America) or by an ISP. This results in one entity being in charge of the forward DNS zone and another entity being in charge of the reverse DNS zone. The information is not usually synchronized, leading to results like 43-10.any.icann.org.

A PTR record can also be used for security purposes to verify that a domain is allowed to connect to a service. For example, say that pc-salsa1-1 (10.10.20.1) connects to an FTP server that allows only machines in the salsa domain to make the connection. When the connection is made, the FTP server knows only the IP address of the machine making the connection (10.10.20.1). The server uses the IP address to request the name assigned to that IP address. A connection is made to the salsa domain server, and the salsa DNS server returns pc-salsa1-1 as the machine assigned to 10.10.20.1. The FTP server recognizes that this is a salsa domain machine and authorizes the connection.

CNAME Record (Canonical Name Record)
An alias of a hostname

A **CNAME record (Canonical name record)** is generally called an *alias*. It allows another name to be defined and points to the real name. A CNAME record is mapped to an A record. Much as with an A record query, it is not necessary to specify the option for a CNAME record when using **dig** or **nslookup**. Both commands yield a canonical name of a hostname, if it exists. The following example reveals that www.iana.org is actually an alias for the A record ianawww.vip.icann.org:

```
C:\nslookup www.iana.org
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
www.iana.org     canonical name = ianawww.vip.icann.org.
Name:  ianawww.vip.icann.org
Address: 192.0.32.8
```

Aliases are useful in applications such as virtual web hosting. Being able to create multiple names and map those names to one canonical name that in turn associates to one IP address allows multiple websites to be served by one server. The effect is seamless to general users. As a matter of fact, this is how most virtual services and cloud services operate. For example, say that the website www.example.com moved to a cloud service provider (CSP) by creating a CNAME record and then mapped the website to a specific cloud service provider's server. Although general users still use the website www.example.com, the destination where the service is hosted is now different.

An **NS record (Name Server record)** is another mandatory RR for a zone. It specifies the name of the authoritative name server of the domain. The record must map to a valid A record, not an IP address or a CNAME. NS records are associated with a domain rather than with a particular host. Therefore, you need to look up the name server information based on the domain. The following example demonstrates the use of the **nslookup** command to look up the NS records of the domain example.com:

NS Record (Name Server Record)
A record that specifies the name of the authoritative name server of the domain

```
C:\nslookup -query=NS example.com
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
example.com nameserver = a.iana-servers.net.
example.com nameserver = b.iana-servers.net.
```

An **MX record (Mail Exchange record)** specifies the email-handling server of a domain (that is, the server to which all the incoming emails to the domain go). The MX record must also map to a valid A record, not to an IP address or a CNAME. The MX record is a crucial piece of information in today's Internet. Without correct MX records, emails to the domain will stop flowing. The following example demonstrates the use of the **nslookup** command to search the MX records information of the domain network-b.edu:

MX Record (Mail Exchange Record)
A record that specifies the email-handling server of a domain

```
C:\nslookup -query=MX network-b.edu
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
network-b.edu  mail exchanger = 20 mx02.cloud.example.com.
network-b.edu  mail exchanger = 30 mx03.cloud.example.com.
network-b.edu  mail exchanger = 10 mx01.cloud.example.com.
```

Note

This command is issued for information on MX for the entire domain, just like the command for the NS information.

In this case, the MX records yield three email servers for the domain network-b.edu. Each server has a different preference number. The lowest preference number signifies the most preferred server.

Email service is a popular service offered by many cloud service providers. Many entities do not have resources to manage the volume of email going to and coming from their domains. Much as CNAME records are used to map to a cloud server, MX records can be used for email. To move the email service of a domain to a cloud service, the MX needs to be changed to the cloud service provider's email servers. As shown in the preceding example, the domain network-b.edu is using cloud.example.com as the email cloud service.

TXT Record (Text Record)
A record that is used to hold arbitrary text information for the domain

SPF
Sender Policy Framework

A **TXT record (Text record)** is used to hold arbitrary text information for a domain. Besides storing arbitrary information or comments for the domain, this record is increasingly being used to validate the authenticity of a domain. One of its popular applications is to authenticate the email sender domain. The **SPF** (Sender Policy Framework) can be entered into a TXT record. This piece of information can be used as a validation of the legitimate sources of email from a domain. Another application is for the cloud service providers to validate the authenticity of the domain ownership. Many cloud service providers ask for proof of domain ownership by providing the domain owner with a token value that needs to be added to the TXT record. The following example shows the TXT record with the specific token value (**t=**) for a cloud service.

```
C:\nslookup -query=TXT network-b.edu
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
Network-b.edu  text = "v=msv1 t=3b6735dd2923c44e99c313ac4adb65"
```

DKIM
Domain Keys Identified Mail

On a related note, Domain Keys Identified Mail (**DKIM**) enables an organization to take responsibility for a message in transit. This is a way of determining whether a message should be trusted for further handling or delivery. Essentially, DKIM provides a way to validate a domain name identity with an associated message through cryptographic authentication.

SRV Record (Service Record)
A record that is used to identify a host (or hosts) that offers a specific type of service

An **SRV record (Service record)** is used to identify a host or hosts that offer a specific type of service. It is sometimes called a *service location record*. The syntax of this type of record is unique. The SRV record has the syntax *_service._protocol.name* (for example, _ldap._tcp.network-b.edu or _http._tcp.example.com). The SRV record provides typical host information, and it also provides the TCP or UDP port of the service. The SRV record is used all the time with Microsoft Windows, especially in the Active Directory (AD) environment. The following example shows the SRV record of _ldap._tcp.network-b.edu, which enables a client to locate a server that is running the LDAP service for the domain network-b.edu:

```
C:\nslookup -query=SRV _ldap._tcp.network-b.edu
Server: 192.168.1.1
Address: 192.168.1.1#53

_ldap._tcp.network-b.edu  service = 0 100 389 dc2.network-b.edu.
_ldap._tcp.network-b.edu  service = 0 100 389 dc1.network-b.edu.
```

The output in this example shows two servers that can provide the service. Both of them have priority value 0, which is the highest, and weight value 100. Both of them provide the LDAP service on TCP port 389.

AAAA Record (Quad-A Record)
A DNS record for IPv6

A AAAA record (Quad-A record) is the DNS record for IPv6. It is very important that IPv6 addresses be added to the name server to make it possible for the DNS server to be reachable for IPv6. Therefore, today's DNS servers need to have both A and AAAA records.

DNS is susceptible to a number of threats, such as DNS poisoning (aka DNS spoofing), an attack that exploits vulnerabilities in DNS and directs Internet traffic away from the intended server to a fake server. DNS poisoning is dangerous because it can spread to other DNS servers. A related attack is ARP poisoning, which links the attacker's MAC address with a legitimate address.

Figure 10-7 illustrates the steps involved in manually updating DNS A records:

1. A client PC updates the A record when an IP address is requested for a computer.
2. The user obtains the PC name and the PC's MAC address and sends this information to the network administrator or the NOC.
3. The NOC issues an IP address to the client, updates the NOC database of clients on the network, and enters a new A record into the primary DNS server. The entry is made only on the primary DNS server.
4. The entry is later replicated on the secondary DNS server.



FIGURE 10-7 Manually updating the A record.

Dynamically Adding a Client to a Campus Network A new A record can be entered dynamically when a client computer obtains an IP address through DHCP registration (see Figure 10-8.) The DHCP server issues an IP address to the client and at the same time sends an updated A record to the network's primary DNS server. The client name and the IP and MAC addresses are stored in the DHCP database.

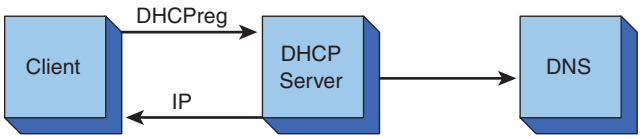


FIGURE 10-8 Dynamic updating of the A record using DHCP.

Why obtain the MAC address when entering information into DNS? The A record is used to keep track of all the machines operating on the network. The MAC address is a unique identifier for each machine. The MAC address is also used by BOOTP, which is a predecessor to DHCP; in this case, a MAC address is specifically assigned to one IP address in the network.

IPAM
IP address management, a process used for managing IP address space in a network that integrates DHCP and DNS and ensures that each service is aware of changes, thereby avoiding conflicts with IP user space

Today, IP address management (**IPAM**) is used for managing IP address space in a network. IPAM integrates both DHCP and DNS and ensures that each service is aware of changes, thereby avoiding conflicts with IP user space. You will also see the term *clustering*, which is a technique used to group network devices or storage according to function.

In modern networks, you will often find that there are third-party/cloud-hosted DNS servers. Some organizations prefer not to manage their DNS servers. In such networks, internal DNS requests are served by internal DNS, and external requests are served by external DNS.

Section 10-5 Review

This section covers the following Network+ exam objectives.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

This section examines DNS.

1.6 Explain the use and purpose of network services.

This section describes various server types and record types.

Test Your Knowledge

1. What server provides name translations for the hostname to an IP address?
   a. Root server
   b. TLDs
   c. DNS server
   d. Web server
2. Which of the following does a DHCP server dynamically assign to a machine on an as-needed basis?
   a. MAC address
   b. IP address
   c. Protocol address
   d. All of these answers are correct.
   e. None of these answers are correct.

10-6 NETWORK MANAGEMENT PROTOCOLS

The focus of this section is on the use of the Simple Network Management Protocol (SNMP) for maintaining network equipment. This section also provides an overview of the SNMP management information base and configuring SNMP on a router.

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, and proper management tools must therefore be in place.

A fundamental network management tool is **SNMP (SNMPv1)**, Simple Network Management Protocol. SNMPv1, developed in 1988, is widely supported in most modern network hardware. SNMP is a connectionless protocol that uses UDP for transmission of data to and from UDP 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. An MIB describes the structure of the management data of a device subsystem using a hierarchical namespace that contains object identifiers (OIDs). Each OID identifies a variable that can be read or set via SNMP. For example, the MIB object ifDescr has the OID 1.3.6.1.2.1.2.2.1.2. This particular OID is used to return a description of the router's interfaces, as demonstrated in Figure 10-9. This figure shows an SNMP software tool being used to collect interface description information. The IP address of the router is 10.10.10.1, and **get request ifDescr** was sent to port 161, the UDP port for SNMP. As you can see, the tool returns descriptions of the interfaces.

SNMP (SNMPv1)
Simple Network Management Protocol (version 1), a connectionless protocol that uses UDP for the transmission of data to and from UDP port 161

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

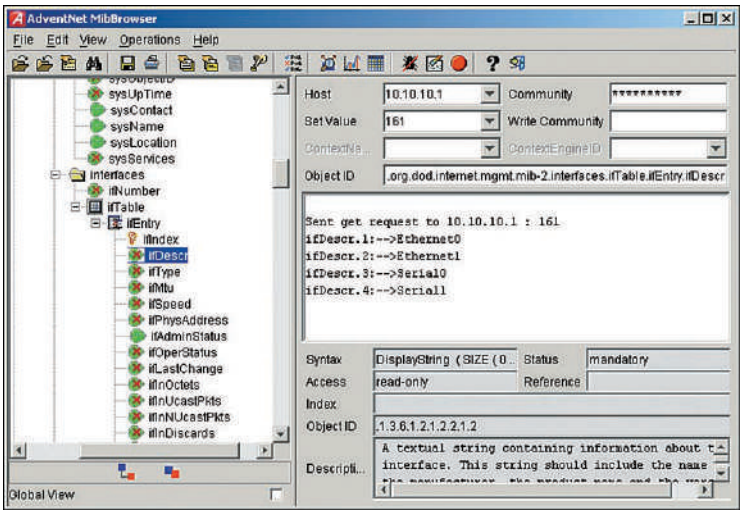


FIGURE 10-9 An example of using an SNMP software management tool to obtain descriptions of a router's interfaces using the MIB **ifDescr**.

Configuring SNMP

To obtain SNMP data, SNMP must be configured on the router. This section shows how to configure SNMP on a Cisco router.

The first step in configuring SNMP on a Cisco router is to enter the router's configuration mode by using the **conf t** command:

```
RouterB #conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

At the router's **(config)#** prompt, you enter the command **snmp community** [*community string*] [*permissions*], where *community string* can be any word, and

the *permissions* field is used to establish whether the user has the permission read only (**ro**), write only (**wo**), or both (**rw**). The options for configuring SNMP on a router are shown here:

```
RouterB(config)# snmp community ?
WORD SNMP community string
```

In this example, the router is connected to the computer running the SNMP management software, as shown in Figure 10-10. The router's configuration mode is entered, and the **snmp community public ro** command is issued. The word **public** is used as the community string—the password used by the SNMP software to access SNMP (port 161) on the router. **ro** sets the permission to read only:

```
RouterB(config)# snmp community public ro
```



FIGURE 10-10 The setup for connecting the SNMP management software tool to the router.

In the next example, the community string password is set to **makesecret**, and the permission is set to read write (**rw**). Once again, the router's **(config)#** mode is used, and the command **snmp community makesecret rw** is entered:

```
RouterB(config)# snmp community makesecret rw
```

The configuration for SNMP can be verified by using the **show run** command from the router's privileged mode prompt. A portion of the configuration file that lists the SNMP configuration for the router is shown here:

```
RouterB# sh run
snmp-server community makesecret RW
```

Figure 10-11 shows the setup of the configured router and the computer running the SNMP management software. The SNMP management software issues the MIB to the router at port 161, and the router returns the response. Figure 10-11 shows another example of using SNMP to obtain interface information about a router. The SNMP manager in this case is configured with the host IP address 10.10.10.1, the set value (port number) 161, and the 10-character community string **makesecret**, shown as * * * * * * * * * *. The MIB **ifSpeed** is sent to the router, and a status is provided for each of the interfaces. The data displayed shows the speed settings for the router's interfaces.

An SNMP monitor, as shown in Figure 10-12, is a tool used to obtain traffic data statistics. In this example, the SNMP management program issues the MIB **ifOutOctets**, which returns the number of octets of data that have left the router. (The router has a counter that keeps track.) The first result is **ifOutOctets 7002270**. The next result is **ifOutOctets 7002361**.

The SNMP management program collecting the statistics keeps track of the time interval between measurements and the number of octets that have passed. This information can be used to calculate the average traffic flow by hour, day, week, or month, depending on the information needed.

Note

The router's counter does not reset unless the router is rebooted.

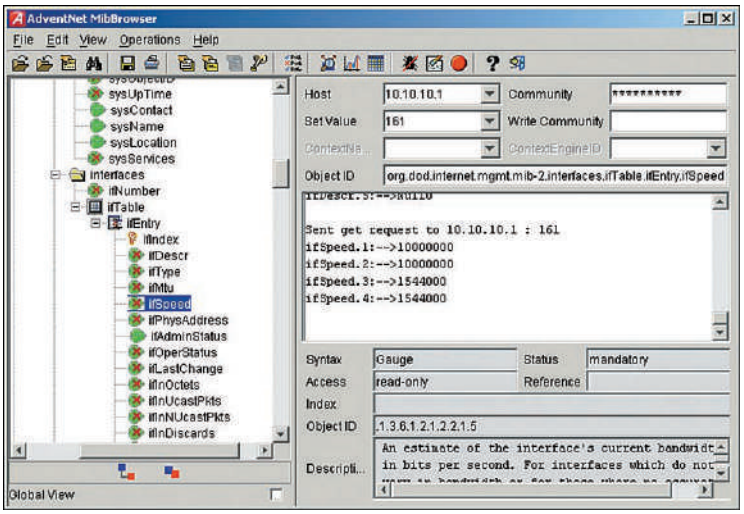


FIGURE 10-11 Using an SNMP software management tool to obtain interface speed settings.

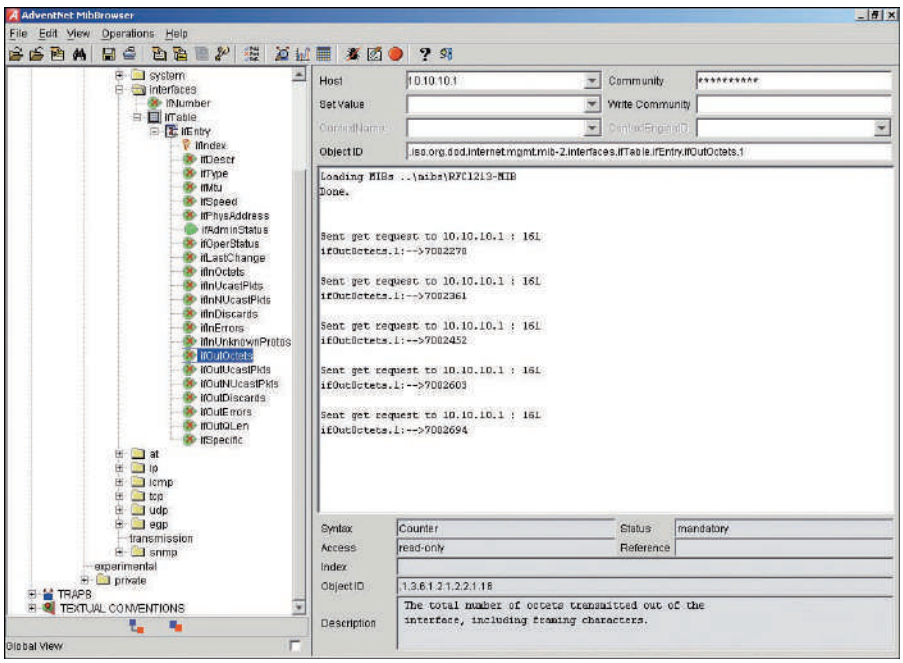


FIGURE 10-12 An example of using SNMP to collect data traffic statistics.

SNMPv2
Simple Network Management Protocol version 2

SNMPv3
Simple Network Management Protocol version 3

Two other versions of SNMP have been developed for network management: **SNMPv2** and **SNMPv3**. SNMPv2, which was developed in 1993, was not directly compatible with SNMPv1. SNMPv2 attempted to address security issues, but many variants ended up being developed, and SNMPv2 was never fully accepted by the networking industry. One of the variants, called SNMPv2c (Community-based SNMP version 2), was adopted more widely than the others. SNMPv3, which was developed in 1998, achieved the important goal of maintaining compatibility with SNMPv1 and adding security to SNMP. The security features of SNMPv3 include confidentiality, integrity, and authentication. *Confidentiality* means the packets are encrypted to prevent snooping, *integrity* ensures the data being transferred has not been tampered with, and *authentication* means the data is from a known source.

SNMP enables gathering of statistical information from network devices; however, it does not dive deep into IP information, such as the source, destination, or protocol of each data packet. NetFlow allows for such data collection. NetFlow is a push technology; this means that NetFlow data is pushed from a network device to a collector. Cisco created NetFlow in 1996 for acquiring IP traffic operational data in order to provide network and security monitoring, traffic analysis, and IP accounting. Currently, there are 10 versions of NetFlow. NetFlow version 5 is the most common version deployed on many network devices from different vendors. NetFlow version 9 is the first version to support IPv6, and this version has now been standardized by the IETF to NetFlow version 10, also known as Internet Protocol Flow Information Exchange (IPFIX).

Even though NetFlow was developed by Cisco, it is not a Cisco-proprietary protocol. Many network vendors have adopted NetFlow to collect their IP traffic flow statistics. Nonetheless, there are still variants of the NetFlow protocol available to the public. For example, JFlow is Juniper's IP traffic flow technology. It is similar to NetFlow version 5; however, it is a flow sampler technology, which samples the number of packets as defined in the router configuration. Created by InMon, sFlow (Sampled Flow) is another traffic flow technology. Similar to JFlow, sFlow is a sampling technology that is designed to collect a large amount of statistical network information. It collects many performance counters, so it collects different information than NetFlow and JFlow. It can be thought of as SNMP on steroids. Its main deployment is in high-speed switched networks with big support from HP, Extreme, and Alcatel. sFlow is not compatible with NetFlow or JFlow.

There is one thing that all these flow technologies have in common: All the flow information has to be exported or sent to the collector. The *collector* stores and analyzes the flow information. There are many flavors of flow collector software available. Some of them can even collect all different type of flows (NetFlow, JFlow, and sFlow) and are able to correlate information among them.

Note

Because a flow technology is a push technology from a network device, enabling flow on a device could increase the CPU utilization of the device. This is especially true for a device such as a busy router that is dealing with a heavy load of network traffic. It is important to constantly monitor the CPU health of a device when you turn on a flow technology.

Let's consider some examples of how to configure NetFlow on Cisco routers. The first steps are to define the version of NetFlow, the source of the export, and the destination and the listening UDP port to which the flows will be exported:

```
RouterA (config)# ip flow-export source Loopback0
RouterA (config)# ip flow-export version 5
RouterA (config)# ip flow-export destination 10.10.101.19 5000
```

Next, you need to enable NetFlow on an interface by using the command **ip route-cache flow**. This command enables NetFlow on the physical interface and its associated subinterfaces, if there are any. Then you enter the command **ip flow ingress** to enable NetFlow on particular subinterfaces. In this example, the Gigabit 1/0 interface is enabled with NetFlow monitoring:

```
RouterA (config)# int GigabitEthernet1/0
RouterA (config-if)# ip flow ingress
```

You can verify NetFlow information by using a **show** command. The command **show ip flow export** shows a NetFlow configuration and its basic statistics. Note that all the flow information has to be sent to the collector, which stores and analyzes the flow information. There are many flavors of flow collector software available. Some of them can even collect all information.

Another network management technique is to use port mirroring or SPAN (Switched Port Analyzer). Port mirroring is a capability offered by many network switches to monitor all the data packets seen on a specified port or ports. With switch port mirroring enabled, the switch sends a copy of all data traffic seen on its port to another port. The data can then be captured and analyzed as needed. Port mirroring is essential for monitoring and logging network traffic without having to install a device in line with the traffic and disrupt the network traffic flow.

Section 10-6 Review

This section covers the following Network+ exam objectives.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section introduces SNMP, OIDs, and MIBs.

5.3 Given a scenario, use the appropriate network software tools and commands.

This section examines NetFlow, which is a software data collection tool.

Test Your Knowledge

1. Which of the following is the *best* example of a fundamental network management tool?
   a. SNMP
   b. **ping**
   c. **trace route**
   d. Documentation
2. Which of the following best characterizes a MIB? (Select all that apply.)
   a. A management Internet base is a UDP protocol used by SNMP.
   b. A management information base is a collection of standard objects that are used to obtain performance data on a networking device.
   c. A management information base is a collection of standard multicast addresses that are used to obtain certain configuration parameters.
   d. A management information base is a collection of standard objects that are used to obtain certain configuration parameters.

10-7 ANALYZING NETWORK TRAFFIC

A key issue in network management is network monitoring, which involves collecting utilization and error statistics. This section examines the typical campus network data traffic that a network administrator monitors. Examples are presented for hourly, daily, weekly, and monthly plots that demonstrate how to examine the traffic plots for potential problems.

The previous section introduces SNMP, which is a protocol used in network management. That section includes an example that shows how to obtain the number of octets leaving a router. You can use this type of information in a campus network to monitor the flow of data for many points in the network. You can obtain statistics for hourly, daily, weekly, and monthly data traffic. This section discusses plots of network router utilization obtained via a router's SNMP port and provides a look at packet/traffic analysis.

Figure 10-13 is a plot of a router's hourly data traffic. The plot shows the average number of bits coming into the router and the average number of bits going out. Network administrators need to be familiar with the typical hourly data traffic patterns for their networks. Notice the decrease in data traffic in the early morning and the dramatic increase in data traffic around noon. The traffic clearly shows some type of disturbance around noon. The plot shows that the bit rate significantly increases for a few minutes. This is not necessarily a problem, but it is something that the network administrator should watch.

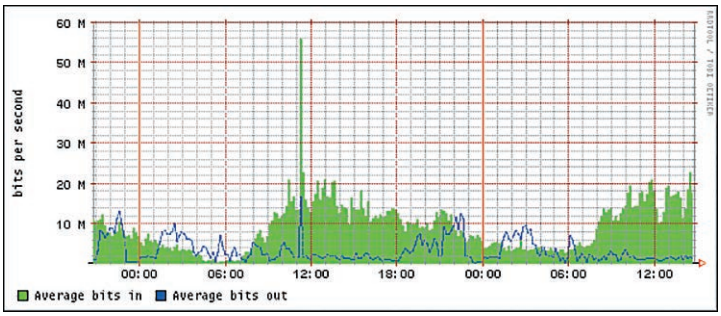


FIGURE 10-13 An hourly plot of a router's data traffic in and out.

Figure 10-14 shows a daily plot of network activity for the same router. During the administrator's log review, he noted that the cycle of the data traffic from morning to night is as expected: heavy data traffic about noon and very low data traffic in the mornings. An interesting note is that the noon data traffic spikes on the first Wednesday and then repeats the following Wednesday. Whatever is causing the change in traffic appears to happen on Wednesdays. If this sudden change in data traffic turned out to be something of concern, a protocol analyzer could be set up to capture the data traffic on Wednesdays around noon so that the traffic pattern could be examined and explained.

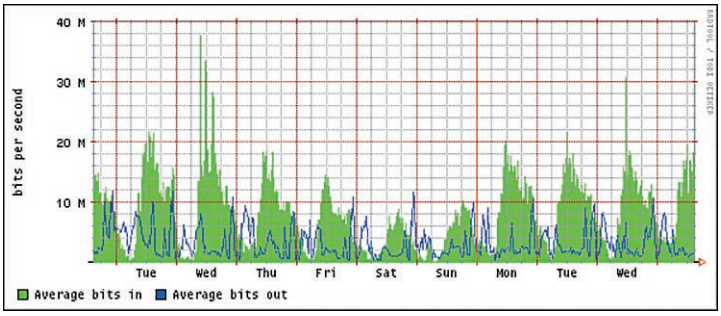


FIGURE 10-14 A daily plot of a router's data traffic.

Sometimes an administrator needs a graph of the network traffic over a longer period of time. Figure 10-15 shows the data traffic through the same router over a six-week period. This plot shows some consistency except for a change from week 11 to week 12. Most likely this change can be explained by examining the network trouble reports and maintenance logs to see if this router was briefly out of service.

Note

It is imperative that network devices maintain the correct time. Incorrect time will result in miscorrelation of the log events. It is recommended that all network devices synchronize their clocks with a reliable NTP (Network Time Protocol) server so that they all have the same clock source and report the same time when reporting information in their logs.

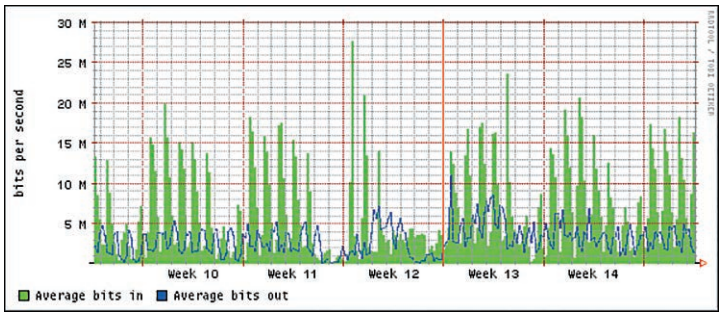


FIGURE 10-15 A weekly plot of a router's data traffic.

To justify the expansion of a network's capability (for example, higher data rate or better core or distribution service), a network administrator needs to show the data traffic statistics. Figure 10-16 is a plot of the router's monthly data traffic. As you can see, there is a significant decrease in data traffic in the summer. The plot also shows that the network was down once in the June–July period and again in January. The manager wants to know whether there is justification to increase the data rate of the router to 1Gbps from the current rate of 100Mbps. There is probably not justification to make this upgrade, at least not immediately. The maximum measured average data rate is about 16Mbps. The router's 100Mbps data rate does not seem to be causing any traffic congestion problems.

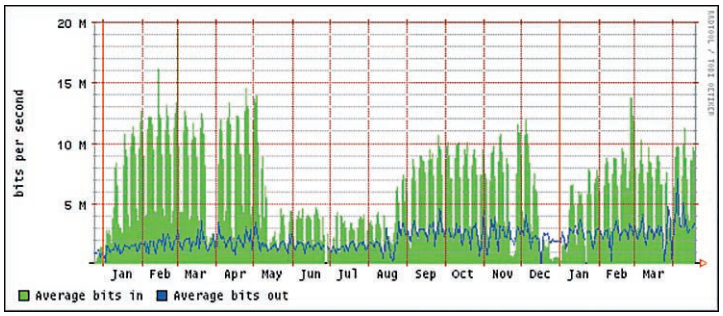


FIGURE 10-16 A monthly plot of a router's data traffic.

A network administrator can use SNMP monitors to collect information in addition to utilization in bits per second (bps) for capacity planning. Most NOCs also collect SNMP information, such as packets per second, errors per second, unicasts per second, multicasts per second, and broadcasts per second. All this information can be graphed for better visualization and helps illustrate the overall health of the network through time, as shown in Figure 10-17.

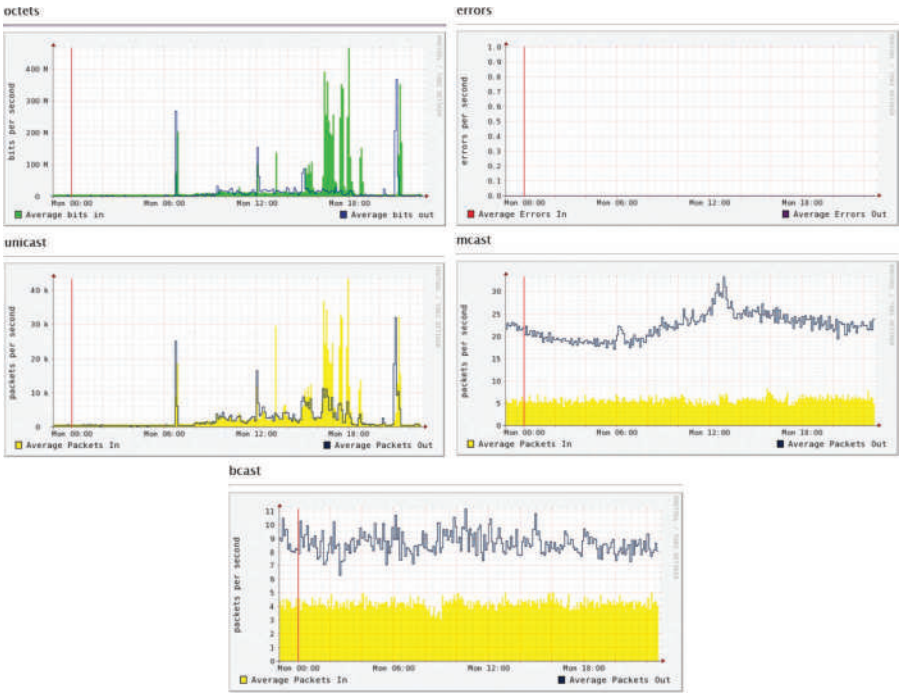


FIGURE 10-17 Network graphs: (a) octets, (b) errors, (c) unicast packets, (d) muliticast packets, (e) broadcast packets.

A network administrator must have some expected performance measures (that is, baselines or metrics) for the network. An administrator needs to know the expected normal usage of the network, what type(s) of normal data traffic is expected, what is typical of outbound and inbound Internet data traffic, and who the "big" data users on the network are. Data traffic patterns vary significantly for each network, and each network has its own typical data traffic. Also, data traffic changes during the day. Data traffic is bidirectional, which means it has both transmit/outbound and receive/inbound. **Outbound data traffic** is data leaving a network, and **inbound data traffic** is data entering a network.

Outbound Data Traffic
Data traffic leaving a network

Inbound Data Traffic
Data traffic entering a network

One of the areas network administrators monitor is the typical utilization of network bandwidth. Figure 10-18 is a utilization/errors graph of an uplink connection to and from a network. This uplink connection continuously generates large numbers of errors, correlated to the graph of spikes in utilization. Errors at this magnitude will render the connection almost useless, and the issue must be dealt with as soon as possible.

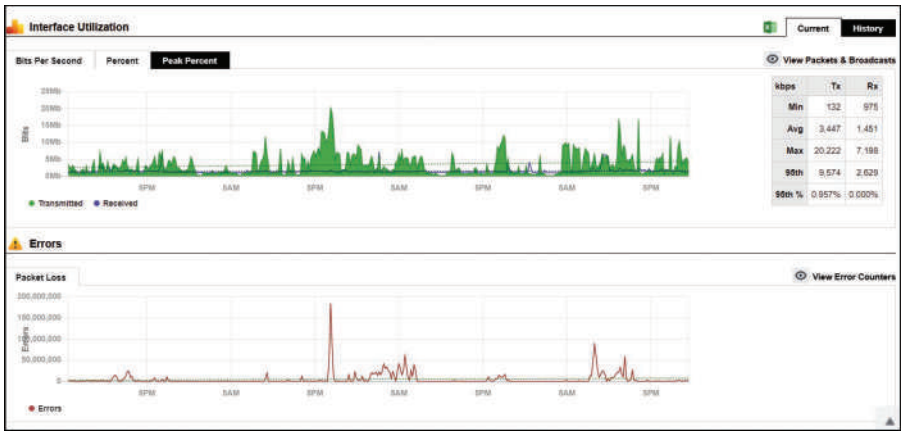


FIGURE 10-18 A utilization/errors strip chart for an Internet feed.

The data traffic graph capture shown in Figure 10-19 provides a view of the data traffic activity for an Internet connection to and from a campus network. The graph is collected via NetFlow instead of SNMP.

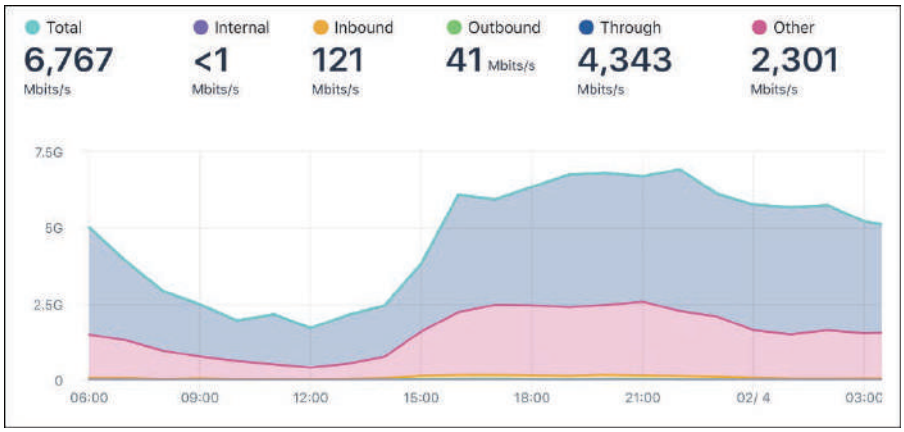
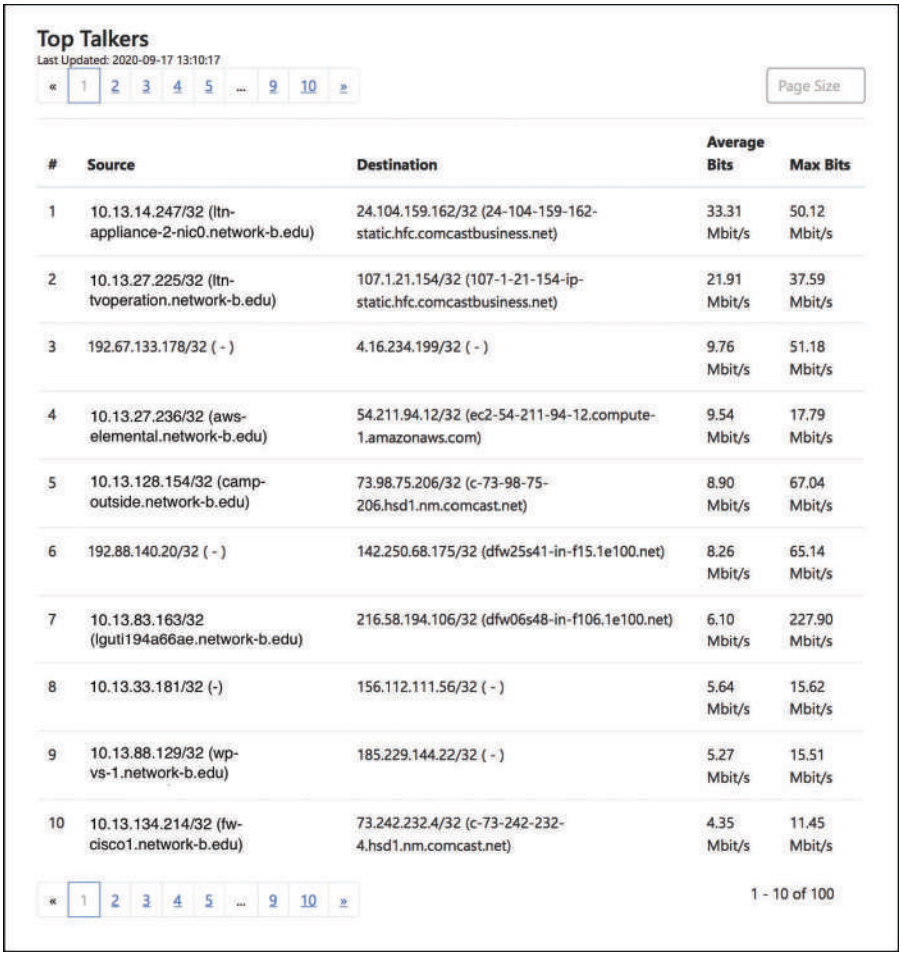


FIGURE 10-19 A view of network Internet traffic activity.

NetFlow collects information based on packet flow information sent from a network device. Therefore, it can offer more details than SNMP, based on packet activity.

Figure 10-20 shows the Top Talkers view of conversations on the campus Internet feed. The Top Talkers information captures the IP addresses between the source and destination as well as the bandwidth usage between them. As you can see in this example, the top conversation is between the machines at IP addresses 10.13.14.247 and 24.104.159.162. The 10.13.14.247 machine is on the local network (hence the source). This one conversation is consuming, on average, 33Mbps of the network's Internet bandwidth/throughput. This chart provides a network administrator with a quick look at which host computer is tying up the network resources. It is

not possible to make a reasonable guess whether this is a normal network layer graph for the network by looking at only this one picture. You can determine this, however, if you have knowledge of expected behavior over the long term.



Top Talkers

Last Updated: 2020-09-17 13:10:17

« 1 2 3 4 5 … 9 10 » Page Size

#	Source	Destination	Average Bits	Max Bits
1	10.13.14.247/32 (ltn-appliance-2-nic0.network-b.edu)	24.104.159.162/32 (24-104-159-162-static.hfc.comcastbusiness.net)	33.31 Mbit/s	50.12 Mbit/s
2	10.13.27.225/32 (ltn-tvoperation.network-b.edu)	107.1.21.154/32 (107-1-21-154-ip-static.hfc.comcastbusiness.net)	21.91 Mbit/s	37.59 Mbit/s
3	192.67.133.178/32 (-)	4.16.234.199/32 (-)	9.76 Mbit/s	51.18 Mbit/s
4	10.13.27.236/32 (aws-elemental.network-b.edu)	54.211.94.12/32 (ec2-54-211-94-12.compute-1.amazonaws.com)	9.54 Mbit/s	17.79 Mbit/s
5	10.13.128.154/32 (camp-outside.network-b.edu)	73.98.75.206/32 (c-73-98-75-206.hsd1.nm.comcast.net)	8.90 Mbit/s	67.04 Mbit/s
6	192.88.140.20/32 (-)	142.250.68.175/32 (dfw25s41-in-f15.1e100.net)	8.26 Mbit/s	65.14 Mbit/s
7	10.13.83.163/32 (lgutl194a66ae.network-b.edu)	216.58.194.106/32 (dfw06s48-in-f106.1e100.net)	6.10 Mbit/s	227.90 Mbit/s
8	10.13.33.181/32 (-)	156.112.111.56/32 (-)	5.64 Mbit/s	15.62 Mbit/s
9	10.13.88.129/32 (wp-vs-1.network-b.edu)	185.229.144.22/32 (-)	5.27 Mbit/s	15.51 Mbit/s
10	10.13.134.214/32 (fw-cisco1.network-b.edu)	73.242.232.4/32 (c-73-242-232-4.hsd1.nm.comcast.net)	4.35 Mbit/s	11.45 Mbit/s

« 1 2 3 4 5 … 9 10 » 1 - 10 of 100

FIGURE 10-20 The Top Talkers view.

Furthermore, NetFlow has the ability to capture more information, such as protocol information. Figure 10-21 provides a look at the top applications by protocol, as collected by NetFlow.

Figure 10-22 shows the packet size distribution of packets (in bytes) being delivered to and from the campus network's Internet connection. The average packet size, as shown at the top of the chart, is 1420 bytes. The packet size for IP packets is limited to 1500 bytes.

The packet size is related to the *maximum transmission unit* (*MTU*). MTU is the value (in bytes) of the largest packet size that can be sent across the network link. For Ethernet networks, the MTU is 1500 bytes. An MTU black hole may occur as a result of a misconfigured router not delivering data packets properly. In this case, the router is called an *MTU black hole router*.

Application	Internal Mbits/s	Inbound Mbits/s	Outbound Mbits/s	Through Mbits/s	Other Mbits/s	Total Mbits/s
https	-	46.84	2.74	1,845.25	1,382.50	3,277.33
http	<0.01	11.86	0.41	837.67	255.75	1,105.70
condor	-	-	-	1,018.91	-	1,018.91
http-alt	-	-	<0.01	938.82	3.66	942.48
http-proxy	-	2.81	0.38	335.35	336.18	674.72
---	<0.01	4.90	0.90	447.59	126.75	580.15
Zoom	-	3.53	6.15	432.98	114.54	557.20
rootd	-	-	-	347.02	-	347.02
pcsync-http	-	-	-	197.86	-	197.86
Twitch	-	0.20	-	92.03	59.80	152.03
Steam Games Download	-	-	-	4.08	80.64	84.72
plethora	-	7.30	-	27.64	27.97	62.92
Github	-	-	-	16.13	38.66	54.78

FIGURE 10-21 The application layer table.

Packet Size	Internal Mbits/s	Inbound Mbits/s	Outbound Mbits/s	Through Mbits/s	Other Mbits/s	Total Mbits/s
1420	-	3.31	0.23	3,247.85	822.61	4,074.00
1500	-	15.13	2.44	780.09	437.80	1,235.47
1378	-	0.65	0.11	49.87	340.93	391.57
1418	-	-	-	202.29	13.06	215.35
1492	-	0.18	-	87.75	85.53	173.46
1417	-	-	-	149.76	8.23	158.00

FIGURE 10-22 The packet size distribution table.

In addition to SNMP and NetFlow, SIEM (security information and event management) is another type of IT system that can be used to provide a holistic view and real-time analysis of an organization's network and security. A network administrator can use SIEM to correlate the log information and alerts generated by the network or security hardware, servers, and applications. These network device logs—such as traffic logs, audit logs, event logs, or access logs—can collectively provide useful information. Depending on the logging levels or severity levels, they can provide very detailed information. The most detailed level is the debug level; this level should not be left enabled indefinitely as it will generate a large amount of data and will fill up the buffer resource. A SIEM system combines the functionalities security information management (SIM) and security event management (SEM). SIM provides long-term historical information and analysis based on event and log data collected through time. SEM provides real-time monitoring and analysis, and it automates the event management of incident reports and notifications.

The SNMP statistics, flows, and SIEM data collected are based on what the network equipment reports. However, that may not represent or reflect the true user experience. Sometimes, to measure the network data from users' perspectives, statistics have to be collected at the client's end. Simple programs (for example, **ping**, which is available in every OS, **traceroute**, which is available in macOS and Linux, and **pathping** and **tracert**, which are available in Windows) can be used on a user computer to get details about how the network performs. Also, users can use bandwidth speed testers, which are available for free on many service provider websites, to test connection throughput and report on download and upload speeds. Another good tool that can be used to test and measure bandwidth capacity is iPerf, which can be run in a server/client mode. These programs represent a very good set of network troubleshooting tools commonly used at the client's end.

By keeping and examining logs of data traffic, a network administrator can spot potential network problems and plan for possible future expansion of a network.

Section 10-7 Review

This section covers the following Network+ exam objectives.

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

This section introduces MTU (Maximum Transfer Unit). For Ethernet, the MTU is 1500 bytes.

5.3 Given a scenario, use the appropriate network software tools and commands.

This section examines the use of SNMP and NetFlow.

Test Your Knowledge

1. The network administrator notices that the plot of a router's data traffic varies from hour to hour. What does this information tell the network administrator?
   a. This is most likely normal operation.
   b. It would be a good idea to compare this hourly plot with expected hourly plots of the router's data traffic.
   c. It would be a good idea to run diagnostics on the router.
   d. The router needs to be rebooted.
2. Data traffic plots are not necessary for which of the following?
   a. Hourly plots
   b. Daily plots
   c. Weekly plots
   d. Monthly plots
   e. None of these answers are correct.

3. What is the expected utilization for an Ethernet network?

   a. The utilization is based on the CSMA/CD throughput, which is defined by the telco.

   b. You can answer this question if you know the expected utilization of the network, which is usually 10Gbps.

   c. The expected utilization is defined by the data traffic in each network. There is not a single answer for all networks.

   d. It varies based on the cost of using the network and the expected number of remote access clients.

10-8 NETWORK ANALYZER: WIRESHARK

This section introduces the use of the Wireshark protocol analyzer. You will want to have students download and install Wireshark on their computers. This section gives students an opportunity to analyze some previously captured files.

Wireshark
A software protocol analyzer

This section introduces techniques for using a protocol analyzer to examine how networking packets are exchanged in a TCP/IP network. By using a protocol analyzer, such as **Wireshark** or tcpdump, you can develop a better understanding of the protocols being used and how the data packets are being transferred. This section focuses on using the Wireshark protocol analyzer.

The Wireshark software includes many advanced features for packet capture and traffic analysis. Using this software will help you learn more about packet transfer and networking protocols. In this section, you will gain an introductory understanding of the capabilities and techniques for using a sophisticated software protocol analyzer to capture and decode data packets and then inspect the packet contents. You can use a packet analyzer to investigate how information is being transferred in a network. In addition, the information provided by the protocol analyzer enables you to detect, identify, and correct network problems. This section guides you through the steps of using the Wireshark protocol analyzer.

Downloading and Installing Wireshark

To download and install the latest version of the Wireshark software, follow these steps:

1. Visit www.Wireshark.org, click **Download Wireshark**, and select your corresponding operating system.
2. Click **Run** when the dialog box appears to initiate the download process.
3. At the setup wizard prompt, select **Next** and agree to the license agreement.
4. Choose the components you would like to install and click **Next** to continue.
5. Select program shortcuts and click **Next** to continue.
6. Use the default directory paths specified in the setup menu and click **Install** to start the installation process.

When the Wireshark software is installed, you are ready to begin using it.

Using Wireshark to Capture Packets

In most cases, you will want to capture data packets from your own network. The following steps describe how to use Wireshark to capture packets:

1. In Windows, click **Start > Programs > Wireshark** and select **Wireshark** to start the program. In macOS, go to the **Applications** folder and then select **Wireshark** to start the program.
2. To capture packets on an operating network, select the interfaces in which you would like to obtain the capture (see Figure 10-23) by going to **Capture > Interfaces**. After selecting your interfaces, click **Start** to start capturing, as shown in Figure 10-24. You can also get to the interface list by clicking **Interface List** on the Wireshark home screen.
3. To examine the packets, stop the simulation by clicking **Capture > Stop**. Remember that there must be some activity on your network for packets to be transferred. You might see little traffic activity if your network is in the lab and there is limited network activity. You can always use the **ping** command to generate some network data activity, if needed.

To open a saved capture file, click **File > Open** or click **Open** on the Wireshark home screen.

To change capture options, click **Capture > Options** and change the options to your preferred settings.

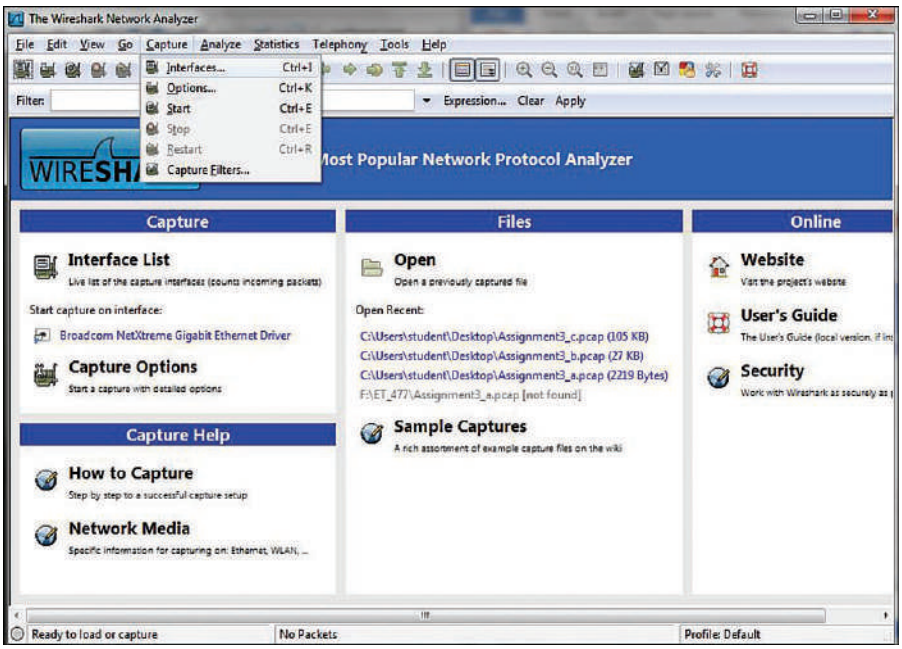


FIGURE 10-23 Initializing Wireshark to capture data packets from a network.

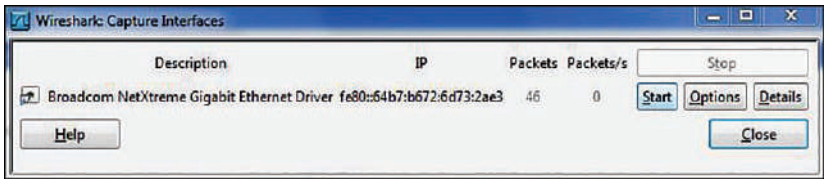


FIGURE 10-24 Starting a capture.

Using Wireshark to Inspect Data Packets

In this section, you will see how to use the Wireshark software to examine or inspect the packets transferred in the process of pinging a computer. In this section you will use a captured file that was created using the procedure discussed in the previous section.

Follow these steps to use Wireshark with a file provided at the book's companion website:

Note

If you haven't already, download the Wireshark files from the textbook's companion website. (See the Introduction for more information on the companion website.) You need these files in the following steps.

1. In Windows, Click **Start > Programs > Wireshark** to start the network analyzer. (The procedure for starting the Wireshark network analyzer is the same for a macOS operating in the dual-boot mode with Windows 10.)
2. In Wireshark, click **File > Open** and select the Wireshark file folder. Double-click the **Ch10-6.cap** file to open it.

When you have opened the Ch10-6.cap capture in Wireshark, you should see the captured packets displayed on the detail view screen, as shown in Figure 10-25. The information on the screen in this example shows the transfer of packets that occurs when one computer pings another. In this case, computer 1 pinged computer 2. The MAC and IP addresses are listed for your reference in Table 10-4.

TABLE 10-4 **MAC and Assigned IP Addresses for Computer 1 and Computer 2**

Name (Hostname)	MAC Address	IP Address
Computer 1	00-10-A4-13-99-2E	10.10.10.1
Computer 2	00-10-A4-13-6C-6E	10.10.10.2

In this example, a **ping** command is issued from computer 1 to computer 2:

```
ping 10.10.10.2
```

As you can see in packet number 1 in Figure 10-25, computer 1 issues an **Address Resolution Protocol (ARP)** request on the LAN. Remember that ARP maps an IP address to a MAC address. In this example, the source of the packet is 00-10-A4-13-99-2E (computer 1). The destination address on the local area network (LAN) shown is BROADCAST, which means this message is being sent to all computers on the network. A query (**Q**) being asked is who has the IP address 10.10.10.2 (**PA**). In Figure 10-26, the ARP request basically says, "Who has 10.10.10.2?"

Address Resolution Protocol (ARP)
A protocol used to map IP addresses to MAC addresses

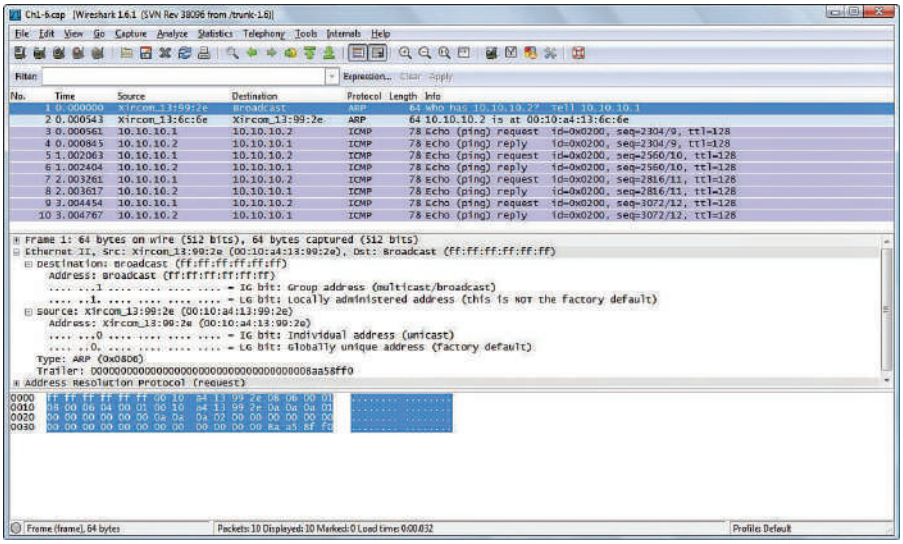


FIGURE 10-25 The captured packets showing the **ping** from computer 1 to computer 2.

The highlighted area (number 2) in Figure 10-26 shows computer 2 replying to computer 1 with its MAC address. This is an **ARP reply**, a response that returns the MAC address. The source of the ARP reply is 00-10-A4-13-6C-6E (computer 2), which is replying that the MAC address for 10.10.10.2 is 00-10-A4-13-6C-6E (HA). In this case, the owner of the IP address replied to the message.

ARP Reply
A response that returns the MAC address

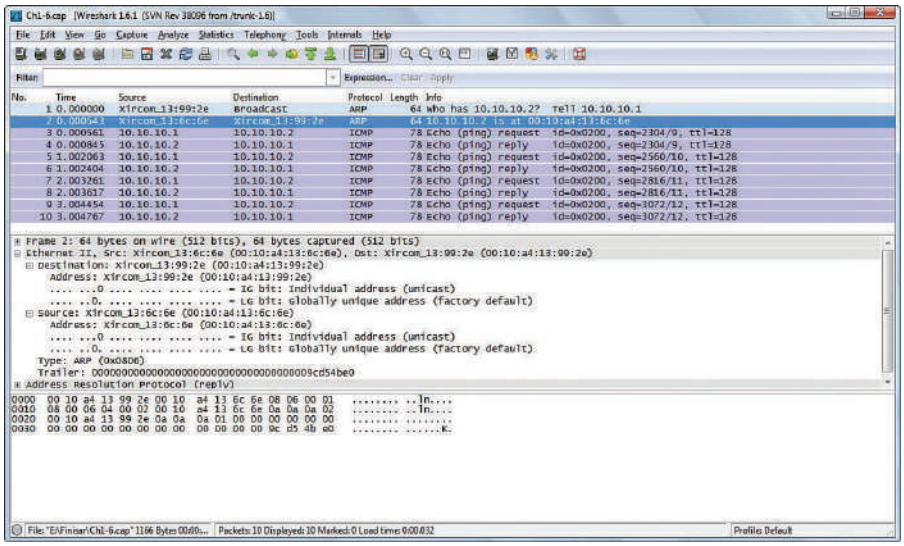


FIGURE 10-26 Computer 2 replying to computer 1 with its MAC address.

Echo Request
The part of the ICMP protocol that requests a reply from a computer

Figure 10-27 shows computer 1 sending an **echo request** directly to computer 2. An echo request is the part of the ICMP protocol that requests a reply from a computer. Notice in the echo request that the destination address is 00-10-A4-13-6C-6E (computer 2's MAC address), and the source is 00-10-A4-13-99-2E (computer 1's MAC address). Recall that computer 1 now knows the MAC address for IP address 10.10.10.2, so the **ping** request can be sent directly. In this step, computer 1 uses the ICMP **ping** command to verify network connectivity. The highlighted area in Figure 10-28 (number 4) shows computer 2's echo reply. This series of echo requests and replies repeats three more times, for a total of four cycles.

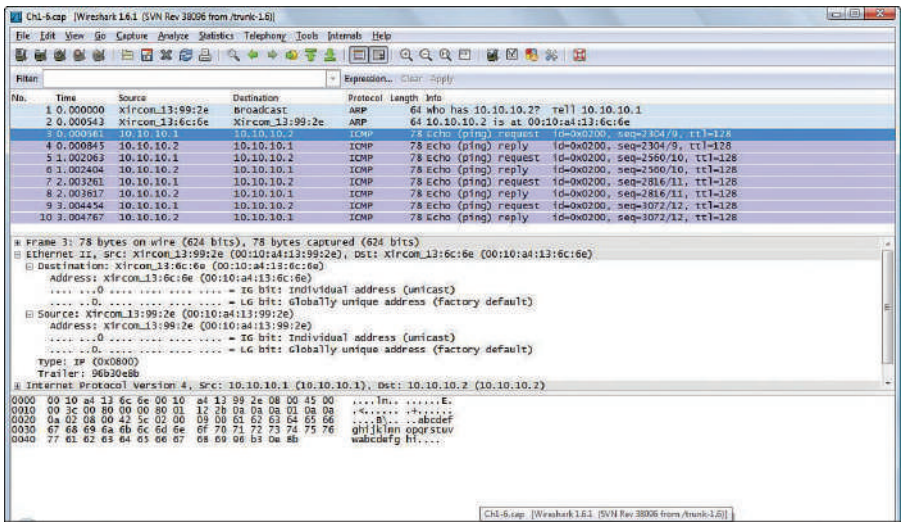


FIGURE 10-27 Computer 1 is sending an echo request to computer 2.

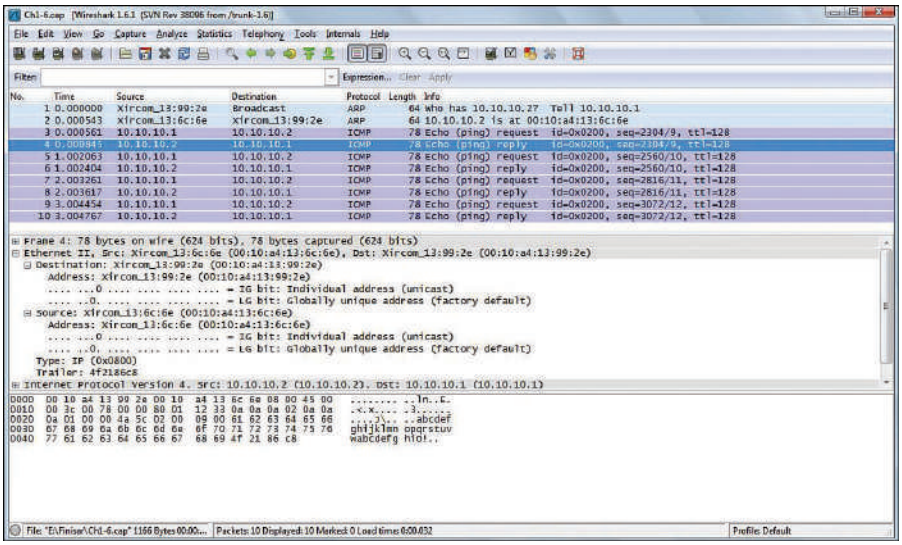


FIGURE 10-28 The echo reply received by computer 1.

Section 10-8 Review

This section covers the following Network+ exam objective.

5.2 Given a scenario, use the appropriate tool.

This section introduces the use of the Wireshark network protocol analyzer. It shows the steps for capturing and displaying data packets, focusing on the packets exchanged during an ARP request.

Test Your Knowledge

1. True or false: The purpose of an echo request is to obtain the MAC address for a given IP address.

   False

2. True or false: The purpose of an ARP reply is to acquire the IP address.

   True

10-9 ANALYZING COMPUTER NETWORKS: FTP DATA PACKETS

FTP
File Transfer Protocol

This section explores the data packet contents of a File Transfer Protocol (**FTP**) data transfer. It uses as an example a captured file that is available for download from the book's companion website. This file, 10-D.cap, contains several TCP transactions. This section uses that packet IP address for reference.

Figure 10-29 shows the setup for this data capture, including the MAC addresses for the client and server. The beginning of the FTP session is shown in packet 5 in Figure 10-30a. The packet shows that a connection is being made from a Windows server to port 1054 on a client computer. In packet 8, the client is responding with the username **administrator**. In packet 9, the server is telling the client that a password is required. The client responds with the password **Chile** in packet 11.



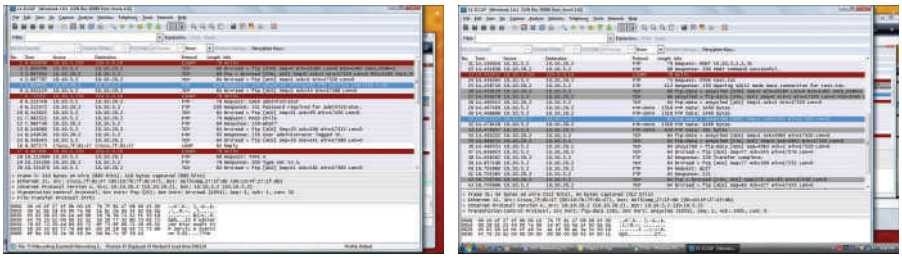
FIGURE 10-29 The computer setup for the FTP packet transfer.

SFTP
Secure File Transfer Protocol

Notice that the password is in plaintext (not encrypted). This is why most FTP applications use Secure FTP (**SFTP**) at port 22. With SFTP, all messages between the server and the client are encrypted.

SFTP (FTP over SSH) and FTPS (FTP over SSL) are the two main protocols available for secure FTP transfers. SFTP and FTPS both offer high levels of data encryption.

In packet 14, the server acknowledges that the user **administrator** is connected to the server. In packet 18, the client is notifying the server that an ASCII data transfer is requested. This is indicated in the Type A statement. In packet 19, the server acknowledges that an ASCII transfer is requested (**Type set to A**). Packet 24 in Figure 10-30b is a request from the client to start the data packet transfer from the server. The text **STOR text.txt** signifies this. In packet 25, the server indicates that it is opening the ASCII mode for the transfer. When the FTP connection is established, the port numbers change to handle the data transfer, as shown in packet 31, with SP = 20 and DP = 1055. Packets 38, 40, and 41 are the closing of the FTP transfer. These FTP data packets are part of a TCP connection. In this example, a TCP connection must have been both established and closed. (The TCP initial handshake and the connection closing for this FTP session are presented in Section 6-2 in Chapter 6.)



(a) (b)

FIGURE 10-30 (a) The beginning of the FTP data packet transfer and the request for an ASCII data transfer by the client. (b) The FTP data packet transfer and the closing of the FTP transfer.

Section 10-9 Review

This section covers the following Network+ exam objectives.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

This section examines Secure File Transfer Protocol (SFTP).

5.3 Given a scenario, use the appropriate network software tools and commands.

This section examines the use the Wireshark protocol analyzer.

Test Your Knowledge

1. True or false: The purpose of an echo request is to obtain the MAC address for a given IP address.

   True

2. True or false: The purpose of an ARP reply is to acquire the IP address.

   False

3. Which TCP port number(s) does SFTP use?

   a. 20
   b. 25
   c. 22
   d. 80, 443

4. When "type set to A" is requested by the client, what is the type of FTP transfer?

   a. Binary
   b. Mixed Mode
   c. ASCII
   d. None of the above

10-10 TROUBLESHOOTING IP NETWORKS

This section introduces the techniques and issues involved in troubleshooting modern computer networks. Make sure students develop a good understanding of the concepts presented in this section.

The network environment today is very different from the network environment of a decade ago. No longer are computing devices stationary; we now have mobile computing devices like laptops, tablets, and phones that constantly move in and out of networks. It is more difficult now to restrict the type, make, model, and operating system of the devices that can be on a network, especially on public or open networks. Most networks today are embracing the concept of **BYOD** (bring your own device), which allows users to connect their own computing devices to a network. BYOD adds complexity to the network environment.

BYOD
Bring your own device, a policy that allows users to connect their own computing devices to a network

BYOD used to refer to devices like personal computers and mobile devices that users will need connecting, but that scope now has expanded. This is due to the growing number of Internet of Things (**IoT**) devices, which are any network devices that are connected to the Internet. These devices are sometimes referred to as **smart devices**. These devices are not just computers but include household appliances and devices like TVs, refrigerators, washers, dryers, and thermostats. Smart devices are appearing everywhere. They can communicate over the Internet, and people can communicate with them over the Internet as well. Many different types of device hardware with different operating systems are therefore using different protocols to access a network. However, they all rely on IP networks, and they all operate within the realm of OSI layers.

IoT
Internet of Things devices that are connected to the Internet

Smart Device
A device that is networkable and connected to the Internet

This section discusses troubleshooting of IP network problems. When a network problem occurs, it is typically reported by users or detected by network monitoring tools and then routed through the standard IT troubleshooting protocol of the organization.

Many organizations implement some kind of trouble tracking system, and the first line of support is typically the help desk, sometimes referred to as *tier 1 support*. All the problems are filtered through tier 1; information is gathered, and problem symptoms are identified. If a problem is reported by users, the help desk interacts with and questions users to get as much problem information from them as possible. The help desk consults documentation for known problems and checks for recent changes on the network. Sometimes, help desk staff try to duplicate a user's problems in order to better understand the symptoms. Most basic problems can be solved at this level; those that can't are escalated to more advanced tiers.

A network problem should be well documented by the time it reaches the next level of support. With a problem defined and information gathered, it is time to figure out what happened. All probable causes should be considered to really establish a theory of probable cause. Again, it is a good idea to determine whether anything has changed that could have caused the problem. Typically, you base a theory on what is obvious or stands out the most regarding an issue. Then you can start troubleshooting to test the theory to confirm or deny the actual cause of the problem.

Note

If multiple network problems are reported at the same time, each of them should be worked on individually.

There are many troubleshooting approaches, but the following are some of the recommended structured troubleshooting approaches based on the OSI seven-layer model:

- **Bottom-to-top (or bottom-up) approach:** This approach involves starting at the physical layer (layer 1) of the OSI model and working up to the application layer (layer 7).
- **Top-to-bottom (or top-down) approach:** This is the opposite of the bottom-to-top approach: Network troubleshooting starts from the application layer (layer 7) and works down to the physical layer (layer 1).
- **Divide-and-conquer approach:** This approach divides the OSI layers in half and starts at the middle of the stack, which is the network layer (layer 3). The network layer is examined first and then the troubleshooting steps can move up or down, depending on the findings at the network layer.
- **Spot-the-difference approach:** In this common troubleshooting approach, a comparison between the working and non-working network environment or configurations is made. This approach uses the differences as guides in troubleshooting.

In troubleshooting, if your theory is not confirmed, you have to establish a new theory. If the theory is confirmed, then you need to establish a plan of action to resolve the problem and implement the solution. It is very important to analyze and identify the potential impacts of a solution.

Many organizations have a formal change control policy that provides guidelines for the change process and how it can be implemented. With or without a change control policy, a proposed solution must be reviewed and approved before it is implemented. It is a best practice to communicate to all the affected parties regarding the changes that will be made due to a solution.

Also, implementations that may cause network disruptions are typically scheduled after hours or during low usage times. After the implementation of a solution, there must be a verification of full system functionality; what was operational before must still be operational. Also, you must verify whether a proposed solution solves the problem. If so, you should look for any preventive measures and implement them. If the problem still exists, you have to go back to the list of probable causes and come up with another solution.

The last step—and the most important one—is to document everything: findings, actions, and results. In the world of networking, history does repeat itself. Documentation can save network administrators time and effort when the same problem occurs in the future. In addition, it is a way to share knowledge with other network administrators, who may have to deal with the very same problem.

Bottom-to-Top (or Bottom-Up) Approach
A network troubleshooting approach that starts at the physical layer of the OSI model and works up to the application layer

Top-to-Bottom (or Top-Down) Approach
A network troubleshooting approach that starts from the application layer and works down to the physical layer

Divide-and-Conquer Approach
A network troubleshooting approach that divides the OSI layers in half and starts at the middle of the stack, which is the network layer

Spot-the-Difference Approach
A network troubleshooting approach in which a comparison between working and non-working network environments or configurations is made

The methodology just described establishes an overall baseline for dealing with network problems. It can also lend itself to many IT-related problems. The following sections describe some techniques that are commonly used to troubleshoot some well-known IP networking problems.

Verifying Network Settings

One of the first steps—if not the first step—of network troubleshooting is to verify the network settings. This means simply verifying the network identity of the device and ensuring that its network configuration settings are correct for the network that it is connected to. You need to verify that the settings are valid and the device is on the right network. Knowledge of the network environment is necessary. Each network or subnet has its own permissible IP address range, subnet mask, and gateway. The device's network configuration must match what the network or subnet is configured for.

In Windows, the command **ipconfig /all** yields network settings such as IP address, subnet mask, gateway, and DNS server. On macOS and Linux, the **ifconfig** command yields the basic IP address and subnet mask information for each interface name, such as en0, en1, and so on. Newer Linux versions use the command **ip address show** instead of **ifconfig**. On macOS, the command **ipconfig getpacket [***interface_name***]** obtains the same network information retrieved by the Windows command **ipconfig /all**. On Linux, there is no single command that can display all network information.

Investigating IP Address Issues

If a device's IP address is wrong for a network, that device will not be able to communicate at all. In a situation where an incorrect IP address is given as the destination, the router sends the data packet to an incorrect device. Sometimes, the IP address of a device is correct and the device is on the right network, but there is a duplicate IP address. In that case, the device will cease to work on the network or will work sporadically, depending on the operating system. The IP conflict situation does not happen as often when network devices all get their IP settings from the DHCP server. An IP address conflict typically happens when the IP settings are manually configured, therefore resulting in a misconfigured device. Most operating systems do a good job of detecting an IP conflict and issue an error message. In most cases, the OS software prevents the devices from using the conflicted IP address and reports the offending device information, including the MAC address. This information can be used to track down the culprit.

There can also be a duplicate MAC address on a network. This occurs rarely because the MAC address value is not configurable in most operating systems. Therefore, it has to be intentionally manipulated. A duplicate MAC address causes intermittent connectivity issues on the two devices with the same MAC address that are on the same network segment or the same VLAN. Some switches, like Cisco switches, report a MAC flapping event when they detect duplicate MAC addresses on different ports.

Finding Subnet Mask Issues

Because the subnet mask (or netmask) defines the size of the network, when a device has an incorrect subnet mask or an incorrect netmask, it creates a mismatch

in the network size, and it also could potentially result in different network addresses and broadcast addresses from the intended network configuration. This may result in no connectivity between devices. It may also result in no connectivity beyond the network if the subnet mask caused its default gateway to be on a different network.

Looking for Gateway Issues

When a device needs to communicate to other devices that are not on the same network or on the Internet, it needs a gateway. When the gateway is wrong or when there is an incorrect gateway, the device has no connectivity beyond its network. A basic ping test can be used to verify a gateway issue; you can ping another device on the same network and then try to ping other IP addresses outside the network. When the gateway is down or is not reachable, you see symptoms similar to those you see when you have a wrong gateway. A simple ping test to the gateway IP address can verify the gateway's existence.

Identifying Name Resolution Issues

Name resolution issues are some of the most overlooked network issues. When name resolution is not working properly, users tend to mistake the problem for the network being down because they cannot do their typical activities, like browsing the web, checking email, and using network services. Most of these activities are designed to work with hostnames, not IP addresses. Therefore, name resolution is needed to translate the human-readable hostnames to IP addresses.

Name resolution, as discussed earlier in this chapter, relies on DNS servers. Incorrect DNS server information will result in names not resolving. When the DNS server cannot be reached, there is no way to obtain the IP address of the destination, which results in a lack of connectivity to the intended destination. In order to troubleshoot this, it is best to remember a handful of well-known IP addresses both inside the network and outside, on the Internet. If you can successfully ping those IP addresses, the basic IP connectivity is there.

Note

A popular IP address on the Internet that you can ping is 8.8.8.8, which is one of Google's public domain name servers.

Another step in troubleshooting DNS issues is to verify whether the configured DNS servers are reachable and operational. To verify whether a DNS server is reachable and operational, you use the command **nslookup**. If it yields an error, as shown here, then you know the DNS servers are having issues:

```
C:\ nslookup www.google.com
;; connection timed out; no servers could be reached
```

Investigating DHCP Issues

With all the issues mentioned previously, misconfiguration of the network settings is not the issue if a computer obtains its network configuration settings from the DHCP (Dynamic Host Configuration Protocol) server and if DHCP is working

properly. If a computer is configured to use DHCP and cannot contact its DHCP server or if the DHCP server is not available, most operating systems automatically self-assign an IP address by using Automatic Private IP Addressing (APIPA), which uses the reserved IP address range 169.254.0.0 to 169.254.255.255. (Sometimes this is also referred to as a *169 IP address* because its starting prefix is always 169.) This address is very recognizable and a great indication when a computer cannot obtain its DHCP configuration settings.

Another DHCP issue that causes a computer to receive a 169 IP address is exhausted DHCP scope. This could happen when the DHCP server cannot lease out an IP address due to its DHCP pool being depleted. To typical users, though, getting a 169 IP address may be confusing because it looks to them just like any other IP address. Often during troubleshooting, when asked if a computer has an IP address, users answer yes. IT support has to be mindful to inquire further about the IP addresses that users obtain.

Another issue that can arise with DHCP is a rogue DHCP server scenario. Every network has a legitimate DHCP server, from which it should get its authentic network configuration settings. However, when there is an illegitimate DHCP server (called a rogue DHCP server) on the same local network and it is serving out a different set of network configuration settings, the information is invalid and, in most cases, will lead to no connectivity to those DHCP devices. A rogue DHCP server sometimes occurs unintentionally as a result of misconfiguration of a network device. This happens more frequently than you might think as many devices bought from stores come preconfigured with many network services enabled, from web services to file sharing services to DHCP. When such a device is connected to a local network, it may inadvertently become a rogue DHCP server and start responding to DHCP requests.

To remedy a rogue DHCP server issue, you need to track it and shut it down. From a client's perspective, this is a difficult issue to resolve, as the client may not have access to track or the ability to shut down the server. The best the client could possibly do is to manually change the network configuration, but this is only a temporary solution. A user can verify the identity of a DHCP server by using the command **ipconfig /all** on Windows.

DHCP Snooping
A feature that can be enabled to specify the trusted DHCP source where a switch blocks the DHCP messages from the untrusted sources

Fortunately, network switches today have a feature to safeguard against non-legitimate DHCP servers. This feature, called **DHCP snooping**, can be enabled to specify the trusted DHCP source; the switch then blocks DHCP messages from the untrusted sources.

In order to configure DHCP snooping properly, you must enable it globally with the command **ip dhcp snooping**. Then you need to specify the trusted DHCP interface with the command **ip dhcp snooping trust:**

```
Switch(config)# ip dhcp snooping
Switch(config)#
Switch(config)# int gigabitEthernet 0/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)#
```

The trusted interface is the interface to which the legitimate DHCP server is connected or sending its DHCP information. All other switch interfaces without the trust configuration are considered untrusted. Any DHCP message seen coming from these untrusted ports will be filtered.

Checking for Blocked TCP/UDP Ports

Of all the issues discussed in this section, blocked TCP/UDP ports are some of the most difficult ones to diagnose; these issues can be very time-consuming to troubleshoot. To typical users, this type of problem appears like a sporadic connectivity issue as they can connect to certain services but not others. Even network administrators who have good knowledge of TCP/UDP ports and what services they represent can be stumped. For example, if TCP port 25 is blocked, users can receive emails but cannot send emails. To make the issue more complicated, if UDP port 53 is blocked, DNS communications are not permissible. This might appear to be a DNS server issue, but it is actually not. TCP and UDP ports are usually blocked at the routers or firewalls as part of the access list or filter list. Therefore, troubleshooting this issue may require collaboration with a router or firewall administrator.

Section 10-10 Review

This section covers the following Network+ exam objectives.

4.3 Given a scenario, apply network hardening techniques.
This section introduces DHCP snooping and the configuration steps you can take to prevent it.

5.1 Explain the network troubleshooting methodology.
Many troubleshooting concepts are presented in this section, including divide-and-conquer.

5.3 Given a scenario, use the appropriate network software tools and commands.
This section introduces common network service issues.

5.5 Given a scenario, troubleshoot general networking issues.
This section examines issues such as gateway issues.

Test Your Knowledge

1. BYOD devices allow users to do which of the following?
   a. Connect their own devices to a network
   b. Set an IP address
   c. Set a MAC address
   d. All of the above are correct.
2. Which of the following is true of the Internet of Things?
   a. It is a collection of smart devices.
   b. It is a collection of typical devices that are networkable and connected to the Internet.
   c. It relies on IP networks and operates within the realm of the OSI layers.
   d. All of the above are correct.

SUMMARY

This chapter shows a network protocol analyzer in action and explains the steps for capturing data packets as well as analyzing the captured data. This chapter also presents the steps for troubleshooting router and switch interfaces. This chapter introduces analysis of data traffic a network administrator might monitor and the various commands to use. In this chapter, you've also learned about the function of DHCP and DNS network services and how to analyze network data traffic by using SNMP, NetFlow, and Wireshark. This chapter concludes with a look at troubleshooting wireless and IP networks.

QUESTIONS AND PROBLEMS

Section 10-2

1. What are the two key elements used by the general population when accessing websites on the Internet?

   The Internet name of a website and its public IP address

2. What is the purpose of IANA?

   IANA was set up to be in charge of the Internet management authorities or registration authorities.

3. .com is an example of which of the following?

   a. The DNS root zone for a cc top-level domain
   b. The DNS root zone for a d top-level domain
   c. The DNS root zone for a g top-level domain
   d. The DNS root zone for an int top-level domain

4. What does gTLD stand for?

   a. Global top-level domain
   b. Generic top-level domain
   c. Gated top-level domain
   d. None of the above

5. What are the .int domain registries?

   .int is the intergovernmental domain registries which are exclusive registrations for intergovernmental treaty organizations, such as the United Nations (un.int) and NATO (nato.int).

6. What is the purpose of the Repository of IDN (Internationalized Domain Name) Practices?

   This repository, also known as the language table registry, allows for domain name registration containing international characters (for example, müller.info).

7. What are the three primary functions of IANA? (Select three.)

    a. Domain name management
    b. Portal assignment
    c. Numbers resource management
    d. Protocol assignment
    e. ASE number allocation

8. What organization is responsible for IP address assignment in North America?

    American Registry for Internet Numbers (ARIN)

9. ARIN is responsible for assigning IP addresses to which of the following? (Select two.)

    a. Internet service providers
    b. Home networks
    c. Corporate networks
    d. Larger numbers of end users

10. Which of the following are world Regional Internet Registries?

    a. AfriNIC
    b. AFrNIC
    c. LACNIC
    d. ARIN
    e. AIRN

11. What is the purpose of the in-addr.arpa domain?

    It is the reverse DNS lookup for IPv4 addresses on the Internet.

12. Who handles the assignment of domain names?

    a. CANN
    b. Domain registrars
    c. Network administrators
    d. TLDs

13. What protocol is used to query databases that store user registration information for an Internet domain name and IP space?

    a. whois protocol
    b. whereis protocol
    c. whatis protocol
    d. None of the above are correct.

Section 10-3

14. In regard to campus DHCP service, IP address assignment is based on what?

    The subnet where the computer is located

15. How are BOOTP and DHCP related?

    DHCP is a superset of BOOTP, and both use ports 67 and 68.

16. Define lease time.

    The amount of time that a client can hold an IP address

17. What networking function is required if a DHCP server is not on the same LAN? Why is this networking function required?

    A DHCP relay is required because the computer doesn't have a routable address until one is assigned by the DHCP server.

18. What command enables a DHCP relay on a Cisco router?

    ip helper [*IP address of the DHCP server***]**

19. Why is packet 14 in the captured DHCP packets shown in Figure 10-4 (shown earlier in the chapter) a broadcast?

    The host computer still doesn't have an IP address.

20. What are the port numbers for DHCP?

    Port 67: DHCP server

    Port 68: DHCP client

21. What command is used to initiate the DHCP process?

    ipconfig /renew

22. What happens if a DHCP server is not available?

    a. The client issues a global broadcast to search for an available DHCP server.

    b. The host computer issues a unicast packet to the 169.254.1.1 address and then obtains an IP address.

    c. A DHCP client uses a self-assigned IP address via Automatic Private IP Addressing (APIPA).

    d. The **ipconfig /redo** command is automatically issued to establish connectivity.

23. What command do you use on a router to enable the DHCP relay function?

    ip helper [*ip address of the DHCP server***]**

24. What information is contained in an MT Offer (DHCP Offer) packet? (Select three.)

    a. Default gateway
    b. Leased time
    c. Internet address
    d. IP address of the DNS server
    e. Hostname

25. What does a gratuitous ARP broadcast do?

    It informs everyone on the network that it is now the owner of a particular IP address.

26. What is the purpose of the command **ip dhcp pool address-pool**?

    This command establishes an DHCP pool with the name **address-pool**.

27. The following commands are entered into a router. Explain what they do.

```
RouterA(dhcp-config)# dns-server 192.168.10.52
RouterA(dhcp-config)# domain-name networks.com
RouterA(dhcp-config)# default-router 192.168.10.1
```

    These commands define the DNS server, the domain name, and the gateway to the DHCP pool.

28. What information does a NOC typically associate with an IP address?

    The NOC database contains the MAC address, the IP address, and the name of the person who uses the computer.

Section 10-4

29. How is IP addressing typically handled in a home network?

    IP addressing for a home network is managed by a router or wireless router that connects to the ISP. The ISP issues an IP address to the router from an available pool of IP addresses managed by the ISP. The computers in the home network are issued private IP addresses by the router.

30. What happens in Port Address Translation (PAT)?

    A port number is attached to a network connection. This port number identifies the device that is establishing a connection to the Internet. This number is used when a data packet is returned to the home network. The port number identifies the device that established the Internet connection, and the router can deliver the data packet to the correct device.

31. A router on a home network is assigned IP address 128.123.45.67. A computer in the home network is assigned the private IP address 192.168.10.62. This computer is assigned the public IP address 128.123.45.67:1922. Which IP address is used for routing data packets on the Internet? Is overloading being used?

    The IP address 128.123.45.67:1922 is used for routing the data packets on the Internet. Yes, overloading is being used because one routable IP address is being shared by the home network.

32. For Cisco routers, what is a local address?

    A local address is any IP address that is on the inside of or internal to the network.

33. For Cisco routers, what is a global address*?*

    A global address is used to define any IP address that is on the outside of or external to the network.

34. If the interface FastEthernet0/0 is the interface for the internal private LAN and the interface FastEthernet0/1 is the interface facing the public Internet, what configuration commands are used, and what are the appropriate NAT interfaces?

```
RouterA(config)# interface FastEthernet0/0
RouterA(config-if)# ip nat inside
RouterA(config)# interface FastEthernet0/1
RouterA(config-if)# ip nat outside
```

35. What does the following command do?

```
RouterA(config)# ip nat inside source static 10.10.20.1
128.123.14.10
```

    This command maps the inside private IP address 10.10.20.1 to the outside public IP address 128.123.14.10 entirely. This host appears to the outside world as 128.123.14.10 and is accessible from the outside via the very same public IP address.

36. What does the following command do?

```
RouterA(config)# ip nat inside source static tcp 192.168.12.5 443
12.0.0.5 443
```

    This command maps TCP port 443 of the inside IP address 192.168.12.5 to the TCP port 443 of the outside IP address 12.0.0.5. This covers all secure web traffic ports.

37. What does the following command do? Does this bring up any security concerns?

```
RouterA(config)# ip nat inside source static 10.10.20.1 15.1.1.2
```

This command maps the inside private IP address 10.10.20.1 to the outside public IP address 15.1.1.2 entirely. There is no port translation when the internal host 10.10.20.1 is making a connection outside. This host appears to the outside world as 15.1.1.2 and is accessible from the outside via the very same public IP address. In the event that an internal server needs to be reached from the outside, static NAT can be used. However, this brings up a security concern of exposing an IP address entirely to the external network, so static NAT is usually discouraged.

38. The command **show ip nat translation** is entered on a router. The following information is displayed. What does it show?

```
RouterA# show ip nat translation
Pro Inside global  Inside local     Outside local   Outside global
tcp 15.1.1.2:35425 10.10.20.1:35425 55.105.35.15:80 55.105.35.15:80
```

The **Pro** column lists the protocol (for example, TCP, UDP, ICMP) being translated. **Inside global** is the global IP address used by the inside IP address after the NAT process. **Inside local** is the inside IP address. **Outside local** corresponds to the destination IP address of the inside local address before NAT translation. **Outside global** corresponds to the destination IP address of the inside global address after NAT translation.

39. What is the maximum theoretical number of ports that a single IP address can use?

About 64,000

Section 10-5

40. List 11 top-level domains.

.com, .net., .org, .edu, .mil, .gov, .us, .ca, .info, .biz, .tv

41. What is the purpose of a root server in DNS?

The root server knows the IP addresses for the top-level domains.

42. An administrator wants to obtain a domain name for a new network. What is the first step?

Go to www.internic.net and select a company that registers domain names.

43. Where are the hostname and IP address for a computer stored for a campus DNS service?

In the A records

44. How is it possible for the command **ping www.networkB.edu** to find the destination without an IP address?

    DNS provides name-to-IP address translation for www.networkB.edu.

45. What is the purpose of a reverse DNS lookup? Where is it used?

    It returns a hostname for an IP address. A reverse DNS lookup is used to verify that a connection is being made by a machine from an authorized network.

46. What is the purpose of a forward DNS lookup?

    A forward DNS lookup provides a translation of a domain name or a hostname to an IP address.

47. What does the root hints file contain?

    A list of the most up-to-date root servers

48. In regard to the Internet, what is a domain?

    A domain is an Internet domain name that represents an organization or entity.

49. What is an authoritative name server?

    It is a name server that is authorized and configured to answer DNS queries for a particular domain or zone.

50. Explain how a machine obtains the IP address of a website on the Internet.

    Refer to Section 10-5.

51. The following entry is made on a Linux server. Describe what it does.

```
[admin@noc ~]$  dig +trace www.example.com
```

    This command traces every step of the name lookup process.

52. What does it mean to be a non-authoritative name server?

    A non-authoritative name server does not contain a copy of the domain requested; therefore, it is not authorized to answer the query.

53. What is a fully qualified domain name (FQDN)?

    It contains the full path of a domain name.

54. What is the difference between a domain and a zone?

    There is no difference. These terms are used interchangeably.

55. What is the Start of Authority (SOA) record?

    It marks the start of a zone and provides the technical details of the zone, such as zone name, the primary authoritative name server, the email address of the domain administrator, the serial number of the domain, the TTL (Time to Live) of the domain, and the refresh, retry, and expiration times for the secondary name server.

56. Which record is a mapping of an IP address to a hostname and is sometimes referred to as a reverse record?

    The PTR (Pointer) record

57. What does the following information show?

```
www.iana.org
canonical name = ianawww.vip.icann.org.
```

    This shows that www.iana.org is actually the name of an A record for ianawww.vip.icann.org.

58. Where is the authoritative name server of a domain listed?

    In the NS record

59. What is the purpose of the TXT record?

    It is used to hold arbitrary text information for the domain.

Section 10-6

60. Which port number does SNMP use, and which transport protocol?

    Port 161 and UDP

61. What information does the SNMP MIB get request ifDescr return from a router?

    A description of the router's interfaces

62. What is the purpose of an MIB?

    It is a collection of standard objects that are used to obtain configuration parameters and performance data on networking devices.

63. Which SNMP MIBs can be used to return the number of octets of data that have left the router interface?

    if out Octets

    Note: the plots show both inbound and outbound bits.

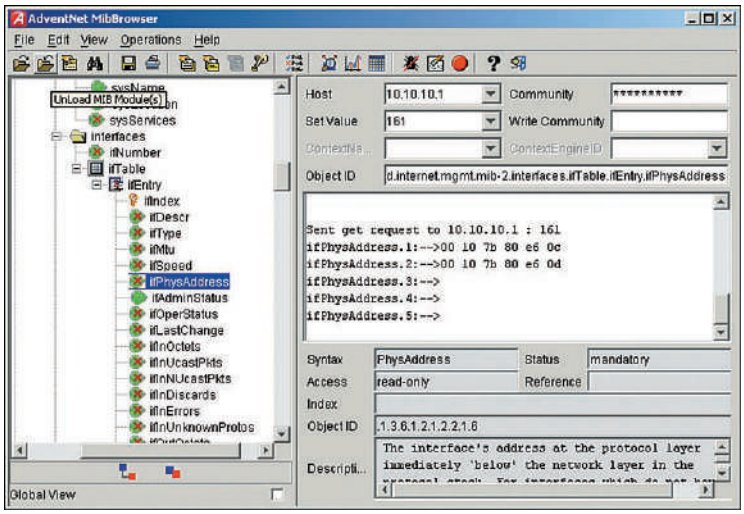


FIGURE 10-31 Figure for problems 64–68.

64. In Figure 10-31, which MIB was issued?

    IfPhysAddress

65. In Figure 10-31, what information is returned?

    The physical (MAC) address for the networking device

66. In Figure 10-31, which port number is used?

    Port 161

67. In Figure 10-31, which protocol is being used? How do you know?

    SNMP, because the connection is to port 161 (which is a well-known port number)

68. In Figure 10-31, who is the manufacturer of this networking device?

    The OUI 00-10-7b indicates that this is a Cisco router.

Section 10-7

69. What is an expected percentage utilization for a network?

    The answer varies for different networks, and there is not a single specific answer.

70. If you suspect that you have a physical OSI layer 1 issue with a router interface, which SNMP information can help you investigate the issue?

    Errors per second

71. What is outbound data traffic?

    Data traffic leaving the network

72. What does MTU stand for, and what is the significance of the MTU?

    MTU stands for maximum transmission unit, which indicates the value (in bytes) of the largest packet that can be sent across a network link.

73. What does SIEM stand for, and what is SIEM used for?

    SIEM stands for security information and event management. It can be used to provide a holistic view and real-time analysis of an organization's network and security.

74. What does SEM stand for?

    Security event management

75. What is iPerf used for?

    It is used to test and measure bandwidth capacity.

Section 10-8

76. What does ARP stand for?

    Address Resolution Protocol

77. What is the purpose of an ARP request?

    It looks for a station's MAC address when its IP address is already known.

78. What does ICMP stand for?

    Internet Control Message Protocol

79. What is an echo request?

    It is part of ICMP that requests a reply from a computer.

80. What is the purpose of a protocol analyzer?

    A protocol analyzer has the capability to capture and decode data packets and to inspect the contents of the packets. This enables a network administrator to investigate how information is being transferred in the network. In addition, this information enables a user to detect, identify, and correct network problems.

Included on the companion website in the Wireshark capture file folder is a network packet capture file Ch10-a.cap. Open this file using Wireshark. Problems 81–85 refer to this file.

81. What are the three MAC addresses used in this capture?

    00-10-A4-13-99-2E

    00-B0-D0-25-BF-48

    00-10-A4-13-6C-6E

82. Which IP addresses correspond to each MAC address?

    00-10-A4-13-99-2E: 10.10.10.1

    00-B0-D0-25-BF-48: 10.10.10.3

    00-10-A4-13-6C-6E: 10.10.10.2

83. Which packet IDs correspond to ARP requests?

    000001

    000005

84. Which packet IDs correspond to ARP replies?

    000002

    000006

85. Which computers are pinging which computers?

    10.10.10.1 is pinging 10.10.10.2

    10.10.10.3 is pinging 10.10.10.1

Section 10-9

86. What are the server port numbers for an FTP transfer?

    Ports 20 and 21

87. How does a client notify a server that an ASCII data transfer is requested?

    By sending a Type A statement

Included on the companion website in the Wireshark capture file folder is a network packet capture file 10-hw.cap. Open this file using Wireshark. Problems 88–96 refer to this file.

88. What routing protocols are used in this network?

    RIP and EIGRP

89. In the FTP exchange, what operating system is the server running?

    Windows 2000 (from Packet ID# 5)

90. What is the destination address for the FTP server?

    10.10.20.2 (from Packet ID# 2)

91. What is the source address for the FTP transfer?

    10.10.5.2 (from Packet ID# 2)

92. What is the username sent to the FTP server?

    Aaron (from Packet ID# 7)

93. What is the password sent to the FTP server?

    Taco (from Packet ID# 11)

94. What is the name of the file sent over FTP?

    data (from Packet ID# 23)

95. What are the contents of the file?

    The results of a ping to 10.10.20.2 (from Packet ID# 28)

96. From Packet ID# 8, what is the FTP server requesting from the host?

    The password for Aaron

Section 10-10

97. How does the top-to-bottom, or top-down, approach to troubleshooting work?

    Network troubleshooting starts from the application layer (layer 7) and works down to the physical layer (layer 1).

98. How does the bottom-to-top, or bottom-up, approach to troubleshooting work?

    This approach starts at the physical layer (layer 1) of OSI and works up to the application layer (layer 7).

99. What is the divide-and-conquer approach to troubleshooting?

    This approach divides the OSI layers in half and starts at the middle of the stack, which is the network layer (layer 3).

100. What is the spot-the-difference approach to troubleshooting?

     This approach involves making a comparison between working and nonworking network environments or configurations.

101. What is a change control policy?

     It is a policy that provides guidelines for the change process. It is a best practice to communicate to all the affected parties regarding the changes that will be made due to a solution.

102. Why is documentation important?

     History does repeat itself, and documentation will save network administrators time and effort when the same problem occurs in the future. In addition, documentation enables network administrators to share information with each other.

103. What command would yield the network settings IP address, subnet mask, gateway, and DNS server on a Windows computer?

     a. **ifconfig**
     b. **ipconfig**
     c. **ipconfig /all**
     d. **netstat -a**

104. Which command displays a network interface configuration in Linux?

    a. **ifconfig**
    b. **ipconfig**
    c. **ipconfig /all**
    d. **netstat -a**

105. Why is a gateway address needed?

    a. It connects to other networking devices in a LAN.
    b. It allows a device to communicate with other devices that are not on the same network or on the Internet.
    c. It is used to eliminate the need for a router. The PC just forwards a packet to the gateway, and TCP/IP delivers it.
    d. It is used to eliminate the need for a router. The PC just forwards a packet to the gateway, and DNS/DHCP delivers it.

106. How can you verify the existence of a gateway?

    a. Configure a reverse DNS lookup.
    b. Issue the **ping** command to 8.8.8.8. A reply indicates existence of the gateway.
    c. Ping another device on the same network and then try to ping other IP addresses outside the network.
    d. Use **nslookup** to verify that the gateway is reachable and operational. If it yields an error, the gateway is not having issues.

107. To verify if DNS is reachable and operational, which of the following commands do you use?

    a. **lookup**
    b. **nslookup**
    c. **n-slookup**
    d. **dns-lookup**

108. Which of the following is true of a self-assigned IP address?

    a. Automatic Private IP Addressing (APIPA) uses the reserved IP address range 169.254.0.0 to 169.254.255.255.
    b. Automatic Private IP Addressing (APIPA) uses the reserved IP address range 127.254.1.0 to 127.254.254.255.
    c. Automatic Private IP Addressing (APIPA) uses the reserved IP address range 168.254.1.0 to 169.254.255.255.
    d. Automatic Private IP Addressing (APIPA) uses the reserved IP address range 10.10.1.0 to 10.254.254.255.

109. What is DHCP snooping?

a. A feature that can be disabled to specify the trusted DHCP source; the switch will block the DHCP messages from the untrusted sources.

b. A feature that can be enabled to specify the trusted DNS source; the switch will then block the DHCP messages from the untrusted sources.

c. A feature that can be enabled to specify the untrusted DHCP source; the switch will pass the DHCP messages to the untrusted sources.

d. A feature that can be enabled to specify the trusted DHCP source; the switch will block the DHCP messages from the untrusted sources.

110. What command is used to globally enable DHCP snooping?

a. **ip dhcp snoop**

b. **ip dhcp snooping**

c. **tcp/ip dhcp snooping**

d. **tcp dhcp snooping**

Certification Questions

111. What command do you use to set the trusted DHCP interface?

a. **ip dhcp trust**

b. **ip dhcp trust snooping**

c. **ip dhcp snoop trust**

d. **ip dhcp snooping trust**

112. Write the Cisco router commands for configuring SNMP on a Cisco router. Assume a community string for networking and set the permissions to read-only. Show the router prompts.

```
router# snmp community networking ro
router# snmp community network ro
router(config)# snmp community networking ro
```

113. Which of the following are examples of ccTLDs? (Select two.)

a. .net

b. .uk

c. .org

d. .au

114. What command is used to release a current IP address on a Windows computer?

ipconfig /release

115. What is dynamic NAT?

It is a one-to-one mapping from an available global pool of IP addresses.

116. The command **show run** is entered on a Cisco router. Describe what the output **SNMP-server test RO** means.

a. It indicates that SNMP services have been disabled on the router.

b. It indicates that SNMP services have been configured on the router, the community string is **test**, and access is limited to read-only.

c. RO indicates that SNMP server has a Request for Offset.

This page intentionally left blank

11
CHAPTER

Network Security

Chapter Outline

11-1 Introduction
11-2 Intrusion: How Attackers Gain Control of a Network
11-3 Denial-of-Service
11-4 Security Software and Hardware
11-5 Managing Network Access
11-6 Router Security
11-7 Switch Security
11-8 Wireless Security
11-9 Remote Access and VPN Technologies
11-10 Physical Security
Summary
Questions and Problems

Objectives

- Examine how attackers gain control of a network
- Understand how denial-of-service attacks are initiated
- Examine the security software and hardware used to protect a network
- Understand VPN technologies
- Understand wireless security issues

Key Terms

social engineering
password cracking
dictionary attack
brute-force attack
packet sniffing
IPsec
on-path/man-in-the-middle
ARP cache poisoning
evil twin
session hijacking
buffer overflow
netstat -a
netstat -b
nmap
penetration testing
virus
worm
malware
logic bomb
zero-day attack
ransomware
denial-of-service (DoS)
distributed denial of service (DDOS)
directed broadcast
permanent DoS (PDoS)
spoof
reflective/amplified DoS attack
deauthentication attack
coordinated attack
firewall
access control list (ACL)
access-list permit ip any any
demilitarized zone (DMZ)/screened subnet
packet filtering
proxy server
stateful firewall
intrusion detection system (IDS) and intrusion prevention system (IPS)
packet shaper
authentication, authorization, and accounting (AAA)
role-based access control (RBAC)
line password
EXEC (privileged EXEC)
Type 7
Type 5
transport input none
crypto key generate rsa
logging
NTP
range
802.1X
switch port security (or port security)
sticky
BPDU Guard
Root Guard
jamming
SSID

Key Terms continued

beacon
Open Authentication
shared-key authentication
WEP
WPA
TKIP
AES
CCMP
LEAP (Lightweight Extensible Authentication Protocol)
EAP
RADIUS
war driving
war chalking
V.44/V.34
V.92/V.90
asymmetric operation
cable modem
DOCSIS
ranging
xDSL
DSL
ADSL
discrete multitone (DMT)
RAS
VPN
VPN headend
IP tunnel
remote access VPN
site-to-site VPN
client-to-site VPN
GRE
mGRE
PPP
PAP
CHAP
MD5
SHA
PPTP
L2F
L2TP
AH
ESP
DES, 3DES
IKE
ISAKMP
Diffie-Hellman
access control
surveillance
testing
motion detection
access control hardware
badge reader
locking rack
locking cabinet
access control vestibule/ mantrap
smart locker
factory reset
physical access control device
smart speaker
smart doorbell
sanitize device

An enterprise network is vulnerable to many types of network attacks. While network attacks can't be prevented, you can take steps to minimize the impact an attack has on a network. This chapter provides an overview of network security.

11-1 INTRODUCTION

A campus network is vulnerable to many types of network attacks. While network attacks can't be prevented, some steps can be taken to minimize the impact an attack has on the network. Students need to learn how attackers gain control of a network and how network administrators can minimize the potential for attacks.

The first type of attack examined in this chapter is intrusion, where an attacker gains access to a remote network system. There are many ways an attacker can gain access to a network, including social engineering, password cracking,

packet sniffing, vulnerable software, and viruses. These issues are examined in Section 11-2, "Intrusion: How Attackers Gain Control of a Network." The goal of a denial-of-service attack is to prevent services to a machine or network from working. This can be accomplished by flooding a network with lots of data packets or by hacking vulnerable software. For example, a particular software package might reboot if a certain sequence of data packets is sent to the host computer; this is a common problem because many software packages have this vulnerability. Section 11-3, "Denial-of-Service," examines denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.

Techniques for using security software and hardware such as firewalls to protect a network are examined in Section 11-4, "Security Software and Hardware." This section discusses the role of stateful firewalls in protecting a network. Section 11-5, "Managing Network Access," examines trusted sources more closely and explores the concepts and techniques used to identify trusted sources, grant access to trusted sources, and manage trusted source accessibility. Section 11-6, "Router Security," examines router security. Section 11-7, "Switch Security," examines switch security. Section 11-8, "Wireless Security," examines wireless security. Section 11-9, "Remote Access and VPN Technologies," examines both remote access and VPN technologies. The chapter concludes with Section 11-10, "Physical Security," which provides a brief overview of physical security for a networking facility.

Table 11-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 11-1 **Chapter 11 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes.	11-9
1.5	Explain common ports and protocols, their application, and encrypted alternatives.	11-3, 11-5, 11-6, 11-9
1.6	Explain the use and purpose of network services.	11-2, 11-3, 11-6
1.7	Explain basic corporate and datacenter network architecture.	11-2
1.8	Summarize cloud concepts and connectivity options.	11-2, 11-4, 11-9
2.0	**Network Implementations**	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	11-2, 11-4, 11-9
2.2	Compare and contrast routing technologies and bandwidth management concepts.	11-4

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
2.3	Given a scenario, configure and deploy common Ethernet switching features.	11-2, 11-4, 11-7
2.4	Given a scenario, install and configure the appropriate wireless standards and technologies.	11-2, 11-6, 11-8
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	11-5
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	11-2, 11-4, 11-5
4.0	**Network Security**	
4.1	Explain common security concepts.	11-3, 11-5, 11-8, 11-9
4.2	Compare and contrast common types of attacks.	11-2, 11-3
4.3	Given a scenario, apply network hardening techniques.	11-4, 11-8, 11-9
4.4	Compare and contrast remote access methods and security implications.	11-2, 11-8
4.5	Explain the importance of physical security.	11-4, 11-6, 11-10
5.0	**Network Troubleshooting**	
5.3	Given a scenario, use the appropriate network software tools and commands.	11-2, 11-3

11-2 INTRUSION: HOW ATTACKERS GAIN CONTROL OF A NETWORK

This section examines the many ways an attacker can gain control of a network. It covers social engineering, password cracking, packet sniffing, vulnerable software, buffer overflows, viruses, and wireless vulnerabilities. It is essential that students understand the potential for network intrusions and how attackers can get in. The section includes steps for protecting a network. If possible, demonstrate for students how easy it is to grab information from a network.

Hackers use many techniques to gain control of a network (see Figure 11-1). A network administrator needs to be aware of the various ways an intruder can gain network access and even control. A hacker already knows all the information presented in this chapter, and a network administrator needs to know it, too, to protect a network.

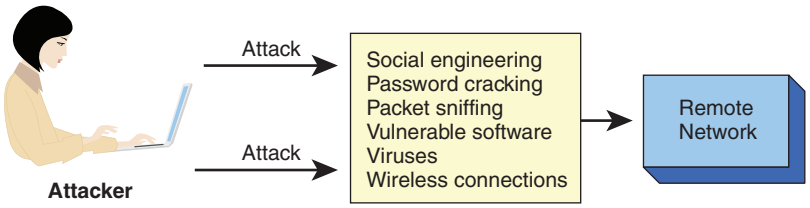


FIGURE 11-1 Some of the ways an attacker can gain access to a remote network.

Social Engineering

Social engineering is a method intruders use to get enough information from people to gain access to a network. For example, an attacker may call a network user and claim to be from the computer support division for the network. The attacker tells the user there is a problem with the user's account and asks for the user's username and password (see Figure 11-2). The user may blindly provide the information, not realizing that the person calling is not associated with the network and is in fact an attacker. Based on the user's information, the attacker now has an account from which to attack the network. This is just one example of social engineering. Attackers may also search through discarded trash to gain access to user passwords.

Social Engineering
A process by which an intruder obtains enough information from people to gain access to a network

As the number of users increases, so do the possible ways to attack the network. It is important to educate users about not sharing information on how they access the network and always requiring identification from support staff.

Another form of social engineering is shoulder surfing. As the name implies, shoulder surfing involves an attacker looking over a victim's shoulder to steal valuable information that the victim is entering into a computer or other device. The information can be a password, a PIN, credit card information, a Social Security number, or some other piece of sensitive information. Shoulder surfing can be thwarted with the use of special screen filters and user awareness training.

Social engineering tactics can also be used to gain access to physical facilities. For example, with tailgating, an intruder gains access to a facility or restricted area by sneaking in after an authorized person has opened the door to the area. This is done without consent and awareness of the authorized person. Piggybacking is similar to tailgating, but with the consent and the awareness of the authorized person.

Phishing is probably the most infamous kind of social engineering. It involves tricking a user into giving out credentials by redirecting the user to a fake website—for a bank account or email account, for example—that requires the person's username and password. Typically, phishing propagates through emails that ask users to click a link within the email that takes them to a phishing website.



FIGURE 11-2 An example of social engineering.

Password Cracking

Password Cracking
An attack in which the attacker tries to guess a user's password

If an attacker has access to a user's network but can't get the password from the user, the attacker may try **password cracking**. This can be done via brute-force or by checking for weak passwords. Most networks require users to use strong passwords and have policies specifying password complexity and length. Most operating systems support strong password policies. Avoiding common passwords is very important in preventing network intrusion.

Dictionary Attack
An attack that involves using known passwords and many variations (uppercase and lowercase and combinations) to try to log in to an account

Brute-Force Attack
An attack in which the attacker uses every possible combination of characters to guess the password

In password cracking, an attacker may try to guess the user's password. One method for doing so is a **dictionary attack** (see Figure 11-3), which involves using known passwords and many variations (uppercase and lowercase and combinations) to try to log in to an account. This is why many network systems prompt you not to use a dictionary word as a password. In a **brute-force attack**, the attacker uses every possible combination of characters for the password. Some attackers use a combination of brute-force and dictionary attacks.

The password cracking scenario can also extend to a wireless network as an attacker may perform WPA/WEP/WPS attacks to try to gain access to a wireless LAN. Cracking encrypted systems requires an attacker to collect information. For example, a lot of information is transmitted with 802.11 packets in a wireless system. An attacker can use this information to extract the WEP key from this data. It is not simple but can be done.

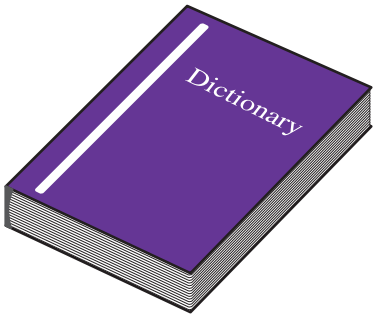


FIGURE 11-3 A dictionary attack.

The following guidelines can help prevent password cracking:

- Don't allow passwords that are dictionary words.
- Don't allow a user to use their username as a password—or their username spelled backward.
- Limit the number of login attempts.
- Require that passwords be strong, which means they are sufficiently long (no less than eight characters) and include a combination of letters, numbers, and symbols (for example, Ab1&G25hamxYmx).
- Require that passwords be changed often.

Packet Sniffing

Another way attackers can obtain a password is by sniffing the network's data packets. An attacker must be able to see network data packets in order to conduct **packet sniffing**. The attacker has to insert a device on the network that enables her to see the data packets (see Figure 11-4). The attacker then watches the data packets until a Telnet or FTP data packet passes (or a packet from one of the many of the other applications that have unencrypted logins). Many of these applications pass the username and password over the network in plaintext (that is, in human-readable form). If the attacker captures all data packets from a user's computer, the chances are good that the attacker can obtain the user's login name and password on one of the network's computers. The way to prevent this is by encrypting the username and password. An encrypted alternative to Telnet is Secure Shell (SSH). The packets that pass across an SSH connection are encrypted. Secure Sockets Layer (SSL) is an encryption protocol used by web servers. For example, the packet transmission is encrypted with SSL when a credit card number is entered. There is also a secure version of FTP called Secure FTP (SFTP).

Packet Sniffing
An attack technique that involves watching the contents of data packets

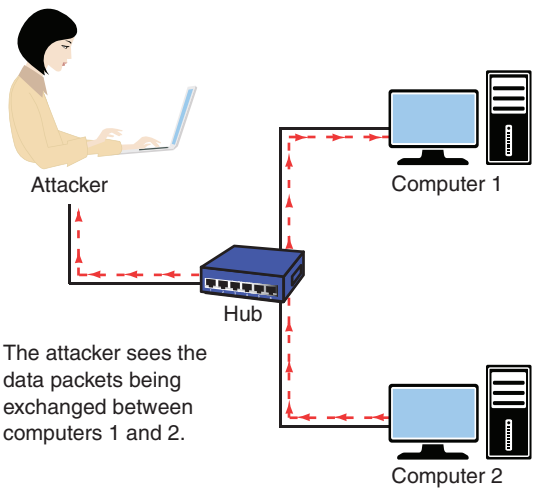


FIGURE 11-4 An example of packet sniffing.

SSL is the predecessor to the Transport Layer Security (TLS) protocol, which is the most current and widely used security protocol. However, people still refer to both SSL and TLS as the SSL protocol. TLS is designed to ensure privacy between communicating parties. TLS ensures that no third party can eavesdrop on or tamper with any messages between a server and a client. TLS requires that both the client and the server use certificates to verify their identities. SSL certificates have to be signed by a trusted certificate authority (CA) in order to be trusted by SSL-type applications. Web browsers should report untrusted SSL certificates or security certificate errors. When a website's SSL certificate is untrusted, an untrusted SSL certificate could be a result of many factors. One common issue or factor is that the SSL certificate may have expired. Another is that the SSL certificate may be self-signed by the server rather than by a trusted CA.

Datagram Transport Layer Security (DTLS) is a variation of the SSL protocol that provides the same type of security features as SSL, including integrity, authentication, and confidentiality, but it uses the UDP protocol.

Tunneled Transport Layer Security (TTLS) is similar to TLS in that it also ensures privacy, but it does not require that each party be issued a certificate. Instead, only the authentication server is issued a certificate. The client authentication requires a password, but the password credentials are transported in a securely encrypted tunnel that is established based on the server certificate.

IPsec
IP Security, a protocol that encrypts each packet prior to transmission across the network link

In these examples, the security is implemented at the application layer. Security can also be implemented at layer 3, using IP Security (**IPsec**). With IPsec, each packet is encrypted prior to transmission across the network link. IPsec is also used to encrypt VPN tunnels (see Section 11-9).

On-Path Attack (Man-in-the-Middle Attack)
An attack in which an attacker gets in the middle of a conversation between others in order to become the recipient of all information sent by victim computers

ARP Cache Poisoning
An attack in which an attacker changes the MAC addresses of the ARP cache, or "poisons the ARP cache" so that conversations get redirected to the attacker

Evil Twin
An attack in which a rogue wireless access point poses as a legitimate one by broadcasting a legitimate SSID and eavesdrops on the wireless network

Packet Sniffing Attacks

Many network attacks are based on packet sniffing techniques where they require proper physical placement on the network in order to capture packets and to perform an attack. Some packet sniffing or sniffing attacks are:

- **On-path attack (man-in-the-middle attack):** This is an attack in which an attacker gets in the middle of a conversation between others in order to become the recipient of all information sent by victim computers.
- **ARP cache poisoning:** This is a technique used in on-path/man-in-the-middle attacks. Network devices on the same network segment communicate using MAC addresses. These MAC addresses are stored in the ARP cache, which contains IP address-to-MAC address mappings. If an attacker can change MAC addresses in the ARP cache—that is, "poison the ARP cache"—the conversations are redirected to the attacker.
- **Evil twin:** This is an on-path/man-in-the-middle attack in which a rogue wireless access point poses as a legitimate access point by broadcasting a legitimate SSID and eavesdrops on the wireless network. Typical users only recognize the SSID and do not know which APs are broadcasting this wireless network. Attackers can use the evil twin to collect information from wireless users connecting through this wireless access point.

- **Session hijacking:** This is another form of on-path/man-in-the-middle attack. As the name implies, it is an exploitation technique that involves stealing and taking control of an active network session; it involves exploitation of a valid computer session to gain unauthorized access to information or services on a computer. It is synonymous with the exploitation of web session control by stealing a session cookie and using it to establish a session with a remote server that still thinks the session is valid.

Session Hijacking
An attack that exploits web session control by stealing a session cookie and using it to establish a session with a remote server that thinks the session is valid

- **VLAN hopping:** This on-path/man-in-the-middle exploitation is an attack to gain information or resources that are available only in specific VLANs by using switch spoofing or double-tagging. Switch spoofing works by tricking a switch into thinking that another switch is forming a trunk port to gain access to all the VLANs allowed on the trunk port. A double-tagging attack works by embedding a second 802.1Q tag inside the frame; this second tag allows the frame to be forwarded to a VLAN that the original 802.1Q did not intend.

Vulnerable Software

In the process of writing large amounts of code, errors happen that can open access to the code and to a network. An attack that capitalizes on such errors is a **buffer overflow**. A buffer overflow occurs when a program attempts to put more data into a buffer than it was configured to hold, and the overflow writes past the end of the buffer and over adjacent memory locations. The program stack contains data as well as instructions that it runs. Say, for example, that a program includes a variable size of 128 bytes. It is possible that the programmer didn't include instructions to check the maximum size of the variable to make sure it is smaller than 128 bytes. An attacker will look through pages and pages of source code, searching for a vulnerability that allows her to issue a buffer overflow. The attacker finds the variable and sends data to the application assigned to that variable. For example, a web application could have a vulnerability with long URLs assigned to a variable within it. If the attacker makes the URL long enough, the buffer overflow could allow her code to be placed in the stack. When the program counter gets to the inserted code, the inserted code is run and the attacker gains remote access to the machine, as illustrated in Figure 11-5.

Buffer Overflow
A situation that occurs when a program tries to put more data into a buffer than it was configured to hold

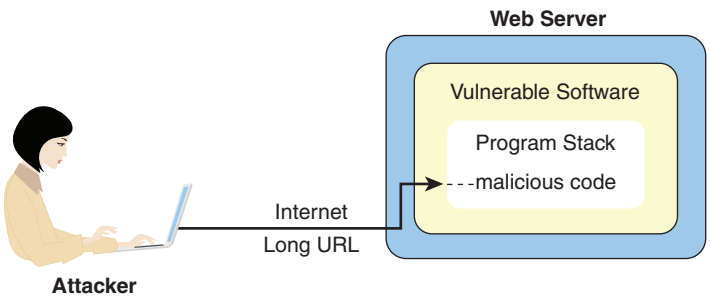


FIGURE 11-5 An example of a buffer overflow attack.

Sometimes buffer overflows don't allow instructions to be run but rather cause an application to crash. This type of overflow is used in denial-of-service attacks. A common way that attackers use buffer overflow attacks is to set up a *backdoor* to gain entry into a computer. The attacker creates an application on a port and then connects to the port. The attacker can also use the backdoor to place viruses on the computer. For example, say that an attacker, using vulnerability scanning software, finds a vulnerability in the source code for an operating system, such as the SSL code on a web server. The attacker downloads malicious code onto the server and then connects to the machine and instructs the code to begin attacking other machines.

Preventing Vulnerable Software Attacks

To prevent vulnerable software attacks, it is important to keep software patches and service packs for the operating system current and to update software regularly.

Also, it is important to disable unused ports. Turn off all services and ports that are not needed on a machine. For example, if a machine does not use web service, turn off this service. Leaving unused services on is like leaving the windows and doors to your house open: You are just inviting an attacker to come in. If you aren't using a service, shut off access to it. You can use the command **netstat -a** to display the IP ports currently open on the Windows operating system. This command shows who is connected to a machine and the port numbers. This is an important step for maintaining port security. The following is an example of using this command:

netstat -a
The command used to display the ports currently open on a Windows operating system

```
c: netstat -a

Active

Proto  Local Address          Foreign Address        State
TCP    pcsalsa2:1087          PC-SALSA2:0            LISTENING
TCP    pcsalsa2:1088          PC-SALSA2:0            LISTENING
TCP    pcsalsa2:1089          PC-SALSA2:0            LISTENING
TCP    pcsalsa2:1090          PC-SALSA2:0            LISTENING
TCP    pcsalsa2:135           PC-SALSA2:0            LISTENING
TCP    pcsalsa2:1025          PC-SALSA2:0            LISTENING
TCP    pcsalsa2:1087          salsa.chile.Edu:80     ESTABLISHED
TCP    pcsalsa2:1088          salsa.chile.Edu:80     ESTABLISHED
TCP    pcsalsa2:1089          salsa.chile.Edu:80     CLOSE_WAIT
TCP    pcsalsa2:1090          salsa.chile.Edu:80     CLOSE_WAIT
TCP    pcsalsa2:137           PC-SALSA2:0            LISTENING
TCP    pcsalsa2:138           PC-SALSA2:0            LISTENING
TCP    pcsalsa2:nbsession     PC-SALSA2:0            LISTENING
UDP    pcsalsa2:nbname              *:               *
UDP    pcsalsa2:nbdatagram          *:               *
```

Another useful command is **netstat -b**, which shows the executable involved in creating a connection or listening port. The following example shows that Chrome web browser was used to establish the connection:

netstat -b
The command used to display the executable involved in creating a connection or listening port

```
c: netstat -b

Active Connections

Proto  Local Address          Foreign Address        State           PID
TCP    pc-salsa:1152          salsa.chile.edu:http   ESTABLISHED     876
[chrome.exe]
```

The ports that are listening are just waiting for a connection. For example, ports 135 and 137 shown in the preceding **netstat -a** example are the NetBIOS and file sharing ports for Microsoft. Every port that is established shows the status **LISTENING**, and each one can accept a connection. For example, if an application is vulnerable and is listening, then the machine is vulnerable to an attack. It is good idea to check which applications are running on a machine. And again, it is a good idea to turn off ports that are not needed. The steps for turning off ports depend on the application. For example, if port 80 (HTTP) is running, you can go to the Windows services and turn off the web application.

An excellent security tool that runs on Linux as well as Windows and macOS is **nmap**. You can install this application on Linux by using the command **yum install nmap**, if it's not already installed. A network administrator can use this port scanner to scan a local computer or other computers internal to the network to determine what network ports and services are being made available to users. For example, the command **nmap localhost** can be entered to scan the Linux machine named **localhost**. Figure 11-6 shows the results of such a scan. The scan shows that FTP, Telnet, SMTP (email server), SunRPC (network file server), and X11 (the GUI for Linux) are all available. Notice that each service has a port number assigned to it. (Port numbers are introduced in Chapter 5, "Interconnecting the LANs.") For example, FTP is on port 21 and is running TCP. Telnet is running on port 23 and is also running TCP. A network administrator may decide that the FTP service or the non-secure Telnet service is a security threat and needs to be disabled. It is important to always disable unnecessary services.

nmap
A Linux and Windows port scanner

You can also use the **nmap** command to scan machines outside your network by simply substituting an IP address for the machine name. For example, you could use **nmap 192.168.12.5** to scan the machine at IP address 192.168.12.5. Note that you should only use the **nmap** port scanning utility on your own machines!

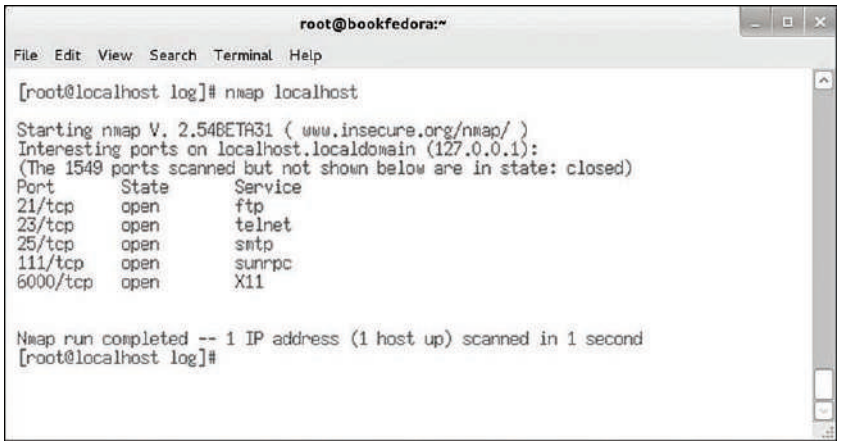


FIGURE 11-6 An example of using the **nmap** command to scan a local computer to determine what network ports and services are being made available to users.

A network/system administrator faces many important issues, but security should be the top concern. When you go out to install a new service or are maintaining existing systems, the most important issue is the system security, which involves preventing outside threats. You need to fully understand the implications of installing software and how its installation can possibly affect the overall network. The following is a list of some questions to consider when installing software:

- Who will be the users of the software, and what applications are they going to be running?
- Will the users need special permissions?
- Will the software being installed require a firewall?
- Does the software introduce any security threats?

Penetration Testing
Testing that evaluates the security of a network

Another type of testing that can help protect a network is **penetration testing**. A penetration test helps evaluate the security of a network. It is accomplished by trying to exploit vulnerabilities in the network, including identifying any potential problems with the operating systems, services, and applications as well as verifying user adherence to policies. Penetration testing also validates any protection mechanisms that are currently in place.

Virus
A piece of malicious computer code that, when opened, can damage hardware, software, or other files

Malware

A **virus** is a piece of malicious computer code that, when run on a machine, can damage its hardware, software, or other files. A computer virus is typically attached to an executable file and can be spread when the infected program is run. A computer virus is spread through sharing of infected files or emails with attached files that are infected with the virus.

Problems caused by viruses include the following:

- Annoyance
- Clogging up of the mail server
- Denial-of-service
- Data loss
- Open holes for others to access the machine

Viruses used to be a problem passed along by exchanging computer disks. Today, most viruses are exchanged via attachments to email (see Figure 11-7). For example, a user might receive an email that says "Look at this!" trying to coax him into opening the attachment. By opening the attachment, the user could possibly infect his computer with a virus.

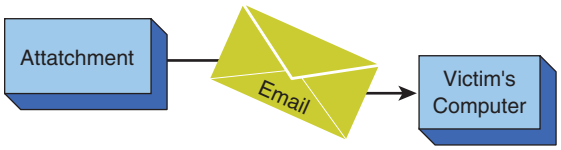


FIGURE 11-7 An example of how computer viruses are spread.

A computer **worm** is a type of computer virus that attacks computers, typically proliferating by itself (self-replicating); it can deny service to networks. A computer worm does not need to be attached to an executable file to be distributed but can use the network to send copies of itself to other computers. A common objective of a worm is to establish a backdoor in the infected computer, which enables an attacker to access to someone's computer.

Worm
A type of virus that attacks computers, typically proliferates by itself, and can deny service to networks

The following are measures that can help prevent viruses:

- Open only attachments that come from known sources. Keep in mind, however, that email addresses can be spoofed or a message can come from a known person whose computer has been infected.
- Require that the emails you receive be digitally signed so you can verify the sender.
- Always run antivirus/anti-malware software on client machines. Antivirus/anti-malware software is not 100% effective but will catch most viruses.
- Include email server filters to block specific types of emails or attachments.
- Keep antivirus/anti-malware software up to date.
- Keep the operating system and application software current.
- Use personal firewalls, when possible (see Section 11-4).

Malware
Malicious software

Logic bomb
A type of malware that can reside in a system undetected until a predefined event triggers the bomb to go off

Zero-Day Attack
An attack that exploits a software vulnerability that is unknown to the developer

Ransomware
A form of malware that attempts to hold a user's files ransom, often for monetary gain

The term **malware** (short for *malicious software*) is used to encompass all malicious programs intended to harm, disrupt, deny, or gain unauthorized access to a computing system. Viruses and worms are considered infectious malware.

A **logic bomb** is a type of malware that can reside in a system undetected until a predefined event triggers the bomb to go off. When it goes into effect, the logic bomb could be as destructive as wiping out the system files or corrupting data files or databases, or it could be more annoying than destructive, such as rebooting the system. When software is vulnerable, it is very difficult to guard against possible exploits or **zero-day attacks**. A zero-day attack is an attack that exploits a software vulnerability that is unknown to the developer. Because the developer is not aware of it, there is no patch to fix it.

In recent years, **ransomware** has become the most feared type of malware. Its aim is to attack computer files and encrypt them, rendering the files inaccessible to victims. These ransomware-encrypted files could be important to an organization (for example, budget files) or sentimental to individuals (for example, family photos). A victim of ransomware is asked to pay ransom money to get the decryption key to retrieve the files.

Note

It is important to understand that an intruder can gain network access or even control of your network. And remember that hackers already know the information presented in this chapter. Network administrators need to know how to protect their networks.

Section 11-2 Review

This section covers the following Network+ exam objectives.

1.7 Explain basic corporate and datacenter network architecture.
This section states that it is important to keep the operating system and application software current.

1.8 Summarize cloud concepts and connectivity options.
This section mentions that IPsec is a method used to encrypt VPN tunnels.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
This section discusses rogue wireless access points.

2.3 Given a scenario, configure and deploy common Ethernet switching features.
This section discusses a double-tagging attack that works by embedding a second 802.1Q tag inside a frame; this second tag allows the frame to be forwarded to a VLAN that the original 802.1Q tag did not intend.

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

This section discusses how a rogue wireless access point poses as a legitimate one by broadcasting a legitimate SSID and eavesdrops on the wireless network.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section examines firewalls and the importance of using personal firewalls when possible.

4.2 Compare and contrast common types of attacks.

In this section, an evil twin is categorized as an on-path/man-in-the-middle attack.

4.4 Compare and contrast remote access methods and security implications.

This section examines an encrypted alternative to Telnet, the Secure Shell (SSH) protocol.

5.3 Given a scenario, use the appropriate network software tools and commands.

*This section shows that the command **netstat -a** can be used to display the IP ports that are currently open on the Windows operating system.*

Test Your Knowledge

1. Which of the following best defines *social engineering*?
    a. It's a way for a host to obtain enough information to prevent intrusion.
    b. It's intrusion prevention from information passed along via email.
    c. It's a way for an intruder to obtain enough information to gain access to the network.
    d. It's a technique for breaking passwords.
2. An attacker may try to guess a user's password by using which of the following techniques?
    a. Password sniffing
    b. Password cracking
    c. Password sampling
    d. Password interrogation

11-3 DENIAL-OF-SERVICE

Most students have heard of denial-of-service attacks, so they will likely be interested in learning more about this concept. Students should recognize that preventing denial-of-service attacks requires preventing attackers from gaining access to the network. You can have students prepare a report on DoS and DDoS attacks and have them identify the latest threat to networks.

Denial-of-Service (DoS)
An attack in which service is denied to a computer, network, or server

A **denial-of-service (DoS)** attack is an attack in which service is denied to a computer, network, or network server. Denial-of-service attacks can be made against individual machines, on a network that connects machines, or on all machines simultaneously.

A denial-of-service attack can be initiated by exploiting software vulnerabilities. For example, a software vulnerability might permit a buffer overflow, causing a machine to crash. This affects all applications, even secure applications. A vulnerable software DoS attack affects a system by making it reboot repeatedly. DoS attacks can also occur on routers via the software options available for connecting to a router. For example, SNMP management software is marketed by many companies and is supported by many computer platforms. Many SNMP packages use similar core code that could contain the same vulnerability.

Another denial-of-service attack is a SYN attack. This refers to the TCP SYN (synchronizing) packet (introduced in Chapter 6, "TCP/IP"). With a SYN attack, the attacker sends many TCP SYN packets to a host, opening up many TCP sessions. The host machine has limited memory set aside for open connections. If all the TCP connections are opened by the SYN attack, other users cannot access services because the connection buffer is full. Most current operating systems take countermeasures to prevent SYN attacks.

Denial-of-service attacks can affect network bandwidth and the endpoints on a network. The classic example is a smurf attack, which requires few resources from the attacker. The attacker sends a small packet and gets many packets in return. The attacker picks a victim and an intermediate site. Figure 11-8 shows a smurf attack with an attacker site, an intermediate site, and a victim site. The intermediate site has subnets 10.10.1.0 and 10.10.2.0. The victim is at 10.10.1.0. The attackers send a packet to 10.10.1.255, which is a broadcast address for the 10.10.1.0 subnet. The attacker then spoofs the source address information, making it look as if the packet came from the victim's network. All the machines on the 10.10.1.0 subnet send a reply to the source address. Remember that the attacker has spoofed the source address, so the replies are sent to the victim's network. If this attack were increased to all the subnets in the 10.0.0.0 network, an enormous number of data packets would be sent to the victim's network. Such an attack enables an attacker to generate a lot of data traffic on the victim's network without requiring the attacker to have many resources.

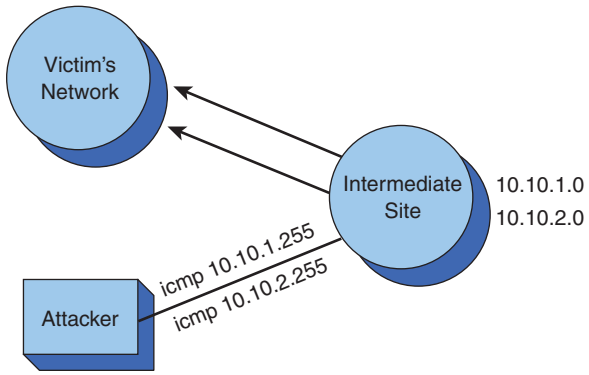


FIGURE 11-8 An example of a smurf attack.

This type of attack is not new, and you can take certain steps to stop a network from becoming an intermediate site. Cisco routers have an interface command that blocks broadcast packets to a subnet. This prevents a network from becoming an intermediate site for a network attack such as this. Make sure this command or a similar command is a default or has been enabled on the router's interface:

```
no ip directed-broadcast
```

Directed Broadcast
A broadcast that is sent to a specific subnet.

Aren't layer 3 devices supposed to stop broadcasts? This is true for general broadcasts (all 32 bits set to 1s or F F F F F F F F or 255.255.255.255). Routers always stop such broadcasts. The type of broadcast used in this attack is a **directed broadcast**, which is passed through the router. The **no ip directed-broadcast** command enables only the router to reply.

Some DoS attacks are truly malicious. For example, a **permanent DoS (PDoS)** attack is a very malicious type of attack that aims to sabotage hardware and render it useless. A PDoS attack can damage a hardware system to the point that it requires replacement or reinstallation. However, not all DoS attacks have malicious intent; some are friendly and unintentional. A friendly/unintentional DoS is typically caused by heavy legitimate traffic to a server or a website that inadvertently overwhelms the server resources or the network connection. The server or network cannot handle the massive volume of traffic, and users are likely to experience unresponsive service.

Permanent DoS (PDoS)
A malicious attack that aims to sabotage hardware and render it useless

To prevent a network from becoming a host for an attacker, you can use access lists to allow only specific sources from the network to enter the router's interfaces. For example, say that network B connects to a router. Only packets sourced from network B are allowed to pass through the router. The downside of this is that it becomes a maintenance problem: Keeping track of the access lists can be challenging for a network administrator, and processing access lists on the router is processor intensive and can slow the throughput of the packets. However, using access lists does help eliminate spoofed packets. An attacker may **spoof** by not using his IP address but instead inserting an IP address from the victim's network or another network as the source IP address. A lot of software on the Internet enables people to spoof IP addresses.

Spoof
To insert a different IP address in place of an IP packet's source address to make it appear that a packet came from another network

Reflective/ Amplified DoS Attack
An attack that is carried out using spoofing and that is a combination of a reflection attack and an amplification attack

A **reflective/amplified DoS attack** is an attack that is carried out using spoofing and that is a combination of a reflection attack and an amplification attack. The attacker spoofs the victim's IP address and sends requests to many different servers or devices that respond to that type of request. The devices all then reply back to the victim's IP address, which is unable to process the overwhelming amount of traffic.

A recent type of reflective/amplified DoS attack uses DNS servers that are configured as open resolvers on the Internet. Attackers spoof a victim's IP address and send a small DNS zone transfer query request for a list of open DNS servers; the servers respond with a huge zone transfer list (hence *amplified*). These amplified responses are then sent back to the victim, overwhelming the victim's resources. Much like DNS amplification attacks, some reflective attacks use public Network Time Protocol (NTP) servers. In this case, a botnet sends the old NTP remote command **monlist**, requesting a list of the last 600 hosts that were connected to the server, and spoofs the source IP address to be the victim. Again, this DoS attack is used to overwhelm the victim and bring down the system.

Deauthentication Attack
An attack in which an attacker sends a frame to the wireless access point with a spoofed address to make it look like it came from the victim, resulting in the access point disconnecting the victim's connection from the AP

Another notable DoS attack using a spoofing technique is a wireless **deauthentication attack**. An attacker sends a deauthentication message to the wireless access point (AP) with the victim's MAC address, resulting in the access point disconnecting the victim's connection from the AP.

The only way to truly prevent yourself from becoming a victim of a denial-of-service attack is to avoid ever being connected to any network or to any other users. That's really not practical today. However, there is a way to detect attacks and to minimize their impact. Some security appliances, discussed in the next section 11-4, can help prevent and mitigate these types of attacks. Also, you can set a *honeypot*, a staged computer system or environment that is specifically set up with security vulnerabilities open for attacks. It is used to gain information about attacks and sometimes can draw attacks away from an actual critical system.

Distributed Denial-of-Service Attacks

DDoS
Distributed denial-of-service attack

The number of packets that can be generated by a single packet (as in a smurf attack) can be limited on a router; however, attackers now use worms to distribute attacks. In a **distributed denial-of-service (DDoS)** attack, the attacker does a port scan and looks for an open port or a software application that is vulnerable to attack. The machine is *hacked* (attacked) and distributes the malicious software. The attacker repeats this for many victim machines. After the software is on the victim machines, the attacker can issue a command or an instruction that starts the attack on a specific site. The attack comes from a potentially massive number of machines the worm has infected.

Coordinated Attack
A type of distributed denial-of-service attack that is deliberately directed against a specific target and orchestrated by a controller source such as the command-and-control server in a botnet

Typically, DDoS attacks are deliberate; they are considered to be coordinated attacks. A **coordinated attack** is a type of DDoS attack that is deliberately directed against a specific target and orchestrated by a controller source such as the command-and-control server in a botnet. In recent news, the Anonymous group has been synonymous with these coordinated attacks and has planned many attacks to deliberately bring down websites to send a political message. A botnet is a prime example of coordinated DDoS. A *botnet* is a group of infected or compromised computers on the Internet that are used to launch coordinated denial-of-service attacks against another system on the network. A botnet computer is controlled via an Internet Relay Chat (IRC) channel by a server called a command-and-control server.

To stop DDoS attacks, you must stop intrusions to the network, as discussed in Section 11-2. All the mitigation steps discussed in that section can help prevent intrusions. However, there is no silver bullet when it comes to preventing intrusions.

Section 11-3 Review

This section covers the following Network+ exam objectives.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

This section examines reflective attacks using public Network Time Protocol (NTP) servers.

1.6 Explain the use and purpose of network services.

This section discusses a DoS attack that uses DNS servers that are configured as open resolvers on the Internet.

4.1 Explain common security concepts.

This section discusses a way to detect attacks and to minimize their impact: You can set a honeypot, a staged computer system or environment that is specifically set up with security vulnerabilities open for attacks.

4.2 Compare and contrast common types of attacks.

This section discusses the threat posed by a botnet, which is a group of infected or compromised computers on the Internet that are used to launch coordinated denial-of-service attacks against another system on the network.

5.3 Given a scenario, use the appropriate network software tools and commands.

This section discusses how an attacker does a port scan and looks for an open port or a software application that is vulnerable to attack.

Test Your Knowledge

1. A service being denied to a computer can be a result of which of the following?
   a. Improperly configured WEP
   b. Spoofing
   c. Denial-of-service
   d. Phishing
2. What mitigating steps can help prevent DDoS attacks? (Select all that apply.)
   a. Use macOS.
   b. Apply software patches regularly.
   c. Run antivirus/anti-malware software.
   d. Implement a firewall.
   e. Turn on Telnet service.

11-4 SECURITY SOFTWARE AND HARDWARE

This section examines antivirus/anti-malware software as well as personal firewalls. Examples in this section demonstrate how to configure firewall settings for Windows, macOS, and Linux. This section also introduces access lists and web filter appliances.

A healthy network starts from within, and the most basic component in a network is an individual computer. An individual computer should have protection similar to that of its network. Remember that the fundamental goal of DDoS is to take control of vulnerable machines and launch an attack. This can be prevented. Even though it is not cost-effective to guard each computer with dedicated hardware, there is a plethora of security software that can help.

Personal Firewalls

One type of software protection that is readily available for a computer is a personal firewall. Most operating systems today (Windows, macOS, and Linux) are equipped with personal firewalls, although these firewalls may not be enabled by default. Personal firewall software is typically based on basic packet filtering inspections, where the firewall accepts or denies incoming network traffic based on information contained in the packets' TCP or IP headers. Some personal firewalls provide more granular control to allow specific hosts or subnets. Some personal firewalls also offer an application-based firewall, where trusted programs can be defined. In this case, the firewall allows network traffic originated from or destined to the trusted programs.

In the Windows operating system world, firewall protection has evolved from being a simple firewall in Windows XP to allowing more granular control in Windows 10. The Windows 10 firewall enables both packet filtering and an application-based firewall. In addition, the firewall software has both inbound and outbound control. In the Linux world, **iptables**—a network packet filtering firewall program—has been a de facto firewall program for a long time. The recent macOS deploys PF (Packet Filter) as its OS firewall. PF is a BSD-based stateful packet filter firewall. The following sections demonstrate how to configure firewall settings for Windows 10, macOS, and Linux.

Note

Incorrect host-based firewall settings can result in network issues or loss of network connectivity for a computer. It is a good idea to create a firewall rule and try it out—and to do this with only one rule at a time.

Antivirus/Anti-malware Software

The first line of defense against viruses, worms, and general malware is antivirus/anti-malware software. Recommended practice is to have an antivirus program installed on every computer. Even though antivirus/anti-malware software cannot provide 100% protection, it does protect against most viruses.

Antivirus software matches *signatures* or *definitions* against viruses and worms. Each virus or worm has its own traits, which are defined in a signature or a definition. When a new virus or worm is found, a new signature or definition has to be created. Most of the commercial antivirus companies have new signatures/definitions ready and available for their customers to download within hours of the spread of new malware. This is why it is important to keep antivirus software up-to-date. Most antivirus software is launched at the startup of the operating system, and it tries to update its signatures or definitions at that time. When a virus is found on a computer, the virus program is usually quarantined or removed. Popular antivirus software is available from Microsoft, McAfee, Norton, Trend Micro, Sophos, and AVG.

Configuring Firewall Settings for Windows 10

Follow these steps to configure firewall settings in Windows 10:

1. Click **Start**, type **control panel** in the search box, and select **Control Panel**. Select **System and Security** and then **Windows Defender Firewall**. Windows Defender Firewall, as shown in Figure 11-9, presents two options: Check firewall status and Allow an app through Windows Firewall.
2. Select **Check firewall status** to display the status window shown in Figure 11-10. This screen indicates that the firewall is on for the public network connection named **Network**, and the firewall is blocking all connections to the programs that are not on the list of allowed programs.

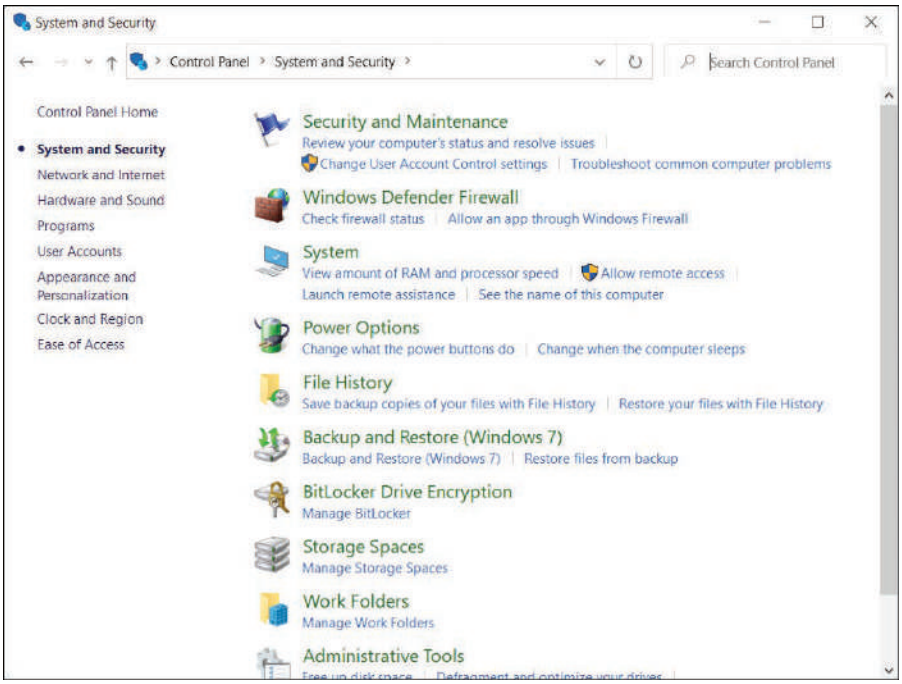


FIGURE 11-9 Windows Firewall in Windows 10.

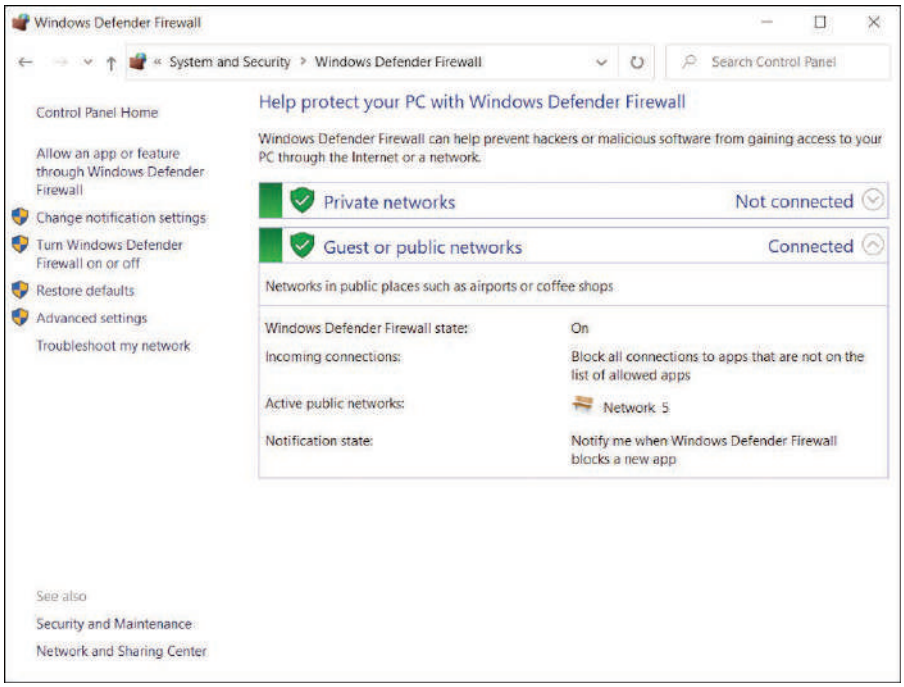


FIGURE 11-10 Windows 10 Firewall status.

3. Select **Allow an app or feature through Windows Firewall** to display the apps that are allowed to communicate through Windows Firewall, as shown in Figure 11-11. This screen shows the programs that are allowed through the firewall, depending on which network location profile the computer is using. Every time a Windows 10 computer makes a new network connection for the first time, Windows 10 prompts the user to identify whether the network connection is for a home/work (private) location or a public location. It then adjusts the firewall and security settings accordingly.

4. To use the Windows 10 advanced firewall settings, click the **Advanced settings** option in the left column of the firewall status window in Figure 11-10. Figure 11-12 shows the Windows Defender Firewall with Advanced Security window that appears.

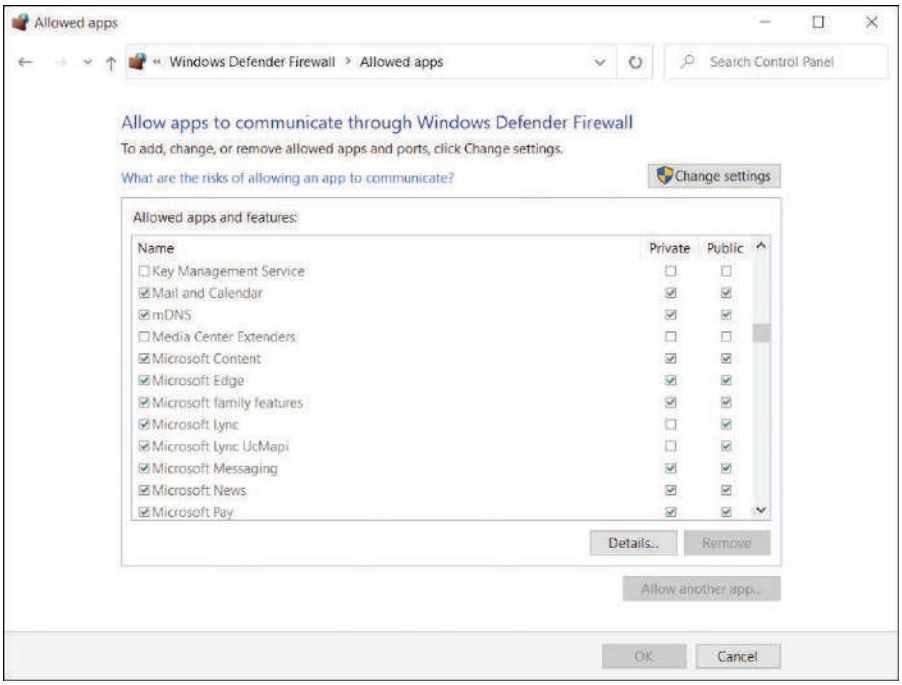


FIGURE 11-11 Windows 10 allowed apps.

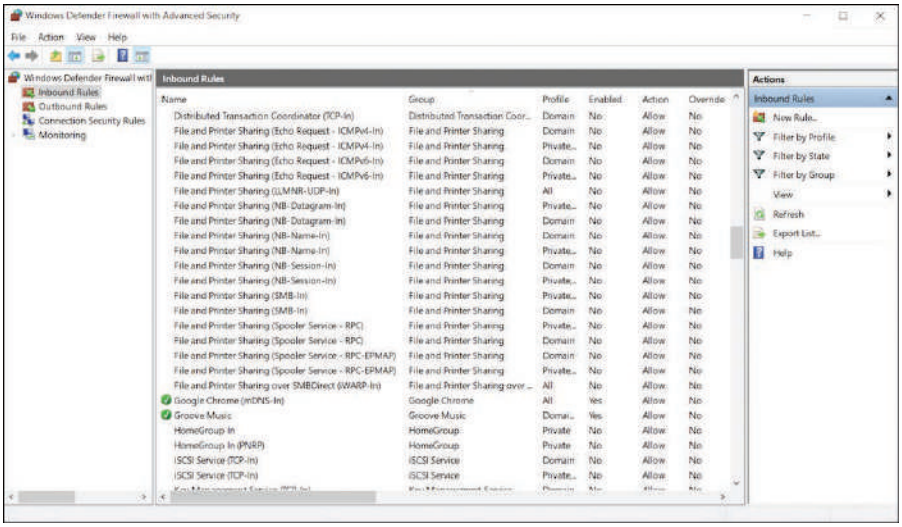


FIGURE 11-12 Windows 10 advanced firewall settings.

To see how the advanced options work, this example examines an inbound file and printer sharing rule in Windows 10 (Echo Request – ICMPv4-in), which is known as a ping request in Windows 7 and Windows 8. This is a simple rule to control the ping traffic to the computer. In the window

shown in Figure 11-12, select **Inbound Rules**, and the middle pane shows all the inbound firewall rules. There are a lot of rules, but not all of them are enabled. The enabled rules are indicated by the value **Yes** in the column **Enabled**. Right next to the **Enabled** column is the **Action** column, which displays the action **Allow** to allow a connection or **Block** to deny a connection.

5. Double-click the rule **File and Printer Sharing (Echo Request – ICMPv4-in)** in the middle pane, and the properties window shown in Figure 11-13 appears. Select the **General** tab of this window, and you see that this rule is currently set to **Disabled**, and the action is set to **Allow the connection**. By selecting the **Enabled** box and changing the action to **Block the connection**, you change the conditions of the rule to be active and to block all incoming echo request traffic.

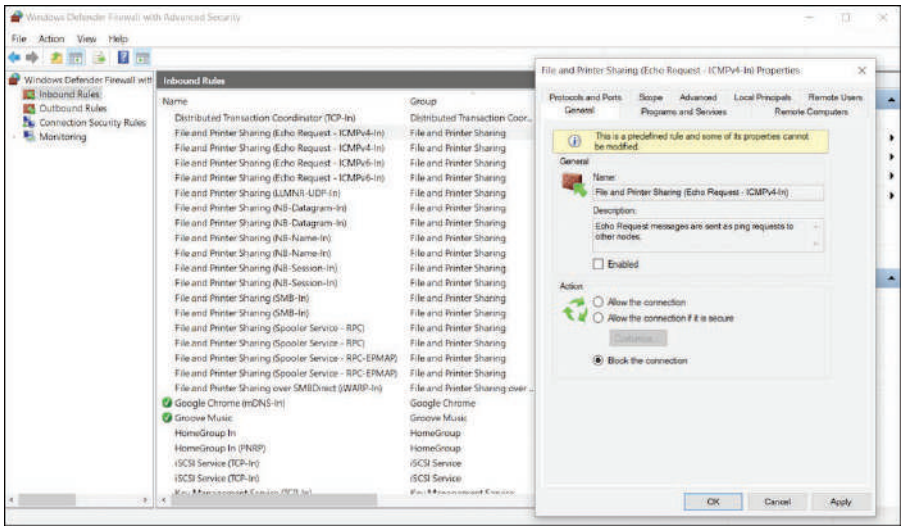


FIGURE 11-13 Windows 10 echo request properties.

6. Select the **Protocols and Ports** tab to see the window shown in Figure 11-14. You can see how the firewall program matches the echo request by defining its protocol as an ICMPv4 protocol. Click the **Customize** button to bring up the Customize ICMP Settings window, which shows Echo Request selected for the ICMP type.

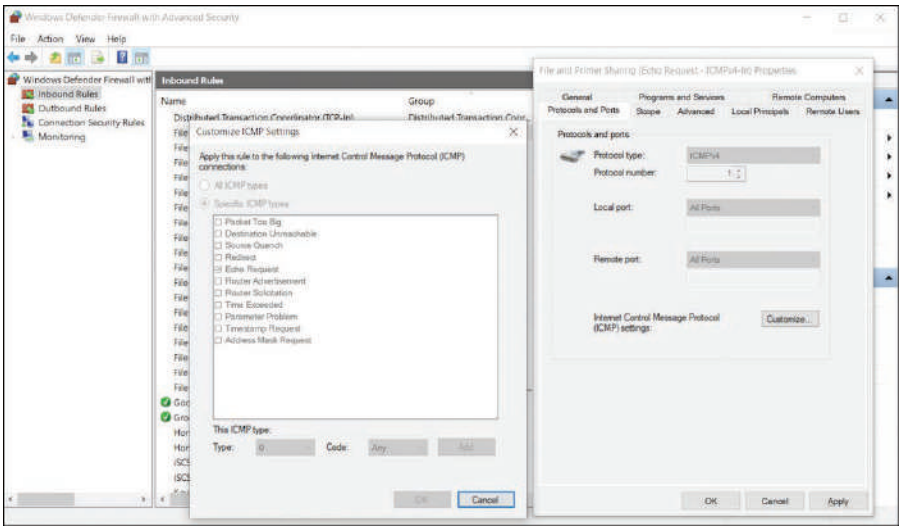


FIGURE 11-14 Windows 10 echo request protocols and ports.

Configuring Firewall Settings for macOS

To start the macOS firewall configuration, follow these steps:

1. Go to **System Preferences** and select **Security & Privacy**.
2. In the Security & Privacy window, select **Firewall**. The firewall window displays the status of the firewall and lets you turn off the firewall (see Figure 11-15).

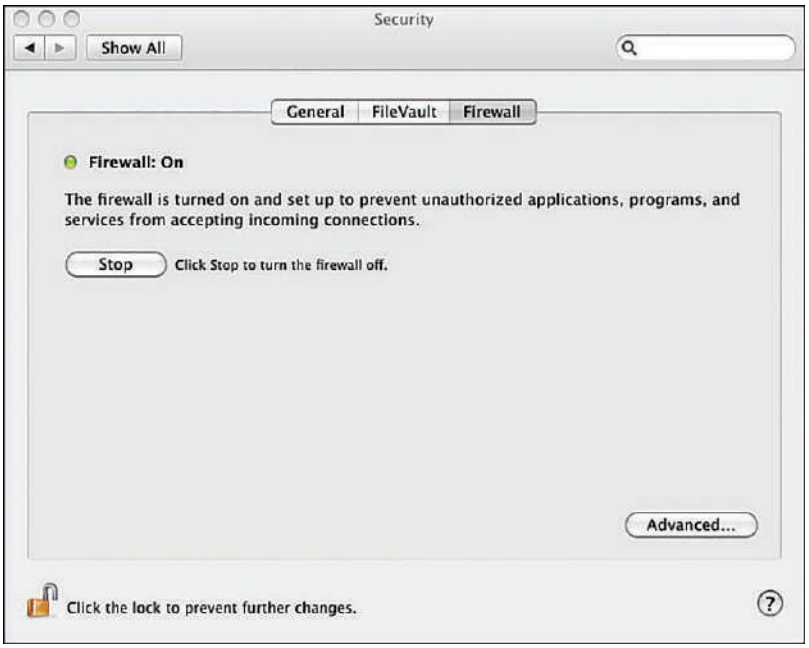


FIGURE 11-15 macOS firewall.

3. Click the **Firewall Options** button to open another window for more advanced settings, as shown in Figure 11-16. These are the firewall options:

   - **Block all incoming connections:** This option blocks all incoming connections except a limited list of necessary services, such as DHCP and DNS.
   - **Automatically allow signed software to receive incoming connections:** Because macOS runs an application-based firewall, this option adds all the digitally signed applications certified by Apple to the trusted list. The connections to and from these applications are trusted. The window above the option enables manual entry of your own trusted software.
   - **Enable stealth mode:** This option basically stops the computer from responding to an ICMP ping request packet. This makes it difficult for attackers to identify the computer.

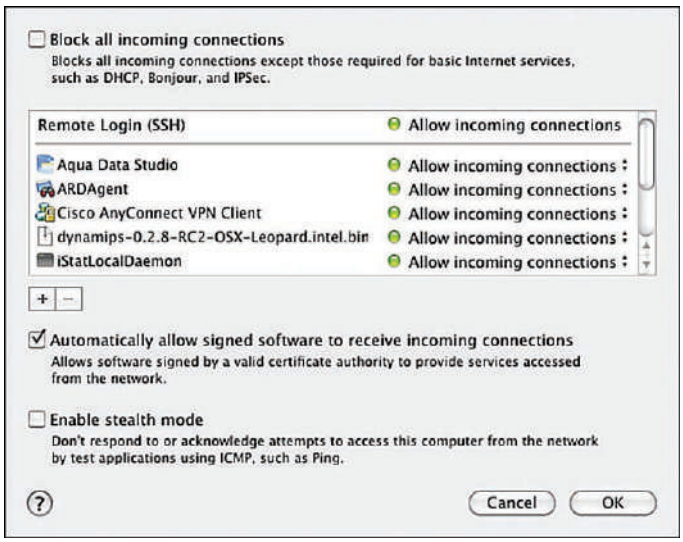


FIGURE 11-16 macOS advanced settings.

Configuring Firewall Settings for Linux

The command to view, add, modify, and delete the Linux firewall configuration is **iptables**. For example, to view the firewall configuration, simply issue the command **iptables-list** as root or use **sudo iptables-list**. To use these commands, you must be connected as root or must open **System Preferences** and select **Security**.

Figure 11-17 shows the output of the command **iptables-list**. It shows a list of chains: INPUT, FORWARD, OUTPUT, and RH-Firewall-1-INPUT. A chain can consist of firewall rules or another chain. Obviously, the only chain in this example that contains firewall rules is RH-Firewall-1-INPUT. This chain allows incoming HTTP, HTTPS, SSH, SMTP, domain (DNS), and IMAP traffic and rejects any incoming traffic that does not match the allowed list.

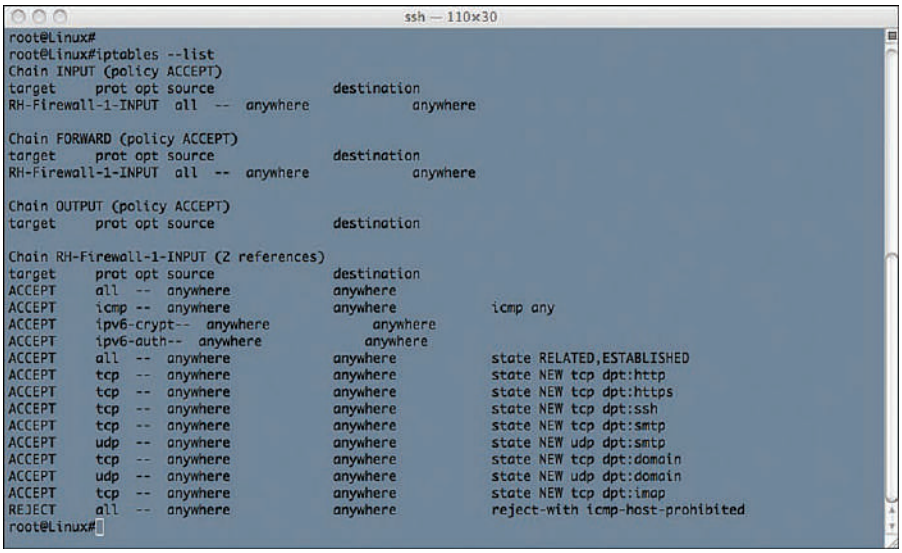


FIGURE 11-17 Linux **iptables**.

Firewalls

Firewalls are used in computer networks for protection against the network elements (such as intrusions and denial-of-service attacks). An **access control list (ACL)** is a basic form of firewall protection, although an access list is not stateful and is not by itself a firewall. ACLs can be configured on a router, on a true dedicated firewall, or on a host computer for restricting access to the computer and the network.

Firewall
Hardware or software used to protect a computer network

Access Control List (ACL)
A basic form of firewall protection

An access list consists of permit and deny statements to control traffic into and out of the network interface. There is an implicit denial at the end of an access list in Cisco routers, and this statement alone blocks all data packets. In order to allow other data packets that do not match the ACL's permit and deny statements to enter and exit the LAN, the command **access-list permit ip any any** must be added to the last line of an access list to explicitly allow all other data packets. If the intention is to deny other data packets that match the permit statements, then the explicit permit statement is not needed. In the following example, the instruction is for access list 100, and it tells the router to deny IP packets from a host with IP address 192.168.9.2 to any destination and to permit IP packets from any source to any destination:

access-list permit ip any any
The instruction added to the last line of an access list to allow all other data packets to enter and exit the router

```
RouterB(config)# access-list 100 deny ip host 192.168.9.2 any
RouterB(config)# access-list 100 permit ip any any
```

Because an ACL is placed at a firewall's ingress or egress interface, incorrect ACL settings cause network issues or may inadvertently allow unwanted traffic into the network. You have to be very careful when configuring ACL rules. Firewalls allow traffic from inside the network to exit but don't allow general traffic from the outside to enter the network. A firewall monitors the data traffic and recognizes where packets are coming from. A firewall allows packets from the outside to enter

the network if they match a request from within the network. Traditional firewalls are based on three technologies:

- Packet filtering
- Proxy server
- Stateful packet filtering

Demilitarized Zone (DMZ)/Screened Subnet
An area of a network that is used to isolate servers

In general, you want to place a firewall close to the machines you want to protect (for example, the network servers). You should not assume that the clients on the network will never attack your system. Clients can and will get viruses on their machines. It is best practice to create **demilitarized zones (DMZs)** for the outside servers, and put them in places on the network where they are isolated. DMZ is a term borrowed from the military that refers to a buffer zone that separates a trusted internal network from the untrusted external networks. That way, if the machines are compromised, the intruder will have limited access to the inside of the network. A DMZ is also referred to as a **screened subnet** or a *perimeter network*.

Packet Filtering
Protection in which a limit is placed on the information that can enter the network

With **packet filtering**, a limit is placed on the packets that can enter the network. Packet filtering can also limit information moving from one segment to another. ACLs are used to enable a firewall to accept or deny data packets. Packet filtering has some disadvantages:

- Packets can still enter the network by fragmenting the data packets.
- It is difficult to implement complex ACLs.
- Not all network services can be filtered.

A network administrator also has the option of configuring IP exclusions by using the firewall settings. This can be beneficial in improving the accuracy of reports.

Proxy Server
A setup in which clients go through a proxy to communicate with secure systems

Clients use a **proxy server** to communicate with secure systems using a proxy. The client gets access to the network via the proxy server. This step is used to authenticate the user, establish the session, and set policies. The client must connect to a proxy server in order to connect to resources outside the network. Proxy servers have some disadvantages:

- A proxy server can run very slowly.
- Adding services can be difficult.
- There can be a potential problem with network failure if the proxy server fails or is corrupted.

Stateful Firewall
A firewall that keeps track of data packet flow

With a **stateful firewall**, the inbound and outbound data packets are compared to determine whether a connection should be allowed. This includes tracking the source and destination port numbers and sequence numbers as well as the source and destination IP addresses. This technique is used to protect the inside of a network from the outside world but still allow traffic to go from the inside to the outside and back. A firewall needs to be stateful in order to accomplish this.

What if a campus network has a web server? How are outside users allowed access? Holes must be opened in the network to allow data packets to pass through. The three most common traffic types that require holes to be opened are web servers, DNS, and email. A firewall must be modified so that anybody can connect to the web server via port 80. But what if a vulnerability is discovered on port 80 for the server's operating system? When ports are open, the network administrator must continually upgrade the software so that vulnerabilities are removed. The web server also might need to have its own firewall. Most firewalls can perform deep packet inspection, which can catch some protocol vulnerabilities.

A firewall is usually placed inline between a trusted (internal) network and an untrusted (external) network. Its primary function is to protect the trusted network. Figure 11-18 shows an example of how a perimeter firewall can be deployed. A perimeter firewall is physically placed between the public Internet and the internal networks. All incoming traffic is considered untrusted and is inspected by the firewall according to its rules. Sometimes, a firewall might be connected to a campus router. A router might be needed to aggregate multiple networks or to handle more complicated network routing. At the firewall, NAT or PAT is typically configured to handle the translation between the private IP addresses and the public IP addresses.

A big problem with firewalls is that users assume that a firewall catches all possible problems. This assumption is incorrect. A user might be slow to update patches and fixes to software. Then, for example, an attacker might send an email message with an attachment to a user, and the user might open the attachment and unknowingly load on his computer a Trojan horse that scans all the machines on the LAN, checking for any possible open ports and compromising the entire LAN. A firewall is not an end-to-end solution.

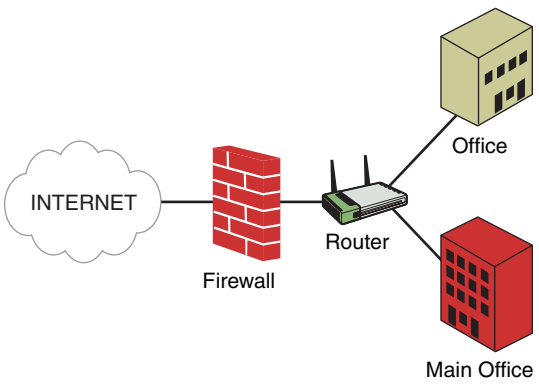


FIGURE 11-18 Perimeter firewall deployment.

Other Security Appliances

Many security appliances on the market today help protect networks. Most of these appliances work in conjunction with or as supplements to a firewall. **Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs)** both monitor and analyze network traffic. In real time, they identify misuse and anomalies on the network. They can detect intrusions by matching network packets with

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
Systems that identify misuse and anomalies on a network

signatures for known attacks or activities that are classified as bad. A network anomaly can be detected by building up a profile of the system being monitored and detecting significant deviations from that profile. An IDS is designed to monitor both inbound and outbound data traffic and report on any suspicious activity that could indicate an attack. An IPS has the capability to stop or prevent malicious attacks that it detects in real time by interacting with the firewall. In addition, host-based intrusion detection systems (HIDSs) are software based. A HIDS monitors a computer system for changes such as system file modifications, changes to the registry, file changes, and system logs. HIDS software packages are configured to prevent malicious activity on the host system, and if an unauthorized change or activity is detected, an alert is issued. Based on policy settings, the central server could be notified or the activity could be blocked.

Another appliance that is widely deployed is a web filter or content filter appliance. Lots of places have very strict policies on how users can use the network. Web traffic is often monitored and filtered, and a web filter appliance is designed to handle that. In the K–12 school environment, web filtering is critical. The Children's Internet Protection Act (CIPA) requires K–12 school districts to implement filtering to block adult, illegal, and offensive content from minors. A web filter appliance has a database containing inappropriate websites. It monitors web traffic via HTTP and HTTPS and matches that traffic against the database. If an inappropriate website is detected, it is either discarded or the user is redirected to a security web page for further action. The web filter appliance's database is updated perpetually. Also, there is an option for a network administrator to manually mark a website as inappropriate.

Instead of blocking unwanted traffic or content, you can use an appliance that can throttle or shape network traffic based on type, source, or destination; such a device is called a **packet shaper**. This device sits between a campus network and the outside network. The device is set up so that all data traffic, incoming and outgoing, passes through it. The packet shaper box is configured with a set of rules that are used to prioritize data traffic. This is extremely important when it comes to managing your network's data bandwidth/throughput. A packet shaper can be used to set rules to limit download traffic from the Internet. It can also be used to make sure applications such as VoIP are given higher priority so that their operation and quality of service are not affected.

Packet Shaper
A device that sits between a campus network and an outside network that is configured with a set of rules that are used to prioritize data traffic for shaping the bandwidth

A relatively new firewall technology called a next-generation firewall (NGFW) combines traditional firewall functionalities with all the special network functions of network appliances, such as IPS, deep packet inspection, bandwidth control, antivirus, and malware inspection. NGFWs are sometimes also referred to as layer 7 firewalls.

An important aspect associated with security appliances is making sure IT staff are continually updated on technology and that they receive proper training. In addition, it is important to make sure critical systems are protected by a UPS and regularly backed up. Also, you should validate that the security appliances incorporate redundancy and that they will not be single points of failure.

Computer Forensics

Computers are subject to attacks, and in some cases, crimes are committed. Therefore, network technicians and network administrators must know the proper steps to take to preserve evidence. The following are some basic guidelines for first responders:

- No action should change data held on a computer or storage media that may be subsequently relied upon in court.
- In circumstances where a person finds it necessary to access original data held on a computer or storage media, that person must be competent to do so and must be able to give evidence explaining the relevance and the implications of the actions.
- An audit trail or some other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- The person in charge of the investigation has the overall responsibility for ensuring that the law and these principles are adhered to.

There are six stages of a forensics examination:

1. **Readiness:** This includes appropriate training, regular testing, and verification of software and equipment, familiarity with legislation, and ensuring that the onsite acquisition (data extraction) kit is complete and in working order.
2. **Evaluation:** The evaluation process includes receiving instructions, clarifying the instructions, completing risk analysis, and allocating resources.
3. **Collection:** This stage involves collecting evidence and interviewing relevant personnel as well as the IT administration responsible for the affected system.
4. **Analysis:** This stage involves using appropriate tools to provide thorough and repeatable analysis of the compromised system.
5. **Presentation:** In this stage, the examiner provides a structured report on the findings of the examination. This also includes addressing key points and any additional information relevant to the investigation.
6. **Review:** In this stage, the examiner should review what went wrong, what was done properly, and what can be learned and improved on based on the incident.

This is only a brief overview of computer forensics and the concept of preserving evidence. A network technician should make sure a qualified forensics specialist is involved if a crime has been committed.

Section 11-4 Review

This section covers the following Network+ exam objectives.

1.8 Summarize cloud concepts and connectivity options.

Figure 11-18 shows an example of perimeter firewall deployment.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section introduces proxy servers, layer 7 firewalls, and content filters.

2.2 Compare and contrast routing technologies and bandwidth management concepts.

This section discusses how a packet shaper can be used to set rules to limit download traffic from the Internet. It can also be used to make sure applications such as VoIP are given higher priority so that their operation and quality of service are not affected.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section examines the basics of firewall protection. It examines firewall rules as well as port security and stateful inspection of data packets.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section examines the basics of firewall protection. It examines firewall rules as well as port security and stateful inspection of data packets.

4.3 Given a scenario, apply network hardening techniques.

As discussed in this section, an access control list (ACL) is a basic form of firewall protection, although an access list is not stateful and is not by itself a firewall.

4.5 Explain the importance of physical security.

This section indicates that most security appliances work in conjunction with or as supplements to a firewall. Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) can be used to monitor and analyze network traffic.

Test Your Knowledge

1. A stateful firewall does which of the following?
   a. Keeps track of data packet flow
   b. Keeps track of data collisions
   c. Enables the access list
   d. Prevents unnecessary pings
2. True or false: An advantage of a firewall is that it catches all possible problems.

   False

11-5 MANAGING NETWORK ACCESS

This section helps students explore the concepts and technologies used to identify a trusted source. It provides information on authentication, authorization, and accounting.

The previous section focuses on blocking unwanted traffic from entering a network and allowing traffic from a trusted source into the network. This section examines the concept of a trusted source more closely and explores the concepts and techniques used to identify a trusted source, grant access to a trusted source, and manage accessibility for a trusted source.

Authentication, authorization, and accounting (**AAA**, pronounced "triple-A") is a framework for controlling access to computing resources, enforcing policies, and auditing usage. AAA defines fundamental security building blocks that are the core of network management and security, as its name implies.

Authentication, Authorization, and Accounting (AAA)
A framework for controlling access to computing resources, enforcing policies, and auditing usage

Authentication defines who and what a user is. It has to happen first. Without successful authentication, there will not be authorization and accounting. This process provides a mechanism to identify a valid user. The most common practice is for a user to supply a username and password. The AAA server checks and verifies the authentication credentials. If the credentials are valid, the user is granted access to the network. If not, the authentication fails, and access is denied. A password is a common authentication factor based on something a user knows. Other authentication factors are what a user has (for example, a smart card), what a user is (for example, biometric), and what a user does (for example, handwriting).

Kerberos is a network authentication protocol that is widely used in enterprise environments. A Kerberos server issues a special token or ticket to its authenticated users, and it uses this ticket to validate user access to a resource or a service. This process, called single sign-on (SSO), permits a user to authenticate only once, and after successful authentication, the user is trusted to access other services or systems based on the ticket.

Authorization defines what a user is allowed to do. As the process after authentication, it governs the privileges and tasks a user can perform after gaining access to a network or system. Authorization determines whether a user has the authority to perform particular tasks or to access certain resources. For example, a user may gain access to a network switch and may only be authorized to view the switch and not to make any changes to it. As with authentication, authorization is negotiated at the AAA server, which enforces all the user access policies. Authorization based on a user's role and responsibilities is called **role-based access control (RBAC)**. RBAC uses the security principle of least privilege to enforce access policy at a more fine-grained level. As the name implies, the least privilege principle involves giving a user only the privileges necessary to perform a job. RBAC is a fundamental building block of a Zero Trust model, which is a newer security model in identity and access management (IAM). The Zero Trust model—whose motto is "Never Trust. Always Verify"—makes sure every access request to the IT resources is authenticated and authorized.

Role-Based Access Control (RBAC)
Authorization based on a user's role and responsibilities

Accounting defines and keeps track of what users do. Simply put, this process keeps track and records all the activities by all users. While these activities can be logged by the AAA server, in most cases, they are carried out as part of the

system log (syslog), which records and stores all the events related to the system. It is best practice to send all the accounting activities to a centralized syslog for keeping track of auditing and logging so that the events from all network devices can be monitored, analyzed, and correlated. The analytics can be used for resource planning, capacity planning, network trend monitoring, and security analysis.

Cisco offers authentication, authorization, and accounting service as a way to centrally manage and control user access for its routers and switches. AAA supports two of the most commonly used access protocols:

- **RADIUS (Remote Authentication Dial-In User Service):** The most widely used AAA protocol today is RADIUS, which was developed by Levingston Enterprise during the heyday of modem dial-ups in the early 1990s to manage users who connect and use a network service. RADIUS is now an IETF standard networking protocol that is widely used for authenticating remote users, authorizing user access, and accounting for user activities.
- **TACACS+ (Terminal Access Controller Access-Control System Plus):** Cisco routers and switches can communicate with RADIUS or TACACS+ servers for central authentication. AAA enables local authentication based on the router's local user database, enables line passwords, and allows other access protocol types.

Another technology that uses the AAA framework is network access control (NAC), sometimes known as network admission control. NAC is a security mechanism that can be implemented on a network to register, authenticate, authorize, and enforce security policies on all endpoint devices before they are allowed to access the network. NAC has gained popularity as a method to manage and keep track of the devices involved in a BYOD (bring your own device) policy. NAC can be deployed in many forms—hardware appliance, virtual appliance, client agent, or clientless agent. It can be used to manage the onboarding and offboarding of mobile devices. NAC typically interfaces with a RADIUS server for device authentication.

To manage network devices and resources properly, an organization must have a good policy for change management for network device configuration, as well as standard procedures for network maintenance. To prepare for disaster recovery, an organization must have a backup plan that covers backing up network equipment configurations and archiving for recovery process.

One of the most fundamental elements of network operations is documentation. Documentation can consist of network drawings and wiring diagrams, asset management, and vendor documentation. Network diagrams help engineers visualize and understand how things are connected. Asset management gives engineers details of their network equipment, from model numbers to software versions and locations.

Another security device is UTM (unified threat management), which is an all-in-one solution that integrates a wide range of security features into one appliance. A UTM appliance may consist of a firewall, a network IDS/IPS, a VPN, a gateway antivirus/anti-malware, gateway anti-spam, load balancing, and content filtering. This type of appliance is popular in small to medium businesses where the network is too big and complicated. It helps reduce administrative overhead time and cost.

Section 11-5 Review

This section covers the following Network+ exam objectives.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

This section mentions syslog, which records and stores all the events related to a system.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section says that it is best practice to send all the accounting activities to a centralized syslog to keep track of auditing and logging so that the events from all network devices can be monitored, analyzed, and correlated.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section states that to prepare for disaster recovery, an organization must have a backup plan that covers backing up network equipment configurations and archiving for recovery process.

4.1 Explain common security concepts.

This section introduces single sign-on (SSO) and Kerberos.

Test Your Knowledge

1. What is UTM?
   a. Unified traffic management is an all-in-one solution that integrates a wide range of security features into multiple appliances.
   b. Unified threat management is an all-in-one solution that integrates a wide range of security features into multiple appliances.
   c. Unified threat management is an all-in-one solution that integrates a wide range of security features into one appliance.
   d. Unified threat management is a stand-alone solution that interrogates devices that have not followed proper protocols.
2. What is the most widely used AAA protocol today?
   a. RADIUS
   b. TLS
   c. A+
   d. Telnet

11-6 ROUTER SECURITY

This section introduces router security. The emphasis of this section is on best practices for router security, including physical security for operating systems. This section introduces commands for controlling router access and encryption. It also introduces control of router services and logging of router activity.

Routers perform essential services for networks. A router is typically deployed at the perimeter of a network. Therefore, it is the first line of defense for the network. Compromise of a router can lead to many issues on the network, such as degrading network performance, denial of network services, exposure of network configuration details, and exposure of the sensitive data. A poorly configured router can easily become a compromised router, thereby reducing the overall security of the network and potentially exposing the internal network to scans and attacks. This section focuses on best practices for configuring a network router to avoid or prevent serious security problems.

Physical security is always at the top of the list of security best practices. A router should be placed in a secure area where it is accessible only to authorized personnel. The easiest access to a router is via its console port. Someone who gains access to the premises can easily take physical control of a router. Even a router secured with a password is not safe in the event of physical access: A router's password can be recovered by someone who has console access. Even worse, the router can become disabled or damaged, and all network services will be halted until the situation is repaired.

The operating system of a router is another crucial component that a network administrator must keep up to date. However, the latest version of a router's OS may have had only limited exposure to testing. Most network administrators wait before upgrading to the latest version to make sure there are no side effects or bugs. Most network administrators settle for the latest stable release of the router operating system rather than the very latest one.

Configuration hardening can limit the exposure of a router. This section focuses on configuration hardening of Cisco routers. The same concepts apply to other vendors' routers; however, their configuration method and commands will be different.

Router Access

Local access and remote access to a router are the common ways of gaining control of a router, and such access must be restricted to only authorized personnel. A typical way of securing local access or remote access is to create a password. Two types of passwords are used on a router: the line password and EXEC (privileged EXEC) password.

Line Password
A password used to gain access to a router

The **line password** is used to gain access to a router. This password should be used in conjunction with the command **service password encryption**. This global command encrypts the password and displays it in encrypted form. It is not strong encryption, but it can be used to provide low-level security.

The **EXEC (privileged EXEC) password** used to be enabled with the **enable password** command, but that command has been replaced by the **enable secret** command, which provides stronger password encryption.

EXEC (privileged EXEC) password
A password used to gain access to EXEC commands

Cisco IOS uses a number of password protection schemes. The command **enable password** is a **Type 7** protection scheme, which uses a Cisco encryption algorithm. The command **enable secret** is a **Type 5** protection scheme and uses the MD5 hash. MD5 is not considered secure today, so other protections schemes are commonly used. For example, Cisco Type 8 uses SHA-256, and Type 9 uses a script hash. These password protections can be enabled by using the command **enable algorithm-type sha256** for Type 8 and **enable algorithm-type sha256** for Type 9.

Type 7
A protection scheme that uses a Cisco encryption algorithm

Type 5
A protection scheme that uses an MD5 hash for encryption

A security step beyond typical password protection is to create user accounts for authorized personnel. Doing so makes it possible to track and log each time a system is accessed. You can create a local user account on a router by using the command **username** [*name*] **privilege** [*level*] **password** *[password_string*]:

```
RouterA(config)# username admin privilege 10 password @dm1np@$$wd
```

Cisco provides 16 levels (0 through 15) of privileges. Each level is preassigned commands that can be run. Level 15, which is the highest level, is equivalent to privileged EXEC mode. The command **username admin privilege 10 password @dm1np@$$wd** creates a local user called **admin** with privilege level 10.

The drawback of creating a local user is that the same user has to be created on every router on the network—and this is not a scalable approach. AAA, as mentioned earlier, is a framework for controlling access to computer resources AAA typically involves the use of RADIUS and TACACS+, so Cisco routers can communicate with RADIUS or TACACS+ servers for central authentication. AAA enables authentication based on the router's local user database, enables line passwords, and other access protocols. The following example shows how to configure AAA on a Cisco router:

```
RouterA(config)# aaa new-model
RouterA(config)# aaa authentication login default local group tacacs+
RouterA(config)# aaa authorization exec default local group tacacs+
if-authenticated
```

Once the authentication method is defined, it can be applied to any access entry point, either local or remote. The local access can be via the console port or the auxiliary port. The remote access is via vty (virtual terminal). The following example shows how to configure a console port with security access. It enforces the authentication by using the local user database and a timeout of 5 minutes if the user input is not detected. Also, it prevents the remote access to the console port via reverse Telnet with the command **transport input none**:

transport input none
A command that prevents remote access to the console port via reverse Telnet

```
RouterA(config)# line con 0
RouterA(config-line)# login local
RouterA(config-line)# exec-time 5 0
RouterA(config-line)# transport input none
```

Remote access to the router can be accomplished via Telnet or SSH. Telnet is a default transport protocol into a router, but its unencrypted traffic is a big security

crypto key generate rsa
A command used to generate an RSA key

flaw. Therefore, using SSH is recommended whenever possible. Enabling SSH transport requires an extra step of generating an RSA key. To generate an RSA key, the hostname and the domain name must be preconfigured on the router; this information will be used as part of the key. To generate the key, the command **crypto key generate rsa** is issued:

```
RouterA(config)# crypto key generate rsa
```

After the RSA key is generated, the remote vty access can be configured with SSH as the transport. The following is an example of configuring the vty remote access with SSH:

```
RouterB(config)# access-list 15 permit 10.10.20.0 0.0.0.255
RouterB(config)# access-list 15 deny any
RouterA(config)# line vty 0 4
RouterA(config-line)# access-class 15 in
RouterA(config-line)# login authentication default
RouterA(config-line)# transport input ssh
RouterA(config-line)# exec-time 5 0
```

This configuration uses the default login authentication defined earlier in this section. The command **transport input ssh** enforces SSH as the only access method. **access-class 15** defines the access list of the network that is allowed to connect to the router via SSH. Finally, the EXEC timeout minutes is set to 5 minutes.

Router Services

A router has many services enabled by default. These services vary from vendor to vendor. Unnecessary services should be disabled, and any services deemed necessary should be tightened. TCP/IP services such as echo, discard, daytime, chargen, bootp, finger, identd, and SNMP are enabled automatically on a Cisco router, but most of them are not needed. You can disabled them globally as follows:

```
RouterA(config)# no service tcp-small-servers
RouterA(config)# no service udp-small-servers
RouterA(config)# no ip bootp server
RouterA(config)# no service finger
RouterA(config)# no ip identd
```

Services such as echo, discard, daytime, and chargen are considered TCP and UDP small services and can be disabled using **no service tcp-small-servers** and **no service udp-small-servers**. Some services might be needed, such as Simple Network Management Protocol (SNMP) and HTTP. These services need to be tightened. The SNMP default community string must not be used, and the new community string must be difficult to guess. Read/write access should be avoided at all costs, and read-only access should be configured. Also, SNMP access should be restricted to certain known SNMP agents. Better yet, SNMP version 3 should be used instead. The following is an example of SNMP configuration on a Cisco router with read-only access and restricted access, as defined in access list 10:

```
RouterA(config)# snmp-server community M@ke1tD1ff1cuLT ro 10
```

Cisco IOS supports web-based remote administration, which is easier and more intuitive to use than the CLI mode that is available for Telnet or SSH. However, HTTP has no encryption. Therefore, web-based administration via HTTP can reveal passwords. Therefore, you should avoid HTTP as well as Telnet. More recent Cisco IOS software versions, starting from release 12.2(15)T, provide another option: HTTPS with end-to-end SSL encryption. The following example illustrations this option:

```
RouterA(config)# no ip http server
RouterA(config)# ip http secure-server
RouterA(config)# ip http access-class 15
RouterA(config)# ip http authentication aaa
```

This configuration shows that the normal HTTP service is disabled, and the HTTPS service is enabled instead. HTTP access is also restricted with access list 15, and AAA authentication is enabled.

Besides disabling unnecessary services running on the router, some services or features that Cisco routers utilize should be disabled. It is recommended that services such as CDP, remote configuration downloading, and source routing be disabled, if they are not used.

Cisco devices use Cisco Discovery Protocol (CDP) to identify each other on a LAN segment. CDP, which is enabled automatically, allows anyone on the network to collect network information. You disable CDP as shown here:

```
RouterA(config)# no cdp run
```

You can disable the remote configuration by using the command **no service config**:

```
RouterA(config)# no service config
```

This stops a router from loading its configuration from the network, which is not secure. A router is capable of loading its startup configuration from local memory, which is more secure than loading the configuration from the network.

Source routing can be used in many kinds of attacks. When you disable this feature, as shown here, the router disregards IP packets containing source route information:

```
RouterA(config)# no ip source-route
```

On the interface level, any unused interfaces should be disabled so that they cannot participate in any network activity. Directed broadcasts allow a host on another network segment to initiate a broadcast to a different network segment. This can be used as a denial-of-service attack such as a smurf attack. This feature should be disabled. Newer IOS versions disable the directed broadcast by default.

The router interfaces should not act as intermediaries for ARP or ARP proxy. An ARP proxy extends ARP traffic between two network segments. This is not desirable and should be avoided. Also, a router can be used to relay ICMP messages that can be used by attackers, and the generation of these messages should be disabled on the interface. ICMP messages that are commonly exploited include Host unreachable, Redirect, and Mask reply. The following example shows a configuration to secure the router interface in these ways:

```
RouterA(config)# interface fastethernet0/1
RouterA(config-if)# shutdown
RouterA(config)# interface fastethernet0/2
RouterA(config-if)# no ip directed-broadcast
RouterA(config-if)# no ip proxy-arp
RouterA(config-if)# no ip unreachables
RouterA(config-if)# no ip redirects
RouterA(config-if)# no ip mask-reply
```

Logging

Logging
A process that allows an administrator to analyze the events that occur and use the information uncovered to correlate and find the issues

Logging, which is a critical part of security, allows an administrator to analyze events that occur and use the information on those events to correlate and find issues. Cisco routers and switches provide a great deal of logging events. These devices can log system errors, network and interface status, login access, access list matches, routing changes, and many more types of events. Cisco's log messages can be directed to the console, terminal line, memory buffer, and syslog server. There are 8 levels (from 0 to 7) of log severity:

- **Level 0:** Emergencies
- **Level 1:** Alerts
- **Level 2:** Critical
- **Level 3:** Errors
- **Level 4:** Warnings
- **Level 5:** Notifications
- **Level 6:** Informational
- **Level 7:** Debugging

NTP
Network Time Protocol, a protocol that can be set up to synchronize the router's clock with the time server

For best security, it is recommended that syslog logging and buffered logging at the debugging level be set up. To keep accurate logs, the correct time has to be set up on a router. This step is often skipped. Cisco routers and switches support Network Time Protocol (**NTP**), which can be set up to synchronize a router's clock with the time server. To correlate the time with the log events, a timestamp service needs to be initiated. The following example shows the log configuration of a Cisco router:

```
RouterA(config)# service timestamps log datetime msec
RouterA(config)# logging on
RouterA(config)# logging buffered 16000 debugging
RouterA(config)# logging trap debugging
RouterA(config)# logging 172.20.20.20
```

This example consists of enabling timestamp service for logging with the date and time down to millisecond detail. Logging is enabled with the simple command **logging on**. A 16KB memory buffer is reserved for logging at the debugging level. In addition, the debugging level log messages will be sent to a syslog server with the IP address 172.20.20.20.

The log information can be verified with the command **show log**. Note that the logging configuration discussed in this section can and should be deployed the same way with switches.

Section 11-6 Review

This section covers the following Network+ exam objectives.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

This section mentions that Cisco routers and switches support Network Time Protocol (NTP), which can be set up to synchronize a router's clock with the time server.

1.6 Explain the use and purpose of network services.

This section discusses the authentication, authorization, and accounting (AAA) framework for centrally managing and controlling user access.

4.5 Explain the importance of physical security.

This section discusses physical security, which is an important part of security. For example, a router should be placed in a secure area where it is accessible only to authorized personnel.

Test Your Knowledge

1. Why is it important to keep the operating system on a router up to date?

   For security reasons (However, most network administrators wait to make sure the latest version is bug-free before installing it on a router)

2. What are the two types of passwords on a router?

   a. The access link and port number

   b. The line password and EXEC password

   c. The SNMP access line and FTP link

   d. The Ping password

11-7 SWITCH SECURITY

This section introduces best practices for switch security. It looks at switch port security and setting special features based on Spanning Tree Protocol and Dynamic Trunking Protocol.

Switches are common network devices. Typically, there are more switches than routers on a network. The router features discussed so far in this chapter can also be found in most network switches. Some features are enabled by default, and some can be enabled manually, depending on the manufacturer. Many users treat network switches just like other plug-and-play computing devices: They think that

if a switch is powered on and the network device connecting to it can access the network, the switch must be working properly. This is not entirely true, though; a network administrator needs to know what switch features are enabled and disabled.

The focus of this section is on manageable Cisco switches; however, some of these concepts may apply to other switch vendors as well.

Before putting a switch into a production environment, you should know what the switch is doing and what it is capable of doing. Much as an administrator should know about a computer's CPU speed, RAM amount, disk space, and operating system version, an administrator needs to know about a switch's capabilities, operating system version, configuration, and running services.

On Cisco switches, you can use the simple command **show version** (or **sh ver**) to find information on the switch hardware, such as make, model, software version, switch interfaces, and system uptime:

```
Switch# sh ver
Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version
12.2(44)SE6, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 09-Mar-09 17:09 by gereddy
Image text-base: 0x00003000, data-base: 0x02000000

ROM: Bootstrap program is C3750E boot loader
BOOTLDR: C3750E Boot Loader (C3750E-HBOOT-M) Version 12.2(35r)SE,
RELEASE SOFTWARE (fc1)

psltenant-sc-feed-56-2 uptime is 11 weeks, 1 day, 2 hours, 10 minutes
System returned to ROM by power-on
System restarted at 09:17:32 MDT Fri May 5 2017
System image file is "flash:/c3750e-universalk9-mz.122-44.SE6.bin"

cisco WS-C3750E-24TD (PowerPC405) processor (revision B0) with
245760K/16376K bytes of memory.
Processor board ID CAT1113R13L
Last reset from power-on
1 Virtual Ethernet interface
1 FastEthernet interface
28 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:1B:54:A0:12:80
Motherboard assembly number     : 73-10313-10
Motherboard serial number       : CAT111357E8
Model revision number           : B0
Motherboard revision number     : B0
Model number                    : WS-C3750E-24TD-S
```

```
Daughterboard assembly number    : 800-28590-01
Daughterboard serial number      : CAT1113564G
System serial number             : CAT1113R13L
Top Assembly Part Number         : 800-27546-01
Top Assembly Revision Number     : A0
Version ID                       : V01
CLEI Code Number                 : COM7J10ARA
Hardware Board Revision Number   : 0x01


Switch Ports Model              SW Version        SW Image
------ ----- -----              ----------        ----------
*      1 30  WS-C3750E-24TD     12.2(44)SE6       C3750E-UNIVERSALK9-M


Configuration register is 0xF
```

To view the current running configuration of a switch, you can use the command **show running-configuration**. This command shows the current running state of the switch, as well as what features and services the switch is expected to be running. If some services or features are enabled but are not needed, they should be disabled. The commands **show version** and **show running-configuration** are basic commands that give you a good overview of a switch and a starting point for troubleshooting. After you use these commands, you should document the switch information as a best practice.

Switch Port Security

Switches are commonly used in the access layer of the network hierarchy. The access layer connects users who share common network resources and bandwidth. Directly interfacing with users can create security challenges, as there is no telling what will be connecting to the switch access ports. The more control or policy that can be enforced at the switch port level, the better off the network will be. Because switch interfaces or ports directly connect users or network equipment, they should be securely configured to prevent malicious attacks or exploitations. A fundamental security rule and best practice is to disable any unused switch ports. There are more ports on switches than on routers.

range
A command that makes it easier to apply the same security policy on a group of switch ports

When applying the same command to a group of switch ports, you can use the **range** command, which makes it easier to apply the same security policy on switch ports. The following example shows the commands to shut down a group or a range of interfaces:

```
SwitchA(config)# interface range Gigabitethernet1/1-24
SwitchA(config-if)# shutdown
```

802.1X
An IEEE standard protocol for access control and authentication; also called dot1x

These commands shut down all the switch ports electronically. When someone tries to physically connect to a port, no physical link will come up. This is the easiest and quickest way to restrict physical wired access to a network. **802.1X**, sometimes referred to as dot1x, is a more advanced technique that can be used to authenticate users to gain access to wired and wireless networks.

802.1X is an IEEE standard access control and authentication protocol that prevents unauthorized devices from connecting to a network through publicly accessible ports unless they are properly authenticated. With 802.1X, a switch is in communication with an authentication server, and the authentication server authenticates each device connected to a switch port before services are made available to the device.

By default, VLAN 1 is always enabled on every switch—even when no other VLANs are configured. Switches automatically carry traffic on VLAN 1, so VLAN 1 is a default native VLAN. It is recommended as a best practice to avoid using VLAN 1 but rather to create different VLANs for different purposes and to change the native VLAN to one of those new VLANs. Not only does this help prevent VLAN 1 from being exploited, it helps segregate network traffic based on type or designated group. This practice is part of the network segmentation technique, which involves creating a logical segment for ease of control and management.

Switch Port Security (or Port Security)
Switch commands used to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port

Some built-in port security commands are available from many switch vendors, including Cisco. **Switch port security**, or **port security**, can be configured to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port. The command to enable port security is **switchport port-security**, and this command has to be issued at the interface level. You can configure a switch port to restrict access by setting a maximum number of MAC addresses, or you can configure it to allow only known MAC addresses to pass traffic.

To configure the maximum number of MAC addresses on a switch port, you use the command **switchport port-security maximum [***number***]**. To configure a port to allow certain MAC addresses to pass traffic, you use the command **switchport port-security mac-address [***mac_address***]** or **switchport port-security mac-address sticky**.

sticky
A command option that causes the configured MAC address to appear in the running configuration of the switch and be saved in the startup configuration

You can use the command **port-security mac-address [***mac_address***]** to manually get the configured MAC address into the running configuration. You can use the command **switchport port-security mac-address sticky** to automatically enter the dynamically learned MAC addresses into the running configuration. With the **sticky** option, the configured MAC address appears in the running configuration of the switch and is saved in the startup configuration. This way, when the switch reboots, the configured MAC address remains part of the configuration. Along with the security configuration, you need to define a violation action. When a violation occurs, one of the selected violation actions—protected, restrict, or shutdown—takes effect:

- **protected:** This violation action drops packets from the violated MAC address(es).
- **restrict:** This violation action is the same as the protected mode, but it also sends SNMP trap messages to the SNMP server.
- **shutdown:** This violation action shuts down the port and puts the port in the **ERRDISABLE** state.

The following is an example of configuring port security to allow a maximum of only two MAC addresses per port and, if a violation occurs, to shut down the switch port:

```
SwitchA(config)# interface Gigabitethernet1/10
SwitchA(config-if)# switchport port-security maximum 2
SwitchA(config-if)# switchport port-security mac-address sticky
0011.2233.440a
SwitchA(config-if)# switchport port-security mac-address sticky
0011.2233.440b
SwitchA(config-if)# switchport port-security violation shutdown
```

When a port is in the **ERRDISABLE** state, manual intervention is needed to enable the port again. You need to issue the command **shutdown** and then **no shutdown** to reenable the port. Another way of reenabling a port from the **ERRDISABLE** state is to configure the **errdisable** recovery feature. The following example shows the **errdisable** configuration to recover a port from a port security violation after 10 minutes:

```
SwitchA(config)# errdisable recovery cause psecure-violation
SwitchA(config-if)# errdisable recovery interval 600
```

Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that prevents ARP spoofing, which leads to ARP poisoning or ARP cache poisoning. With ARP spoofing, an attacker sends a forged ARP packet to change either the MAC or IP address information of the intended target to that of the attacker so that traffic will be forwarded to the attacker. DAI requires help from DHCP snooping (refer to Chapter 10, "Managing the Network Infrastructure"). The DHCP snooping feature must be configured in order to establish the DHCP snooping database, which contains valid mappings of MAC addresses and IP addresses. To enable DAI, configure DHCP snooping and then issue the following command:

```
SwitchA(config)# ip arp inspection vlan [VLAN_ID]
```

The switch inspects and compares all the ARP packets against entries in the DHCP snooping database. If the MAC address or IP address in an ARP packet does not match a valid entry, the packet is dropped.

Note

ARP spoofing is not the same as MAC spoofing. With MAC spoofing, an attacker modifies its original MAC address to another MAC address or the MAC address of someone else.

STP Special Features

Spanning Tree Protocol (STP) is a very common protocol used in every network switch. STP is a layer 2 protocol designed to prevent loops within switched networks. STP builds a topology based on BPDU (bridge protocol data unit) messages. A vulnerability associated with STP is that an STP-enabled device within

a network can actively change the STP topology by sending an unexpected BPDU message. To prevent such an event, features such as BPDU Guard and BPDU Filter can be used.

On STP-enabled switches, a switch port has to go through four STP states—block, listen, learn, and forward—before it can pass traffic. This process can take 30 to 50 seconds. To reduce this time, a switch port can be configured with STP PortFast, which speeds up the STP process and transitions the port into a forwarding state, bypassing the listen and learn state. Typically, an STP PortFast interface is used to directly connect a host device, which does not send BPDU messages. **BPDU Guard** is used to prevent STP PortFast from receiving any BPDU message to modify the spanning tree topology. Upon receipt of a BPDU, BPDU Guard puts the interface configured for STP PortFast into the **ERRDISABLE** state. By default, BPDU guard is disabled. The following commands demonstrate how to globally enable BPDU Guard on a Cisco switch and how to configure STP PortFast on an interface:

BPDU Guard
An option that is used to prevent STP PortFast from receiving any BPDU message to modify the spanning tree topology

```
SwitchA(config)# spanning-tree portfast bpduguard default
SwitchA(config)# interface gigabitethernet 1/0/13
SwitchA(config-if)# spanning-tree portfast
```

BPDU Guard can also be enabled at the interface level with the following command:

```
SwitchA(config)# interface gigabitethernet 0/1
SwitchA(config-if)# spanning-tree bpduguard enable
```

BPDU Filter offers another way to deal with BPDUs. Keep in mind that BPDU Guard prevents a switch port from receiving any BPDU messages, but it does not prevent it from sending them. The BPDU Filter feature effectively disables STP on the selected ports by preventing them from sending and receiving any BPDU messages. The switch port ignores all BPDUs received and sends no BPDUs. Much like BPDU Guard, BPDU Filter can be configured globally or on an individual port. The global command is **spanning-tree portfast bpdufilter default**. The command to enable BPDU Filter at the interface level is **spanning-tree bpdufilter enable**.

Root Guard
An STP feature that allows participation in spanning tree and BPDU messages as long as the attached device does not attempt to become the root bridge

Root Guard is another feature that can be used to protect the STP topology. Unlike BPDU Guard, Root Guard allows participation in spanning tree and BPDU messages as long as the attached device does not attempt to become the root bridge. Essentially, Root Guard provides a way to enforce the root bridge placement in a network. If an unauthorized device starts sending BPDU messages with a better bridge ID, Root Guard disables the switch port on which those BPDU messages were received. The switch port is in the **ERRDISABLE** state. The Root Guard feature can be enabled only at the interface level. It is recommended to apply this feature to switch ports that are not connected to the root bridge. The following is the command used in interface configuration mode to enable Root Guard:

```
SwitchA(config-if)# spanning-tree guard root
```

Section 11-7 Review

This section covers the following Network+ exam objective.

2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section examines switch port security commands used to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

Test Your Knowledge

1. What command displays a switch's system uptime on a Cisco switch?
   a. **show version (or sh ver)**
   b. **show uptime**
   c. **show up-count**
   d. **show up count /all**
2. Before putting a switch into a production environment, which of the following should you do?
   a. Verify the MAC address
   b. Register the IP address
   c. Know what the switch is doing and capable of doing
   d. None of the above are correct.

11-8 WIRELESS SECURITY

A network administrator must be aware of the security issues related to configuring a wireless LAN. This section examines the basic issues of wireless LANs and provides suggestions about how to make sure a wireless network is secure. Students need to understand that wireless security features must be turned on. If they aren't turned on, students should expect that anyone can gain access to the network. Remind students of the basic premise of network security: preventing an attacker from gaining access to the network. This section provides overviews of WPA3, WPA2, WPA, and WEP.

This section provides an overview of securing 802.11 wireless LANs. A network administrator must be aware of security issues when configuring a wireless LAN. It is important to remember that radio frequency (RF) signals will pass through the walls, ceilings, and floors of a building even with low signal power. Therefore, the assumption should never be made that wireless data is confined to only the user's area. A network administrator must assume that the wireless data can be received by an unintended user if the network is not secured. In other words, an unsecured wireless LAN is open to network security threats.

Jamming
A problem in which a wireless network is overwhelmed with wireless traffic, thereby preventing authorized users from accessing the network

An additional issue is that RF signals used in wireless communications are open. This means that anybody who has the right type of equipment can create problems. One particular problem is called **jamming**, in which a wireless network is overwhelmed with wireless traffic, thereby jamming the network and preventing authorized users from accessing the network.

To address threats to WLAN security, a network administrator must ensure that the WLAN is protected by firewalls and intrusion detection. Most importantly, a network administrator must make sure that the wireless security features are turned on. Surprisingly enough, many WLANs are placed on a network without the available wireless security features being turned on. Many times, a user in a WLAN assumes that no one would break into their computer because nothing important exists on the system. This may be true, but to an attacker, the user has one very important item: access to the wired network through an unsecured client.

SSID
Service set identifier

Beacon
A device that is used to identify a wireless link

WLANs use an **SSID** (service set identifier) to authenticate users, but the SSID is broadcast in radio link beacons about 10 times per second. In WLAN equipment, the **beacons** are transmitted so that a wireless user can identify an access point to connect to. The SSID can be turned off so that it isn't transmitted with a beacon, but it is still possible for the SSID to be obtained through packet sniffing. As discussed earlier in this chapter, packet sniffing is a technique used to scan through unencrypted data packets to extract information. In this case, an attacker uses packet sniffing to extract the SSID from data packets. Disabling SSID broadcasting makes it so most client devices (such as Windows devices and Apple devices) won't notice that the wireless LAN is present. This at least keeps casual snoopers off the network. Enterprise-grade access points implement multiple SSIDs, with each configured SSID having its own VLAN and wireless configuration. This enables the deployment of a common wireless LAN infrastructure that supports multiple levels of security, which is important for some venues, such as airports and hospitals (where there are both public and private users).

IEEE 802.11 supports two ways to authenticate clients:

Open Authentication
A null authentication that can enable any client to authenticate to an access point

Shared-Key Authentication
A type of authentication in which the client and the access point share a key called a pre-shared key (PSK)

WEP
Wired Equivalent Privacy

- **Open Authentication:** This is basically a null authentication that can enable any client to authenticate to an AP as long as the client knows the correct SSID.
- **Shared-key authentication:** With this type of authentication, the client and the access point share a key called a pre-shared key (PSK), which is a secret that was previously shared between two parties. The client sends a shared key authentication request, and then a packet of text called a challenge text is sent by the access point to the client with the instruction to encrypt the text and return it to the access point. This requires that Wired Equivalent Privacy (**WEP**) be turned on. WEP is used to encrypt and decrypt wireless data packets. The exchange and return of the encrypted text verifies that the client has the proper WEP key and is authorized to be a member of the wireless network.

It is important to note that shared-key authentication is extremely vulnerable. As a result, it's standard practice to avoid the use of shared-key authentication. An example of the setting for WEP encryption is provided in Figure 11-19. In

Figure 11-19a, the user has the WEP options Disabled (No Privacy), 64-bit WEP (Privacy), and 128-bit WEP (More Privacy). Figure 11-19b shows the wireless security settings in Windows (some of which are described later in this section).

It is well known that WEP is a weak wireless security system. It doesn't use strong enough encryption to secure a wireless network. The RC4 algorithm is used for encryption in WEP. WEP has a couple of weaknesses. For one thing, challenge text in WEP is sent in plaintext. In addition, the WEP initialization vector is only 24 bits and is always static. WEP also does not use key management, and its pre-shared key never changes. Because of these factors, it is not very difficult to obtain the pre-shared key for WEP. Despite its weaknesses, WEP does provide some basic security, and using it is certainly better than operating a network with no security.

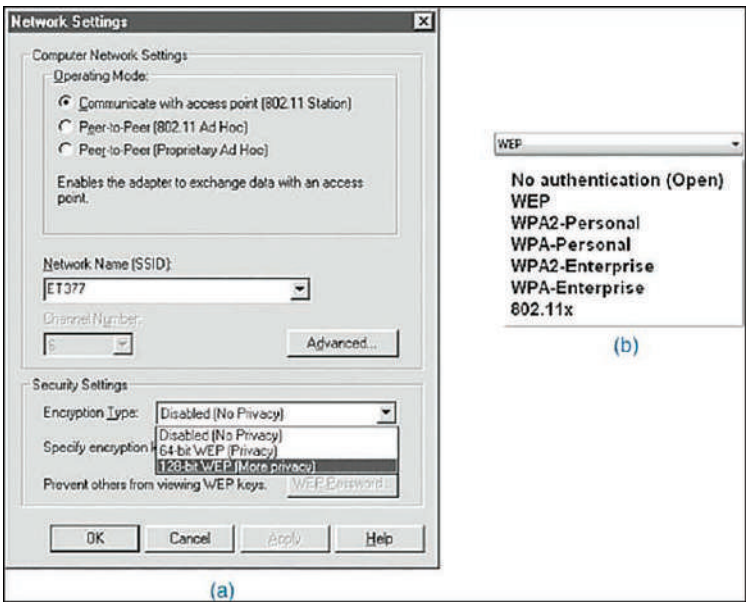


FIGURE 11-19 An example of setting WEP encryption on a wireless client.

WPA, WPA2, and WPA3 provide better security than WEP. **WPA** (Wi-Fi Protected Access) supports the user authentication provided by 802.1X and replaces WEP as the primary way for securing wireless transfers. WPA, like WEP, uses RC4 as the encryption algorithm, but it provides a key management mechanism via **TKIP** (Temporal Key Integrity Protocol). TKIP basically generates a sequence of WEP keys based on a master pre-shared key and rekeys periodically every 10,000 packets (file integrity monitoring). TKIP also uses an integrity check value to ensure that the packet is not tampered with. If tampering is detected, WPA stops using the current key and rekeys.

WPA2 is an improved version of WPA. It uses **AES** (Advanced Encryption Standard) as its encryption algorithm and **CCMP** (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) as its key management protocol. There are two versions of WPA2: WPA2-Personal and WPA2-Enterprise.

WPA
Wi-Fi Protected Access, a protocol that replaced WEP for securing wireless transfers

TKIP
Temporal Key Integrity Protocol, a protocol that provides key management for WPA

AES
Advanced Encryption Standard, the encryption algorithm used by WPA2

CCMP
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, the key management protocol used by WPA2

WPA2-Personal authorizes wireless users using pre-shared keys, while WPA2-Enterprise authorizes wireless users via a server authentication to accommodate and manage a bigger user pool in an enterprise environment.

WPA3, which is the latest version of WPA, provides greater wireless security for Wi-Fi-certified devices. Like WPA2, WPA3 offers both Personal and Enterprise versions. WPA3-Personal introduces Simultaneous Authentication of Equals (SAE), which helps prevent dictionary attacks on the password or passphrase. SAE generates a unique key for each password attempt, tremendously slowing down brute-force attacks. WPA3-Enterprise uses 192-bit AES encryption, and WPA3-Personal uses 128-bit AES encryption with an option for 192-bit AES encryption.

An encryption algorithm and key management alone cannot truly secure a wireless connection. The 802.1X standard enhances wireless security by incorporating authentication of the user. The original authentication framework was Extensible Authentication Protocol (EAP). There are a variety of EAP standards. Cisco Systems uses an 802.1X authentication system called **LEAP (Lightweight Extensible Authentication Protocol)**. With LEAP, the user must enter a password to access the network. This means that if the wireless client is being used by an unauthorized user, the password requirement will keep the unauthorized user out of the network. EAP-FAST (EAP-Flexible Authentication via Secure Tunnel) is another Cisco-proprietary EAP standard developed to overcome some vulnerabilities found in LEAP. For non-Cisco standards, EAP-TLS (EAP-Transport Layer Security) was the original and universally used wireless authentication standard. PEAP (Protected Extensible Authentication Protocol) was developed by Microsoft, Cisco, and RSA Security. PEAP is widely supported by wireless vendors and is becoming the authentication standard to use. PEAP, EAP-TLS, and EAP-FAST do not require client certificates. EAP-TLS requires a client-side certificate.

LEAP (Lightweight Extensible Authentication Protocol)
A wireless security system used by Cisco

WPA is considered to be a higher level of security for wireless systems. In the 802.1X system, a user requests access to the wireless network via an access point. The next step is for the user to be authenticated. At this point, the user can only send EAP messages. Extensible Authentication Protocol (**EAP**) is used in WPA, WPA2, and WPA3 by the client computer and the access point. The access point sends an EAP message requesting the user's identity. The user (client computer) returns the identity information that is sent by the access point to an authentication server. The server then accepts or rejects the user's request to join the network. If the client is authorized, the access point changes the user's (client's) state to authorized. Remote Authentication Dial-In User Service (**RADIUS**) is sometimes used to provide authentication. This type of authentication helps prevent unauthorized users from connecting to the network. In addition, this authentication helps keep authorized users from connecting to rogue access points or unauthorized access points.

EAP
Extensible Authentication Protocol, a protocol used in WPA, WPA2, and WPA3 by the client computer and the access point

RADIUS
Remote Authentication Dial-In User Service, a type of authentication that helps prevent unauthorized users from connecting to a network

Another way to further protect data transmitted over a WLAN is to establish a VPN connection. Doing so protects data from attackers. The following are basic guidelines for wireless security:

- Make sure the wireless security features are turned on.
- Use firewalls and intrusion detection on a WLAN.
- Improve authentication of a WLAN by incorporating 802.1X features.

- Consider using third-party end-to-end encryption software to protect data that might be intercepted by an unauthorized user.
- Whenever possible, use encrypted services such as SSH and Secure FTP.
- Update system firmware on a regular basis.

With the popularity of Wi-Fi hotspots, there has been a big increase in war driving and war chalking. **War driving** is a process in which attackers search for locations with open or weak wireless networks so that they can gain more access to the network and collect information or data from connecting users. **War chalking** involves leaving marks or symbols on the premises, outside the premises, or online to notify other hackers about the wireless vulnerabilities of the location. As drones have become easier to obtain, war driving has evolved into *war flying*—in which drones are used to gather wireless information from the air.

War Driving
A process in which attackers search for locations with open or weak wireless networks, so that they can gain more access to the network and collect information or data from connecting users

War Chalking
A process that involves leaving marks or symbols on the premises, outside the premises, or online to notify other hackers about the wireless vulnerabilities of the location

Bluetooth is not an 802.11 technology, but it is part of the 802.15.1 standard, and it suffers from exploitations similar to those that plague 802.11 wireless devices. Some notable Bluetooth exploits are Bluejacking and Bluesnarfing. Bluejacking is considered to be more annoying than harmful as it involves sending unsolicited text messages to other Bluetooth devices in the vicinity. Bluesnarfing is truly an attack to gain unauthorized access of another Bluetooth device over the Bluetooth connection with the intention of obtaining information stored on the Bluetooth device.

Note

An exploit involves using something for one's own advantage—such as taking advantage of a software bug—whereas a vulnerability can cause unintended behavior.

The bottom line is that the choice of the level of security within a network needs to be based on multiple factors. For example, what is the cost/benefit ratio for increased security? How will incorporating or not incorporating increased wireless security affect users? A network administrator needs to make some important decisions regarding wireless security before it is installed and the network becomes operational.

Section 11-8 Review

This section covers the following Network+ exam objectives.

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.
This section talks about the measures to take with SSIDs.

4.1 Explain common security concepts.
This section says that RADIUS is sometimes used to provide authentication. This type of authentication helps prevent unauthorized users from connecting to the network.

4.3 Given a scenario, apply network hardening techniques.
This section provides an overview of wireless security.

4.4 Compare and contrast remote access methods and security implications.
This section examines authentication in wireless networks.

Test Your Knowledge

1. True or false: Disabling SSID broadcasting will make it so that most client devices (such as Windows devices and Apple devices) won't notice that the wireless LAN is present.

   True

2. What are the two methods IEEE 802.11 supports for authenticating clients? (Choose two.)

   a. Closed-key authentication
   b. Slip-key authentication
   c. Open Authentication
   d. Shared-key authentication

11-9 REMOTE ACCESS AND VPN TECHNOLOGIES

This section addresses the technologies used to facilitate remote access to a network. It provides an overview of the analog, digital, and hybrid techniques used for establishing remote network connections via telephone line, as well as the limitations of modem connections. This section also provides an overview of the V.92/90 standard (for hybrid connections) and high-speed access using cable modems and DSL. This section also covers the last piece needed for remote access: the remote access server.

This section examines an important network tool: the virtual private network (VPN). A VPN is very important for helping to secure an external connection to a network. Students should understand the protocols used in the creation of tunnels, including GRE, mGRE, PPTP, L2F, and L2TP. They also need to understand IPsec and related security issues.

This section addresses the technologies used to facilitate remote access to a network. It includes an overview of analog, digital, and hybrid techniques used for establishing remote network connections. This section covers many of the broadband technologies that can be used, some of which are still prevalent in rural areas where the latest newer technologies like fiber-to-the home (FTTH) are not available. In fact, many areas of the United States are still struggling to get high-speed broadband connections to residential homes. It is therefore important to understand these technologies and their evolutions.

This section covers the limitations of modem connections and discusses the V.92/V.90 standard (for hybrid connections). Next, this section examines high-speed access using high-speed cable modems and high-speed remote digital access using DSL. This section concludes with the last piece needed for remote access: the remote access server.

Analog Modem Technologies

Analog modems were a breakthrough technology that paved the way for many other broadband technologies. Thanks to modems, voice frequency (analog) channels of the public switched telephone network (PSTN) can be used for the transmission of digital data.

To transport data over analog channels, the data must be converted to an analog form that can be sent over the bandwidth-limited voice-grade channels. On voice-grade telephone lines, bandwidth is limited by transformers, carrier systems, and line loading. Each of these factors contributes to attenuation of all signals below 300Hz and above 3400Hz. While the bandwidth from 300Hz to 3400Hz is suitable for voice transmission, it is not appropriate for digital data transmission because the digital pulse contains *harmonics* (higher frequencies) that are well outside this range. Transmitting data via a phone requires the conversion of a signal to fit totally within the 300Hz–3400Hz range. This conversion is provided by a modem.

There were several major modem standards for providing high-speed modem connections to analog telephone lines. **V.44/V.34** is totally analog and supports data rates up to 33.6Kbps, and **V.92/V.90** is a combination of digital and analog and supports data rates up to 56Kbps. A V.92/V.90 modem connection requires a V.92- or V.90-compatible modem and an Internet service provider (ISP) that has digital line service to the phone company. The data transfer with V.92/V.90 is called **asymmetric operation** because the data rate connection to the service provider is typically at V.34 speeds, whereas the data rate connection from the service provider is at the V.92/V.90 speed (56Kbps). The difference in the data rates in asymmetric operation is due to the noise introduced by the analog-to-digital conversion.

The old-style modem link from your computer to the PSTN (your telephone connection) is typically analog. This analog signal is converted to digital at the phone company's central office. If the ISP has a digital connection to the phone company, an analog-to-digital conversion is not required. However, the signal from the ISP through the phone company is converted back to analog for reception by your modem. The digital-to-analog process does not typically introduce enough noise to affect the data rate. Figure 11-20 shows the digital–analog path for V.92/V.90.

V.44/V.34
The standard for all analog modem connections with a maximum data rate of up to 34Kbps; V.44 provides improved data compression, smaller file sizes that provide faster file transfers, and improved web browsing

V.92/V.90
The standard for a combination analog and digital modem connection with a maximum data rate of 56Kbps; V.92 provides a quick-connect feature that cuts down on negotiation and handshake time compared to V.90

Asymmetric Operation
Modem operation in which the data transfer rates to and from the service provider differ

Note

Even though the number of dial-up users in the United States has declined over the years, the technology is still used in some rural areas in the United States and many international countries. It is still therefore important to have an understanding of this technology.

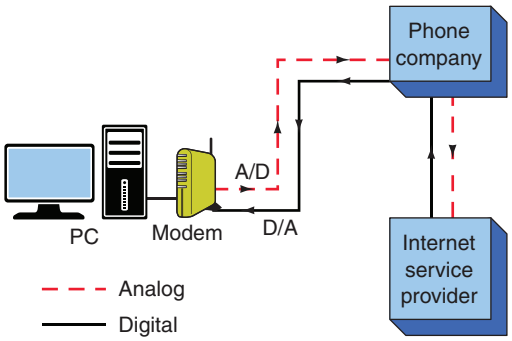


FIGURE 11-20 The digital–analog data path for V.92/V.90.

Cable Modem
A modem that can use the high bandwidth of a cable television system to deliver high-speed data to and from the service provider

DOCSIS
Data Over Cable Service Interface Specification, an international standard that enables high-speed data transfers over the cable system

Ranging
A technique that cable modems use to determine the time it takes for data to travel to the cable headend

xDSL
A generic representation of the various DSL technologies that are available

DSL
Digital Subscriber Line, a technology that uses existing copper telephone lines to carry data

The modem dial-up connection was considered to be the first out-of-band management for networks. A company would use a dedicated dialup modem to connect to the network or network devices. This out-of-band connection provided an alternative to dedicated access to the network to manage the network equipment. In contrast, traditional in-band management involves using a LAN to manage network equipment.

Cable Modems

Cable modems provide an alternative way to access a service provider. Data Over Cable Service Interface Specification (**DOCSIS**) is an international standard that enables high-speed data transfer over the cable system. Cable modems capitalize on their high-bandwidth network to deliver high-speed two-way data. Data rates range, on average, from 128Kbps to 200Mbps upstream (from the computer to the cable headend) and from 10Mbps to 1000Mbps downstream (from the cable headend to the computer). Cable modem connections can also be one-way when the television service implemented on the cable system precludes two-way communication. In this case, the subscriber connects to the service provider via the traditional telephone and receives the return data via the cable modem. The data service does not impair the delivery of cable television programming. Currently, cable systems use the Ethernet protocol to transfer data over the network. Many subscribers use the same upstream connection. This leads to potential collision problems, so a technique called **ranging** is used. With ranging, each cable modem determines the amount of time needed for its data to travel to the cable headend. This technique minimizes the collision rate, keeping it to less than 25%.

xDSL Modems

An **xDSL** modem is another high-speed Internet access technology. **DSL** stands for *Digital Subscriber Line*, and the *x* in xDSL represents the various types of DSL technologies currently available. DSL technology uses existing copper telephone lines to carry data. Copper telephone lines can carry high-speed data over limited distances, and the DSL technologies use this capability to provide high-data-rate connections. However, the actual data rate depends on the quality of the copper cable, the wire gauge, the amount of crosstalk, the presence of load coils, the bridge taps, and the distance to the phone service's central office.

DSL is the base technology in xDSL services. It is somewhat related to the ISDN service; however, the DSL technologies provide a significant increase in bandwidth, and DSL is a point-to-point technology. ISDN, in contrast, is a switch technology and can experience traffic congestion at the phone service's central office. Table 11-2 lists the available xDSL services and their data rates. Primary Rate Interface (PRI) is a form of ISDN that generally is carried over a T1 line and can provide transmission rates up to 1.544Mbps. PRI supports 23 B (bearer) channels and one 64Kbps D channel for data signaling. Basic Rate Interface (BRI) provides 2 B channels and 1 D channel for 144Kbps transmission rates.

TABLE 11-2 **xDSL Services and Data Rates**

Technology	Data Rate	Distance Limitation
ADSL	1.5Mbps–8Mbps downstream; up to 1.544Mbps upstream	18,000 ft.
IDSL	Up to 144Kbps full-duplex	18,000 ft.
HDSL	1.544Mbps full-duplex	12,000 ft. to 15,000 ft.
SDSL	1.544Mbps full-duplex	10,000 ft.
VDSL	13Mbps–52Mbps downstream; 1.5Mbps–16Mbps upstream	1,000 ft. to 4,500 ft.
VDSL2	Up to 100Mbps full-duplex	12,000 ft.

DSL services use filtering techniques to enable the transport of data and voice traffic on the same cable. Figure 11-21 shows an example of the ADSL frequency spectrum. Note that the voice channel, the upstream data connection (from the home computer), and the downstream data connection (from the service provider) each occupies its own portion of the frequency spectrum. **ADSL (Asymmetric DSL)** is based on the assumption that the user needs more bandwidth to receive transmissions (downstream link) than for transmission (upstream link). ADSL can provide data rates up to 1.544Mbps upstream and 1.5Mbps–8Mbps downstream.

ADSL (Asymmetric DSL)
A service that provides up to 1.544Mbps from the user to the service provider and up to 8Mbps back to the user from the service provider

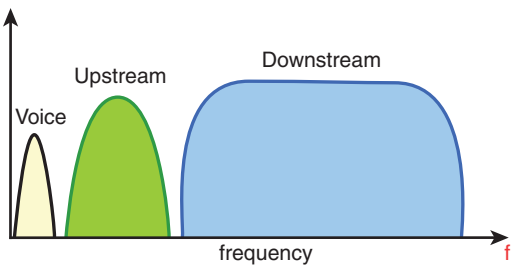


FIGURE 11-21 The ADSL frequency spectrum. (Source: *Modern Electronic Communication* 9/e, by G. M. Miller & J. S. Beasley, 2008, p. 502. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

The bandwidth of a copper telephone line is limited to 300Hz–3400Hz. The xDSL services use special signal-processing techniques for recovering received data and a unique modulation technique for inserting the data on the line. For ADSL,

Discrete Multitone (DMT)
A multicarrier technique used to transport digital data over copper telephone lines

a multicarrier technique called **discrete multitone (DMT)** modulation is used to carry data over the copper lines. It is well understood that the performance of copper lines can vary from site to site. DMT uses a technique to optimize the performance of each site's copper telephone lines. A DMT modem can use up to 256 subchannel frequencies to carry the data over copper lines. A test is initiated at startup to determine which of the 256 subchannel frequencies should be used to carry the digital data. The system selects the best subchannels and splits the data over those available for transmission.

Of the xDSL options, ADSL is receiving the most attention today because its data modulation technique, DMT, is already an industry standard. Figure 11-22 provides an example of an xDSL network. The ADSL system requires an ADSL modem, which must be compatible with the service provider. In addition, a POTS splitter or a DSL filter is needed to separate the voice and data connections. For residential applications, a DSL filter is generally placed in line with the phone connection to remove any of the high-frequency upstream data noise that gets into the voice frequency spectrum (refer to Figure 11-21). A filter is required for all telephone connections to eliminate noise interference any time a computer is in use on the connection.

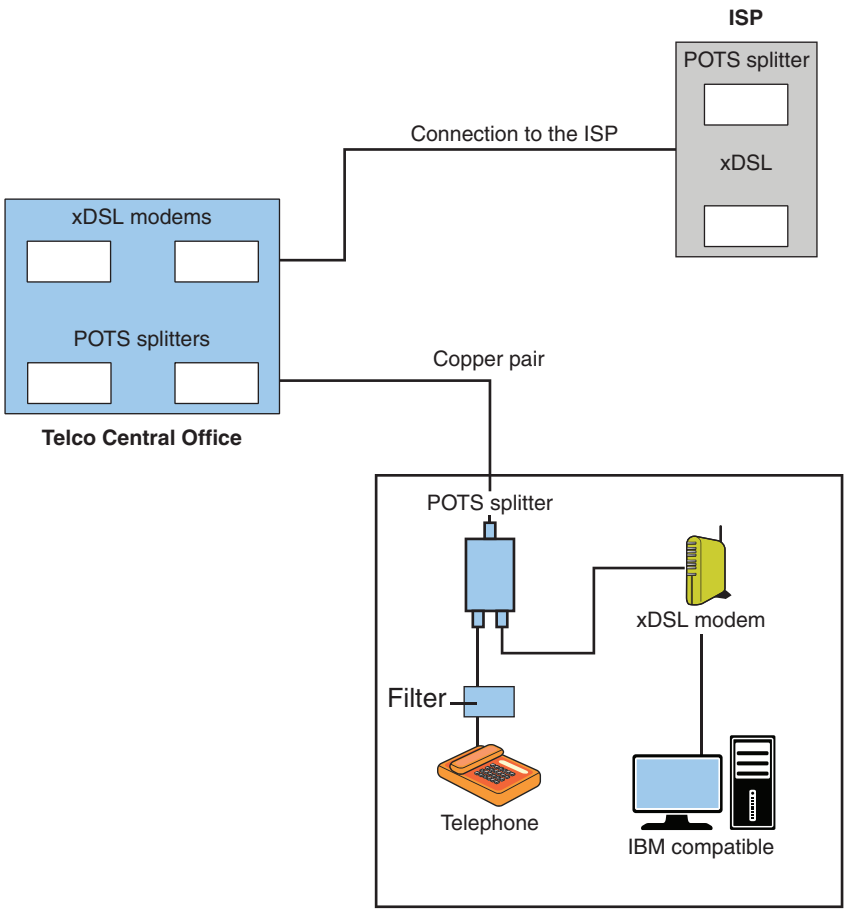


FIGURE 11-22 An xDSL connection to an ISP. (Source: *Modern Electronic Communication* 9/e, by G. M. Miller & J. S. Beasley, 2008, p. 503. Copyright ©2008 Pearson Education, Inc. Upper Saddle River, NJ.)

Remote Access Server

The remote access server (**RAS**) is the last piece needed to complete a dial-up connection to a network. The RAS provides a way for an outside user to gain access to a network. The connection to a RAS can be provided through a telephone line provided by the PSTN; in other words, the basic telephone service or the dial-up connection could also be via cable modem or DSL technology.

RAS
Remote access server, a server that provides a way for an outside user to gain access to a network

The protocol typically used for connecting to a RAS, Point-to-Point Protocol (PPP), helps establish a dial-up connection, manages data exchanges between the user and the RAS, and manages the data packets for delivery over TCP/IP.

The server connects to the PSTN through a modem (analog, cable, or DSL) to the telephone connection. The outside client also connects a PC to the PSTN through a modem, as illustrated in Figure 11-23.

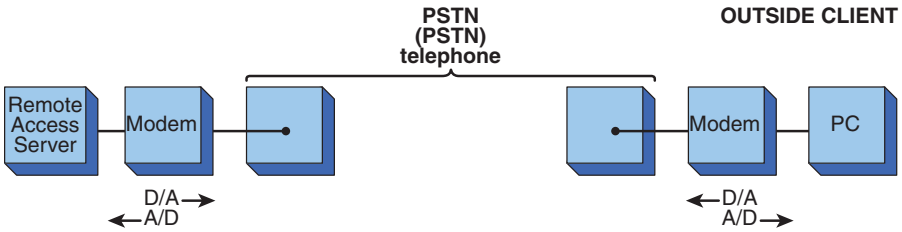


FIGURE 11-23 A RAS connection.

It is important for an organization to have a remote access policy, regardless of the technology the client is using.

Virtual Private Network

When a network is protected behind a firewall, it is sometimes referred to as a *private* network. Only computers on the same private network are considered to be trusted. Public access to this kind of network could be very limited. Access to a private network requires that special permission be granted on the firewall. Imagine a sales company that has its sales workforce throughout the country. The salespeople need to access the company's servers and databases at company headquarters, which is protected behind a firewall. It would be a network administrator's nightmare to have to grant individual access through the company's firewall. This type of setup would not allow for flexibility and mobility. A virtual private network (**VPN**) offers a solution to this problem. As the name implies, a VPN extends a private or trusted network over public infrastructure like the Internet. A VPN accomplishes this by establishing a secure connection between the remote end and the private network (private VLAN), therefore enabling the remote clients to become part of the trusted network. A network appliance that is designed to manage a secure VPN connection is called a *VPN concentrator*. A VPN concentrator is essentially an advanced router or a dedicated appliance that has been enabled to handle multiple VPN connections (VPN tunnels) into a network and hence acts as a **VPN headend**.

VPN
Virtual private network, an extension of a private or trusted network over public infrastructure like the Internet

VPN Headend
A device that handles multiple VPN connections (VPN tunnels) into a network

IP Tunnel
A secure VPN connection between two endpoints that encapsulates an IP packet in another IP packet

Remote Access VPN
A VPN that is used to facilitate network access for users in remote office networks or remote users who travel a lot and need access to the network

Site-to-Site VPN
A VPN that is used to create a virtual link from one site to the other and essentially replaces the traditional WAN-type connection used in connecting typical sites

Client-to-Site VPN
A VPN that provides mobile users a way to remotely access their information from a home network

GRE
Generic Routing Encapsulation, a tunneling protocol developed by Cisco for use as a site-to-site VPN solution

A secure VPN connection between two endpoints is known as an **IP tunnel**. A tunnel is created using an encapsulation technique, which encapsulates the data inside a known protocol (IP) that is agreed upon by the two endpoints. A tunnel creates a virtual circuit between the two endpoints and makes the connection appear like a dedicated connection even though it spans the Internet infrastructure. Three types of VPNs are commonly used today:

- **Remote access VPN:** A remote access VPN is used to facilitate network access for users in remote office networks or for remote users who travel a lot and need access to the network. The client usually initiates this type of VPN connection.
- **Site-to-site VPN:** A site-to-site VPN is used to create a virtual link from one site to another. It essentially replaces the traditional WAN-type connection used in connecting typical sites. This type of VPN requires network hardware such as a router or a firewall to create and maintain the connection. A traditional site-to-site VPN is a hub-and-spoke network. DMVPN (Dynamic Multipoint Virtual Private Network) is a spoke-to-spoke network technology. In this type of secure VPN network, data between sites is exchanged without requiring data traffic to pass through an organization's VPN.
- **Client-to-site VPN:** This type of VPN provides mobile users a way to remotely access their information from the home network.

VPN Tunneling Protocols

This section provides a quick overview of the protocols used in the creation of VPN tunnels. One of the original tunneling protocols is Generic Routing Encapsulation (**GRE**), which was developed by Cisco in 1994 and is still being used today. GRE is commonly used as a site-to-site VPN solution because of its simplicity and versatility. It is the only tunneling protocol that can encapsulate up to 20 types of protocols. In the past, when protocols such as AppleTalk, Novell IPX, and NetBEUI roamed the network, GRE was the tunneling protocol of choice to carry these protocols to other remote sites.

Establishing a GRE tunnel through the IP telco cloud to connect Router A with Router C requires that the source and destination addresses of the physical network connection be defined. For example, in Figure 11-24, Router A connects to the telco cloud via the router's Serial0/1 interface. The IP address 192.168.210.5 with subnet mask 255.255.255.0 has been assigned to the Router A Serial 0/1 interface. Router C (the remote router) connects to the telco cloud via its Serial0/1 interface. The IP address assigned to Router C's Serial 0/1 interface is 192.168.100.3 with subnet mask 255.255.255.0. (*Note:* Any interface that connects to the telco cloud can be used to set up the VPN interface.) A tunnel is then established on each of the routers. The tunnel is assigned an IP address that is used in the home network. For example, the home network is a 10.0.0.0 network; therefore, the tunnel between Router A and Router C will have a 10.*x.x.x* IP address. The tunnel between Router A and Router C is called *tunnel 0* and is assigned IP addresses 10.10.30.1 and 10.10.30.2. After the tunnel has been created across the IP network, the two routers appear to be on the same 10.10.30.*x* network.

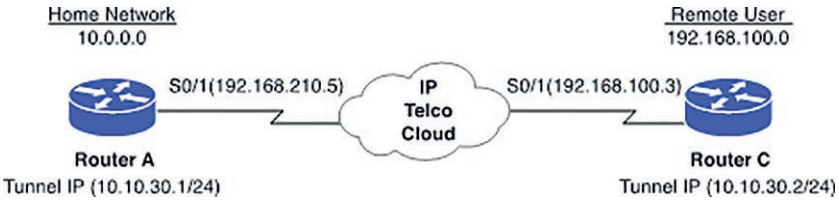


FIGURE 11-24 A GRE tunnel through an IP telco cloud.

The tunnel connection makes it appear as if remote users are part of the home network. This is accomplished by encapsulating the IP packet. The first packet uses the IP address that the remote user will use after the connection has been made. The encapsulation is used to transport the data across the networks.

Let's look at the configuration steps required on Router A and Router C to establish a GRE tunnel. In this case, you assign the tunnel 0 interface on Router A IP address 10.10.30.1. Then you need to define the IP destination and source address for the tunnel. Referring to Figure 11-24, the source IP address for tunnel 0 from Router A is 192.168.210.5, and the destination IP address for the remote interface on Router C is 192.168.100.3. After you configure the tunnel source and destination IP addresses, the router prompts that the "line protocol on Interface Tunnel0" changed state to up. The Router A configuration is as follows:

```
RouterA(config)# int tunnel0
RouterA(config-if)# ip 10.10.30.1 255.255.255.0
RouterA(config-if)# tunnel destination 192.168.100.3
RouterA(config-if)# tunnel source 192.168.210.5
00:31:37: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up
```

The Router C configuration is as follows:

```
RouterC(config)# int tunnel 0
RouterC(config-if)# ip address 10.10.30.2 255.255.255.0
RouterC(config-if)# tunnel destination 192.168.210.5
RouterC(config-if)# tunnel source 192.168.100.3
```

This simple example shows a point-to-point GRE tunnel being established between two routers. There are also Multipoint GRE (**mGRE**) tunnels, in which case you have a hub site and multiple spokes. The spokes have normal GRE configuration, and the hub site has mGRE configuration. GRE tunnels are appropriate for establishing permanent VPN connections between routers for remote offices of a company. However, a remote user who travels will have to establish a VPN connection directly from his or her PC, through an ISP and the VPN server in the home network.

mGRE
Multipoint GRE
A protocol that can be used to enable one node to communicate with many nodes

The tunneling protocols commonly used in remote access VPNs are mentioned throughout the rest of this section. To better understand remote access VPNs, you should at least understand the importance of Point-to-Point Protocol (**PPP**). In the days when modems and dial-ups were common, PPP was the key to the remote

PPP
Point-to-Point Protocol, the de facto protocol of dial-up networking

PAP
Password Authentication Protocol, a simple plaintext (unencrypted) authentication method that has been superseded by CHAP

CHAP
Challenge Handshake Authentication Protocol, an encrypted authentication method that uses the MD5 file hashing algorithm

MD5
Message Digest 5, a hashing algorithm

SHA
Secure Hash Algorithm, a secure hash algorithm that includes cryptographic algorithms and secure protocols for the protection of sensitive, unclassified information

PPTP
Point-to-Point Tunneling Protocol, a protocol developed jointly by Microsoft, 3Com, and Alcatel-Lucent that was designed to work in conjunction with PPP

L2F
Layer 2 Forwarding Protocol, a Cisco protocol that does not require any VPN client software

access solution; it was the de facto protocol of dial-up networking. In those days, people would make a dial-up connection to their ISP and establish a PPP session to the Internet. Even though authentication is optional for PPP, most implementations of PPP provide user multifactor authentication using protocols such as Password Authentication Protocol (**PAP**) or Challenge Handshake Authentication Protocol (**CHAP**). PAP is a simple, plaintext (unencrypted) authentication method, which has been superseded by CHAP, an encrypted authentication method that uses the **MD5** file hashing algorithm. Due to its vulnerabilities, MD5 was replaced by Secure Hash Algorithm (**SHA**), which is a secure hash algorithm required by law for use in certain government applications. It includes cryptographic algorithms and secure protocols for the protection of sensitive, unclassified information. SHA comes in several types: SHA-0, SHA-1, SHA-2, and SHA-3.

Later, Extensible Authentication Protocol (EAP) was introduced as another PPP authentication method. During the PPP authentication phase, the ISP dial-up server collects user authentication data and validates it against an authentication server such as a RADIUS server. The RADIUS server supports many methods of user authentication, including PAP, CHAP, and EAP. Even though PPP dial-up is not as prevalent today as it once was, the concepts of central authentication still lend themselves to many technologies and applications.

Point-to-Point Tunneling Protocol (**PPTP**) was developed jointly by Microsoft, 3Com, and Alcatel-Lucent in 1996. It has never been ratified as a standard. Microsoft was a big advocate of PPTP and made PPTP available as part of Microsoft Windows Dial-up Networking. A PPTP server was included in Microsoft NT 4.0 Server, and PPTP was widely used as a remote access solution. PPTP was designed to work in conjunction with PPP. A PPTP client software would establish a PPP connection to an ISP, and once the connection was established, it would make the PPTP tunnel over the Internet to the PPTP server. The PPTP tunnel uses a modified GRE tunnel to carry its encapsulated packet for IP transmission. Figure 11-25 illustrates a typical PPTP connection and other tunneling protocols. PPTP does not have any authentication mechanism, so it relies heavily on the underlying PPP authentication.

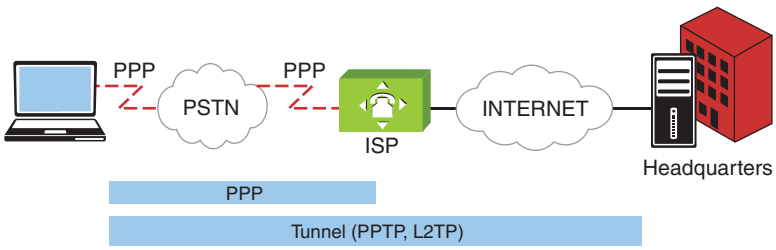


FIGURE 11-25 Tunneling with PPTP and L2TP.

Layer 2 Forwarding Protocol (**L2F**) was developed by Cisco around the same time as PPTP. L2F was not used widely in the consumer market due to its requirement of L2F hardware. Unlike PPTP, where the VPN client software is installed and

initiated from the client, L2F does not require any VPN client software. A L2F connection is intended to be made using L2F hardware. This hardware is designed to be at the ISP. A client would make a typical PPP connection to the ISP. The ISP then initiates the L2F tunnel connection on UDP port 1701 to the L2F server at the corporate headquarters. This requires coordination between the ISP and the corporate network. L2F relies on the PPP authentication to be passed on to the corporate authentication server.

Layer 2 Tunneling Protocol (**L2TP**), which was developed by the Internet Engineering Task Force (IETF) in 1999, was created with the intention of merging two incompatible proprietary tunneling protocols, PPTP and L2F. L2TP is considered to be an enhancement of the two previous protocols. It does not require specific hardware and can be initiated directly from the client. L2TP tunnel encapsulation is done on UDP port 1701. L2TP allows for tunnel authentication, so it does not have to rely heavily on the underlying PPP. If L2TP is used over an IP network where PPP is not used, the tunnel can be created with its own authentication mechanism.

All of the previously mentioned tunneling protocols lack one important security feature: encryption. Encryption can guarantee data confidentiality in a tunnel. IPsec offers encryption features that the other protocols lack. IPsec was designed to provide secure end-to-end connections. A VPN can take advantage of IPsec to provide network layer encryption as well as authentication techniques. IPsec is versatile in that it can be implemented easily in a remote access VPN (for remote file access) or a site-to-site VPN. For IPv6, IPsec is even more integral as it is embedded within the IPv6 packets.

IPsec uses two primary security protocols: Authentication Header (**AH**) and Encapsulating Security Payload (**ESP**). AH guarantees the authenticity of the IP packets. It uses a one-way hash algorithm such as MD5 or SHA to ensure the data integrity of the IP packets. ESP provides confidentiality to the data messages (payloads) by way of encryption. It uses symmetrical encryption algorithms such as Data Encryption Standard (**DES**), Triple Data Encryption Standard (**3DES**), and Advanced Encryption Standard (AES). However, MD5 is no longer a recommended hash algorithm, and DES/3DES are no longer recommended for encryption.

Before an IPsec tunnel can be established, quite a few security parameters have to be negotiated and agreed upon by both ends. IPsec uses the Internet Key Exchange (**IKE**) protocol to manage such processes. IKE is a hybrid protocol that encompasses several key management protocols, most notably Internet Security Association and Key Management Protocol (**ISAKMP**). Many times, the terms IKE and ISAKMP are mentioned alongside each other. There are two negotiation phases that the two network nodes must perform before the IPsec tunnel is complete. IKE Phase 1 is a phase in which the network nodes authenticate each other and set up an IKE SA (Security Association). In Phase 1, the **Diffie-Hellman** key exchange algorithm is used to generate a shared session secret key to encrypt the key exchange communications. This phase essentially sets up a secure channel to protect further negotiations in Phase 2. IKE Phase 2 uses the secure channel established in Phase 1 to negotiate the unidirectional IPsec SAs—inbound and outbound—to set up the IPsec tunnel. This is where the parameters for AH and ESP are negotiated.

L2TP
Layer 2 Tunneling Protocol, an IETF protocol created to merge two incompatibles proprietary tunneling protocols, PPTP and L2F

AH
Authentication Header, a security protocol that guarantees the authenticity of IP packets

ESP
Encapsulating Security Protocol, a security protocol that provides confidentiality to the data messages (payloads) by way of encryption

DES, 3DES
Data Encryption Standard, Triple Data Encryption Standard

IKE
Internet Key Exchange, a hybrid protocol that encompasses several key management protocols

ISAKMP
Internet Security Association and Key Management Protocol

Diffie-Hellman
A key exchange algorithm that is used to generate a shared session secret key to encrypt the key exchange communications

Configuring a Remote Client's VPN Connection

A remote client's VPN connection requires client software. (In contrast, clientless VPNs typically make use of a web browser interface.) Also, remote VPN connections typically offer two types of VPN tunnels:

- **Full tunnel:** All network traffic from the VPN client computer traverses the established VPN connection.
- **Split tunnel:** Network traffic to a specific network destination from the VPN client computer is configured to traverse the established VPN connection.

The following sections demonstrate how to configure a VPN remote client running Windows 10 or macOS. These examples assume that the client has permission to connect to the VPN server on your home network.

Configuring a Windows 10 VPN Client

To start the Windows 10 VPN client configuration, complete the following steps:

1. Click Start, select **Settings > Network and Internet > Network and Sharing Center**, and select **Set up a connection or network**.
2. On the left pane panel, select **VPN** and click **Add a VPN connection**.
3. On the next screen, make the following settings:
   - For the VPN provider, select **Windows (built-in)**.
   - For the connection name, enter a name for the VPN connection (for example, **salsa-vpn**).
   - For the server name and address, input the Internet address or the name of the VPN server.
   - For the VPN type, select **Automatic**.
   - For the type of sign in info, select **User name and password**.

   Click the **Save** button to complete the setup.
4. To establish a VPN connection, go back to the VPN window, selecting the VPN connection you just created, and click **Connect**.
5. Enter your username and password and click **OK** to connect.

Configuring a macOS VPN Client

To configure a VPN remote client running macOS, follow these steps:

1. Click the **Apple icon > System Preferences > Network** and then click the plus sign to create a new service.
2. In the new window that appears, select **VPN** as the new interface.

3. Select the appropriate VPN type, depending on the server configuration (either L2TP over IPsec, Cisco IPsec, or IKEv2).
4. Leave the service name set to the default or specify a new name and then click **Create** to create a new VPN service.
5. Click **Apply** to save the configuration.
6. Establish a VPN connection by selecting the VPN service under the **System Preferences > Network** window and clicking the **Connect** button. You can also establish a VPN connection by clicking the **VPN** icon at the top of the macOS main screen. The VPN connection to the home network VPN server should now be made.

Remember that the remote client must have a user account and password on the VPN server. In this example, the user's account name is jtest. The IP address 172.16.59.31 is assigned to the VPN remote client by the VPN server when a connection is made. The available IP addresses were specified when the VPN server was configured. As shown in Figure 11-26, running a **tracert** (**traceroute**) from the VPN client (172.16.59.31) to the server on the VPN network (172.16.59.2) shows a single hop. The VPN remote client appears to be on the same home network.

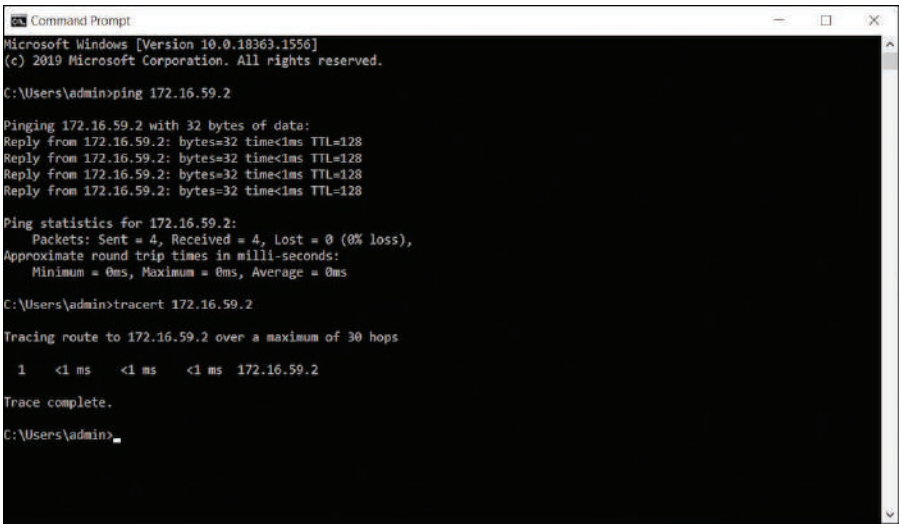


FIGURE 11-26 The traceroute from the VPN server to the VPN remote client.

Configuring a Cisco VPN Client

This section examines the setup of an end-to-end encrypted VPN connection using the Cisco VPN client software called Cisco AnyConnect Secure Mobility Client—or simply Cisco AnyConnect. Such connections can be used for both onsite and mobile (remote) users. The latest Cisco AnyConnect client is capable of using SSL/TLS or IPsec with IKEv2 as a transport protocol for the VPN connection.

The first step in setting up a Cisco VPN client is to install the software on the server that is to be used to establish the VPN connections. The VPN server in this case will most likely be a Cisco ASA (Adaptive Security Appliance), which has replaced the Cisco VPN concentrator platform. The Cisco AnyConnect client software must be licensed for each server installation and uploaded onto the server. The clients can then connect to the server and download the Cisco AnyConnect client software for installation. An individual requesting the software must have network access to the software. This usually requires that the user must have an authorized username and password. (The procedure to download the Cisco AnyConnect client software may differ depending on the organization.) After the software is installed, Cisco AnyConnect can be found in the Cisco folder under the Windows 10 All Apps menu.

Figure 11-27 shows the window that appears after you start the VPN client. This VPN status window indicates the current VPN status, which in this case is "ready to connect." In this window, you enter the hostname or IP address of the VPN server in the drop-down menu (see Figure 11-28) and click the **Connect** button.

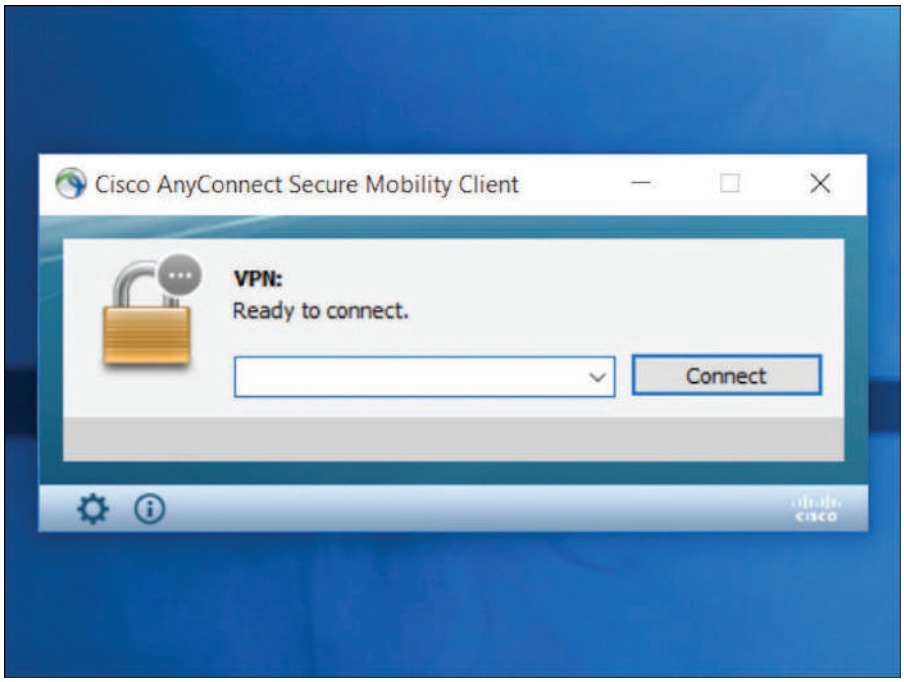


FIGURE 11-27 The VPN client status window appears after you start the VPN client software.

Note

The Cisco VPN client software attempts to set up a connection profile for the client. The available connection profiles for the client are configured when the server software is installed.

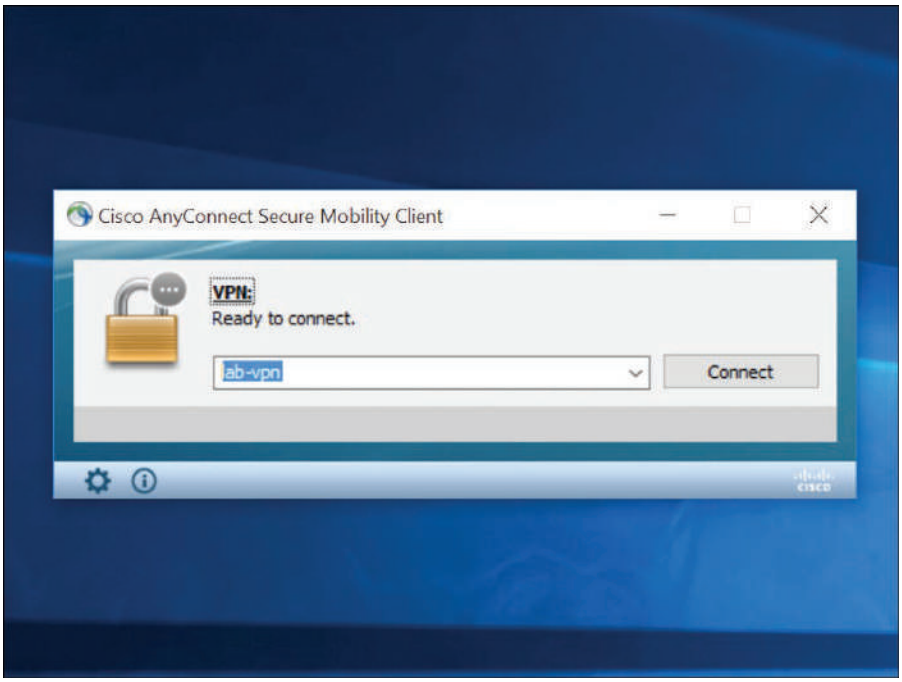


FIGURE 11-28 The connection screen for establishing a VPN link.

The drop-down menu may list the connection profiles and the last successful VPN connections. The next window displayed is the initial handshake screen with a VPN group profile called **banner**, as shown in Figure 11-29.

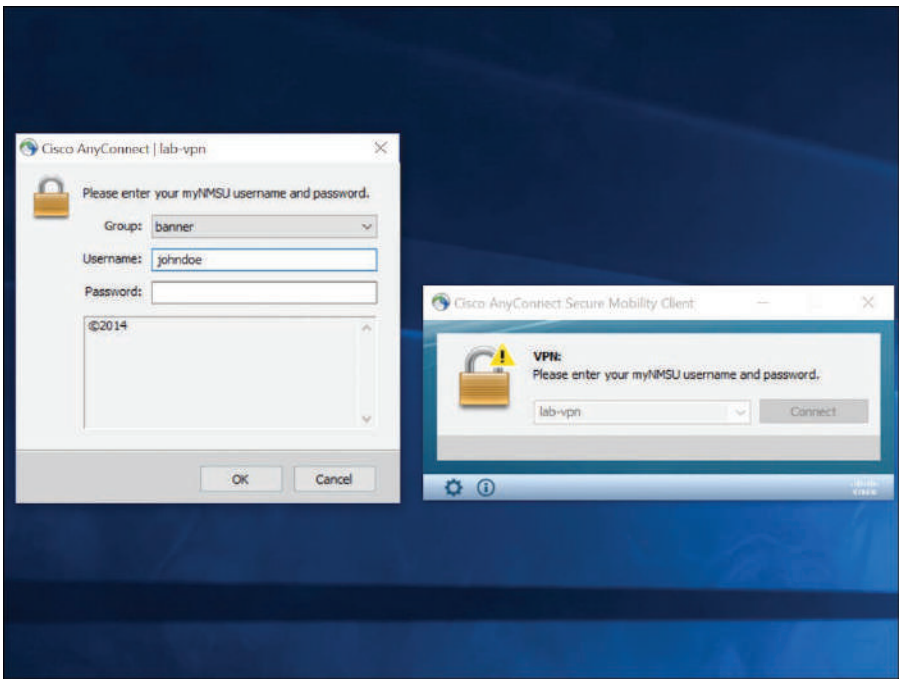


FIGURE 11-29 The initial handshake screen for the VPN client.

The next window (see Figure 11-30) shows that you have successfully connected to the VPN. The Cisco AnyConnect icon shows up with a "connected" status in the Windows taskbar at the bottom-right of the computer screen.

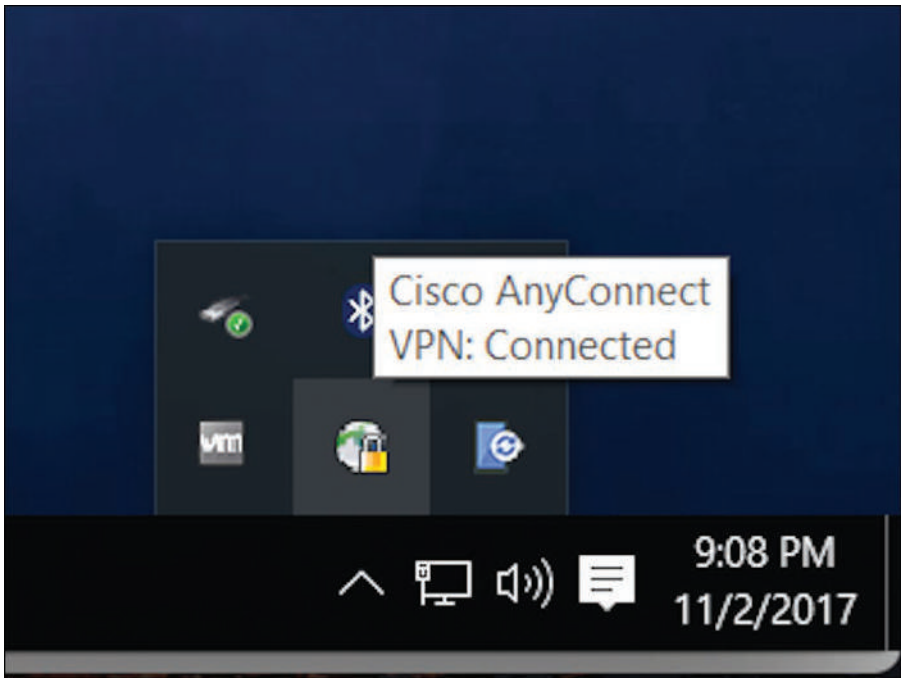


FIGURE 11-30 The menu showing that the VPN client has successfully connected to the virtual private network.

After the VPN connection has been established, you can click the **Cisco AnyConnect** icon and select **Open AnyConnect** to open the VPN status window. Then you can click the **Advanced Window** icon at the bottom left of the status window, and the preferences for the VPN connection are displayed (see Figure 11-31).

The next window, shown in Figure 11-32a, lists the statistics for the VPN session. It shows the IP addresses for both the VPN server and client. Another screen, Figure 11-32b, shows the route details for this VPN connection. The secure routes are the destination routes that will be protected by the VPN connection. All traffic to these destinations will traverse the VPN tunnel. The non-secured routes will not use the VPN connection.

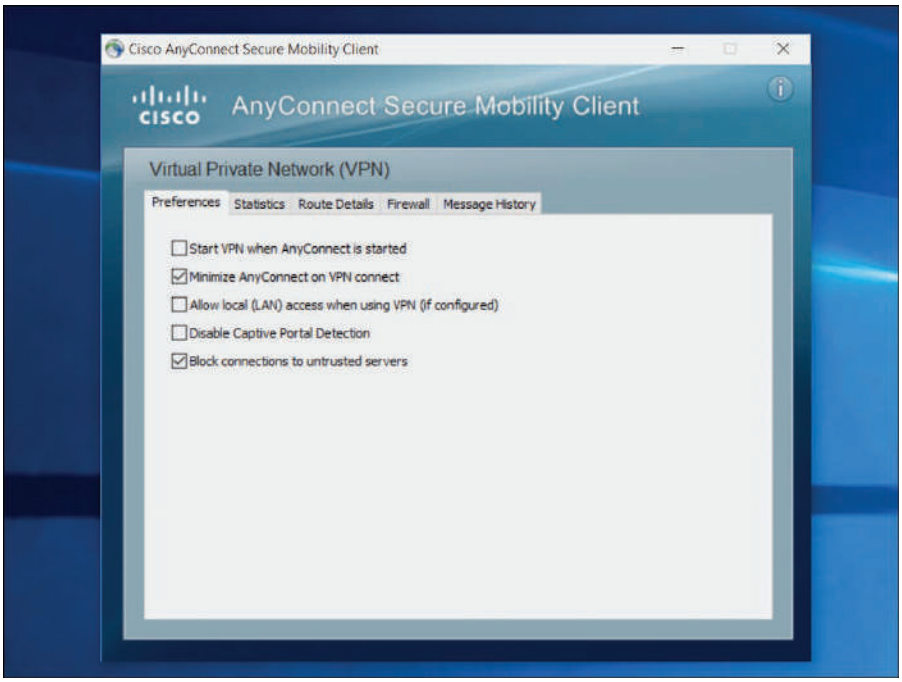


FIGURE 11-31 The Preferences window for the VPN client.

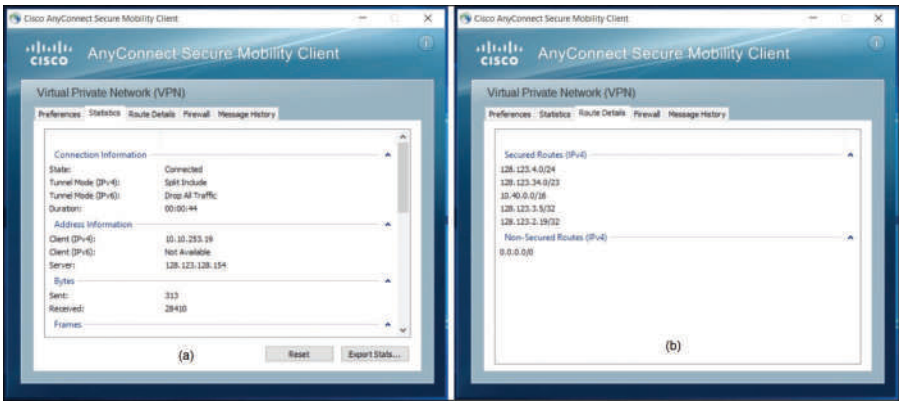


FIGURE 11-32 The Statistics window (a) and Route Details window (b) for the VPN client.

As you have seen here, configuring the Cisco AnyConnect VPN client software requires setting up the software on both a server and a client computer. Each type of VPN connection has a use, and a network administrator must be familiar with setting up VPN connections on different operating systems.

Section 11-9 Review

This section covers the following Network+ exam objectives.

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

This section discusses various tunneling protocols.

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

This section examines two primary security protocols used by IPsec: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH guarantees the authenticity of the IP packets, and ESP provides confidentiality to the data messages (payloads) by way of encryption.

1.8 Summarize cloud concepts and connectivity options.

This section examines the setup of an end-to-end encrypted VPN connection using the Cisco VPN client software Cisco AnyConnect.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section talks about cable modems.

4.1 Explain common security concepts.

This section examines Remote Authentication Dial-In User Service (RADIUS).

4.3 Compare and contrast remote access methods and security implications.

This section discusses the remote access servers used for phone dial-up connections.

Test Your Knowledge

1. True or false: Discrete multitone is a single-carrier technique used for transporting digital data over copper telephone lines. A test is initiated at startup to determine which of 256 subchannel frequencies should be used to carry the digital data.

   True

2. True or false: The data transfer for V.92/90 is called asymmetric operation because the data rate connection to the ISP is at V.24 speeds, whereas the data rate connection from the ISP is at V.92/90 speeds.

   False

3. What is the purpose of an IP tunnel?

   a. An IP tunnel creates a physical circuit between two endpoints and makes the connection appear like a dedicated connection even though it spans the network infrastructure.

   b. An IP tunnel creates a virtual circuit between two endpoints and makes the connection appear like a dedicated connection even though it spans the Internet infrastructure.

c. An IP tunnel creates a physical circuit between two endpoints and makes the connection appear like a dedicated connection even though it spans the internal network infrastructure.

d. An IP tunnel creates a physical circuit between two endpoints and makes the connection appear like a dedicated connection even though it spans the internal Internet infrastructure.

4. What must happen before an IPsec tunnel can be established?

a. Security parameters have to be negotiated and publicly agreed upon by both ends.

b. IKE Phase 1 is a phase in which both network nodes authenticate each other and set up an IKE SA. IKE Phase 2 uses the plaintext channel established in Phase 1 to negotiate the unidirectional IPsec SAs, inbound and outbound, to set up the IPsec tunnel.

c. IKE Phase 1 is a phase in which one network node authenticates the other and sets up an IKE SA. IKE Phase 2 uses the open channel established in Phase 1 to negotiate the unidirectional IPsec SAs, inbound and outbound, to set up the IPsec tunnel.

d. Security parameters have to be negotiated and agreed upon by both ends.

11-10 PHYSICAL SECURITY

This section examines the important and often-overlooked task of providing physical security for a networking facility. The objective of physical security in this case is to protect personnel, data, hardware, and software from any physical actions that could cause any type of loss and/or damage.

There are three significant components of physical security:

- **Access control:** Physical security measures include access control cards, biometric access and access control systems, and lockable fencing.
- **Surveillance:** Surveillance often includes cameras monitoring the facility and the perimeter. Notification systems such as sensors for intrusion detection and even smoke detectors and heat sensors should also be included.
- **Testing:** An IT facility should have in place a good testing procedure for the physical security system. It is important to make sure the facility can quickly detect any intrusions and recover from any disruptions. Testing procedures should be conducted on a regular basis and updated as needed.

Access Control
Physical security measures such as access control cards, possibly biometric access control systems, and lockable fencing

Surveillance
Monitoring that often includes cameras watching a facility and the perimeter as well as notification systems such as sensors for intrusion detection

Testing
A procedure for evaluating a physical security system

The objective of this section is to make sure you have a clear understanding of how to establish and maintain good physical security. The technologies used to safeguard sensitive information in IT facilities are complex and expensive. Most facilities already have in place someone who is responsible for overseeing the physical protection plan.

In terms of physical security, the ideal situation is to have a security bubble surrounding a facility: It would involve providing physical protection with a 360-degree view of potential threats, keeping foot traffic to a minimum, and minimizing physical access. This type of bubble is not practical, however.

All IT facilities have some data that is transferred via wireless (Wi-Fi) connections. In fact, many sites within an IT facility are constantly being accessed by users locally and from the Internet, as well as by hackers. How can you make sure that their access is controlled? What measures or testing do you have in place to make sure you have a robust network? Integrating network security and enabling all software security features is recommended for any facility, and so is incorporating physical protection.

Physical security is designed to protect data, people, equipment, facility, and any critical company assets. You need to make sure that staff are willing to use the methods chosen for access control. A good access control system works only if users are willing to use it. So, it is very important to have a good employee training program to make sure every employee understands the rules.

All facilities have points for both ingress (going in) and egress (going out) foot traffic. Obviously, you will need some form of access control for these points. Controlled access to a facility begins at the doors (both front and back) and is for any person who has authority and whose job responsibilities require specific access to designated areas.

Security in any organization needs to incorporate multiple layers of access control. It can include any of the following **physical access control devices**:

Physical Access Control Device
A device that is used to make sure personnel or visitors have adequate permission to access various facilities

- Perimeter fencing
- Video monitoring
- Building access control using badges and proximity (prox) cards
- Access control vestibules/mantraps
- Biometric scanning (fingers and retina)
- Locked access to equipment and documentation

Access Control Hardware

Access Control Hardware
Hardware used to identify and authenticate someone entering a facility

The purpose of **access control hardware** is to identify and authenticate someone entering a facility. It is similar to computer access control. Authentication factors can be based on the following:

- **Something you know:** This could be a code, a password, or a PIN.
- **Something you have:** This could be a key, a security card, or a token.

- **Something you are:** This could be a biometric factor, such as voice, fingerprint, retina, or iris recognition.

A number of types of access control hardware are used in the industry to prevent unauthorized physical access. They are used to make sure that personnel or visitors have adequate permissions to access various facilities. Access can be controlled on site or remotely. The following are some examples of common access control hardware:

- **Badge readers:** An access badge typically includes a photograph and information that identifies the user. The user's level of access is usually not encoded on the badge. When a user places a badge on or moves a badge close to the badge reader, the card reader reads the identifier information from the card and searches its access control database to determine whether the user is allowed access to the premises. Proximity cards are commonly used for badges.

Badge Reader
A card reader that gathers information from a card or badge and searches an access control database to determine whether the user is allowed access to the premises

- **Biometric scanners:** Compared to badge readers, biometric scanners are more sophisticated and higher cost, but they are very effective. Biometric scanners authorize users based on who they are and so provide a very effective way of identifying users. It is very difficult to fake fingerprint, voice, and retina scans. Biometrics can be used in place of access badges or used with access badges for additional security.
- **Access control vestibule (previously known as a mantrap):** An access control vestibule is typically two interlocking doors in which the first set of doors must be closed before the second set of doors can open. This arrangement, which is sometimes called a sally port, an air lock, or a mantrap, is designed to limit the number of people who can access a particular area at one time. An additional security check can be enforced once a person is in an access control vestibule.

Access Control Vestibule/Mantrap
A control device that consists of two interlocking doors in which the first set of doors must be closed before the second set of doors can open

- **Locking racks:** Critical equipment for an IT facility is often mounted in racks, and rack security is a major concern. You need to know when racks are accessed and when equipment is changed or removed. Racks typically need to be locked as a part of building and access security.

Locking Rack
A rack that can lock to protect critical equipment for an IT facility

- **Locking cabinets:** In the IT world, locking cabinets is another step in physical protection. Having critical equipment and documents locked up provides an additional layer of access control. A locked room helps minimize unauthorized access to IT equipment, and locked cabinets provide another layer of protection.

Locking Cabinet
A cabinet that can lock to protect critical equipment and documents

Detection Methods

After a person gains access to a facility, security surveillance should continue to be enforced. It is important to do real-time monitoring of people who are inside the

facility and keep track of their locations. The following are examples of some of the most widely used detection methods:

- **Surveillance cameras:** Surveillance cameras have been in use for a long time—since the days of CCTV (closed-circuit television). The technology has advanced from CCTV to IP cameras and from videotape recording to DVR (digital video recorder) and cloud-based recording.
- **Motion detection:** Motion-detection devices detect a change in the position of an object as it relates to its surroundings. There are many options for motion detection, including cameras and lights.

Motion Detection
The use of devices that can detect changes in the position of an object as it relates to its surroundings

Asset Disposal

An important part of physical access security focuses on what to do to with equipment when it reaches the end of its life cycle (EOL) or when it malfunctions. Equipment that contains configuration and proprietary information cannot just be thrown away. Rather, it must be handled according to the asset disposal policy of an organization. The following are common asset disposal practices:

- **Sanitize devices for disposal:** A tech-savvy person may be able to recover personal information from electronic devices (such as computers, hard drives, cell phones, networking equipment, and USB drives) that have been disposed of. It is therefore extremely important that all devices be sanitized before being thrown away. Sanitizing a device means wiping all information from the device.
- **Factory reset:** A factory reset, also called a hard reset or a master reset, restores a device to the factory settings. Applications, data, pictures, are deleted. Such resets are often performed to restore malfunctioning devices. A factory reset typically requires administrative access.

Sanitize Device
Wipe all information from a device

Factory Reset
A hard reset or a master reset that restores a device to the factory settings

Internet of Things (IoT) Security Devices

A lot of technologies are available to aid with physical security. Probably the most interesting of them are the Internet of Things (IoT) devices, which are smart devices that connect to an organization's network as well as the Internet. Their flexibility makes these devices easy to install and connect to a network, but it is imperative to ensure that external access (by hackers) can be prevented. The following are some examples of IoT devices that are commonly used for physical security in homes and offices:

- **IP security cameras:** These devices, which have become very popular in the recent years, are easy to install and connect to a network. Many companies offer cloud security camera services, so that cameras can connect to a cloud provider and send security footage to cloud storage. Users are able to view this footage from a computer or mobile device.

- **Smart lockers:** A smart locker is a storage location that contains technology that can notify a user that a package or document is ready. The locker can provide access instructions and send status notifications.
- **Smart speakers:** A smart speaker is a wireless speaker with an integrated voice assistant. Such devices typically use Wi-Fi or Bluetooth to communicate.
- **Smart doorbells:** A smart doorbell, which can connect to the Internet, can notify the user when someone is at the door. A smart doorbell is essentially a security camera mounted at the door. These devices use Wi-Fi connectivity to simplify installation.
- **Smart thermostats:** A smart thermostat can connect to a phone, a smart speaker, a tablet, or other Internet devices. Options for scheduling heating/cooling cycles and connecting to a home automation system are often included.

Smart Locker
A storage location that contains technology that can notify a user that a package or document is ready, provide access instructions, and send status notifications

Smart Speaker
A wireless speaker with an integrated voice assistant

Smart Doorbell
A doorbell that can connect to the Internet and that can notify a user when someone is at the door

While IoT devices provide many options for physical security, it is important not to assume that these devices are sufficient to protect the facility. Always assume that you need a more secure and robust physical security system.

Section 11-10 Review

This section covers the following *Network+* exam objective.

4.5 Explain the importance of physical security.

This section examines physical security concepts, including IoT security devices.

Test Your Knowledge

1. What are the three significant components of physical security? (Select three.)
   a. Access control
   b. Assistance
   c. Testing
   d. Turning
   e. Surveillance
2. In terms of physical security, which of the following is the ideal situation?
   a. A security sphere over a facility
   b. A security bubble under a facility
   c. A security bubble surrounding a facility
   d. Security guards around a facility

SUMMARY

This chapter presents a short overview of network security. A network administrator needs to not only design, assemble, and maintain a good network but also protect the network and its users from both external and internal (insider) threats. This chapter introduces some of the concepts that are critical to network security. You should understand the following concepts:

- The various ways an attacker can gain control of a network
- How denial-of-service attacks are initiated and how they can be prevented
- How security software like antivirus/anti-malware and personal firewalls works and why this software is important for protecting a computer and a network
- What sources are trusted sources and techniques used to identify trusted sources, grant access to trusted sources, and manage accessibility for trusted sources
- How security appliances such as firewalls, IPSs, and web filters work and why they are important for protecting a network
- How VPN technologies work and how to set up simple VPN clients
- How to secure 802.11 wireless LANs and what security issues a network administrator must be aware of when configuring a wireless LAN
- The importance of physical security in protecting data, people, equipment, facility, and other critical company assets

QUESTIONS AND PROBLEMS

Section 11-2

1. List six ways an attacker can gain access to a network.

   Social engineering, password cracking, packet sniffing, vulnerable software, viruses, wireless connections

2. Describe a way an attacker can use social engineering to gain control of a network.

   A variety of answer are possible. Here is one example: An attacker may pretend to be part of the networking staff and ask for a user's account name and password.

3. Describe how social engineering attacks can be avoided.

   Always require identification. Do not share information about network access.

4. What is a dictionary attack?

   An attack in which the attacker uses known passwords and variations to gain access

5. Can password cracking be prevented? How?

   Password cracking attacks can't be prevented, but they can be avoided if users follow several best practices:

   - Don't use passwords that are dictionary words
   - Don't use usernames (spelled forward or backward) as passwords
   - Use passwords (of eight or more characters) that contain letters, numbers, and special characters
   - Change passwords often

6. How does the use of a networking switch minimize problems with packet sniffing in a LAN?

   Switches don't pass all data traffic to all hosts on a network. An attacker would have to insert a device in between a host and a switch to see the packets.

7. Describe the concept of software vulnerabilities.

   A software vulnerability is a defect or coding error that can be used by an attacker to modify a system and gain control.

8. What is a buffer overflow?

   A buffer overflow occurs when a program tries to put more data into a buffer than it was configured to hold.

9. List two ways to prevent attacks on vulnerable software.

   Update application and operating system software regularly.

   Turn off all unused data ports and disable unnecessary services on a computer.

10. What are two simple ways to minimize or prevent viruses?

    Avoid opening email attachments.

    Always run antivirus/anti-malware software.

Section 11-3

11. What is a denial-of-service attack?

    It is an attack in which access to a service is denied to a computer, a network, or a server.

12. Describe a SYN attack.

    An attacker sends many TCP SYN packets to a host, opening many TCP sessions. The excessive number of TCP sessions keeps other users from accessing services.

13. What command do Cisco routers use to block broadcasts to a subnet?

    no ip directed-broadcast

14. Define directed broadcast.

    A broadcast that is sent directly to all hosts in a subnet

15. What security appliance can help prevent malicious attacks?

    IPS (Intrusion Prevention System)

Section 11-4

16. What is the purpose of a firewall?

    It protects a network from unwanted traffic.

17. Why is a stateful firewall important?

    It keeps track of data packet flow.

18. What is the first line of defense against viruses and worms?

    a. A personal firewall
    b. macOS
    c. Antivirus/anti-malware software
    d. The Linux operating system

19. Personal firewall software is typically based on which of the following?

    a. Using only trusted sites
    b. Configuring non-stateful firewall protection
    c. The 802.11X protocol
    d. Basic packet filtering inspections

20. Access lists are which of the following?

    a. A basic form of firewall protection
    b. Basically a firewall
    c. An improvement over firewall protection
    d. A replacement for proxy servers

21. Which of the following is true of packet filtering?

    a. It implies that data rates are smoothed out.
    b. A limit is placed on the packets that can enter the network.
    c. It should be avoided when ACLs are used.
    d. A limit is not placed on the packets that can exit the network.

Section 11-5

22. What is authentication, authorization and accounting (AAA)?

    a. A framework developed to enforce policies
    b. A framework developed to control access to computing resources
    c. A framework to monitor audit usage
    d. All of the above
    e. None of the above

23. Authentication defines ____.

    a. who you are
    b. where you are
    c. what you are
    d. None of the above are correct.

24. A Kerberos server issues a special token or ticket to authenticated users and uses that ticket to validate user access to a resource or a service. What is the term for this process?

    a. Pre-authorization
    b. Prior authorization
    c. Single sign-on
    d. Multi-layer sign-on

25. Accounting defines and keeps track of what?

    a. The RADIUS server
    b. What you do
    c. The Kerberos server
    d. All of the above
    e. None of the above

26. To prepare for disaster recovery, an organization must have which of the following?

    a. Multiple servers
    b. Multiple routers
    c. A wiring plan
    d. A backup plan

27. Which of the following is an all-in-one solution that integrates a wide range of security features into one appliance?

    a. UTM
    b. ATM
    c. UTA
    d. ATU

28. Which of the following is one of the most fundamental elements of network operations ?

    a. Certified cabling
    b. State-of-the-art routers
    c. Multiple software systems
    d. Documentation

Section 11-6

29. What is always on top of the list of any "best security" practices, and why is it important?

    Physical security is crucial. Routers and other important networking equipment should be placed in a secure area that is accessible only to authorized personnel. The easiest access to a router is via its console port, so someone who gains access to the premises can take physical control of a router.

30. What does the following command do?

```
RouterA(config)# username admin privilege 10 password @dm1np@$$wd
and what is level 10
```

    It creates a local user called **admin** with privilege level 10, which is used for system operators and makes **clear** and **debug** commands available.

31. What is the purpose of configuring AAA on a router?

    AAA enables authentication based on a router's local user database and enables line passwords as well as other access protocols.

32. What does the following command do?

```
RouterA(config)# crypto key generate rsa
```

    It generates an RSA key.

33. What does the command **transport input ssh** do?

    It enforces SSH as the access method.

34. What commands can be used to disable services such as echo, discard, daytime, and chargen? (Include the prompts with the commands.)

```
RouterA(config)# no service tcp-small-servers
RouterA(config)# no service udp-small-servers
```

35. What does the following command do?

```
RouterA(config)# snmp-server community M@ke1tD1ff1cuLT ro 15
```

    It configures a Cisco router with read-only and restricted access, as defined in access list 15.

36. What is the purpose of the following commands, and why is it important to use them?

```
RouterA(config)# no cdp run
RouterA(config)# no service config
RouterA(config)# no ip source-route
```

Cisco devices use Cisco Discovery Protocol (CDP) to identify each other on a LAN segment. This feature is enabled automatically and allows anyone on the network to collect network information. The remote configuration is disabled using the command **no service config**, which stops a router from loading its configuration from the network, which is not secure. A router is capable of loading its startup configuration from local memory, which is more secure than loading the configuration from the network. Source routing can be used in many kinds of attacks. When you disable this feature, the router disregards IP packets containing source route information.

37. What command is used to enable logging on a router?

```
RouterA(config)# logging on
```

38. What is the purpose of Network Time Protocol (NTP)?

It is used to correlate the time with log events.

39. Prepare an access list that can be used to prevent spoofing.

```
access-list 102 deny ip 12.12.12.0 0.0.0.255 any log
access-list 102 deny ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny ip 172.16.0.0 0.15.255.255 any log
access-list 102 deny ip 192.168.0.0 0.0.255.255 any log
access-list 102 permit ip any any
```

Section 11-7

40. What single command can be used to shut down multiple switch ports? Assume there are 24 Gigabit Ethernet ports, and each port is specified as GigabitEthernet1/*x*, where *x* is the number of the port. List the commands and the prompts.

```
SwitchA(config)# interface range gigabitethernet1/1-24
SwitchA(config-if)# shutdown
```

41. What command is used to enable port security on a switch? List the command and the prompt.

```
SwitchA(config-if)# switchport port-security
```

42. What does the following command do?

```
SwitchA(config-if)# switchport port-security maximum 2
```

This command configures port security to allow only a maximum of two MAC addresses per port.

43. What command can be used on a switch to limit the number of unicast, multicast, or broadcast packets that each port can receive with a rising threshold of 15Mbps and a falling threshold of 5Mbps?

```
SwitchA(config-if)# storm-control unicast level 1.5 0.5
```

44. What does the following command do?

```
storm-control unicast level pps 7k 3k
```

It configures the unicast storm to discard any unicast packets above 7000 packets per second; unicast traffic will resume if it falls below 3000 packets per second.

45. What are the four states an STP-enabled switch goes through before it can pass data traffic?

Block, listen, learn, and forward

46. What does the command **spanning-tree bpdufilter enable** do on a switch?

It is used to enable BPDU Filter at the interface level.

47. What command is used to enable STP Root Guard? List the command and the prompt.

```
SwitchA(config-if)# spanning-tree guard root
```

48. What does the following command do?

```
SwitchA(config-if)# switchport trunk allowed vlan 5,7,18,20
```

It allows VLANs 5, 7, 18, and 20.

Section 11-8

49. What is the most important thing to do when using a wireless network?

Turn on the wireless security features

50. What is the purpose of wireless beacons?

Beacons are used to verify the integrity of a wireless link.

51. What information can be obtained from a wireless beacon?

The SSID

52. What is the purpose of WEP?

WEP (Wired Equivalent Privacy) is used to encrypt and decrypt wireless data packets. However, WEP is not considered secure today.

53. List five guidelines for wireless security.

Turn on the wireless security features.

Use firewalls and intrusion detection on the LAN.

Improve authentication of the WLAN by incorporating 802.1X security features.

Consider using third-party encryption to protect wireless data.

Whenever possible, use encrypted services such as SSH and Secure FTP.

54. Describe the steps used with WPA2 to authenticate a user.

An access point sends an EAP message requesting the user's identity. The user (the client computer) returns the identity information that is sent by the access point to an authentication server. The server then accepts or rejects the user's request to join the network. If the client is authorized, the access point changes the user's (client's) state to authorized.

55. What is a RADIUS server?

A RADIUS (Remote Authentication Dial-In User Service) server is sometimes used to provide authentication. This type of authentication helps prevent unauthorized users from connecting to a network. In addition, this authentication helps keep authorized users from connecting to rogue, or unauthorized, access points.

Section 11-9

56. What is the bandwidth of a voice channel in the public switched telephone network?

300Hz to 3400Hz

57. Why is data transfer for V.92/V.90 called *asymmetric* operation?

The data rate connection to the service provider is at V.34 speeds, whereas the data rate connection from the service provider is at V.90 speeds.

58. What are the data speeds for V.44/V.34 and V.92/V.90?

V.44/V.34: Up to 33.6Kbps

V.92/V.90: Up to 56Kbps

59. Cable modems use a technique called *ranging*. Define this term.

Ranging is a technique that cable modems use to determine the time it takes for data to travel to the cable headend.

60. What are the data rates for basic access service ISDN and the ISDN primary access channel?

Basic access service: 192Kbps

Primary access channel: 1.544Mbps

61. What is ADSL, and what are its data rates?

ADSL is Asymmetric DSL, which provides up to 1.544Mbps from the user to the service provider and up to 8Mbps back to the user from the service provider.

62. Define discrete multitone.

    Discrete multitone (DMT) is a multicarrier technique used for transporting digital data over copper telephone lines. A test is initiated at startup to determine which of the 256 subchannel frequencies should be used to carry the digital data.

63. What is the purpose of a remote access server?

    It provides a way for an outside user to gain access to a network.

64. What is PPP, and what is its purpose?

    Point-to-Point Protocol (PPP) helps establish a dial-up connection, manages data exchanges between a user and the RAS, and manages data packets for delivery over TCP/IP.

65. What international standard enables high-speed data transfer over the cable system?

    DOCSIS: Data Over Cable Service Interface Specification

66. What is the goal of a VPN tunnel?

    The goal of a VPN tunnel is to make two ends of a network connection appear as if they are on the same subnet. The tunnel makes the remote clients appear as if they are directly connected to the network.

67. List five steps for troubleshooting a VPN tunnel link.

    1. Check the source and destination IP addresses of the tunnel configured on the router.
    2. Make sure the IP addresses on the ends of the tunnel are in the same subnet.
    3. Ping the destination from the source.
    4. Use **show configuration** or **show run** to make sure the source and destinations are properly configured.
    5. If the problem is still not found, try rebooting the routers.

68. What does encryption guarantee?

    Data confidentiality

69. Draw a sketch of the encapsulation of a VPN data packet. Show the IP source and destination address and the VPN tunnel source and destination address encapsulated with the IP packet.

    The diagram should look like Figure 11-24.

70. Explain the expected difference between running a traceroute from a home network to a remote user using the IP address for the remote user's router interface and running a traceroute from the home network to the remote user's VPN tunnel address.

    The traceroute to the router interface shows multiple hops, whereas the traceroute to the remote user's VPN tunnel address shows a direct connection.

71. Identify two tunneling protocols that can be used to configure a remote user's PC.

    PPTP (Point-to-Point Tunnel Protocol)

    L2TP (Layer 2 Tunneling Protocol)

72. What are the two primary security protocols used by IPsec?

    AH (Authentication Header) and ESP (Encapsulating Security Payload)

73. What is IKE?

    IKE (Internet Key Exchange) is a hybrid protocol that encompasses several key management protocols, most notably ISAKMP (Internet Security Association and Key Management Protocol).

74. List the command and the router prompt for configuring an IP tunnel 0 to 172.16.25.1 using the subnet mask 255.255.255.0.

```
RouterA(config)# int tunnel0
RouterA(config-if)# ip 172.16.25.1 255.255.255.0
```

75. What does the following command do?

```
RouterA(config-if)# tunnel destination 192.168.200.5
```

    It specifies the tunnel's destination IP address for the remote interface.

Section 11-10

76. Why is a security bubble an ideal situation for physical security?

    It provides 360 degrees of protection.

77. Provide three examples of access control.

    Any three of the following:

    Perimeter fencing

    Video monitoring

    Building access control using badges and proximity (prox) cards

    Access control vestibules/mantraps

    Biometric scanning (such as fingerprint and retina scanning)

    Locked access to equipment and documentation

78. What is an access control vestibule?

    An access control vestibule device is typically two interlocking doors in which the first set of doors must be closed before the second set of doors can open. This arrangement, which is sometimes called a sally port, an air lock, or a mantrap, is designed to limit the number of people who can access a particular area at one time.

79. List the three factors typically used for authentication.

Something you know, such as a password or PIN.

Something you have, such as a security card or token

Something you are, such as your voice, fingerprint, retina, or iris

Critical Thinking

80. Your network is experiencing an excessive number of pings to your network server. The pings are from outside the network. Someone suggests that you set an access list to block ICMP packets coming into the network. How would you respond?

You can't block ICMP packets because ICMP is a basic TCP protocol used for transferring data packets.

81. Your supervisor informs you that a user on the network has requested a VPN connection. Prepare a response to the supervisor, discussing what is needed to provide the connection.

The answer should include a discussion about how to set up the VPN connection. It would be good to recommend a VPN client software package such as Cisco AnyConnect Secure Mobility Client.

Certification Questions

82. In regard to firewalls, packet filtering accomplishes which of the following?

a. Ensures that not all network services can be filtered

b. Places a limit on the amount of information that can enter a network

c. Simplifies the creation of access lists

d. All of these answers are correct.

83. Which of the following best describe intrusion detection?

a. The monitoring of data packets passing through a network to catch potential attacks

b. The monitoring of data packets passing through a network to catch ongoing attacks

c. The monitoring of data packets with invalid IP addresses that pass through a network.

d. None of these answers are correct.

84. A signature is ____.

a. an IP address of a known hacker

b. an email address of a known attacker

c. an indicator of a known attack

d. None of these answers are correct.

85. Which of the following indicates repeated attempts to make connections to certain machines?

    a. Operation error
    b. Pinging
    c. Tracing
    d. Probing

86. Eavesdropping on network data traffic can be minimized by using which of the following?

    a. Hubs
    b. Switches
    c. Ports
    d. Gigabit Ethernet networks

87. True or false: It is important to block ICMP packets coming into a network to prevent intrusion.

    False

88. What is the name for a broadcast sent to a specific subnet?

    a. Multicast
    b. Broadcast
    c. Directed broadcast
    d. Sweep

89. True or false: The command used to display the ports that are currently open on a machine running a Windows operating system is **netstat -r**.

    False

90. Which of the following is the command used to display currently open ports on a machine running a Windows operating system?

    a. **netstat -a**
    b. **netstat -r**
    c. **netstat -o**
    d. **netstat - a**

91. Which of the following is a piece of malicious computer code that, when opened, starts a program that attacks a computer?

    a. An overflow
    b. A virus
    c. A botnet
    d. Denial-of-service

12
CHAPTER

Cloud Computing and Virtualization

Chapter Outline

12-1 Introduction
12-2 Virtualization
12-3 Cloud Computing
12-4 Enterprise Storage
Summary
Questions and Problems

Objectives

- Describe the concept and benefits of virtualization
- Discuss the concept of the cloud
- Explain the purpose of a hypervisor
- Develop an appreciation for the benefit of outsourcing services to the cloud
- Understand the steps in setting up virtualization on a PC

Key Terms

core
cache
virtualization
VM
guest machine
host machine
hypervisor
VMM
Type 1 hypervisor
Type 2 hypervisor
vMotion, XenMotion, Live Migration
Hyper-V
cloud
outsourcing
cloud service/cloud computing
SLA
MX (Mail Exchange) record
CNAME (Canonical Name) record
infrastructure as a service (IaaS)
platform as a service (PaaS)
software as a service (SaaS)
desktop as a service (DaaS)
scalability
elasticity
multitenancy
SAN
Fibre Channel (FC)
InfiniBand (IB)
iSCSI
NAS

This chapter examines virtualization technology and its applications. Also, it explores cloud computing services. It also presents a look at enterprise storage.

12-1 INTRODUCTION

This chapter introduces the concept of working in the cloud and explains virtualization. A key goal is for students to gain a firm grasp of the terminology related to working in the cloud and virtual systems.

This chapter examines virtualization technology and its applications. Also, it explores cloud computing services. Section 12-2, "Virtualization," presents concepts and techniques related to working in a virtual environment. Section 12-3, "Cloud Computing," introduces cloud computing and explores services related to the cloud. It also presents some of the technical issues required to make data flow to the cloud. Section 12-4, "Enterprise Storage," examines enterprise storage, the most common—and possibly most important—component for a typical user.

Table 12-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 12-1 **Chapter 12 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Fundamentals**	
1.1	Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.	12-4
1.2	Explain the characteristics of network topologies and network types.	12-2, 12-3, 12-4
1.4	Given a scenario, configure a subnet and use appropriate IP addressing schemes.	12-2
1.6	Explain the use and purpose of network services.	12-2, 12-3
1.7	Explain basic corporate and datacenter network architecture.	12-3, 12-4
1.8	Summarize cloud concepts and connectivity options.	12-3, 12-4
3.0	**Network Operations**	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	12-2
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	12-2, 12-3
4.0	**Network Security**	
4.3	Given a scenario, apply network hardening techniques.	12-3

12-2 VIRTUALIZATION

Virtualization is an exciting IT development. Students need to have a good understanding of the terminology used to describe the various virtual technologies. They should also experiment with installing their own virtual environment. This section presents an example of setting up a Windows 10 virtual environment using Microsoft's Hyper-V.

In the past, having multiple CPUs in one computer was not the norm. Only high-end server-class machines had the architecture to take advantage of multi-CPU processing. It used to be expensive to run a server with multiple CPUs, lots of RAM, and a big hard drive. This has changed thanks to developments in microprocessor technology and computer architecture that have led to prices becoming more affordable.

The development of microprocessor technology has seen incredible growth. A single-CPU architecture has evolved to a single CPU with multiple cores. A **core** is an independent processing unit that is responsible for reading and executing program instructions. So, instead of having multiple physical CPUs, a single integrated circuit can contain two or more processors and their associated local caches. A **cache** is a block of memory that is set aside for temporary storage of information.

core
An independent processing unit that is responsible for reading and executing program instructions

cache
A block of memory that is set aside for temporary storage of information

Much like a multiple-CPU architecture, a multicore CPU can execute more than one independent instruction at a time, thereby allowing for true multitasking. A multicore processor is not limited to only the server platform. In the mid-2000s, desktops, laptops, and workstations started to ship with dual-core processors. CPUs have become more affordable, and computers today ship with multicore CPUs. If you are in the market for a computer today, you are like to buy one whose processor has four or more cores.

Also in the mid-2000s, the market started to see a shift from 32-bit CPUs to 64-bit CPUs. In the past, 64-bit CPUs were used mostly in supercomputers and high-end servers. The 64-bit architecture allowed supercomputers and servers to compute twice as many data bits in the same clock cycle. Another big advantage of the 64-bit architecture is the maximum supported RAM. The 32-bit architecture can support only up to 4GB of RAM, whereas the 64-bit architecture can theoretically support 16 exabytes (EBs). This is significant for servers because they can run more programs and support more users at the same time. Overall, the 64-bit architecture provides faster and better performance than the 32-bit architecture.

Operating systems also have evolved to take full advantage of the 64-bit architecture. 64-bit operating systems are readily available. Even personal operating systems like Microsoft Windows now ship with both 32-bit and 64-bit versions. Currently, most operating systems are standardized on CPU platforms such as Intel and AMD and on 32-bit and 64-bit hardware architectures. Microsoft Windows, Linux, and even Mac operating systems can all run on the Intel 64-bit platform. This is an extraordinary convergence, considering where they were in the past.

All these developments in technology have paved the way for virtualization. **Virtualization** is a technology concept that involves creating a virtual computer. This virtual computer can contain but is not limited to a virtual CPU, virtual operating system, virtual storage, virtual network card, virtual firewall, virtual router, or

Virtualization
A technology concept that involves creating a virtual computer

VM
Virtual machine, a virtual computer that lives inside a physical machine

Guest Machine
A virtual computer

Host Machine
A physical machine

virtual NIC (vNIC). A virtual computer—called a virtual machine (**VM**), guest VM, or **guest machine**—can live inside a physical machine—called a **host machine** or virtual host. The virtual host machine can spawn as many guest machines as its physical hardware or platform can allow. A key idea behind virtualization is that the CPU and memory are often underutilized; they are not always tasked with processes to execute. It is extremely common to see the CPU in idle state, not being used by any program. This is more common in personal computers than in servers; computers spend more time in an idle state than in an active state.

When a computer's CPU is idle, in most circumstances, the rest of the hardware—such as RAM, disk I/O, and the NIC—stays idle as well. Virtualization takes advantage of this concept and uses virtualization software to carve out enough CPU processing time, enough RAM, and enough disk space to create a virtual machine within a host machine. The number of active guest machines depends on how powerful the host machine is. (Note that when a guest machine is shut down, it requires only storage space and no other computing resources.)

Hypervisor
Software that is used for managing and controlling the underlying physical hardware and associated virtual hardware

VMM
Virtual machine manager, software for managing and controlling the underlying physical hardware and associated virtual hardware

The software used to provide virtualization is referred to as a **hypervisor**. It provides a virtual machine manager (**VMM**) for managing and controlling the underlying physical hardware and associated virtual hardware.

There are two types of hypervisors:

- **Type 1 hypervisor:** This type of hypervisor, which is commonly used on servers, is loaded directly on the hardware to abstract the hardware to the virtualization layer. It is sometimes called a bare-metal hypervisor. Some well-known Type 1 hypervisors are VMware's vSphere/ESXi, Microsoft's Hyper-V, Linux KVM, Red Hat's Enterprise Virtualization, and Citrix's XenServer.
- **Type 2 hypervisor:** This type of hypervisor, which is commonly used on personal computers, is loaded on an operating system and abstracts the virtualization layer through its host operating system. It is sometimes called a hosted hypervisor. Some well-known Type 2 hypervisors are VMware Workstation, Oracle's VirtualBox, VMware Fusion for Mac, and Parallels for Mac.

Type 1 Hypervisor
A hypervisor that is loaded directly on hardware to abstract the hardware to the virtualization layer; commonly used on servers

Type 2 Hypervisor
A hypervisor that is loaded on an operating system and abstracts the virtualization layer through its host operating system and that; commonly used on personal computers

It used to be that when an organization needed a server, a dedicated server with the right CPU and the right amount of RAM and hard drives would be identified and purchased. The specifications also depended on the functions or services the server would perform. For example, a database server would need to have more memory than a file server, whereas a file server would need to have more storage space.

Virtualization is a more cost-effective way to provide server management and maintenance. Instead of buying different servers for different services, an organization can purchase only one server. For example, a server with two 18-core processors, 24 units of 32GB RAM, and four 6TB hard drives will yield the computing resources of 36 processors, 768GB of RAM, and 24TB of storage space. This server will have enough computing resources to provision many powerful

virtual servers serving different functions. When a virtual server needs more resources in the future, more CPU and RAM can be assigned to it, and more disk space can be provisioned for it. This is all done via the virtualization software, which is more convenient than opening up the physical unit to upgrade CPU, RAM, and hard drives.

An additional benefit of virtualization is that it reduces the physical footprint of a server. The number of physical servers decreases, which reduces the space used in the data center, which helps reduce the power consumption and heat dissipation requirements.

Skeptics of virtualization argue that it presents a single point of failure. Having multiple and critical virtual machines running on one physical server could indeed present a great risk. Every good IT person has been taught not to put all the eggs in one basket. Virtualization software vendors have responded to this problem by introducing a feature that makes it possible to move a live virtual machine from one physical server to another. In the event that a physical host server fails, all the virtual machines can be moved to a designated host server. Many vendors have implemented this concept, using different names. VMware calls it **vMotion**, Citrix calls it **XenMotion**, and Microsoft calls it **Live Migration**.

vMotion, XenMotion, Live Migration
Different vendor options for moving a designated host server in the event of a physical server failure

For individual VM guest machines, taking snapshots is another best practice recommendation for disaster recovery in virtualization. A snapshot of a VM is a copy of the current state of a VM at a particular instant in time. A snapshot, which can be created while the VM is in operation, can be used later to roll back a VM to a previous states—the state for which the snapshot was made. Snapshots can be saved and archived for later use, in much the same way as backup images. Microsoft renamed its Hyper-V snapshots to Hyper-V checkpoints starting in Windows Server 2012 R2.

Because a hypervisor can contain multiple guest VMs, there must be a virtual network for them to communicate. Network functions virtualization (NFV) involves the virtualization of network components. The virtual network works using a similar concept to the physical network: Whereas there are physical network switches to connect physical network devices, in a virtual network, there are virtual switches connecting guest VMs and establishing connections between the virtual network and the physical network. An example of NFV is virtual switches (or vSwitches), which can be created inside a VM host. There are two types of virtual switches:

- **Standard virtual switch (vSwitch):** This is a typical virtual switch, dedicated to one specific host VM; it must be managed from that host VM.
- **Distributed virtual switch (dvSwitch):** Unlike vSwitches, dvSwitches can span multiple host VMs, connecting their virtual networks together. dvSwitches evolved from the distributed switching concept, where the switch forward plane is separate from the control plane, allowing the switch fabric to span multiple locations. A dvSwitch needs to be able to communicate with its central control plane.

Note

When talking about virtual servers and virtual networking, there may be confusion or misunderstanding regarding the term *virtual IP address*. A VM's IP address is not referred to as a virtual IP address; rather, it is just called an IP address. A virtual IP (VIP) address is an IP address created to be shared by a group of network devices. A VIP address is purposely created as a floating IP address to be used with network proxy techniques like Port Address Translation (PAT) and in high availability technologies like load balancing and Virtual Router Redundancy Protocol (VRRP).

The personal computing world has also gained some benefits from virtualization. It used to be that if you wanted to run two or more operating systems simultaneously, you needed to own multiple computers. Today, personal desktops or laptops often have 64-bit multicore CPUs, 4GB of RAM or more, and more than 500GB of disk space. With a Type 1 hypervisor installed, you can run virtual machines of Windows 10, Windows 7, and even Linux at the same time on the same physical computer. Better yet, Mac users can enjoy running virtual machines of Windows and Linux on Mac hardware.

Not everything is designed or allowed to be virtualized, however. A prime example is macOS. No hypervisor at this time is capable of virtualizing macOS. This is not a technical issue because macOS can run on Intel CPUs, just like other operating systems. Rather, Apple has strict licensing restrictions that prohibit running macOS on non-Apple-labeled hardware.

Another example of something that cannot be virtualized is software that requires an attached piece of physical hardware, called a *dongle* or *hardware key*, in order to work properly. In addition, certain systems that require extreme I/O performance, like backup servers, or high-performance computing, like supercomputers, should not be virtualized.

Setting Up Virtualization on Windows 10

Hyper-V
A virtualization program that is part of Windows operating systems

Microsoft provides a virtualization program as part of Windows operating systems. In the personal computing realm, Windows 10 has the client **Hyper-V**, which uses the same virtualization technology on a Windows server. Hyper-V allows users to run more than one 32-bit or 64-bit operating system at the same time on the same computer by running them inside a virtual machine. The Hyper-V featured is not enabled by default.

The following steps show how to configure Hyper-V on a Windows 10 computer:

1. Go to Windows **Control Panel**, select **Programs**, and then select **Programs and Features**. Select **Turn Windows features on or off**. In the dialog that appears, select **Hyper-V** (see Figure 12-1). The computer needs to be restarted in order to enable Hyper-V in Windows 10.

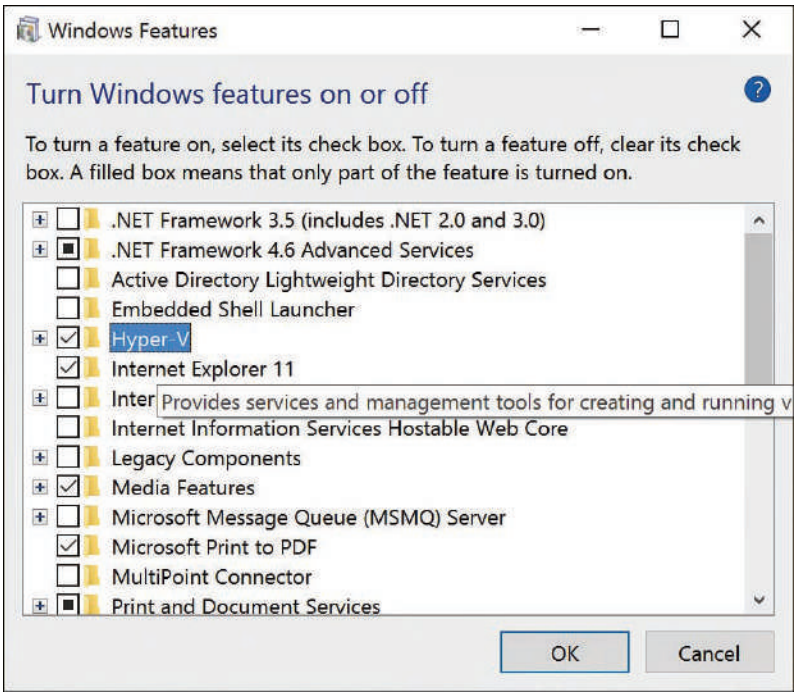


FIGURE 12-1 Enabling Hyper-V.

2. To control virtualization, select **Programs > Hyper-V Manager** or **Administrative Tools > Hyper-V Manager**. The window shown in Figure 12-2 appears.

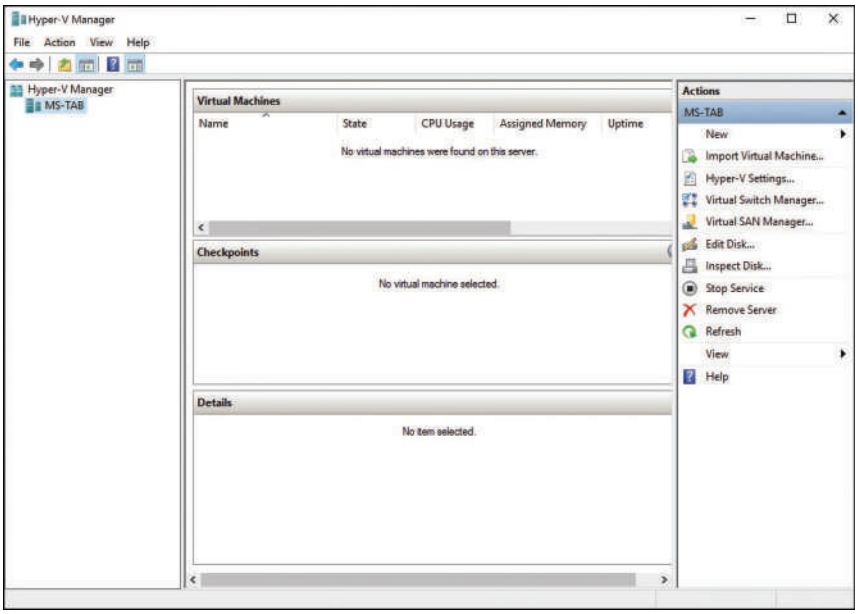


FIGURE 12-2 Using Hyper-V Manager.

3. Before creating any virtual machine, it is recommended that you create a virtual switch to prepare the network environment, so select **Virtual Switch Manager** from the Actions pane. The dialog shown in Figure 12-3 appears.
4. Select the type of virtual switch:
   - **External:** Allows the VM to access all resources available to the physical network, including the host machine and the Internet.
   - **Internal:** Allows the VM to communicate with the host machine only and not the Internet.
   - **Private:** Allows multiple VMs running at the same time to communicate with each other.

   Then click **Create Virtual Switch**.
5. Specify the name of the switch, as shown in Figure 12-4, and click **OK**.

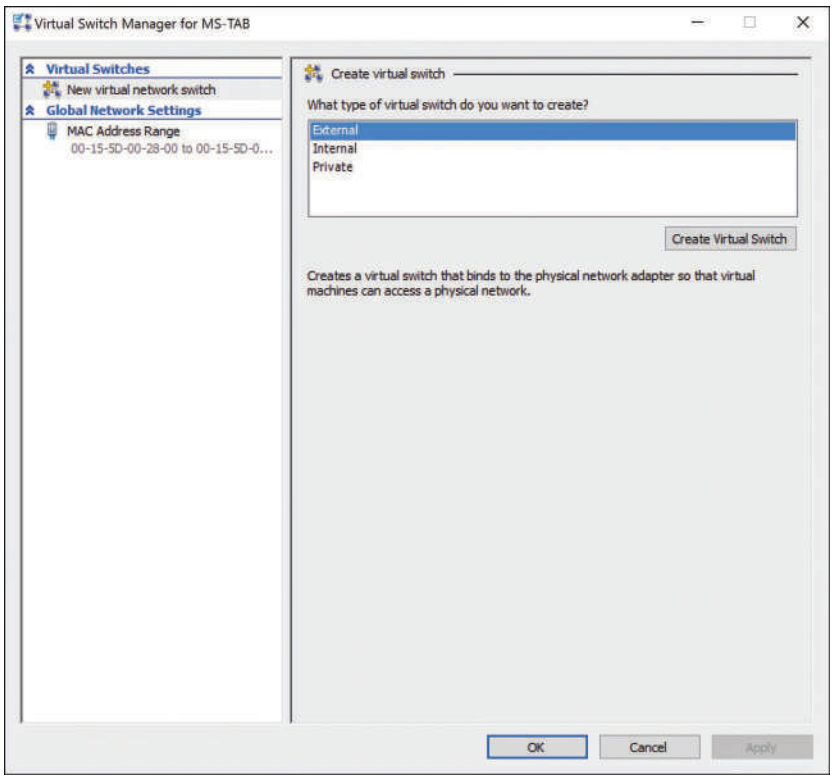


FIGURE 12-3 Creating a virtual switch in Hyper-V.

6. Back in the Hyper-V Manager screen, select **New > Virtual Machine** in the Actions pane to create a virtual machine (see Figure 12-5).

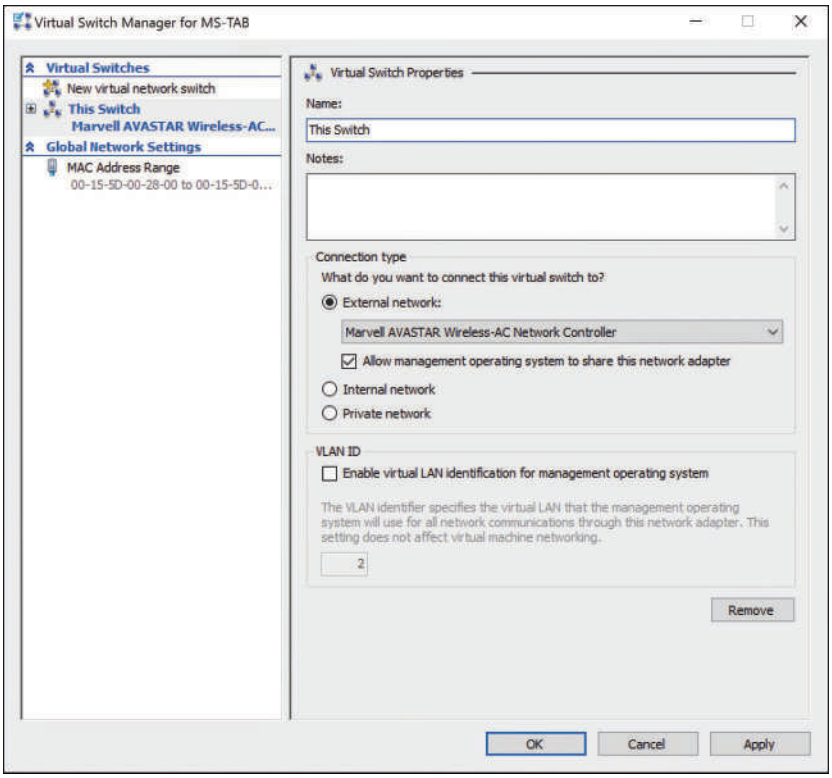


FIGURE 12-4 Specifying the name of a virtual switch.

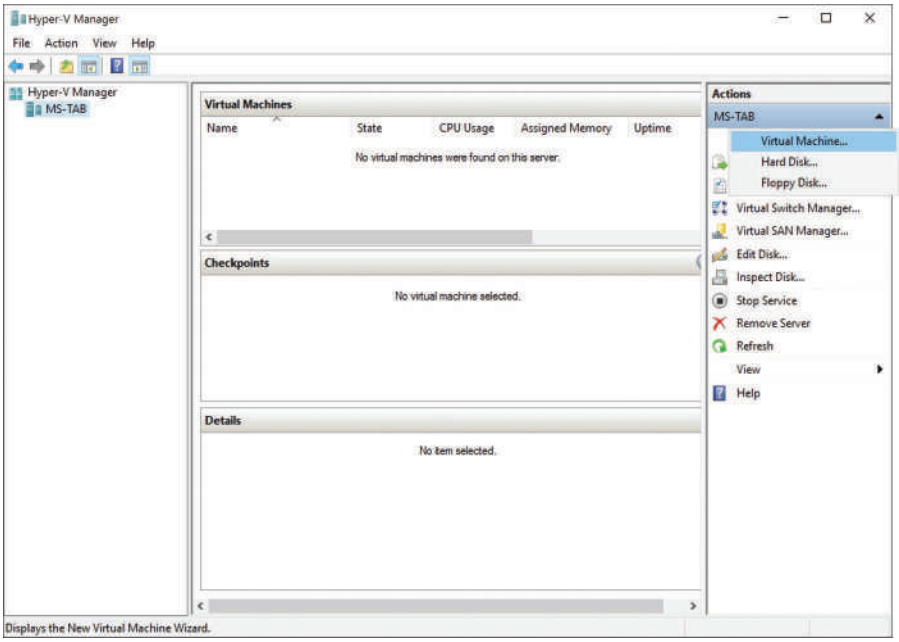


FIGURE 12-5 Creating a virtual machine.

7. Specify the name of the VM and a new installation location (or leave the default location set), as shown in Figure 12-6, and click **Next**.

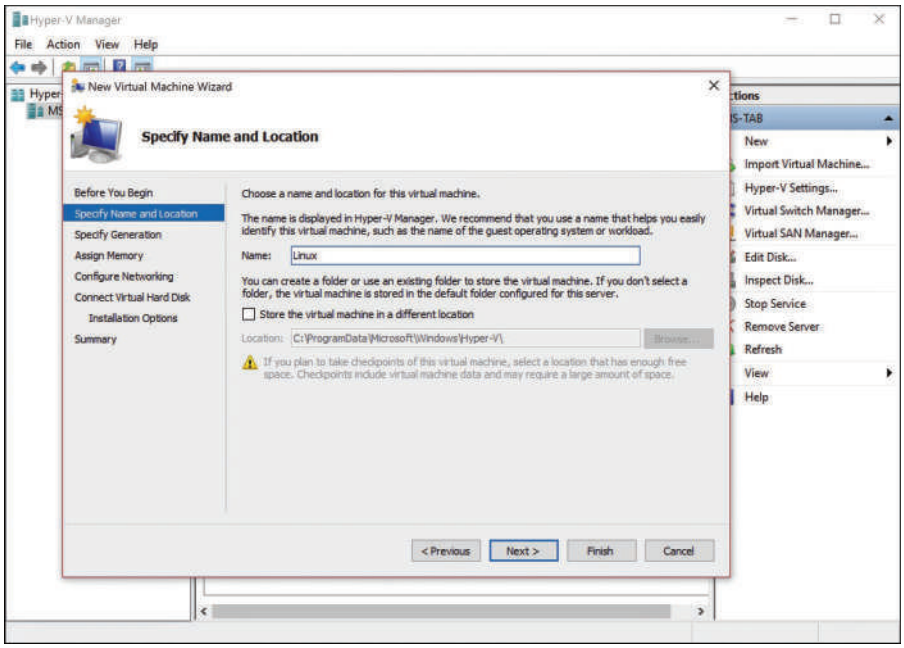


FIGURE 12-6 Specifying the name and location of a virtual machine.

8. Specify the generation of the virtual machine (see Figure 12-7):
   - **Generation 1:** This generation is backward compatible with older versions of Hyper-V and supports both 32-bit and 64-bit virtual machines
   - **Generation 2:** This generation only works with 64-bit virtual machines.

   Click **Next**.
9. In the Assign Memory screen, specify a desired memory size for the VM, as shown in Figure 12-8, and click **Next**.
10. In the Configure Networking screen, from the Connection drop-down, select the name of the virtual switch you created in step 5, as shown in Figure 12-9, and click **Next**. Microsoft creates a virtual network interface card (vNIC) for the VM.

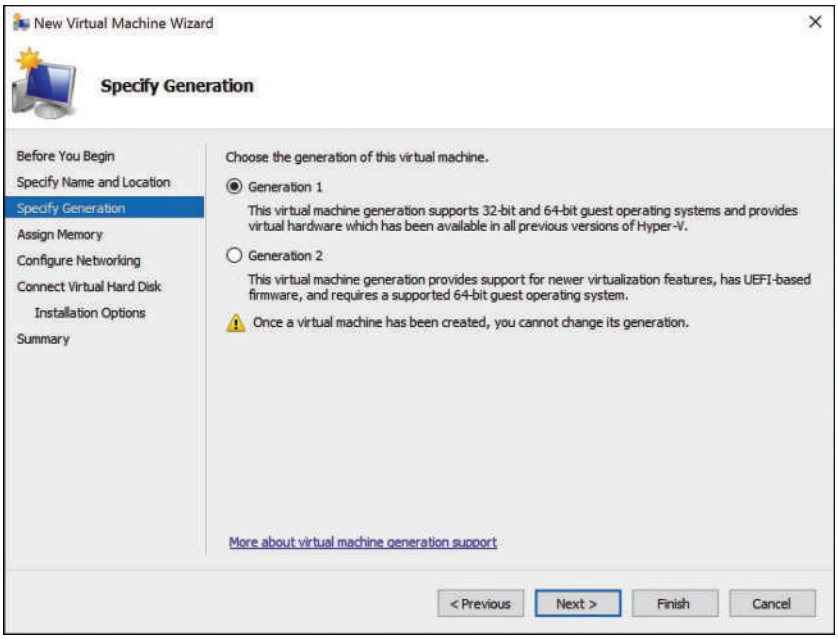


FIGURE 12-7 Specifying the generation of the virtual machine.

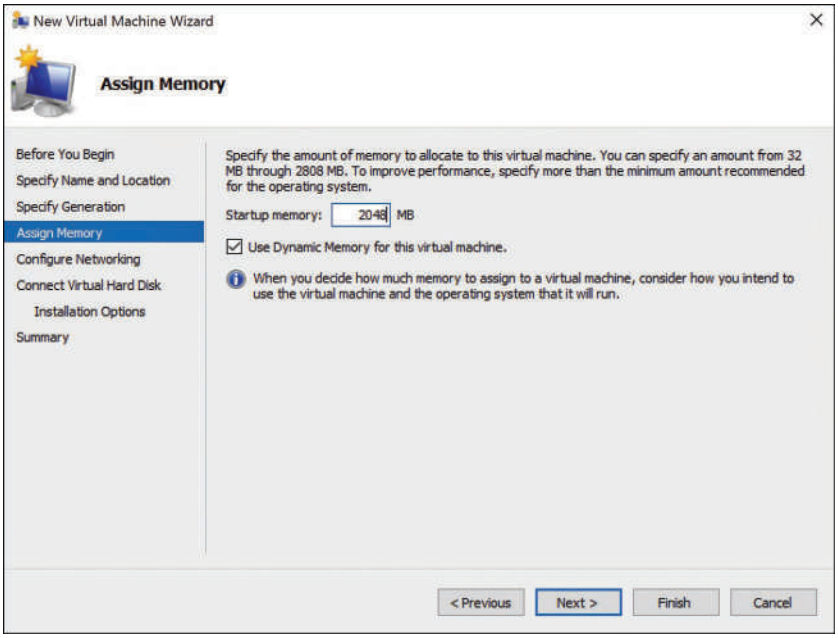


FIGURE 12-8 Specifying the desired memory size for a VM.

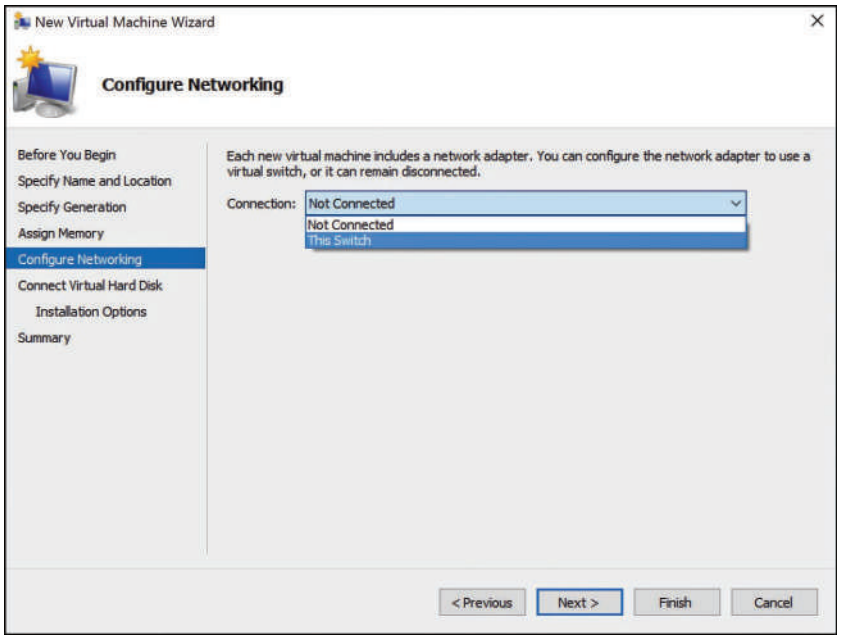


FIGURE 12-9 Selecting the connection name of the virtual switch.

11. In the Connect Virtual Hard Disk screen (see Figure 12-10), adjust the virtual hard disk name, location, and size as necessary and click **Next**.

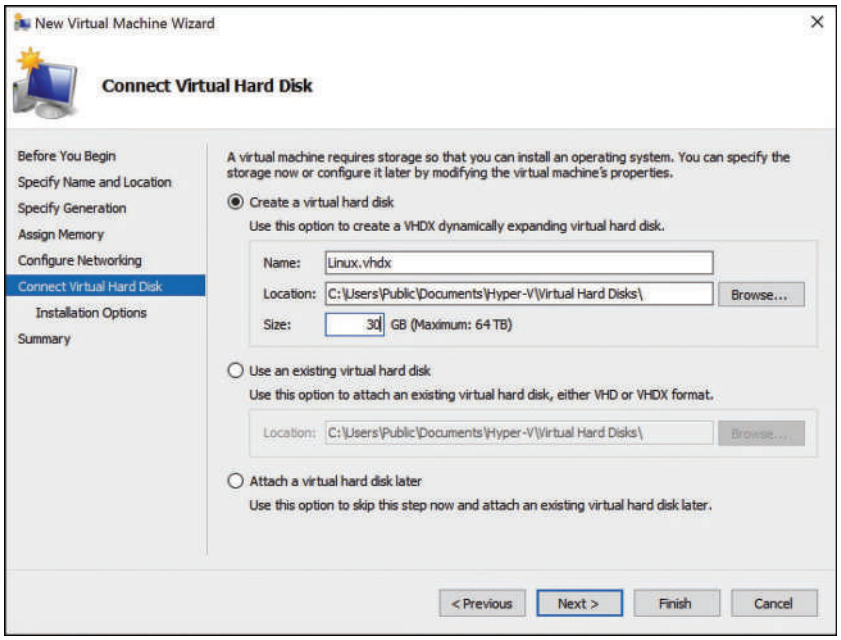


FIGURE 12-10 Specifying a virtual hard disk name, location, and size.

12. In the Installation Options screen, shown in Figure 12-11, select how to install the VM's operating system (from physical media like a CD/DVD, a virtual bootable floppy disk, an image file like an .iso, or a network server). Then click **Next**.
13. Look at the summary of the new VM and click **Finish**.
14. In the Hyper-V Manager that again appears (see Figure 12-12), select **Start** under the VM name from the Actions pane or right-click the VM and select **Connect**.

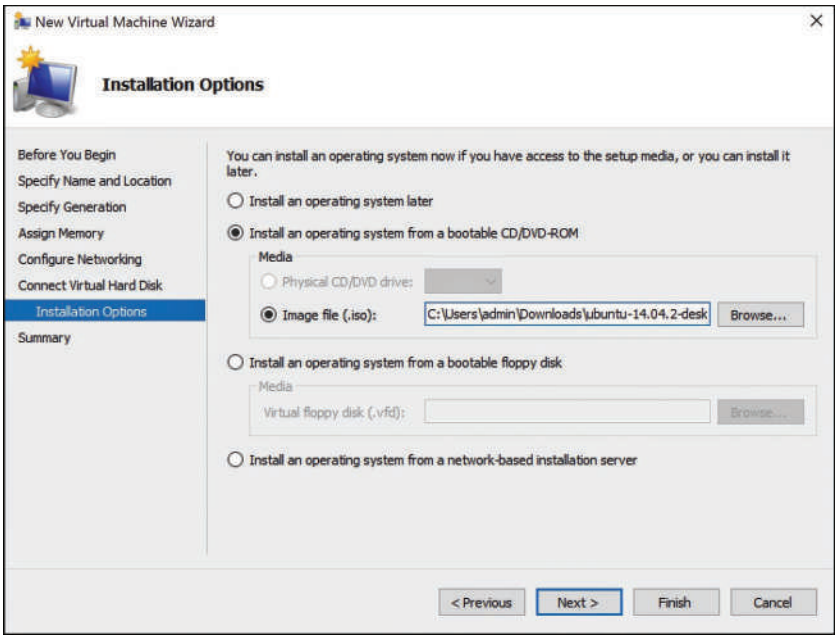


FIGURE 12-11 The options for installing the VM's operating system.

The virtual machine connection shows up, and the usual installation of the operating system can proceed (see Figure 12-13). When it is done, the full-fledged running VM with operating system is ready for use.

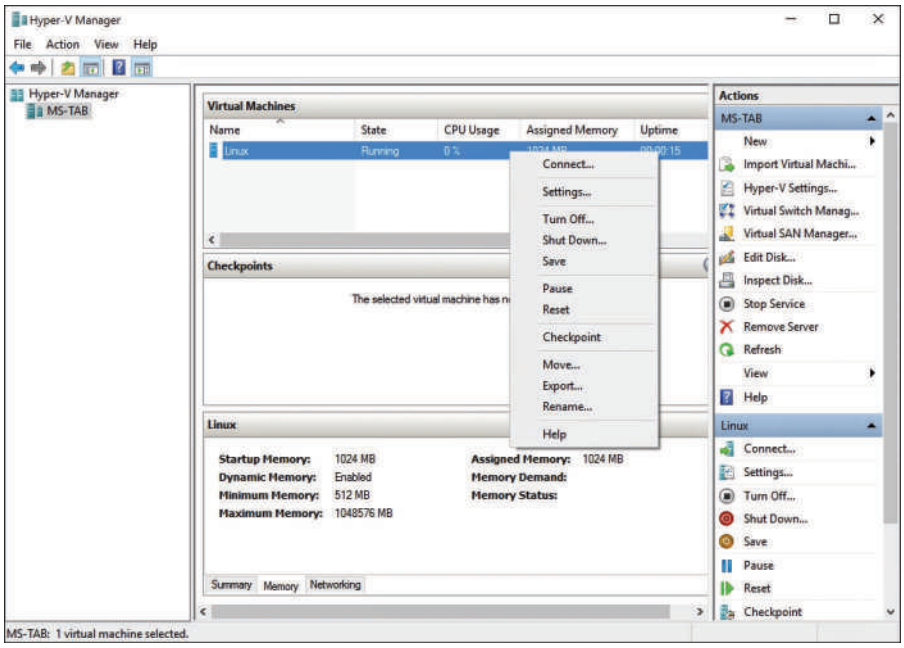


FIGURE 12-12 Starting the new VM.

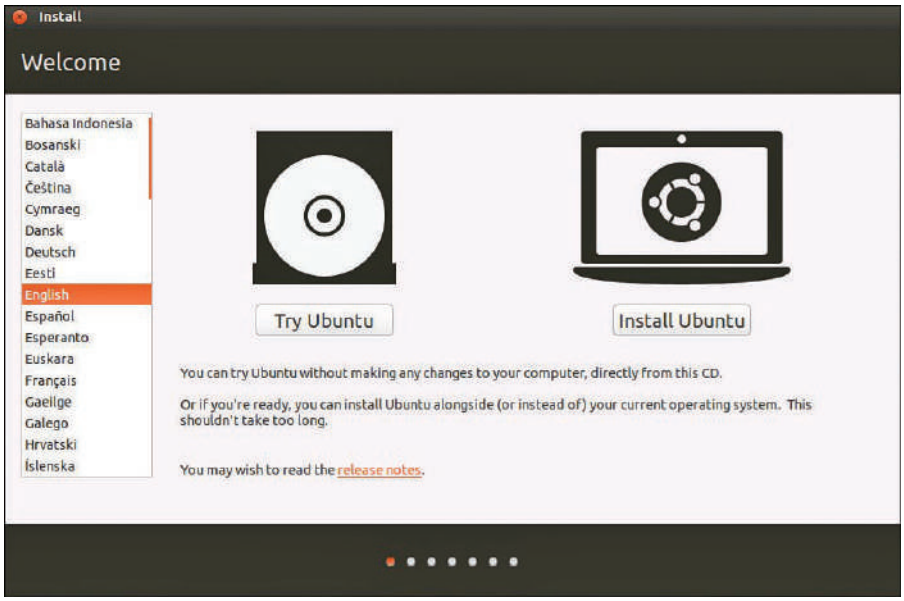


FIGURE 12-13 The final VM screen, showing that the machine is up.

Section 12-2 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.
This section discusses the creation of a virtual network interface card (vNIC) for a VM.

1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
This section states that a virtual IP (VIP) address is an IP address created to be shared by a group of network devices.

1.6 Explain the use and purpose of network services.
This section mentions that certain systems that require extreme I/O performance, like backup servers, or high-performance computing, like supercomputers, should not be virtualized.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.
This section states that the development of microprocessor technology has seen incredible growth. A single-CPU architecture has evolved to a single CPU with multiple cores.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.
This section states that a virtual computer can contain but is not limited to a virtual CPU, virtual operating system, virtual storage, virtual network card, virtual firewall, virtual router, or virtual NIC.

Test Your Knowledge

1. What is Live Migration?
   a. The unofficial term for moving to the cloud
   b. Microsoft's option for moving a designated host server in the event of a physical server failure
   c. A secure protocol for transferring files to the cloud
   d. An option for installing a VM's operating system from an image file
2. What is Hyper-V?
   a. A virtualization program provided by Microsoft
   b. The name for cloud virtual services
   c. A virtualization program developed by Apple
   d. A fast CPU technology designed by AMD

12-3 CLOUD COMPUTING

Make sure students understand that working in the cloud basically means working on the Internet or on an intranet. This section explores services related to the cloud and some of the technical issues required to make data flow to the cloud.

The word *cloud* is such a nontechnical term that when it represents a technology, it sounds vague and nebulous. Cloud computing has been one of the most talked-about technologies in recent years. The term has been thrown around a lot by IT people and users alike ("People can connect to the cloud," "my stuff is stored on the cloud," "I migrate everything to the cloud"). The cloud is magically in the middle of everything. Yet people still don't know what and where the cloud really is. Its famous existence has contributed to many punch lines and created many questions. The bottom line is that **cloud** is just another name for Internet-based services. The National Institute of Standards and Technology (NIST) has provided the following technical and official definition:

Cloud
Another name for the Internet

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

To better understand what the cloud really is, perhaps we should explore outsourcing. **Outsourcing** means obtaining goods or services from an outside source rather than an internal source. When a company outsources a service, it means that someone outside the company has been hired to perform that work or service. In the computing world, if you outsource your IBM mainframe administration to company A, then company A will be responsible for having someone either remotely or locally manage your IBM mainframe system, which is housed on your premises.

Outsourcing
Obtaining goods or services from an outside source rather than an internal source

A cloud service is referred to an *outsourced service*, but the service is not hosted on the local premises, and it does not run on on-premises hardware. With cloud computing, a cloud company is responsible for providing users with a service, and the service can be hosted on the cloud company's hardware and software, which can be anywhere on the Internet.

Cloud service/cloud computing is an outsourced and hosted computing environment that delivers IT services to users via a network. It adds the hosting element to outsourcing. This hosting element typically contains features such as self-service, automation, and application catalogs. This means end users can manage the service directly, or the administrators of the organization that uses the cloud can provision services for users. Two cloud-based services that have been around for some time are email hosting and web hosting.

Cloud Service/Cloud Computing
An outsourced and hosted computing environment that delivers IT services to users via a network

These hosting services have been quite popular because typical users do not want to run their own email servers or web servers. It is much more economical and convenient for them to subscribe to these services. For example, cloud-based email service is offered for free to the public; Google offers gmail.com email accounts, Microsoft offers outlook.com email accounts, Yahoo offers yahoo.com email

accounts, and Apple offers me.com and icloud.com email accounts. Any user can simply create an email account with such a service, and as long as the email username is not being occupied, the user can have it. Even though web-hosting services are typically not offered for free, they have become popular for small business and personal websites. For a small monthly fee, you can run a website with a design chosen from available templates. These services often offer users add-ons like database, shopping cart, or picture gallery options.

Cloud-based services are now being offered to enterprise-level organizations for a subscription price. Consider an email service, for example; instead of maintaining its own email system, a company can offload its email operations to a cloud service provider. And it is very likely to do so because running an enterprise email service involves much more than bringing up a couple of email servers. Many details have to be thought through, from design to implementation to procurement.

If a company handles its email inhouse, email administrators and server administrators need to work together to procure the servers. The size and number of the servers depend on the number of users and their mailbox sizes. In addition, the potential growth of the system must be considered. Because email is critical to every organization, the email system must be designed for high availability as well as high performance and throughput. Typically, this means multiple servers spread throughout multiple data centers. Then, the underlying infrastructure—including the network and storage—has to be considered so that the system can provide the availability that an email system needs. After the system is implemented, support and maintenance are required; someone has to maintain the system; software and the operating system have to be patched and updated.

Cloud email service providers can assume all the roles and responsibilities just described. They use virtualization technology to create a virtual email system for an organization of any size. The email system can live anywhere among many data centers that are dispersed throughout a continent (or many continents for big providers). The cloud service provider is responsible for maintaining the email system, from updating to applying patches. If the system needs more memory or is running out of disk space, the cloud service provider can perform those upgrades. All this is written into the service-level agreement (**SLA**) that the organization has with the cloud service provider.

An important technical point must be mentioned here: Email does not magically flow to the cloud without being directed that way. The DNS resource **MX (Mail Exchange) record** points to the incoming email servers of the organization. The MX record must be changed to the cloud email servers so that all email can be directed to the cloud servers. Manipulating DNS records is a technique often used to direct traffic to the cloud. An organization's website can be hosted in the cloud or cloud site just by changing the DNS A record to the IP address of the cloud server or creating a DNS **CNAME (Canonical Name) record** that points to the cloud server hostname.

Many organizations have responded to cloud computing in a positive way. Many of their services—including critical services like web, email, and enterprise resource planning (ERP)—have been migrated to the cloud. The cloud market is doing well and has captured the attention of many businesses due to its many advantages.

SLA
Service-level agreement, a formal agreement typically between a service provider and a client or an end user, that defines the level of service expected from the service provider

MX (Mail Exchange) Record
The Mail Exchange record, which points to the incoming email servers of an organization

CNAME (Canonical Name) Record
The Canonical Name record, used to specify that a domain name is an alias for another domain

From an economic standpoint, cloud computing is a cost-effective solution. It helps reduce capital costs, technology infrastructure cost, and personnel costs.

Cloud computing has struck a chord with new businesses and small companies, as they do not have to commit excess financial resources on server hardware, software, storage, network equipment, and a data center, and they do not need to hire many knowledgeable workers to manage and maintain the systems. From an operational standpoint, cloud computing helps improve efficiency in system management and maintenance, improve availability, create disaster recovery, and increase accessibility. This relieves the company's IT department of duties related to maintaining the systems and keeping them up-to-date, freeing up IT to spend time on other IT initiatives. With virtualization and dispersed data centers, systems are up and available to users, who are guaranteed to have access to the systems as long as they have Internet access. Every organization, big or small, needs to evaluate a cloud service at some point and decide whether a particular service would be better managed and provided from the cloud or locally.

Cloud Computing Service Models

Cloud computing can be broken down to four major service models:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)
- Desktop as a service (DaaS)

Infrastructure as a Service (IaaS)
A service that focuses on the facilities and infrastructure in the data center and the virtualization and abstraction layer that exists on top of the physical facilities and infrastructure

Infrastructure as a Service (IaaS) Data centers are fundamental parts of most IT infrastructure. Traditionally, companies owned and ran servers in their data center on-premises. To expand their data centers offsite or for disaster recovery purposes, many companies used collocation, with their servers hosted in a shared facility run and operated by a third party. (Note that the function of a data center differs from the function a collocation facility, where a business can rent server space and sometimes other computer and network hardware.) **Infrastructure as a service (IaaS)** goes further, virtualizing the facilities and infrastructure in the data center and the abstraction layer that exists on top of the physical facilities and infrastructure.

IaaS allows for more effective sharing of the underlying physical resources. It encompasses the computing power of servers, storage, network elements, power, and cooling—instead of running servers in the company's data center. It allows an organization to create virtualized servers in the cloud or to virtualize its servers and move its server systems and data center infrastructure to the cloud. This option helps eliminate or reduce the footprint of the on-premises data center. This category of cloud computing is the fundamental and underlying layer of other cloud categories. With on-demand provisioning of different resources in IaaS, infrastructure as code (IaC) has been used to manage or provision this type of cloud IT infrastructure. IaC is a software model that provides the infrastructure configuration and its needed resources in code, configuration files, or templates. The infrastructure

can be efficiently deployed and its resources can be provisioned via the IaC method. Some examples of IaaS are Amazon Web Services (AWS), Microsoft Azure, and Google Compute Engine.

Platform as a Service (PaaS) **Platform as a service (PaaS)** focuses on application development on any desired platform using cloud computing. It incorporates platform elements such as operating systems, databases, programming languages, and middleware installed on top of the abstracted infrastructure. PaaS allows developers to design, test, and implement software on the same platform that their clients will use in a quick, simple, and cost-effective manner. This category of cloud computing service is popular among software developers for web applications and mobile applications as it allows them to frequently change or upgrade platform elements and helps them collaborate on projects. Some examples of PaaS are Google App Engine, Heroku, and Salesforce.

Platform as a Service (PaaS)
A service that focuses on application development on any desired platform utilizing cloud computing

Software as a Service (SaaS) **Software as a service (SaaS)** focuses on application delivery. It provides the applications that run on top of a platform and the abstracted infrastructure, delivered via the Internet. Most SaaS applications can be run directly from a web browser, although some require plug-ins to be installed. Because SaaS eliminates the need to install and run applications on individual computers, it is easy for organizations to streamline their product delivery, maintenance, and support. This category of cloud computing is the most widely used. Email and collaboration tools are among the popular SaaS applications. Some examples of SaaS are Microsoft Office 365, Google Apps, Cisco Webex, and Citrix GoToMeeting.

Software as a Service (SaaS)
A service that focuses on application delivery

Desktop as a Service (DaaS) Recently, another cloud-based service that has gained big momentum is **desktop as a service (DaaS)**. DaaS is based on virtual desktop infrastructure (VDI), which provides a standard way for many organizations to deliver virtual desktops to users from their data center servers. DaaS is a desktop virtualization service hosted by a cloud provider. The provider manages back-end resources such as the desktop operating system, storage CPU, and network. Virtual desktops are delivered to end users over the Internet.

Desktop as a Service (DaaS)
A desktop virtualization service hosted by a cloud provider

Note

Virtual desktop is not to be confused with remote desktop. Virtual desktop uses virtualization to deliver a dedicated virtual host to an end user. Remote desktop, on the other hand, provides a remote desktop connection for an end user to connect to a host computer and to run the host computer remotely. Remote desktop is a popular feature with Windows. Windows uses Remote Desktop Protocol (RDP) to allow users to connect to desktops and servers. Also, a Windows server can be configured as a remote desktop gateway to manage and provide RDP services to connect remote computers.

Advantages of Cloud Computing Service Models Cloud computing service models provide three important benefits:

- **Scalability:** Scalable system infrastructure is designed to accommodate larger workloads while retaining consistent performance. This can be accomplished via vertical scaling (or scaling up), which involves adding more resources

Scalability
The ability of a system to expand the number of users and authentication

Elasticity
The ability of a cloud provider to dynamically grow or shrink the cloud resources to adapt to or match the workloads

Multitenancy
The ability of multiple users to share the same cloud provider resources

such as CPU and memory to the existing infrastructure, or via horizontal scaling (or scaling out), which involves expanding the existing infrastructure with additional new nodes, such as VMs.

- **Elasticity:** A cloud provider can dynamically grow or shrink cloud resources to adapt to or match the workloads.
- **Multitenancy:** Multiple users can share the cloud resources of a cloud provider.

Cloud Infrastructures

IaaS, PaaS, and SaaS use different types of cloud infrastructures. These infrastructures offer different levels of security, resource restrictions, and management. These are the most notable cloud models:

- **Public cloud:** This cloud infrastructure is owned and operated by the cloud service company and made available for general public use.
- **Private cloud:** This cloud infrastructure is operated by an organization and made available only to members of that organization.
- **Community cloud:** This cloud infrastructure offers two or more organizations exclusive access to the infrastructure and computing resources. These organizations may share common policies that allow them to operate in a distributed mode.
- **Hybrid cloud:** This cloud infrastructure offers a combination of at least one private cloud and one public cloud.

Cloud services have caught on because they make service provision extremely effective. Cloud provisioning is often more effective than the current provisioning process in most organizations. For example, bringing up a database server in an organization would traditionally involve many IT groups—perhaps a database administration (DBA) group, a storage group, a server administrator group, and a network group. It takes a considerable amount of effort to bring up a server, including the operating system and the database. The database server then needs to be on the assigned VLAN with the right firewall rules. This whole process might take up to a week in normal operations A cloud service provider (CSP) can accomplish the same process in moments and can serve thousands of clients.

Automation and integration are integral to cloud service provision. Cloud service providers use virtualization automation software to provision a server with specific requirement sets, carve out storage space, automate the database installation, and set up the network connectivity according to needed TCP/IP protocols and bandwidth requirement. All this happens behind the scenes, transparently to users. This automation has been driven by software-defined technologies, which involve using software to control the functions of a system by using virtualization to abstract and automate the workloads or resources. The most talked-about software defined technology is software-defined networking (SDN), which allows a network to be

programmable and provide automated and on-demand delivery of the network-level infrastructure. In the nutshell, SDN consists of three different layers:

- **Application layer:** This is a software program that communicates with the control layer.
- **Control layer:** Controllers interact with both the application layer and infrastructure layer.
- **Infrastructure layer:** This layer consists of network devices such as switches, wireless access points, and routers.

With SDN, the industry is moving toward separating the data plane, which forwards and carries user data traffic, from the control (or management) plane, which performs administration, management, and access control functions. With this separation, these two planes do not share the same process or even the same CPU in many cases. Configuration changes to network devices can be orchestrated and deployed from the central control/management plane. SDN uses automation software to perform a network task or function. SDN then uses orchestration to automate many arranged tasks to complete a process or a workflow.

Software-defined wide area networking (SD-WAN) is another software-defined technology in networking. It is similar to SDN but focuses on providing connectivity for geographically dispersed locations in a scalable and secure way. Another technology is Stratum, which is an open-source switch operating system for software-defined networks.

Integrating systems and data with cloud service providers is not without negatives. Importantly, cloud computing has many inherent security implications. An organization and its cloud providers must take responsibility for different elements of security. Their responsibilities depend on the scope of cloud services provided and the agreements between them. Each party's responsibilities should be defined clearly in an SLA. Also, if an organization must comply with regulations such as the Gramm-Leach-Bliley Act (GLBA) or the Payment Card Industry Data Security Standard (PCI DSS), the cloud providers must be compliant as well. Both GLBA and PCI DSS are discussed in Chapter 13, "Codes and Standards."

Section 12-3 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.
As discussed in this section, a hybrid cloud is a cloud infrastructure that offers a combination of at least one private cloud and one public cloud.

1.6 Explain the use and purpose of network services.
This section states that an organization and its cloud providers must take responsibility for different elements of security. Their responsibilities depend on the scope of cloud services provided and the agreements between them.

1.7 Explain basic corporate and datacenter network architecture.
This section discusses software-defined networking (SDN), which allows a network to be programmable and provides automated and on-demand delivery of the network-level infrastructure.

1.8 Summarize cloud concepts and connectivity options.
This section discusses software as a service (SaaS).

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.
This section discusses facilities and infrastructure support.

4.3 Given a scenario, apply network hardening techniques.
As discussed in this section, a database server needs to be on an assigned VLAN with the right firewall rules.

Test Your Knowledge

1. What is the cloud?

   The cloud is basically the Internet. NIST provides a more detailed definition: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

2. What is a cloud service?

   a. A service that is not available commercially
   b. A combination of intermixing Apple and Microsoft applications
   c. An outsourced and hosted computing environment that delivers IT services to users via a network
   d. A Storage as a Service (SaaS)

12-4 ENTERPRISE STORAGE

This chapter has discussed the computing resources of CPUs and RAM in virtualization and in cloud computing. However, it has not yet mentioned the most common—and possibly most important—component for the typical user: storage. The terms *disk*, *disk drive*, *hard drive*, *drive space*, and *storage space* all refer to a common computer component used to store and retrieve data. Most people are familiar with hard disk drives (HDDs) and USB flash drives. These are individual physical storage drives with fixed capacity.

The enterprise environment no longer just deals with data inside individual computer hard drives. It now deals with central repository storage systems that

house huge amounts of business information, critical data, company databases, and all sorts of digital information. Storage is a critical IT infrastructure. An enterprise storage system is built for business continuity, with redundancy and backup, as well as for performance and scalability. A storage area network (**SAN**) is a typical enterprise storage solution. It is not a typical file server with a lot of disk drives or disk arrays. A SAN is block-level data storage located across a network.

SAN
Storage area network, block-level data storage located across a network

Another example of block-level data storage is a hard drive. A SAN behaves just like a bunch of hard drives or disk arrays on a network, which servers and devices can access as though the SAN were locally attached disk space. A SAN consolidates multiple disk arrays together and uses LUNs (logical unit numbers) to reference different sets of specific storage in a SAN. Dedicated LUNs are then assigned to servers as if they were locally attached disk space. A SAN is typically deployed on its own dedicated network and requires a lot of bandwidth and speed to move data between the storage arrays. The following are some widely deployed storage technologies used in a SAN:

- **Fibre Channel (FC):** This is the original high-speed technology used to connect data storage to servers. As the name implies, the technology uses fiber-optic cables to connect the storage devices into a Fibre Channel network. Every participating device has its own Fibre Channel interface. There may be a Fibre Channel switch connecting these devices in a large deployment. The latest Fibre Channel generation, generation 7, which was introduced in late 2018, can deliver 64Gbps and 256Gbps (4 lanes of 64Gbps) throughput.

Fibre Channel (FC)
The original high-speed technology used to connect data storage to servers

- **InfiniBand (IB):** This technology provides high performance and high throughput with low latency, which makes it a leading technology in interconnecting supercomputers. Much like Fibre Channel, InfiniBand uses its own proprietary interface for connecting devices and storage. The InfiniBand data rate called EDR (Extended Data Rate) was introduced in 2014 and is capable of providing a data rate of 100Gbps. A 2017 data rate addition to InfiniBand is HDR (High Data Rate), which has the fastest storage interface, with a speed of 200Gbps.

InfiniBand (IB)
A technology that provides high performance and high throughput with low latency

- **Fibre Channel over Ethernet (FCoE):** This technology encapsulates Fibre Channel packets and sends them over a 10Gbps or higher Ethernet LAN. The advantage of this technology is that there is no need for a specialized Fibre Channel interface. Fibre Channel can communicate via a 10Gbps NIC. The maximum Fibre Channel frame size is 2148 bytes, which is bigger than the standard Ethernet maximum transmission unit (MTU) size of 1500 bytes. In order to pass the Fibre Channel frames without breaking them down, it is recommended to enable the jumbo frame function on the switch ports. A jumbo frame size can be up to 9216 bytes and is supported by most Gigabit Ethernet switches.
- **Internet Small Computer Systems Interface (iSCSI):** This technology enables the SCSI protocol (which has been around a long time for connecting computers with SCSI devices) to communicate over IP networks. The iSCSI protocol uses TCP ports 860 and 3260. Its speed varies depending on the network.

iSCSI
Internet Small Computer Systems Interface, a technology that enables the SCSI protocol to communicate over IP networks

NAS
Network attached storage, a file-level storage device that can be accessed on a network

Another type of storage that has gained popularity and is much cheaper to deploy than a SAN is network attached storage (**NAS**). Unlike a SAN, a NAS is not a block-level data storage device; it is a file-level storage device that can be accessed on a network. A NAS device has its own Ethernet connection and IP address. A NAS can share its files with multiple clients on a network. Computers can connect to a NAS via protocols like SFTP, SMB, NFS, or AFP. Connecting to a NAS is sometimes referred to as "mapping a network drive."

Section 12-4 Review

This section covers the following Network+ exam objectives.

1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
This section mentions that the maximum Fibre Channel frame size is 2148 bytes, which is bigger than the standard Ethernet MTU size of 1500 bytes.

1.2 Explain the characteristics of network topologies and network types.
This section mentions that a SAN (storage area network) is block-level data storage located across a network.

1.7 Explain basic corporate and datacenter network architecture.
This section examines Fibre Channel (FC), the original high-speed technology used to connect data storage to servers.

1.8 Summarize cloud concepts and connectivity options
This section mentions that an enterprise storage system is built for business continuity, with redundancy and backup, as well as for performance and scalability.

Test Your Knowledge

1. What is a NAS?
   a. Block-level data storage
   b. A file-level storage device that can be accessed on a network
   c. Tape storage with a hard-drive backup
   d. A storage area network
2. Which of the following are true of Fibre Channel over Ethernet (FCoE)? (Select all that apply.)
   a. It is recommended to enable the jumbo frame function on switch ports.
   b. It has the fastest storage interface, with a speed of 56Gbps.
   c. It encapsulates packets and sends them over a 10Gbps or higher Ethernet LAN.
   d. It is a leading technology for interconnecting supercomputers.

SUMMARY

This chapter introduces the basic concepts of cloud computing and virtualization. It also introduces the concept of cloud services and setting up a virtual environment. It also covers enterprise storage systems built for business continuity, with redundancy and backup, as well as for performance and scalability. You should understand the following concepts:

- The terms cloud, cloud computing, and cloud services
- The evolution of computing devices
- The concept of virtualization
- The purpose of a hypervisor and the two types of hypervisors
- The process of setting up virtualization on a Windows computer
- The purpose of a service-level agreement
- The three major categories of cloud computing

QUESTIONS AND PROBLEMS

Section 12-2

1. What is the core relative to a computer?

   The core is an independent processing unit, which is responsible for reading and executing program instructions.

2. What is a cache relative to a computer?

   It is a block of memory set aside for temporary storage of information.

3. Why is a 64-bit architecture an improvement with computer processing? List three reasons.

   It can compute twice as many bits in one clock cycle.

   It increases the maximum supported RAM.

   It can run more programs and support more users at the same time.

4. What is virtualization?

   Virtualization is a technology concept that involves creating a virtual computer.

5. What is the purpose of a hypervisor?

   It is used for managing and controlling the underlying physical hardware and the associated virtual hardware.

6. What is a Type 1 hypervisor?

   This type of hypervisor is loaded directly on the hardware to abstract the hardware to the virtualization layer and is commonly used on servers.

7. What is a Type 2 hypervisor?

   This type of hypervisor is loaded on an operating system and abstracts the virtualization layer through its host operating system and is commonly used on personal computers.

8. How has virtualization helped companies?

   It has brought a more cost-effective way to provide server management and maintenance. Instead of buying different servers for different services, an organization can buy only one server. For example, a server with two 18-core processors, 24 units of 32GB RAM, and four 6TB hard drives will yield the computing resources of 36 processors, 768GB of RAM, and 24TB of storage space. An additional benefit of virtualization is that it reduces the physical footprint of servers.

9. How has virtualization helped the personal computing world?

   A user can run virtual machines of various Windows operating systems as well as Linux at the same time.

10. What limitation is there for creating a macOS virtual machine?

    Apple licensing restrictions

Section 12-3

11. What is cloud computing?

    An outsourced and hosted computing environment that delivers IT services to users via a network.

12. What does it mean to outsource services?

    It means that goods or services are obtained from an outside source rather than from an internal source.

13. What is required to make email flow properly to the cloud?

    The MX record must be changed to the cloud email server.

14. What is an SLA?

    An SLA (service-level agreement) is an agreement made with a provider such as a cloud service provider that describes various roles and responsibilities.

15. With virtualization and dispersed data centers, systems will be up and available to users as long as they have what?

    a. Server access
    b. Software access
    c. Internet access
    d. macOS installed

16. Which of the following is true of infrastructure as a service (IaaS)?

    a. It focuses on software external to the data center that exists on top of the software infrastructure.

    b. It focuses on the facilities and infrastructure within the data center and the virtualization and abstraction layer that exists on top of the physical facilities and infrastructure.

    c. It focuses on the hardware external to the data center that exists under the software infrastructure.

    d. It focuses on the facilities external to the data center that exist on top of the software infrastructure.

17. Which of the following is true of platform as a service (PaaS)?

    a. It focuses on the facilities and infrastructure within the data center and the virtualization and abstraction layer that exists on top of the physical facilities and infrastructure.

    b. It focuses on application development on any desired platform utilizing cloud computing.

    c. It focuses on application delivery.

    d. It focuses on software external to the data center that exists on top of the software infrastructure.

18. Which of the following is true of software as a service (SaaS)?

    a. It focuses on application delivery.

    b. It focuses on the software external to the data center that exists on top of the software infrastructure.

    c. It focuses on the virtual network component and delivery.

    d. It focuses on application development and storage.

Section 12-4

19. What is a SAN?

    SAN, which stands for storage area network, it is block-level data storage located across the network.

20. What is the purpose of a LUN?

    Dedicated logical unit numbers (LUNs) are assigned to servers as if they were locally attached disk space to the servers.

21. What is Fibre Channel (FC)?

    Fibre Channel (FC) is the original high-speed technology used to connect data storage to servers. The technology uses fiber-optic cable to connect storage devices to create a Fibre Channel network. Every participating device has its own Fibre Channel interface.

22. What is InfiniBand (IB)?

    This technology provides high performance and high throughput with low latency, which makes it a leading technology in interconnecting supercomputers. It has the fastest storage interface, with speed of 200Gbps.

23. What is Fibre Channel over Ethernet (FCoE)?

    This technology encapsulates Fibre Channel packets and sends them over a 10Gbps or higher Ethernet LAN. The maximum Fibre Channel frame size is 2148 bytes, so it is recommended to enable the jumbo frame function on the switch ports.

24. What is Internet Small Computer Systems Interface (iSCSI)? What TCP ports does it use?

    This technology enables the SCSI protocol to communicate over IP networks. iSCSI uses TCP ports 860 and 3260.

25. What is a NAS?

    A NAS (network attached storage) is a file-level storage device that can be accessed on a network.

Certification Questions

26. Why is it not recommended to install macOS in a virtual environment?

    a. macOS requires more CPU resources.
    b. Apple has strict licensing restrictions.
    c. It is not possible to use macOS in a virtual environment.
    d. It is not possible to virtualize macOS without a Hyper-V key.

27. A virtual machine is created with 8GB of RAM and 100GB of hard drive space. Which operating system can maximize all of its hardware abstraction potential? (Select all that apply.)

    a. Red Hat Enterprise Linux 64-bit
    b. Windows 10 64-bit
    c. Windows 7 32-bit
    d. Windows XP

28. A physical host machine has four quad-core CPUs, 16GB of RAM, 1TB of hard drive space, and two 1Gbps NICs. If you need to create four Windows 2019 servers, what is the first bottleneck that you should upgrade?

    a. CPU
    b. RAM
    c. Hard drive
    d. NIC

29. Which of the following are Type 1 hypervisors? (Select all that apply.)

    a. VMware ESXi
    b. VMware Workstation
    c. Parallels
    d. Virtual Box
    e. Hyper-V

30. In what situations should you run a Type 2 hypervisor? (Select all that apply.)

    a. When running on a Windows 2019 server
    b. When running on Mac hardware
    c. When running on a computer with CPU and BIOS that supports virtualization
    d. When running on a laptop

13
CHAPTER

Codes and Standards

Chapter Outline

13-1 Introduction
13-2 Safety Standards and Codes
13-3 Industry Regulatory Compliance
13-4 Business Policies, Procedures, and Other Best Practices
13-5 Business Continuity and Disaster Recovery
Summary
Questions and Problems

Objectives

- Explain the safety standards and codes related to IT
- Define the requirement for an organization to have an emergency action plan
- Provide an overview of fire extinguishing systems used to protect critical data-processing equipment
- Describe regulations that can pertain to an IT organization
- Define the business policies and procedures an organization might have to comply with or utilize in the daily management of a data center

Key Terms

OSH Act
OSHA
NFPA
CFR
EAP
FPP
SDS
MSDS
HVAC
biometric system
FERPA
FISMA
GDPR
GLBA
HIPAA
PCI DSS
MOU
SLA
MSA
MLA
NDA
SOW
AUP
onboarding
offboarding
MTBF (mean time between failures)
MTTF (mean time to failure)
MTTR (mean time to recover or repair)
high availability (HA)
First Hop Redundancy Protocol (FHRP)
power distribution unit (PDU)
active/active
active/passive
hot site
cold site
warm site
cloud site
recovery point objective (RPO)
recovery time objective (RTO)

This chapter examines standards, regulatory codes and compliance. Also, it explores business policies, procedures and best practices. It also presents business continuity and disaster recovery concepts.

13-1 INTRODUCTION

This chapter presents topics related to network management and operations. Section 13-2, "Safety Standards and Codes," provides an overview of safety standards and codes, industry regulatory compliance, and business policies and procedures. Section 13-3, "Industry Regulatory Compliance," provides an overview of the numerous rules and regulations an organization must comply with in order to operate. Section 13-4, "Business Policies, Procedures, and Other Best Practices," provides an overview of the rules that organizations must follow. Some of these rules are set by the government and others are developed from best practices for maintaining normal day-to-day operations. Section 13-5, "Business Continuity and Disaster Recovery" examines business continuity and disaster recovery, which are critical for any networking organization.

Table 13-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 13-1 **Chapter 13 CompTIA Network+ Objectives**

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
3.0	**Network Operations**	
3.2	Explain the purpose of organizational documents and policies.	13-2, 13-3, 13-4, 13-5
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	13-5
4.0	**Network Security**	
4.1	Explain common security concepts.	13-2, 13-3, 13-5

13-2 SAFETY STANDARDS AND CODES

This chapter provides an overview of safety standards and codes, industry regulatory compliance, and business policies and procedures. These are important concepts that all personnel involved with networking facilities should understand.

Safety should always be the number-one priority in every operation and for every workplace. Therefore, the U.S. government passed the Occupational Safety and

Health Act (**OSH Act**) in 1970 and created the Occupational Safety and Health Administration (**OSHA**) to oversee and enforce safety standards in the workplace. OSHA's mission is to ensure safe and healthful workplaces by setting and enforcing standards and by providing training, outreach, education, and assistance. Every employer must comply with all applicable OSHA standards.

The National Fire Protection Association (**NFPA**) is an organization that works closely with OSHA on standards and codes to help create safe environments and to prevent accidents due to fire, electrical and related hazards. OSHA has asked NFPA to develop many standards to assist employers and employees in complying with the safety regulations. Compliance with OSHA codes and regulations is mandatory. Although compliance with NFPA standards is not mandatory, through compliance employers can demonstrate and ensure compliance with OSHA requirements. To put it simply, OSHA tells us what to do, and NFPA tells us how to do it. Therefore, many OSHA standards refer to NFPA codes.

Under the OSH Act, OSHA regulations are in Code of Federal Regulations (**CFR**) title 29 part 1910 (commonly represented as 29 CFR 1910). Most workplaces have adopted these regulations as their safety procedures and policies. Some of the applicable and well-known OSHA safety standards are detailed in the following sections.

OSH Act
Occupational Safety and Health Act, 1970 legislation that created the Occupational Safety and Health Administration

OSHA
Occupational Safety and Health Administration, an organization created to oversee and enforce safety standards in the workplace

NFPA
National Fire Protection Association, an organization that works closely with OSHA to create standards and codes to help create safe environments and to prevent accidents

CFR
Code of Federal Regulations

Design and Construction Requirements for Exit Routes (29 CFR 1910.36)

An exit route is a continuous and unobstructed path of travel from any location within a workplace to a place of safety. 29 CFR 1910.36 specifies the basic location requirements for the proper design and construction of exit routes:

- Each exit route must be a permanent part of the workplace.
- Each exit must be separated from other parts of the workplace, and the separation materials must be fire resistant.
- An opening into an exit must be protected by a self-closing fire door that remains closed and must be limited to only allow exit access.
- The number of exit routes must be adequate for all employees to be able to evacuate safely during an emergency.
- Each exit discharge must lead directly outside or to a street, a walkway, a refuge area, a public way, or an open space, which must be large enough to accommodate the building occupants.
- Each exit door must be unlocked from the inside so employees can open the exit door at all times.
- A side-hinged exit door must be used so that the door can swing out in the direction of exit travel.

- An exit route must be at least 7 feet, 6 inches high and at least 28 inches wide at all points.
- An outdoor exit route is permitted, with the same height and width requirement as the indoor exit route.

Maintenance, Safeguards, and Operational Features for Exit Routes (29 CFR 1910.37)

29 CFR 1910.37 specifies requirements for employers to properly maintain exit routes in order to prepare the workplace for a successful emergency evacuation and minimize further danger to employees:

- Each exit route must be free of explosive or highly flammable furnishings and other decorations.
- Exit routes must be arranged so employees will not have to travel toward a high-hazard area.
- Each exit route must not be obstructed by any materials or equipment. It must not go through locked doors or dead-end corridors.
- Safeguards designed to protect employees, such as sprinkler systems, alarm systems, exit lighting, and fire doors, must be working properly.
- There must be adequate lighting for each exit route.
- Each exit must be clearly visible and marked by a sign reading "Exit."
- Each exit door must be free of decorations or signs that obscure the visibility of the exit door.
- If the direction to the exit is not apparent, signs must be posted to show the direction to the exit.
- Each exit sign must be illuminated, and the word "Exit" must be in plainly legible letters.
- Fire-retardant paints or solutions must be maintained often enough to renew their properties.
- During construction, repairs, or alterations, exit routes must be maintained and available at all times.
- Employers must install and maintain an operable alarm system to alert employees of fire and other emergencies.

EAP
Emergency action plan, a plan that facilitates and organizes employer and employee actions during workplace emergencies

Emergency Action Plans (29 CFR 1910.38)

An employer must have an emergency action plan (**EAP**). An emergency action plan facilitates and organizes employer and employee actions during workplace emergencies. If there are more than 10 employees, the plan must be in writing, and

it must be kept in the workplace and available for employee review. An emergency action plan must include the following, at a minimum:

- Procedures for reporting fires and other emergencies
- Procedures for emergency evacuation, including the type of evacuation and exit route assignments
- Procedures for employees who stay behind to continue critical plant operations
- Procedures to account for all employees after evacuation
- Procedures for employees performing rescue or medical duties
- Names or job titles of persons who can be contacted for further information or explanation of duties under the plan

In addition, employers should have an alarm system to alert employees. Employers must designate and train enough people to assist in the safe and orderly emergency evacuation of employees. Employers must review the emergency action plan with each employee when the plan is initially developed, when an employee is initially hired to the job, when actions or responsibilities under the plan change, or when the plan changes.

Fire Prevention Plans (29 CFR 1910.39)

As with having an emergency action plan, an employer is required to have a fire prevention plan (**FPP**). As a matter of fact, the emergency action plan and fire prevention plan typically go hand in hand. Many organizations combine the two plans into one document. The written fire prevention plan must be available to the employees and kept at the workplace. For employers with 10 or fewer employees, the plan may be communicated orally. The purpose of the fire prevention plan is to prevent a fire from occurring or spreading in a workplace. A fire prevention plan must include the following, at a minimum:

FPP
Fire prevention plan, a plan that is meant to prevent fires from occurring or spreading in a workplace

- A list of all major fire hazards, proper handling and storage procedures for hazardous materials, potential ignition sources and their control, and the type of fire protection equipment necessary to control each major hazard
- Procedures to control accumulations of flammable and combustible waste materials
- Procedures for regular maintenance of safeguards installed and heat-producing equipment to prevent the accidental ignition of combustible materials
- The names or job titles of employees responsible for maintaining equipment to prevent or control sources of ignition or fires
- The names or job titles of employees responsible for the control of fuel source hazards

In addition, employers must inform employees of any fire hazards they may be exposed to and must review with each employee the fire prevention plan necessary for self-protection.

Portable Fire Extinguishers (29 CFR 1910.157)

Fire extinguishers are a smaller form of fire suppression. However, when used properly, fire extinguishers can save lives and property by putting out small fires or controlling a fire until additional help arrives. There are five types of fire extinguisher ratings, and each rating denotes a different class of fire:

- **Type A:** These fire extinguishers are used for combustible solid materials such as paper, wood, cloth, and some types of plastic. These extinguishers typically use water and dry chemicals to suppress fire.
- **Type B:** These fire extinguishers are used to suppress fire originated from flammable liquids and gas. These extinguishers typically use foam, powder, or carbon dioxide.
- **Type C:** These fire extinguishers are used on electrical fires originated from sources such as wires, electrical panels, and circuit breakers. These extinguishers typically use dry power or carbon dioxide.
- **Type D:** These fire extinguishers are used on combustible or flammable metals such as magnesium, aluminum, potassium, and sodium. This class of fire can only be suppressed with dry powder extinguishers.
- **Type K:** These fire extinguishers are used to suppress kitchen fires caused by cooking fats, greases, and oils. These extinguishers use wet chemical to suppress this class of fire.

The portable fire extinguishers standard specifies the placement, use, maintenance, and testing of portable fire extinguishers provided for the use of employees. Employers may exempt themselves from most of the portable fire extinguisher requirements if they develop a written emergency action plan that is complete and in compliance with 29 CFR 1910.38. The portable fire extinguishers standard specifies the following:

- Employers must mount, locate, and identify portable fire extinguishers for easy employee access.
- Portable fire extinguishers cannot have carbon tetrachloride or chlorobromomethane extinguishing agents.
- Employers must remove from service portable fire extinguishers that use soldered or riveted shell self-generating soda acid, self-generating foam, and gas cartridge water.
- Employers must provide, select, and distribute portable extinguishers based on the class of anticipated workplace fires; fire extinguishers are classified by their ability to handle specific classes and sizes of fires.

- Employers are responsible for the inspection, maintenance, and testing of all portable fire extinguishers in the workplace.
- Employers must ensure that portable fire extinguishers are fully charged, operable, and kept in their designated place at all times.
- Employers must provide equivalent protection when extinguishers are removed for maintenance or recharging.
- Portable fire extinguishers must be subjected to annual maintenance checks. The maintenance date must be recorded, and the record must be retained for one year after the last entry or for the extinguisher's shelf life.
- Employers must have trained persons with suitable testing equipment, and facilities must conduct hydrostatic testing on portable fire extinguishers.
- Employers must remove portable fire extinguishers that fail hydrostatic pressure testing.

In addition to these requirements, employers must provide training upon initial assignment and at least annually for employees who use fire extinguishers. The training program must familiarize employees with the general principles of fire extinguisher use, fire hazards, and the use of appropriate equipment.

Fixed Extinguishing Systems (29 CFR 1910.160)

Fixed fire extinguishing/suppression systems are commonly used to protect areas containing valuable or critical equipment, such as data-processing rooms, telecommunication switches, and process control rooms. Their main function is to quickly extinguish a developing fire before extensive damage occurs by filling the protected area with a gas or chemical extinguishing agent. The purpose of 29 CFR 1910.160 is to ensure the safety of employees and prevent possible injury, death, or adverse health consequences caused by the extinguishing agent. This standard includes the following requirements:

- If the system becomes inoperable, employers must notify employees and take any necessary temporary precautions to ensure their safety until the system is restored to operating order. Any defects or impairments must be properly corrected by trained personnel.
- A distinctive alarm or signaling system must be capable of being perceived above ambient noise or light levels when the extinguishing system is discharging.
- Effective safeguards must be provided to warn employees against entering discharge areas where the atmosphere remains hazardous to employee safety or health.
- Hazard warning or caution signs must be posted at the entrance to and inside areas protected by fixed extinguishing systems that use agents in concentrations known to be hazardous to employee safety and health.

- Fixed extinguishing systems must be inspected annually by a knowledgeable person to ensure that the systems are maintained in good operating condition.
- The weight and pressure of refillable containers must be checked at least semi-annually.
- Factory-charged nonrefillable containers that have no means of pressure indication must be weighed at least semi-annually. If a container shows a loss in net weight of more than 5%, it must be replaced.
- Inspection and maintenance dates must be recorded, and the record of the last semi-annual check must be maintained until the container is checked again or for the life of the container, whichever is less.
- Employers must ensure that the designated employees who inspect, maintain, operate, or repair fixed extinguishing systems are regularly trained, and their training must be reviewed annually.
- Chlorobromomethane or carbon tetrachloride may not be used as an extinguishing agent where employees may be exposed.
- Fixed extinguishing systems installed in the presence of corrosive atmospheres must be constructed of noncorrosive material or otherwise protected against corrosion.
- Automatic detection equipment must be approved, installed, and maintained in accordance with the fire detection system.
- All systems designed for and installed in areas with climatic extremes must operate effectively at the expected extreme temperatures.
- At least one manual station must be provided for discharge activation of each fixed extinguishing system.
- Manual operating devices must be identified as to the hazard against which they will provide protection.
- Employers must provide and ensure the use of the personal protective equipment needed for immediate rescue of employees trapped in hazardous atmospheres created by an agent discharge.

Fire Detection Systems (29 CFR 1910.164)

Automatic fire detection systems, when combined with other elements of an emergency response and evacuation plan, can significantly reduce property damage, personal injuries, and loss of life due to fire in the workplace. Automatic fire detection systems do this by using electronic sensors to detect the smoke, heat, or flames from a fire and providing early warning. Their main function is to quickly identify a developing fire and alert building occupants and emergency

response personnel before extensive damage occurs. 29 CFR 1910.164 includes the following requirements:

- Employers must restore all fire detection systems and components to normal operating condition as promptly as possible after each test or alarm.
- Employers must maintain all systems in an operable condition.
- Employers are responsible for servicing, testing, and adjusting fire detectors and fire detection systems as often as needed to maintain proper reliability and operating condition. The work must be performed by a trained person.
- Fire detectors must be cleaned at regular periodic intervals.
- Employers must ensure that fire detection equipment is protected from mechanical or physical impact, weather, and corrosion.
- Employers must ensure that fire detectors are supported independently of their attachment to wires or tubing.
- Fire detection systems installed for the purpose of actuating fire extinguishment or suppression systems must operate in time to control or extinguish a fire.
- Fire detection systems installed for the purpose of employee alarm or evacuation systems must provide a warning in time for emergency action and safe escape of employees.
- Employers cannot delay alarms or devices initiated by fire detector actuation for more than 30 seconds unless it is necessary for the immediate safety of employees, which then must be addressed in the emergency action plan.
- Employers must ensure that the number, spacing, and location of fire detectors are based on design data obtained from field experience or tests, engineering surveys, the manufacturer's recommendations, or a recognized testing laboratory listing.

Employee Alarm Systems (29 CFR 1910.165)

The purpose of the employee alarm systems standard is to reduce the severity of workplace accidents and injuries by ensuring that alarm systems operate properly and procedures are in place to alert employees to workplace emergencies. This standard includes the following requirements:

- An employee alarm must be perceived above ambient noise or light levels by all employees. It must be distinctive and recognizable as a signal to evacuate the work area.
- Employers must explain to each employee the preferred means of reporting emergencies. If telephones serve as a means of reporting emergencies, emergency telephone numbers must be posted near telephones or employee notice boards and in other conspicuous locations.

- Employers must establish procedures for sounding emergency alarms in the workplace. For employers with 10 or fewer employees, direct voice communication is an acceptable procedure.
- All devices, components, combinations of devices, or systems constructed and installed must be approved by OSHA.
- All employee alarm systems must be restored to normal operating condition as promptly as possible after each test or alarm.
- Employers must ensure that all employee alarm systems are maintained in operating condition.
- Employers must test the reliability and adequacy of both supervised and unsupervised employee alarm systems. Supervised alarm systems can monitor the condition of their detectors and circuitry, whereas unsupervised alarm systems cannot. Unsupervised employee alarm systems must be tested every two months. Supervised employee alarm systems installed after January 1, 1981, must be tested at least annually and working properly in supervised mode.
- Employers must maintain or replace power supplies to the systems as often as is necessary to ensure fully operational condition.
- Employers must ensure that employee alarms are serviced, maintained, and tested by properly trained persons.
- Employers must ensure that manually operated actuation devices for use in conjunction with employee alarms are unobstructed and readily accessible.

Hazard Communication (29 CFR 1910.1200)

The purpose of 29 CFR 1910.1200 is to ensure that the hazards of all chemicals are classified and the information concerning the classified hazards is communicated to employers and employees. It requires that the chemical manufacturer, distributor, or importer provide safety data sheets (**SDS**), formerly known as material safety data sheets (**MSDS**), for each hazardous chemical it produces or imports. An employer must have an SDS in the workplace for each hazardous chemical it uses. The SDS includes information such as product identifier or manufacturer, physical and chemical properties, chemical hazards, chemical ingredients and composition, first-aid measures, fire-fighting measures, accidental release measures, handling and storage, personal protection, chemical stability and hazardous reactions, and toxicological information.

A network technician needs to be aware of this particularly because network closets are sometimes used incorrectly to temporarily store chemicals. The safety data sheets provide workers and emergency personnel with procedures for handling chemicals in a safe manner.

SDS
Safety data sheets, documents that provide workers and emergency personnel with procedures for handling chemicals in a safe manner

MSDS
Material safety data sheets, an older term for SDS

HVAC Systems

Another building issue for networks is the **HVAC** (heating, ventilation, and air-conditioning) system. HVAC systems are critical for computing and data centers. An HVAC system must be properly planned and maintained to ensure that the operating environment is properly maintained. The physical hardware used in a computer center will have recommendations for temperature and humidity. In addition, maintenance personnel for HVAC systems will have access to protected areas; these people must have proper clearance, and safeguards must be in place to allow non-IT staff to have access to these areas.

HVAC
Heating, ventilation, and air-conditioning, systems that are critical for computing and data centers

Door Access

In computer networks and enterprise data centers, door access is a critical part of physical security. Door access should be controlled through the use of smart cards, proximity cards, or key fobs. Other options for access control include biometrics, such as hand scanners and retinal scanners. **Biometric systems** measure and analyze specific characteristics of the human body—for example, DNA, fingerprints, voice and facial patterns, eye retinas, and hand measurements—for the purpose of authentication. Door access control could also be managed using keypads and cipher locks to ensure that only authorized personnel have entry access. To detect unauthorized access, burglar alarms and motion detection alarms can be deployed. Burglar alarms detect when entry points, such as doors or windows, are opened. Motion detection alarms detect movement within monitored areas. In either case, the alarm will sound and the alert notifications will be sent to the proper authority.

Biometric Systems
Systems that measure and analyze specific characteristics of the human body for the purpose of authentication

In some cases, a security guard could be in a position to help control physical access to these areas. It is a common physical security practice for authorized personnel to wear their ID badges with picture and identification information. The security guard will be responsible for checking and validating their badges before allowing them entry access.

Another type of commonly deployed physical security is video surveillance. Video surveillance can be used in many areas that require monitoring, such as a data center. Video monitoring in computer spaces is also a necessity to prevent theft and to provide a video record of personnel who access the systems. In some video surveillance systems, video monitoring is triggered by motion detection. When any movement or activity is detected in a monitored area, a surveillance camera with motion detection activates itself and starts capturing video footage. It is important to remember that internal threats are a major concern. Video surveillance is available as CCTV (closed-circuit television) or IP-based video. IP-based video surveillance is becoming more popular today. Many home security camera products, such as Ring, Nest, and Arlo, are affordable and easy to install and manage.

Section 13-2 Review

This section covers the following Network+ exam objectives.

3.2 Explain the purpose of organizational documents and policies.
This section provides an overview of safety standards and code, industry regulatory compliance, and business policies and procedures.

4.1 Explain common security concepts.
This section provides an overview of the very important processes and devices used for controlling and monitoring access to a data center.

Test Your Knowledge

1. True or false: The only exception to the rule of having a written emergency action plan (EAP) is when an employer has 10 or fewer employees.

   True

2. True or false: According to OSHA, portable fire extinguishers can be operated by anyone.

   False

3. What provides workers and emergency personnel with procedures for handling chemicals in a safe manner? (Select all that apply.)

   a. EAP
   b. SDS
   c. MSDS
   d. FPP

13-3 INDUSTRY REGULATORY COMPLIANCE

This section provides an overview of the numerous rules and regulations an organization must comply with in order to operate. It is important for an organization to know what regulations it must comply with.

There are numerous rules and regulations nationally as well as internationally. Regulations that pertain to one organization may not pertain to another. An organization must know what regulations it must comply with in order to operate. Organizations from the same industry will most likely have to adhere to the same regulations. Industry regulatory compliance requires adherence to laws, regulations, guidelines, and specifications relevant to the industry's business. The following sections describe some prevalent regulatory compliance laws and regulations from different industries.

FERPA

FERPA stands for Family Educational Rights and Privacy Act, which is a federal law that requires all educational institutions to protect the privacy of student education records. FERPA imposes confidentiality requirements around student educational records, prohibiting institutions from disclosing information such as grades or financial aid without the student's written permission. The law applies equally to electronic and hard-copy records.

FERPA defines *education records* as follows:

> Records that are directly related to a student and that are maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution. These records include but are not limited to grades, transcripts, class lists, student course schedules, health records (at the K–12 level), student financial information (at the postsecondary level), and student discipline files. The information may be recorded in any way, including, but not limited to, handwriting, print, computer media, videotape, audiotape, film, microfilm, microfiche, and e-mail.

FERPA
Family Educational Rights and Privacy Act, a federal law that requires all educational institutions to protect the privacy of student education records

FISMA

FISMA, which stands for Federal Information Security Management Act, is a federal law that was developed to protect government information, operations, and assets against security threats. Every agency is responsible for ensuring information security in the federal government and is subject to FISMA audit. The National Institute of Standards and Technology (NIST) has developed Federal Information Processing Standards (FIPS) to help agencies become FISMA compliant. FIPS 199: Information Systems Security Categorization of Federal Information and Information Systems and FIPS 200: Minimum Information Security Requirements are approved standards by the Secretary of Commerce and required standards by FISMA.

FISMA
Federal Information Security Management Act, a federal law that was developed to protect government information, operations, and assets against security threats

GDPR

GDPR, which stands for General Data Protection Regulation, is a European privacy law that went into effect in May 2018. This law protects personal data rights and restricts how personal data can be collected and used. Even though GDPR is supposed to protect individuals from EU (European Union) countries, this law has a big impact on Internet users around the world because the data can be processed on Internet sites anywhere. GDPR requires Internet companies to clearly inform and ask users for their consent to collect their data. Users also have rights to gain full access to their data from Internet companies that collect their information.

GDPR
General Data Protection Regulation, a European privacy law that protects personal data rights and restricts how personal data can be collected and used

GLBA

GLBA, which stands for Gramm-Leach-Bliley Act, is a federal law that requires all financial institutions to protect customer financial information data, to safeguard the financial information against security threats, and to deny any unwarranted access to financial data. Financial institutions are defined to be institutions that

GLBA
Gramm-Leach-Bliley Act, a federal law that requires all financial institutions to protect customer financial information data, to safeguard the financial information against security threats, and to deny any unwarranted access to financial data

engage in financial institution activities, including services such as loans, financial or investment advice, and insurance. By this definition of that term, the GLBA regulations apply to a wide range of entities, including colleges and universities.

HIPAA

HIPAA
Health Insurance Portability and Accountability Act, a federal law that requires all health-related agencies to protect the personally identifiable information (PII) of patients

HIPAA, which stands for Health Insurance Portability and Accountability Act, is a federal law that requires all health-related agencies to protect the personally identifiable information (PII) of patients. This law specifies the administrative processes, IT standards, and policies and procedures to protect patient information gathered in the healthcare process and also mandates the standardization of electronic transactions, code sets, and identifiers.

PCI DSS

PCI DSS
Payment Card Industry Data Security Standard, a standard set by the Payment Card Industry that holds banks and merchants accountable for any credit card breach

PCI DSS, which stands for Payment Card Industry Data Security Standard, is not a federal law but a standard set by the Payment Card Industry (Visa, MasterCard, Discover, and American Express) that holds banks and merchants accountable for any credit card breach. Compliance with PCI DSS requires all merchants to process, store, and transmit credit card information in a secure environment. It specifies the administrative processes, IT standards, policies, and procedures to protect the privacy and confidentiality of credit card transactions.

Conforming to these stringent and complex regulations takes a great deal of collaboration from many units within an organization. Information technology plays a very important role in fulfilling these mandates because the data that these regulations are trying to protect is stored in some database or server, processed by some software application, and transmitted on some network. Therefore, safeguarding the data requires IT involvement.

International Export Controls

International export controls generally refer to federal laws and regulations governing the export of materials, data, technical information, services, technologies, software, and hardware to foreign countries based on national security, foreign policy, and trade sanctions. The three major export control regulations are the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), and the Office of Foreign Assets Control (OFAC). All these regulations have a common theme of protecting the confidentiality, integrity, and availability of the information that impacts consumers.

An IT organization can use the guidance of NIST's Framework for Improving Critical Infrastructure Cybersecurity to help facilitate compliance. The components of this framework are as follows:

- The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

- The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
- The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- Access to assets and associated facilities is limited to authorized users, processes, or devices and to authorized activities and transactions.
- The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security–related duties and responsibilities consistent with related policies, procedures, and agreements.
- Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets.
- Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
- Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
- Anomalous activity is detected in a timely manner, and the potential impact of events is understood.
- The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
- Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events.
- Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- Analysis is conducted to ensure adequate response and support recovery activities.

- Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
- Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
- Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
- Recovery planning and processes are improved by incorporating lessons learned into future activities.
- Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet service providers, owners of attacking systems, victims, other CSIRTs (computer security incidence response teams), and vendors.

Section 13-3 Review

This section covers the following Network+ exam objectives.

3.2 Explain the purpose of organizational documents and policies.
This section discusses an organization's risk strategy to protect the confidentiality, integrity, and availability of information.

4.1 Explain common security concepts.
As discussed in this section, recovery processes and procedures need to be executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

Test Your Knowledge

1. Why are FERPA and HIPAA important to IT staff?
   a. Both regulations require IT certifications.
   b. The information is typically stored on servers, for which IT personnel are responsible.
   c. IT staff must know the compliance steps to take in the event of a power failure.
   d. They aren't.
2. Which of the following is a compliance standard that is not a federal regulation?
   a. FISMA
   b. FERPA
   c. PCI DSS
   d. GLBA

3. Say that you are working for a loan company. Your loan officers often dispose of the client paperwork by throwing it away in a trash can. What compliance regulation might your company be violating?

   a. GLBA
   b. FISMA
   c. MTTR
   d. HIPAA

13-4 BUSINESS POLICIES, PROCEDURES, AND OTHER BEST PRACTICES

This section provides an overview of the rules that organizations must follow. Some of these rules are set by the government and others are developed based on best practices for maintaining normal day-to-day operations. This section also examines some of the service agreements commonly used as standard business documents in the IT world.

Regulations are mandatory rules that are set by government or authorized entities. Organizations must certify that they have complied with all the rules and also must have a way to show that their compliance can be validated through a process such as an audit. Regulations help set many guidelines and practical standards for day-to-day operations.

There are also rules that can be set between entities without being regulated by government. Similar to regulations, these rules define how business should be done, what services can be exchanged, what the service expectations are, what the rules of engagement are, and so on. These rules, once agreed upon by all parties, may be upheld in a court of law. A court can hold parties accountable and responsible for their actions.

In the IT world, two or more parties can enter into a formal agreement, called a service agreement, that articulates the terms and conditions of a service. The agreement specifies many criteria, which include but are not limited to the nature, description, and scope of the service and how the service will be governed, implemented, operated, tested, reported, and financed. Many types of service agreements are used in business. The following sections describe the agreements most commonly used as standard business documents in the IT world.

Memorandum of Understanding

A memorandum of understanding, or **MOU**, is a formal agreement between two or more parties to establish official service partnerships. It outlines the terms and details of each party's requirements and responsibilities. This document is sometimes called a letter of intent (LOI) because it can be followed with a legally binding contract.

MOU
Memorandum of understanding, a formal agreement between two or more parties to establish official service partnerships

MOUs are much less formal than contracts, but they are far more formal than handshakes. Many IT organizations use MOUs to create guidelines with one another as they contribute their efforts and resources toward important projects or for sharing or exchanging IT services without having to enter into the detailed and complex process of contracts.

Service-Level Agreement

SLA
Service-level agreement, a formal agreement typically between a service provider and a client or an end user, that defines the level of service expected from the service provider

A service-level agreement, or **SLA**, is a formal agreement typically between a service provider and a client or an end user. This agreement defines the level of service expected from the service provider. Unlike MOUs, SLAs do not contain details regarding how a service will be provided or delivered, nor do they provide operational guidelines. SLAs simply define what service the end user should expect to receive as well as the levels of service the service provider guarantees. In case of failure to provide the guaranteed level of service, SLAs define the responsibilities of the service provider to restore the guaranteed level of service.

Internet service is a prime example of a service that is often the subject of SLAs. SLAs for Internet service vary depending on many factors, such as Internet service provider (ISP), type of Internet technology, and class of Internet service. For example, an SLA for business Internet service will be far more stringent and detailed than an SLA for residential Internet service. Most SLAs for business Internet service include the guaranteed speed, the guaranteed Internet service availability or uptime, the expected response time for repair or service restoration, and the service provider's penalty for not meeting the guaranteed service level.

Many organizations use SLAs as a way to benchmark their performance. SLAs are very common and popular among cloud service providers. They are used to assure customers of the quality of the service they will receive.

Master Service Agreement

MSA
Master service agreement, an overarching document that creates a framework for multiple service-level agreements

A master service agreement (**MSA**) is an overarching document that creates a framework for multiple service-level agreements—hence the term *master.* An MSA is typically used when entering into a long negotiation of services, where multiple contracts or agreements might be needed. It is set up as the initial agreement to include most but not all the terms and conditions between two or more parties. These terms, such as service definitions, payment terms, warranties, limitations on liability, and termination, are likely not to change. The purpose of an MSA is to speed up and simplify the process for future subsequent agreements. Future subsequent agreements only need to contain the differences from the MSA, thus reducing the time and involvement from all parties.

Master License Agreement

MLA
Master license agreement, an agreement that defines the owner rights, terms, and conditions related to intellectual property

A master license agreement (**MLA**) defines the owner rights, terms, and conditions related to intellectual property. MLAs are commonly used by software vendors to define how their software can be used and distributed. They also define licensing restrictions and the liabilities and/or penalties associated with a violation. Sometimes, the term MLA is used for an end user license agreement (EULA), which is a more specific agreement for a particular software product.

Non-Disclosure Agreement

A non-disclosure agreement (**NDA**) is a legal agreement to bind a party or parties to not disclose or not share specific information. It protects confidential information, proprietary information, intellectual property, or trade secrets and ensures that the information will not propagate beyond the intended parties. An NDA is usually signed before confidential information is divulged.

NDA
Non-disclosure agreement, a legal agreement that protects confidential information, proprietary information, intellectual property, or trade secrets

Statement of Work

A statement of work (**SOW**) is a document often used in conjunction with an MSA. Whereas an MSA defines general terms of service, an SOW has all the specifics of the service. SOWs define in detail the deliverables, schedules, and time lines, roles and responsibilities, and price agreed by all parties. Under one MSA, there may be multiple SOWs.

SOWs are common in the information technology field when organizations engage third-party companies to implement or deploy new IT services. SOWs are used to define what the service provider is committing to deliver as well as to outline the steps and procedures of work to be done.

SOW
Statement of work, a document often used in conjunction with an MSA that defines in detail the deliverables, schedules, and time lines, roles and responsibilities, and price agreed by all parties

Acceptable Use Policy

Another common policy found in all organizations with IT services is an **AUP**, which stands for acceptable use policy. This type of policy outlines the acceptable use of computer equipment, network, Internet, and other IT-related services. The policy defines rules and constraints that users must accept before accessing IT services. When they accept an AUP, users are held accountable to their actions while using the organization's IT services. Typically, an AUP contains segments referencing the organization's policies and standards as well as on adhering to local and federal laws.

AUP
Acceptable use policy, a policy that defines the constraints and practices the user must agree to in order to have access to a network

Incident Response Policy

An incident response policy provides a computer security incident handling plan to manage risk and minimize adverse effects. It outlines procedures for addressing security incidents and defines roles and responsibilities of all the parties involved. There are six steps in incident response that need to be part of an incident response policy:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Follow-up/Lessons learned

Password Policy

A password policy sets the rules on the computing passwords for an entire organization. Passwords are the most used method of authentication and are key to accessing any IT services, and they must be safeguarded. It is not easy to safeguard everyone's password, and a password policy can help by establishing criteria and rules that everyone in the organization has to follow.

The following are some of the common rules included in a password policy:

- Password strength/complexity defines the composition requirements of a password. Generally accepted password strength characteristics recommended by NIST are that it be at least eight characters or longer. It should contain at least one uppercase letter, contain at least one lowercase letter, contain at least one number, have at least one special character, and not contain the username.
- Password expiration defines the duration for which the password is valid. The expiration time depends entirely on the organization; some prefer 120 days, some prefer 6 months.
- Account lockout defines how many times users are allowed to enter an incorrect password before the account is locked out. Also, there may be a lockout time implemented before a user can try reentering the password.
- Password reset defines the rules or procedures for resetting the user's password.
- Password sharing restricts users from sharing their password with anyone else.

Currently, a big shift is occurring in how NIST views password strength. The newest Digital Identity Guidelines from NIST favor the use of long passphrases instead of composition rules. These guidelines also recommend using multifactor authentication.

Privileged User Agreement

A privileged user agreement establishes expectations for the conduct of individuals granted privileged access to an organization's enterprise systems and services, which may include computing systems, network, databases, data, user accounts, and user processes. This agreement defines different processes to obtain a privileged user account: request, approval, modification, and revocation. The agreement should also entail the type of privileged access granted. The agreement typically has to be signed by the requestor and the approver. It will then be kept as a record for auditing purposes.

Standard Operating Procedure

A standard operating procedure (SOP) is a procedure document that describes routine operations accompanied by step-by-step instructions showing how to

perform them. The purpose of an SOP is to ensure quality and consistency of the operations; the operations are to be carried out correctly and in the same manner. Any unit within an organization can have an SOP to streamline operations. For example, onboarding and offboarding procedures could be part of a unit's SOP, which may detail the list of things that new employees need in order to start performing their required duties, such as physical access, server access, network access, computer assignment, special equipment, and training. The SOP may also address employee termination, listing the access to be revoked and equipment to be returned.

Onboarding and Offboarding Policies

Onboarding and offboarding policies can cover from user access level to device access level. An **onboarding** policy can specify how a new employee is brought into an organization's IT systems. It defines different types of access a new employee would need to do his/her job, depending on the employee's roles and responsibilities. An onboarding policy can also cover how a new device can get connected and gain access to the organization's network. An **offboarding** policy focuses on the termination of employee access and device access when an employee is terminated or no longer in the same role and when a device is decommissioned from the production system.

Onboarding
A policy or process related to how a new employee or device is brought into an organization's IT systems

Offboarding
A policy or process related to terminating employee access or decommissioning a device from a production system

Other Best Practices

An organization can have many policies and procedures, and they typically evolve from IT best practices. Best practices are recommended practices that have been proven effective and efficient for other people to adopt as guidelines. If best practices are followed, it is very likely that an organization will meet the compliance standards. This section describes some well-known and widely adopted best practices.

Documentation is a fundamental and very important part of an organization's operations. Most standards and other compliance documents talk about having good documentation. In networking, documentation typically includes a physical network diagram, a logical network diagram, and a wiring diagram. Good network documentation with detailed information about wiring and port locations is essential for network troubleshooting. When changes are made to a network, the diagrams must be updated. In addition, change management documentation should keep track of any changes, including configuration changes, new installations, or upgrades made to a network and the system. Change management documentation accompanies a change management policy, which governs the change process of an organization; the typical processes are notification, approval, authorized downtime, and notification of change.

Having configuration standards is another widely adopted best practice. Such standards help ensure that every network device has a good baseline configuration that meets both operational and security requirements. NIST provides recommendations on network device hardening, including recommended practices used in changing default credentials, generating new encryption keys, and disabling unused device ports. An SOP for the network team can include a switch configuration standard and a router configuration standard as part of the equipment installation. NIST

also recommends using network segmentation to segregate a network either physically with a dedicated network and hardware or logically with VLANs for security purposes. Therefore, higher-risk and critical areas like data center networks, finance networks, and supervisory control and data acquisition (SCADA) networks end up working on their own networks. Network segmentation creates different zones for these networks for ease of management, control, and auditing.

Role separation, sometimes known as separation of duties, is a practice of separating tasks and assigning them to different responsible groups or employees, therefore limiting full control of services or information and eliminating conflicts of interest. Role separation can be thought of as a check-and-balance process. For example, a network administrator should not be the same person who performs a network compliance audit.

Asset management or inventory management is another best practice. The basic principle is to protect the organization's IT assets and prevent the misuse and loss of assets by establishing a self-inventory that can be used in the audit process. IT assets can include both hardware and software. Inventory management goes from the procurement stage to the assignment stage and then to the disposal stage. It is good to know when an asset was purchased, who was the responsible person, where the asset was located, and when it was disposed. Good inventory management can be much more than tracking assets; it can help predict the system life cycle, which is a factor in IT and budgetary planning.

Another best practice is to consider an IT audit. An audit is an assessment of an organization's IT infrastructure and security controls. An audit can be performed by internal auditors and external auditors. An audit and assessment report can help validate and verify an organization's IT operations and practices. Today, many IT audits by third-party companies are also offered with cybersecurity posture assessment, which provides a way to assess the security status and health of an organization's IT infrastructure.

Section 13-4 Review

This section covers the following Network+ exam objective.

3.2 Explain the purpose of organizational documents and policies.

This section provides an overview of standard business documents.

Test Your Knowledge

1. Your company has suffered an Internet outage for two straight days, and you want to take legal action against the Internet service provider. What document must you review before pursuing legal action?

   a. SLA
   b. MOU
   c. MSA
   d. AUP

2. Which of the following are types of service agreements? (Select all that apply.)

   a. Memorandum of understanding (MOU)
   b. Service-level agreement (SLA)
   c. Master service agreement (MSA)
   d. Statement of work (SOW)
   e. Acceptable use policy (AUP)

13-5 BUSINESS CONTINUITY AND DISASTER RECOVERY

This section examines business continuity and disaster recovery, which is a critical step for any networking organization. This section examines key concepts such as high availability, MTBF, MTTF, and MTTR.

This section examines business continuity and disaster recovery, which is a critical step for any networking organization. This section examines key concepts such as high availability, MTBF, MTTF, and MTTR.

According to ISO 22301 2019, which is a standard for business continuity management systems, business continuity is a corporate capability. This capability exists whenever organizations can continue to deliver their products and services at acceptable predefined levels after disruptive incidents have occurred. Business continuity is a goal of any business.

Business continuity and disaster recovery go hand-in-hand in building resiliency in business operations. A business continuity plan identifies the key products and services of an organization and describes strategies to enable those key assets to stay operational. A disaster recovery plan outlines the process or procedures to recover the services quickly and effectively from after expected and unexpected disruptions in times of crisis. A number of metrics can be used to evaluate the effectiveness of the business continuity and disaster recovery plans:

- **MTBF (mean time between failures):** This metric measures a system's reliability by identifying the average time between failures.
- **MTTF (mean time to failure):** This metric predicts the equipment runtime before a failure requires the equipment to be replaced.
- **MTTR (mean time to recover or repair):** This metric measures the average time it takes to bring a system back from failure.

MTBF (Mean Time Between Failures)
A metric that measures a system's reliability by identifying the average time between failures

MTTF (Mean Time to Failure)
A metric that predicts the equipment runtime before a failure requires the equipment to be replaced

MTTR (Mean Time to Recover or Repair)
A metric that measures the average time it takes to bring a system back from failure

Making backups is a best practice for data protection. Every business must protect its valuable data. Backing up company data is one of the most important functions in IT operations; it is a key for data loss prevention and disaster recovery. Traditionally, companies have backed up their data to a local backup server and

then made a copy to a medium like tape. Today, data can be backed up to a cloud location to help eliminate single points of failure. There are many types of backups, including the following:

- **Full backup:** This is the most complete type of backup, where all data is copied to a designated backup location or medium. A full backup can take a long time, depending on the size of the source. It also can take up a large amount of storage space if archives need to be kept.
- **Differential backup:** This type of backup includes all data that has changed since the last full backup. The first differential backup copy is a full backup, and the subsequent backups are the differences from the previous full backup copy. Differential backups take less time and less storage space than do full backups.
- **Incremental backup:** This type of backup includes only data that has changed since the previous backup copy. The first incremental backup copy is a full backup, and subsequent backups are the differences from the previous copies. This type of backup generally takes the least time and the least storage space.

HA
High availability, a critical concept for business continuity and disaster recovery that refers to information technology systems being in continuous operation for a long time, with minimal downtime

FHRP
First Hop Redundancy Protocol provides default gateway redundancy. In the event of a router failure, there's a backup router that continues to forward traffic for users

High availability (**HA**) is a critical concept for business continuity and disaster recovery. It refers to information technology systems being in continuous operation for a long time, with minimal downtime. Typical high availability systems include hospitals and data centers, which are intended to be in operation 100% of the time. HA eliminates single points of failure by adding high redundancy. It also provides fault tolerance, which enables the ability to failover to a redundant system when a service fails. When there is a failure—whether it is a hardware failure, network failure, or software failure—HA systems must be able to detect failures and to fail over to the redundant system. An HA reliable/redundant system might make it so that failures are not seen, but failures must be noted in the maintenance log.

Examples of HA technologies are load balancing, Virtual Router Redundancy Protocol (VRRP), First Hop Redundancy Protocol (**FHRP**), active–active firewall appliances, and VMware vSphere HA.

The concept of high availability is important to organizations that use the Internet. Most organizations seek to have multiple Internet connections. Having multiple ISPs and having diverse network paths for critical infrastructure are network best practices for high availability and redundancy.

High availability deployments also have been widely deployed in power management. Power loss creates a big disruption in business continuity. HA applied to power management might require supplying electrical power from two or more different sources or separate feeds from the electrical company, sometimes known as *redundant circuits*. Also to create power redundancy, a system can be connected to a backup power source such as a UPS (uninterruptible power supply) or battery

backup. That way, when power is lost, the system is automatically switched over to the backup system. There may be a need to have power generators to generate electrical power in the case of extended power outage. For individual pieces of equipment, having dual power supplies, where each connects to a different power distribution unit (**PDU**), is an easy and practical approach to HA in the event of the loss of one power source.

PDU
Power Distribution Unit

In addition to HA, an organization needs to plan for a disaster recovery site where the mission-critical systems can be housed to bring the organization back up and running if a disaster puts the current data center out of commission. A disaster recovery site must be an offsite facility. Also, different types of disaster recovery sites lend themselves to different disaster recovery or backup setups or architectures:

- **Active/passive:** In this architecture, a disaster recovery site is idle, in standby mode. It becomes a primary active site only when it is needed. This setup may require some downtime to bring the standby site up to take over for the primary site.
- **Active/active:** In this architecture, the primary site and the disaster recovery site are both up and running at the same time. The data can be synchronized between the two sites. Also, load balancing could be deployed to balance the load between the two sites. This strategy is more complex than the active/passive one.

Active/Passive
An architecture in which the disaster recovery site is idle, in standby mode

Active/Active
An architecture in which both the primary site and the disaster recovery site are up and running at the same time

There are a few types of disaster recovery sites:

- **Cold site:** A **cold site** is an empty facility with only power and cooling but no equipment or racks. This type of site can only be used in an active/passive strategy.
- **Warm site:** A **warm site** is a not-yet-operational facility with power, cooling, and rack space; the equipment is onsite but not racked or powered up. This type of site can only be used for active/passive strategy.
- **Hot site:** A **hot site** is a full-blown operational facility with power, cooling, and equipment racked and powered up and connected to the network. It is a duplicate of the current data center. This type of site can be used for both active/active and active/passive strategies.
- **Cloud site:** A **cloud site** is an offsite cloud storage or disaster recovery service provided by a cloud provider. This type of service can be managed by the client or can be completely managed by the third-party cloud provider. This solution offers an organization the advantage of not having to deal with the backup system and the facility. This type of site can be used for both active/active and active/passive strategies.

Cold Site
An empty disaster recovery site with only power and cooling but no equipment or racks

Warm Site
A not-yet-operational disaster recovery site with power, cooling, and rack space

Hot Site
A full-blown operational disaster recovery site with power, cooling, and equipment racked and powered up and connected to the network

Cloud Site
An offsite cloud storage or disaster recovery service provided by a cloud provider

Recovery Point Objective (RPO)
The amount of data loss an organization can afford or tolerate in the event of an outage

Recovery Time Objective (RTO)
The maximum downtime an organization can afford or tolerate to maintain its business continuity

There are two metrics that organizations can use to determine their best option for a disaster recovery strategy:

- **Recovery Point Objective (RPO):** The amount of data loss an organization can afford or tolerate in the event of an outage
- **Recovery Time Objective (RTO):** The maximum downtime an organization can afford or tolerate to maintain its business continuity

Section 13-5 Review

This section covers the following Network+ exam objectives.

3.2 Explain the purpose of organizational documents and policies.
This section examines the concept of high availability (HA), which is a critical concept for business continuity and disaster recovery.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.
This section describes cold, warm, hot, and cloud sites.

4.1 Explain common security concepts.
This section examines business continuity and disaster recovery, which are critical for any networking organization.

Test Your Knowledge

1. With information technology systems, what is meant by the term high availability?
   a. It refers to information technology systems that are in continuous operation with minimal to no downtime.
   b. It refers to information technology systems that are in operation for a long time, with some downtime.
   c. It refers to information technology systems that are expensive to maintain.
   d. It refers to information technology systems that are located at least 100 miles away.
2. With information technology systems, what is a cold site?
   a. A cold site is a not-yet-operational facility with power, cooling, and rack space.
   b. A cold site is an empty disaster recovery facility with only power and cooling but no equipment or racks.
   c. A cold site is a full-blown operational facility with power, cooling, and equipment racked and powered up, with network connectivity.
   d. A cold site is facility without heating and cooling.

SUMMARY

The following key topics are presented in this chapter:

- An introduction to safety standards and codes
- The role of OSHA
- The various Code of Federal Regulations (CFR) standards
- An overview of fire protection systems and exit routes
- An overview of HVAC systems
- A look at door access control
- A discussion of business policies, procedures, best practices, and the prevalent service agreements used as standard business documents in the IT world
- An overview of business continuity and disaster recovery

QUESTIONS AND PROBLEMS

Section 13-2

1. What is OSHA's mission?

   To oversee and enforce safety standards in the workplace

2. True or false: Every employer must comply with all applicable OSHA standards.

   True

3. What is the purpose of the NFPA?

   To create standards and codes to help form safe environments and prevent accidents due to fire, electrical and related hazards.

4. True or false: Compliance with NFPA is mandatory.

   False

5. Provide a definition of an exit route, as defined by 29 CFR 1910.36.

   An exit route is a continuous and unobstructed path of travel from any area within a workplace to a place of safety.

6. What is the purpose of 29 CFR 1910.37, Maintenance, Safeguards, and Operational Features for Exit Routes?

   It specifies requirements for employers to properly maintain exit routes in order to prepare the workplace for a successful emergency evacuation and minimize further danger to employees.

7. What is the purpose of an emergency action plan?

   It facilitates and organizes employer and employee actions during workplace emergencies.

8. True or false: An organization's written FPP must be available to employees and kept at the workplace.

   True

Section 13-3

9. What does FERPA stand for?

   Family Educational Rights and Privacy Act

10. How does FERPA define education records?

    FERPA defines education records as records that are directly related to a student and that are maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution.

11. What does FISMA stand for and what is it?

    Federal Information Security Management Act, a federal law that was developed to protect government information

12. What does GLBA stand for and what is it?

    Gramm-Leach-Bliley Act, a federal law that requires all financial institutions to protect customer financial information data

13. What does HIPAA stand for and what is it?

    Health Insurance Portability and Accountability Act, a federal law that requires all health-related agencies to protect the personally identifiable information (PII) of patients

14. What is the purpose of PCI DSS?

    It is a standard set by the Payment Card Industry (Visa, MasterCard, Discover, and American Express) that holds banks and merchants accountable for any credit card breach

15. How is the IT part of an organization involved with the regulations defined by FERPA, FISMA, GLBA, HIPAA, and PCI DSS?

    Information technology plays a very important part in fulfilling these mandates, as the data that these regulations aim to protect is stored in some database or server, processed by some software application, and transmitted on some network.

16. Which of the following are components of the NIST Framework for Improving Critical Infrastructure Cybersecurity? (Select all that apply.)

    a. The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
    b. Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
    c. Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
    d. The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
    e. Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

17. Which of the following is *not* part of the NIST Framework for Improving Critical Infrastructure Cybersecurity?

    a. Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
    b. Anomalous activity is detected within a one-month period, and the potential impact of events is understood.
    c. Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
    d. Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events.
    e. Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

18. What are international export controls?

    International export controls generally refer to federal laws and regulations governing the export of materials, data, technical information, services, technologies, software, and hardware to foreign countries based on national security, foreign policy, and trade reasons.

Section 13-4

19. What is the purpose of a service agreement relative to the IT world?

    A service agreement specifies many criteria, which include but are not limited to the nature, description, and scope of a service as well as how the service will be governed, implemented, operated, tested, reported, and financed.

20. What does MOU stand for, and what is the purpose of an MOU?

    A memorandum of understanding, or MOU, is a formal agreement between two or more parties to establish official service partnerships.

21. Why do organizations use MOUs?

    To create guidelines with one another as they contribute their efforts and resources toward important projects or for sharing or exchanging of IT services without having to enter into a detailed and complex process of contracts

22. What is a service-level agreement?

    A formal agreement typically between a service provider and a client or an end user

23. How do SLAs differ from MOUs?

    SLAs do not contain details regarding how a service will be provided or delivered, nor do they provide operational guidelines.

24. Which of the following is a prime example of a service commonly covered by an SLA?

    a. Rental space
    b. Food service
    c. Internet service
    d. None of the above are correct.

25. What type of agreement is used when entering into a long negotiation of services when multiple contracts or agreements might be needed?

    a. Service-level agreement
    b. MSDS
    c. Statement of work
    d. Master service agreement

26. Which of the following is used to define deliverables, schedules and time lines, and roles and responsibilities?

    a. Statement of work
    b. Memorandum of understanding
    c. Business plan
    d. PCI DSS

27. True or false: There can be multiple SOWs under one MSA.

    True

28. A master license agreement defines which of the following?

    a. The owner rights, terms, and conditions of the intellectual property
    b. How software can be used and distributed
    c. Licensing restrictions and the liabilities and/or penalties associated with violation
    d. All of the above are correct.
    e. None of the above are correct.

29. What is an NDA? (Select all that apply.)

    a. Neutral data agreement
    b. Non-disclosure agreement
    c. A legal agreement to bind a party or parties to not disclose or not share specific information
    d. A legal agreement to bind a party or parties to disclose but not share specific information

30. Which of the following are steps in an incident response plan? (Select all that apply.)

    a. Preparation
    b. Identification
    c. Containment
    d. Eradication
    e. Recovery
    f. Follow-up/lessons learned
    g. All of the above are correct.
    h. None of the above are correct.

31. What is the purpose of a password policy?

    It sets the rules on the computing passwords for the entire organization.

32. What is a password expiration time?

    It defines the duration for which a password is valid. This expiration time depends entirely on the organization; some prefer 120 days, some may prefer 6 months.

33. What is a privileged user agreement?

    It is an agreement that establishes expectations for the conduct of individuals granted privileged access to the organization's enterprise systems and services that may include computing systems, network, databases, data, user accounts and user processes.

34. What does an SOP define?

    A standard operating procedure (SOP) describes routine operations and step-by-step instructions of for performing them.

35. What is the purpose of role separation in computer networking?

    It is a practice of separating tasks and assigning them to different responsible groups or employees, thereby limiting full control of service or information and eliminating conflicts of interest.

Section 13-5

36. Which of the following is a metric that measures a system's reliability by identifying the average time between failures?

    a. MTTF
    b. MTBF
    c. MTTR
    d. All of the above are correct.
    e. None of the above are correct.

37. Which of the following is a metric that predicts the equipment runtime before a failure requires the equipment to be replaced?

    a. MTTF
    b. MTBF
    c. MTTR
    d. All of the above are correct.
    e. None of the above are correct.

38. Which of the following is a metric that measures the average time it takes to bring a system back from failure?

    a. MTTF
    b. MTBF
    c. MTTR
    d. All of the above are correct.
    e. None of the above are correct.

39. What type of backup includes all data that has changed since the last full backup?

    a. Full backup
    b. Partial backup
    c. Differential backup
    d. Incremental backup

e. All of the above are correct.

f. None of the above are correct.

40. Define high availability.

It refers to information technology systems being in continuous operation for a long time, with minimal downtime.

41. HA deployments have been widely applied to power management. Why is this?

Power creates a big disruption in business continuity. HA applied to power management might require supplying electrical power from two or more different sources or separate feeds from the electrical company, sometimes known as *redundant circuits*. Also to create power redundancy, a system can be connected to a backup power source such as a UPS (uninterruptible power supply) or battery backup.

42. What is a disaster recovery site?

A disaster recovery site is a site where mission-critical systems can be housed to bring an organization back up and running if a disaster occurs.

43. Which of the following types of disaster recovery sites is an empty facility with only power and cooling but no equipment or racks?

a. Cold site

b. Warm site

c. Hot site

d. Cloud site

44. Which of the following types of disaster recovery sites is a full-blown operational facility with power, cooling, and equipment racked and powered up, with network connectivity?

a. Cold site

b. Warm site

c. Hot site

d. Cloud site

Certification Questions

45. Which of these documents should be reviewed in preparation for an OSHA inspection? (Select all that apply.)

a. SDS

b. MOU

c. SLA

d. EAP

46. In IT, what does an acceptable use policy outline? (Select all that apply.)

    a. Use of Network
    b. Use of Break time
    c. Use of Annual leave
    d. Use of Internet
    e. Use of computer equipment

47. A network technician is setting up access for an HVAC technician to do maintenance in the server room. What safeguards need to be in place?

    a. Ensure that a guard is on duty.
    b. Make sure all servers are fully password protected.
    c. Make sure all monitors are turned off.
    d. Make sure the water lines are turned off.

48. Door access to an organization's server room is being scheduled. Which of the following are best practices for door access control? (Select all that apply.)

    a. Require a proximity reader.
    b. Require multiple keys.
    c. Use biometrics.
    d. Require key fobs.
    e. All of the above.

49. What is the name for a formal agreement between two or more parties to establish official service partnerships?

    An MOU, or memorandum of understanding

50. Which of the following is a critical component in avoiding accidents by identifying potential hazards?

    a. Fire extinguisher
    b. Exit route
    c. SDS/MSDS
    d. SLA
    e. None of the above

51. What policy informs users of proper system usage?

    Acceptable use policy (AUP)

This page intentionally left blank

GLOSSARY

? The help command, which can be used at any prompt in the command-line interface for the Cisco IOS software

10GBASE-T Twisted-pair copper capable of 10Gbps

3G/4G Third Generation and Fourth Generation, digital mobile phone technologies developed to provide broadband network wireless services

6to4 prefix A globally routable address that enables IPv6 hosts to communicate over the IPv4 Internet

802.1X An IEEE standard protocol for access control and authentication; also called dot1x

8P8C The proper term for an RJ-45 modular plug

A record (Address record) The most common record in DNS, which maps a hostname to an IP address

AAAA record (Quad-A record) A DNS record for IPv6

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

Access control Physical security measures such as access control cards, possibly biometric access control systems, and lockable fencing

Access control hardware Hardware used to identify and authenticate someone entering a facility

Access control list (ACL) A basic form of firewall protection

Access control vestibule/mantrap A control device that consists of two interlocking doors in which the first set of doors must be closed before the second set of doors can open

access-list permit Ip any any The instruction added to the last line of an access list to allow all other data packets to enter and exit the router

Access point A transceiver used to interconnect a wireless and a wired LAN

ACK Acknowledgment packet, a packet in the TCP three-way connection handshake

ACR A measurement that compares the signal level from a transmitter at the far end to the crosstalk measured at the near end

Active/active An architecture in which both the primary site and the disaster recovery site are up and running at the same time

Active/passive An architecture in which the disaster recovery site is idle, in standby mode

Adaptive cut-through A mode that is a combination of the store-and-forward and cut-through modes

Ad hoc network An independent network

Address Resolution Protocol (ARP) A protocol used to map IP addresses to MAC addresses

Administrative distance A feature used by routers to select the best path when more than one path is available

Administratively down An indication that the router interface has been shut off by an administrator

ADSL (Asymmetric DSL) A service that provides up to 1.544Mbps from the user to the service provider and up to 8Mbps back to the user from the service provider

Advertise To share route information

AES Advanced Encryption Standard, the encryption algorithm used by WPA2

Aging time The length of time a MAC address remains assigned to a port

AH Authentication Header, a security protocol that guarantees the authenticity of IP packets

Alien crosstalk (AXT) Unwanted signal coupling from one permanent link to another

Angled physical contact (APC) A green fiber connector whose endface is polished and has an 8-degree angle

Ant+ An ultra-low-power wireless protocol for wireless sensor networks operating at 2.4GHz

Anycast address An address obtained from a list of addresses

APIPA Automatic Private IP Addressing, a Windows process that automatically configures reserved private IP addresses and subnet masks

Application layer Layer 7 of the OSI model, which interacts with application programs that incorporate a communication component such as an Internet browser and email

Area 0 In OSPF, the root area, or backbone, for a network

Areas Smaller OSPF networks partitioned from a large OSPF network

ARIN American Registry for Internet Numbers, the North American organization that assigns IP addresses to ISPs and end users that are large enough to merit blocks of addresses

ARP cache Temporary storage of recently contacted MAC addresses

ARP cache poisoning An attack in which an attacker changes the MAC addresses of the ARP cache, or "poisons the ARP cache" so that conversations get redirected to the attacker

ARP Reply A network message that returns the MAC address

ARP table Another name for the ARP cache

ARPANET Advanced Research Projects Agency Network, the predecessor to today's Internet

AS Autonomous system; this is a group of networks or a large network that has a unified routing policy

ASN Autonomous systems number, a unique identifier that identifies a group of networks

Association An indication that the destination address is for a networking device connected to one of the ports on a bridge

Asymmetric operation Modem operation in which the data transfer rates to and from the service provider differ

Attenuation Also called insertion loss, the amount of loss in signal strength as it propagates down a wire or fiber strand

AUP Acceptable use policy, a policy that defines the constraints and practices the user must agree to in order to have access to a network

Authentication, authorization, and accounting (AAA) A framework for controlling access to computing resources, enforcing policies, and auditing usage

Auto-medium-dependent interface crossover (MDI-X) A feature that detects the crossover and changes its interface to MDI or MDI-X automatically

Auto-negotiation A process used by interconnected electronic devices to negotiate a link speed

Backbone The primary path for data traffic to and from destinations and sources in a campus network; the main fiber distribution for a network

Backbone cabling Cabling that interconnects telecommunications closets in the same building and between buildings

Backscatter The reflection of radio waves striking an RFID tag and reflecting back to the transmitter source

Badge reader A card reader that gathers information from a card or badge and searches an access control database to determine whether the user is allowed access to the premise

Balanced mode A mode in which neither wire in a wire pair connects to ground

Basic service set (BSS) An independent network

Beacon A radio link transmitted in WLAN systems so that a wireless user can identify an access point to connect to

Beamforming A technique used to direct transmission of a radio signal to a specific device

BGP Border Gateway Protocol is an exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet

Biometric systems Systems that measure and analyze specific characteristics of the human body for the purpose of authentication

BOOTP Bootstrap Protocol, a protocol that enables a computer to discover its own IP address

Bottlenecking Another term for network congestion

Bottom-to-top (or bottom-up) approach A network troubleshooting approach that starts from the application layer and works down to the physical layer

BPDU Guard An option that is used to prevent STP PortFast from receiving any BPDU message to modify the spanning tree topology

Bridge A networking device that uses MAC address information to forward data and interconnect LANs

Bridge protocol data unit (BPDU) A message unit that switches use to share information with other switches that are participating in Spanning Tree Protocol

Bridge table A list of MAC addresses and port locations for hosts connected to the bridge ports

Broadcast A data transmission sent to all connected devices

Broadcast domain A portion of a network in which any broadcast sent out on the network is seen by all hosts

Broadcast storm Excessive numbers of broadcasts

Brute-force attack An attack in which the attacker tries every possible combination of characters for the password

Buffer overflow A problem that occurs when a program tries to put more data into a buffer than it was configured to hold

Building entrance The point where the external cabling and wireless services interconnect with the internal building cabling

Bus topology A system in which the computers share the media (coaxial cable) for data transmission

BWA Broadband wireless access

BYOD Bring your own device, a policy that allows users to connect their own computing devices to a network

Cable modem A modem that can use the high bandwidth of a cable television system to deliver high-speed data to and from the service provider

Cache A block of memory that is set aside for temporary storage of information

Campus network A collection of two or more interconnected LANs in a limited geographic area

Carrier Ethernet An extension of the Ethernet infrastructure that covers much more than just a metropolitan area

CAT6 (category 6) Twisted-pair cable, capable of carrying up to 1000Mbps (1Gbps) of data up to a distance of 100 meters

CAT6a A UTP cable standard that supports 10Gbps data rates over a distance of up to 100 meters

CAT8 Shielded UTP capable of competing with fiber optics

CCIE Cisco Certified Internetwork Expert

CCMP Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, the key management protocol used by WPA2

CCNA Cisco Certified Network Associate

CCNP Cisco Certified Network Professional

CCTLD A country-code (cc) top-level domain

CDMA (code-division multiple access) A communications technology in which spread-spectrum techniques are used to multiplex more than one signal within a single channel

CFR Code of Federal Regulations

CHAP Challenge Handshake Authentication Protocol, an encrypted authentication method that uses the MD5 file hashing algorithm

CIDR Classless interdomain routing, specifies the number of network bits set to a 1 that make up the subnet mask

CIDR block The grouping of two or more class networks together; also called supernetting

Cisco IOS Cisco Internet Operating System, the operating software used in all Cisco routers

Cisco Network Assistant (CNA) A management software tool from Cisco that simplifies switch configuration and troubleshooting

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

Class network address The network portion of an IP address, based on the class of the network

Classes A, B, C, D, and E The five classes of IPv4 addresses

Classful Indicates that IP and subnet addresses are within the same network

Classful addressing Addressing that requires the network portion to be of Class A, Class B or Class C network

Client A computer connected to a network that accesses services from the server

Client/server network A network in which the server handles multiple requests from multiple clients for multiple services

Client-to-site VPN A VPN that provides mobile users a way to remotely access their information from a home network

Cloud Another name for the Internet

Cloud service or cloud computing An outsourced and hosted computing environment that delivers IT services to users via a network

Cloud site An offsite cloud storage or disaster recovery service provided by a cloud provider

CNAME (Canonical Name) record The Canonical Name record, used to specify that a domain name is an alias for another domain

Cold site An empty disaster recovery site with only power and cooling but no equipment or racks

Color map The specification of which wire color connects to each pin on a connector

Collision domain A network segment that has a shared media for interconnecting the devices

COM1, COM2, ... The computer's serial communication ports

Command-line interface (CLI) A type of interface used for inputting commands and configuring devices such as routers

Configuration BPDU A BPDU that switches use to elect the root switch

configure terminal (conf t) A command used to enter a router's or a switch's terminal configuration mode

Connection-oriented protocol A type of protocol that establishes network connections, manages the delivery of data, and terminates connections

Connectionless protocol A type of protocol that transports packets over the network without a connection being established and without any acknowledgment that the data packets arrived at the destination

Console cable A cable that connects a router's console port to a computer's serial port

Content-addressable memory (CAM) A table of MAC addresses and port mapping that a switch uses to identify connected networking devices

Contiguous networks Networks and routes that have the same class network address

Coordinated attack A type of distributed denial-of-service attack that is deliberately directed against a specific target and orchestrated by a controller source such as the command-and-control server in a botnet

copy running-configuration startup-configuration (copy run start) The command for copying the running configuration to the startup configuration

Core An independent processing unit, which is responsible for reading and executing program instructions

Country domain Usually two letters, such as .us (United States) or .ca (Canada), that indicate the domain server for a country

Cross-connect A space where one or multiple cables are connected to equipment or other cables

Crossover cable A cable in which the transmit and receive wire pairs are crossed to properly align the transmit signal on one device with the receive signal on the other device

Crosstalk Signal coupling in a cable

crypto key generate rsa A command used to generate an RSA key

CSMA/CA Carrier sense multiple access with collision avoidance, the Wireless LAN media access method

CSMA/CD Carrier-sense multiple access with collision detection, the Ethernet LAN media access method

CSU/DSU Channel service unit/data service unit, a device used with high speed serial connections

Cut-through A mode in which a data packet is forwarded to the destination as soon as the destination MAC address has been read

Data link layer Layer 2 of the OSI model, which handles error recovery, flow control (synchronization), and sequencing

DB-9 A 9-pin connector

DB-25 A 25-pin connector

DCE Data communications equipment, the serial interface responsible for clocking

Deauthentication attack An attack in which an attacker sends a frame to the wireless access point with

a spoofed address to make it look like it came from the victim, resulting in the access point disconnecting the victim's connection from the AP

Default gateway address The IP address of the networking device used to forward data that needs to leave the LAN

Delay skew A measure of the difference in arrival time between the fastest and the slowest signal in a UTP wire pair

Demilitarized zone (DMZ)/screened subnet An area of a network that is used to isolate servers

Denial-of-service (DoS) An attack in which service is denied to a computer, network, or server

Dense wavelength division multiplexing (DWDM) A system that incorporates the propagation of several wavelengths in the 1550 nm range for a single fiber

DES, 3DES Data Encryption Standard, Triple Data Encryption Standard

Desktop as a service (DaaS) A desktop virtualization service hosted by a cloud provider

Deterministic A type of network in which access to the network is provided at fixed time intervals

DHCP Dynamic Host Configuration Protocol, a protocol that assigns a pool of IP addresses to requesting clients

DHCP ACK A unicast packet sent back to a DHCP client with the same IP address information

DHCP Discover A broadcast message that is sent to all computers in a LAN

DHCP Offer A message of an available IP address from the address pool and other network settings sent by a DHCP server to the client

DHCP Request A message sent by a DHCP client to formally request and confirm the offered IP address with the server

DHCP snooping A feature that can be enabled to specify the trusted DHCP source where a switch blocks the DHCP messages from untrusted sources

Dictionary attack An attack that involves using known passwords and many variations (uppercase and lowercase and combinations) to try to log in to an account

Diffie-Hellman A key exchange algorithm that is used to generate a shared session secret key to encrypt the key exchange communications

Directed broadcast A broadcast that is sent to a specific subnet

Discrete multitone (DMT) A multicarrier technique used to transport digital data over copper telephone lines

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

Dispersion compensating fiber Fiber that acts like an equalizer, canceling dispersion effects and yielding close to zero dispersion in the 1550 nm region

Distance vector protocol A routing algorithm that periodically sends the entire routing table to its neighboring or adjacent router

Distributed feedback (DFB) laser A relatively stable laser that is suitable for use in DWDM systems

Divide-and-conquer approach A network troubleshooting approach that divides the OSI layers in half and starts at the middle of the stack, which is the network layer

DL Diode laser, the preferred light source for moderate-band to wideband fiber-optic communication systems

DKIM Domain Keys Identified Mail

DNS Domain Name System, the Internet's system for translating human-readable names to IP addresses and vice versa

DOCSIS Data Over Cable Service Interface Specification, an international standard that enables high-speed data transfers over the cable system

Domain registrar An organization that has control over the granting of domains within certain top-level domains

DS-0 to DS-3; T1 to T3 Common telecommunication data rates

DS Digital signal

DSL Digital Subscriber Line, a technology that uses existing copper telephone lines to carry data

DSSS Direct-sequence spread spectrum

DTE Data terminal equipment, the serial interface designed for connecting to a CSU/DSU and outside digital communication services

Dynamic assignment A process in which MAC addresses are assigned to a port when a host is connected

Dynamic routing protocol A protocol that dynamically updates a routing table to account for loss of or changes in routes or changes in data traffic

Dynamic VLAN A VLAN in which ports are assigned based on either the computer's MAC address or the username of the client logged on to the computer

EAP (1) Emergency action plan, a plan that facilitates and organizes employer and employee actions during workplace emergencies (2) Extensible Authentication Protocol, a protocol used in WPA, WPA2, and WPA3 by the client computer and the access point

Echo request The part of the ICMP protocol that requests a reply from a computer

EDGE Enhanced Data rates for GSM Evolution, a digital mobile phone technology that provides download speeds of 384Kbps

EIA Electronic Industries Alliance

EIGRP Enhanced Interior Gateway Routing Protocol, a Cisco-proprietary protocol that incorporates the best of the distance vector and link state algorithms

E-LAN service type (E-LAN) A service type that provides connectivity to two or more subscriber sites using the same EVC

Elasticity The ability of a cloud provider to dynamically grow or shrink the cloud resources to adapt to or match the workloads

E-Line service type (E-Line) A service type that provides a point-to-point Ethernet virtual connection between two UNIs

ELTCTL Equal level transverse conversion transfer loss of signal

EMI Electromagnetic interference, which originates from devices such as motors and power lines and from some lighting devices, such as fluorescent lights

enable A command used to enter a router's privileged mode

Endpoint PSE A PoE switch such as the source port on an Ethernet switch that connects to the PD

Enterprise network The network used by a large company

Entrance facilities (EF) Another name for the building entrance

Equipment room (ER) A room that contains complex electronic equipment such as network servers and telephone equipment

Error threshold The point at which the number of errors in the data packets has reached a threshold, and the switch changes from cut-through mode to store-and-forward mode

ESP Encapsulating Security Protocol, a security protocol that provides confidentiality to the data messages (payloads) by way of encryption

Ethernet address, physical address, hardware address, or adapter address Other names for the MAC address

Ethernet service definition An MEF framework that defines the Ethernet service types

Ethernet virtual connection (EVC) An association of two or more UNIs that essentially creates a logical path that connects two or more subscriber sites

E-Tree service type (E-Tree) A service type that provides a hub-and-spoke environment or a root-and-leaf environment

Event A disturbance in the light propagating down a fiber span that results in a disturbance on the OTDR trace

Evil twin An attack in which a rogue wireless access point poses as a legitimate one by broadcasting a legitimate SSID and eavesdrops on the wireless network

EXEC (privileged EXEC) password A password used to gain access to EXEC commands

Extended service set (ESS) A network with multiple access points to extend user mobility

F/UTP Foil over twisted-pair cabling, a higher grade of twisted-pair cable with foil over each of the four wire pairs

Factory reset A hard reset or a master reset that restores a device to the factory settings

Fast Ethernet An Ethernet system operating at 100Mbps

Fast Link Pulse (FLP) A burst that carries configuration information between the ends of a data link

FastEthernet port (FA0/0, FA0/1, FA0/2, ...) FastEthernet ports on a router

FERPA Family Educational Rights and Privacy Act, a federal law that requires all educational institutions to protect the privacy of student education records

FHRP First Hop Redundancy Protocol, a default gateway redundancy protocol

FHSS Frequency hopping spread spectrum, a technique in which the transmit signal frequency changes based on a pseudorandom sequence

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

Fiber cross-connect An optical patch panel used to interconnect fiber cables

Fiber, light pipe, or glass Terms used to describe a fiber-optic strand

Fibre Channel (FC) The original high-speed technology used to connect data storage to servers

Firewall Hardware or software used to protect a computer network

Firewall protection A type of protection used to prevent unauthorized access to a network

FISMA Federal Information Security Management Act, a federal law that was developed to protect government information, operations, and assets against security threats

Flat network A network in which the LANs share the same broadcast domain

Flooding A process that occurs when a switch doesn't have the destination MAC address stored in CAM and transmits a packet out all switch ports except for the port where the packet was received

Forward DNS lookup (forward lookup) Translation of a name to an IP address

FPP Fire prevention plan, a plan that is meant to prevent fires from occurring or spreading in a workplace

Frame A format that provides grouping of information for transmission

FTP File Transfer Protocol, standard protocol to transfer files.

FTTB Fiber-to-the-business, an optical architecture in which a fiber connection to a business provides for the delivery of all current communication technologies

FTTC Fiber-to-the-curb, an optical architecture that provides high bandwidth to a location with proximity to the home and provides a high-speed data link, via twisted-pair, using VDSL

FTTD Fiber-to-the-desktop, an optical architecture that requires a computer to have a fiber NIC

FTTH Fiber-to-the-home, an optical architecture that provides a fiber link to a home

Full channel All the link elements from a wall plate to a hub or switch

Full-duplex Refers to the capability to transmit and receive at the same time

Full IPv6 address An address in which all 32 hexadecimal positions contain a value other than 0

Fusion splicing A long-term splicing method in which two fibers are fused or welded together

Gateway A networking device that enables hosts in a LAN to connect to networks (and hosts) outside the LAN

Gateway of last resort The IP address of the router in a network to which data packets with unknown routes should be forwarded

GBIC Gigabit Interface Converter, a hot-swappable fiber-optic transceiver

GDPR General Data Protection Regulation, a European privacy law that protects personal data rights and restricts how personal data can be collected and used

Gigabit Ethernet 1000Mbps Ethernet

GLBA Gramm-Leach-Bliley Act, a federal law that requires all financial institutions to protect customer financial information data, to safeguard the financial information against security threats, and to deny any unwarranted access to financial data

Graded-index fiber Fiber in which the index of refraction is gradually varied with a parabolic profile

GRE Generic Routing Encapsulation, a tunneling protocol developed by Cisco for use as a site-to-site VPN solution

GTLD A generic (g) top-level domain

Guest machine A virtual computer

H.323 A VoIP protocol that uses port 1720

HA High availability, a critical concept for business continuity and disaster recovery that refers to information technology systems being in continuous operation for a long time, with minimal downtime

Half-duplex A mode in which a communications device can transmit or receive, but cannot do both at the same time

Hand-off The process in which a user's computer establishes an association with another access point

HDLC High-Level Data Link Control, a synchronous proprietary protocol

Hello packets Packets used with the OSPF protocol to verify that links are still communicating

Hex Hexadecimal, base 16

HIPAA Health Insurance Portability and Accountability Act, a federal law that requires all health-related agencies to protect the personal identifiable information (PII) of patients

Hopping sequence The order of frequency changes

Horizontal cabling Cabling that extends out from the telecommunications closet into the LAN work area

Horizontal cross-connect (HC) Also called the floor distributor (FD), the connection between the building distributors and the horizontal cabling to the work area or workstation outlet

Host address Another term for host number

Host machine A physical machine

Host number The portion of an IP address that defines the location of a networking device connected to the network; also called the host address

Hostname The name assigned to a networking device

Hot site A full-blown operational disaster recovery site with power, cooling, and equipment racked and powered up and connected to the network

Hotspot A limited geographic area that provides wireless access for the public

HSPA+ Evolved High-Speed Packet Access, a standard developed to provide network speeds comparable to those of LTE networks; theoretical speeds for download are 168Mbps and uplink 22Mbps

HSSI High-speed serial interface

HTTP Hypertext Transfer Protocol, standard web browsing protocol using TCP port 80

HTTPS Hypertext Transfer Protocol Secure is a secure and encrypted HTTP using TCP port 443

Hub A device that broadcasts the data it receives to all devices connected to its ports

HVAC Heating, ventilation, and air conditioning, systems that are critical for computing and data centers

Hybrid echo cancellation circuit A circuit that removes the transmitted signal from the receive signal

Hyper-V A virtualization program that's part of the Windows operating system

Hypervisor This provides a virtual machine monitor (VMM) for managing and controlling the underlying physical hardware and associated virtual hardware

IANA Internet Assigned Numbers Authority, an organization that governs IP address assignment and Internet domain names

IC fibers Interconnect fibers

ICANN Internet Corporation for Assigned Names and Numbers

ICMP Internet Control Message Protocol, a protocol which verifies that messages are being delivered

IDC Intermediate distribution closet

IEEE Institute of Electrical and Electronics Engineers, one of the major standards-setting bodies for technological development

IEEE 802.3an-2006 10GBASE-T The standard for 10Gbps

IETF Internet Engineering Task Force

IGMP Internet Group Management Protocol, a protocol used for multicasting

IKE Internet Key Exchange, a hybrid protocol that encompasses several key management protocols

IMAP Internet Message Access Protocol, mail protocol using TCP port 143

in-addr.arpa The reverse DNS lookup for IPv4 addresses on the Internet

Incident response policy A policy that describes a computer security incident handling plan to manage risk and minimize adverse effects

Inbound data traffic Data traffic entering a network

Index-matching gel A jellylike substance that has an index of refraction much closer to that of glass than to that of air

InfiniBand (IB) A technology that provides high performance and high throughput with low latency

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

Infrastructure as a service (IaaS) A service that focuses on the facilities and infrastructure in the data center and the virtualization and abstraction layer that exists on top of the physical facilities and infrastructure

Inquiry procedure A process used to determine whether other Bluetooth devices are available

.int An intergovernmental domain registry

Intermediate cross-connect (IC) Also called the building distributor (BD), the building's connection point to the campus backbone, which links the MC to the horizontal cross-connect (HC)

Internet layer The layer of the TCP/IP model that defines the protocols used for addressing and routing data packets

Internet Protocol (IP) A protocol that defines the addressing used to identify the source and destination addresses of data packets being delivered over an IP network

Intranet An internal network that provides file and resource sharing but that is not accessed from the Internet

Intrusion detection system (IDS) and intrusion prevention system (IPS) Systems that identify misuse and anomalies on a network

IoT Internet of Things, a network of smart devices that are connected to the Internet

IP address A unique 32-bit address that identifies on which network a computer is located and differentiates the computer from all other devices on the same network

ip helper A router command that is used to enable a router's DHCP relay function

IP internetwork A network that uses IP addressing for identifying devices connected to the network

ip route The router configuration command for manually setting the next hop IP address

IP tunnel A secure VPN connection between two endpoints that encapsulates an IP packet in another IP packet

IPAM IP address management, a process used for managing IP address space in a network that integrates DHCP and DNS and ensures that each service is aware of changes, thereby avoiding conflicts with IP user space

ipconfig A command used to display a computer's address

ipconfig /all A command that enables the MAC address information to be displayed from the command prompt

ipconfig /release A command used to release the current IP address

ipconfig /renew A command used to initiate the DHCP process

IPng IP Next Generation

IPsec IP Security, a protocol that encrypts each packet prior to transmission across the network link

IPv4 Internet Protocol version 4, the IP version currently being used on the Internet

IPv6 IP version 6

IPX Internetworking Packet Exchange, a networking protocol developed by Novell

ISAKMP Internet Security Association and Key Management Protocol

iSCSI Internet Small Computer Systems Interface, a technology that enables the SCSI protocol to communicate over IP networks

IS-IS Intermediate System-to-Intermediate System, a link state protocol used in many service provider core networks

ISM band Industrial, scientific, and medical band

Isolating the collision domains Breaking a network into segments, where a segment is a portion of the network where the data traffic from one part of the network is isolated from the other networking devices

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

ISP Internet service provider, an organization that provides Internet connections and services to individuals and organizations

Jamming A problem in which a wireless network is overwhelmed with wireless traffic, thereby preventing authorized users from accessing the network

Keepalive packet A packet which indicates that the Ethernet interface is connected to another networking device, such as a hub, switch, or router

L2F Layer 2 Forwarding Protocol, a Cisco protocol that does not require any VPN client software

L2TP Layer 2 Tunneling Protocol, an IETF protocol created to merge two incompatible proprietary tunneling protocols, PPTP and L2F

Last mile The last part of the connection from the telecommunications provider to a customer

Layer 2 switch An improved network technology that provides a direct data connection for network devices in a LAN

Layer 3 network Another name for a routed network

LCL Longitudinal conversion loss

LDAP Lightweight Directory Access Protocol, standard directory protocol using TCP port 389

LDAPS LDAP over SSL, a secure and encrypted LDAP protocol using TCP port 636

LEAP (Lightweight Extensible Authentication Protocol) A wireless security system used by Cisco

Lease time The amount of time that a client can hold an IP address

LED Light-emitting diode, a light source used in fiber-optic communication systems that operate at a slower bit rate and require more modest levels of fiber-coupled optical power

Line of demarcation The point where ownership of telecommunications equipment changes from the telecommunications carrier to the user

Line password A password used to gain access to a router

Link The point from one cable termination to another

Link integrity test A test used to verify that a communication link has been established between two Ethernet devices

Link light An indicator on a switch or hub that shows whether the transmit and receive pairs are properly aligned

Link-local address An address that is designed to be used for and is limited to communications on the local link

Link pulses Pulses sent by two connected devices via twisted-pair cables when data is not being transmitted to indicate that the link is still up

Link state advertisement (LSA) An announcement of updated link state information when routes change

Link state protocol A type of protocol that establishes a relationship with a neighboring router and uses route advertisements to build routing tables

Local area network (LAN) A network of users that share computer resources in a limited area

Locking cabinet A cabinet that can lock to protect critical equipment and documents

Locking rack A rack that can lock to protect critical equipment for an IT facility

Logical address The IP address location of a network and the address location of a host in a network

Logical fiber map A map that shows how fiber is interconnected and data is distributed throughout a campus

Logging A process that enables an administrator to analyze the events that occur and use the information uncovered to correlate and find the issues

Long haul Refers to transmission of data over hundreds or thousands of miles

Loopback A mechanism by which data is routed directly back to the source

LTE/4G Long Term Evolution/Fourth Generation, a wireless communications standard that is designed to provide up to 10 times the speed of 3G networks

MAC address Media access control address, a unique 6-byte address assigned by the vendor of a network interface card

Macrobending Loss due to light breaking up and escaping into the cladding

Main cross-connect (MC) Also called the main distribution frame (MDF) or main equipment room or campus distributor (CD), an area that usually connects two or more buildings and is typically the central telecommunications connection point for a campus or building

Malware Malicious software

Managed switch A switch that enables a network administrator to monitor, configure, and manage select network features

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

Mbps Megabits per second

MD5 Message Digest 5, a hashing algorithm

Mechanical splice A splice in which two fibers are joined together with an air gap, requiring an index-matching gel to provide a good splice

Media converter A device used to adapt a layer 1 (physical layer) technology to another layer 1 technology

Mesh topology A topology in which all networking devices are directly connected to each other

Metro Ethernet Forum (MEF) A nonprofit organization that defines Metro/Carrier Ethernet specifications

Metro Optical Ethernet (MOE) An extension of the Ethernet infrastructure via optical technologies beyond the internal network infrastructure

mGRE Multipoint GRE, a protocol that can be used to enable one node to communicate with many nodes

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

Midspan (midpoint) PSE A PoE switch that is used to provide power to a PD when a powered Ethernet port is not available

MIMO Multiple-input multiple-output, a space-division multiplexing technique in which the data stream is split into multiple parts called spatial streams

MLA Master license agreement, an agreement that defines the owner rights, terms, and conditions related to intellectual property

mm Multimode

Modal dispersion The broadening of a pulse due to the different path lengths through the fiber taken by different modes

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

Motion detection The use of devices that can detect changes in the position of an object as it relates to its surroundings

MOU Memorandum of understanding, a formal agreement between two or more parties to establish official service partnerships

MSA Master service agreement, an overarching document that creates a framework for multiple service-level agreements

MSDS Material safety data sheets, an older term for SDS

MT ACK Message type acknowledgment, a DHCP ACK packet

MT Discover Message type discover, a DHCP Discover packet

MT Offer Message type offer, a DHCP offer packet

MT Request Message type request, a DHCP request packet

MTBF (mean time between failures) A metric that measures a system's reliability by identifying the average time between failures

MTTF (mean time to failure) A metric that predicts the equipment runtime before a failure requires the equipment to be replaced

MTTR (mean time to recover or repair) A metric that measures the average time it takes to bring a system back from failure

MTU Maximum transmission unit

Multicast Describes a message sent to a specific group of hosts on a network

Multicast address An address that is used to send multicast data packets

Multicasting A process in which one host sends data to many destination hosts

Multihomed Having more than one Internet connection

Multilayer switch (MLS) A switch that operates at layer 2 but functions at higher layers

Multilevel encoding A technique used to reduce the bandwidth required to transport data

Multimode fiber A fiber that supports many optical waveguide modes

Multiplexed Combined data packets for transport

Multiport bridge Another name for a layer 2 switch

Multiport repeater Another name for a hub

Multitenancy The ability of multiple users to share the same cloud provider resources

MU-MIMO Multiuser MIMO, use of MIMO technology with eight spatial streams

MX (Mail Exchange) record The Mail Exchange record, which points to the incoming email servers of an organization

NAS Network attached storage, a file-level storage device that can be accessed on a network

NCP Network Control Protocol

NDA Non-disclosure agreement, a legal agreement that protects confidential information, proprietary information, intellectual property, or trade secrets

Near-end crosstalk (NEXT) A measure of the level of crosstalk or signal coupling within a cable, with a high NEXT (dB) value being desirable

NET In IS-IS, the Network Entity Title, an address that is unique to each router

netstat -a A command used to display the IP ports currently open on the Windows operating system

netstat -b A command that shows the executable involved in creating a connection or a listening port

netstat -r A command used to obtain the routing table for a host PC computer

Network address A layer 3 address

Network address translation (NAT) A technique used to translate an internal private IP address to a public IP address

Network congestion A slowdown in network data traffic movement

Network interface card (NIC) The electronic hardware used to interface a computer to a network

Network interface layer The layer of the TCP/IP model that defines how a host connects to a network

Network layer Layer 3 of the OSI model, which accepts outgoing messages and combines messages or segments into packets, adding a header that includes routing information

Network number The portion of an IP address that defines which network an IP packet is originating from or being delivered to

Network slowdown Degraded network performance

Next hop address The IP address of the next networking device that can be used to forward a data packet to its destination

NFPA National Fire Protection Association, an organization that works closely with OSHA to create standards and codes to help create safe environments and to prevent accidents

NLOS Non-line-of-sight

nmap A Linux port scanner

no shutdown (no shut) A command that enables a router's interface

NOC Network operations center

Non-Internet-routable IP address An IP address that cannot be routed on the Internet

NS record (Name Server record) A record that specifies the name of the authoritative name server of the domain

nslookup and dig Commands that query the specified DNS server and retrieve the requested records associated with the domain name provided

NTP Network Time Protocol, a protocol that can be set up to synchronize the router's clock with the time server

Numerical aperture A measure of a fiber's ability to accept light

Numerics Numerical representations

NVP Nominal velocity of propagation

OC Optical carrier

OFDM Orthogonal frequency division multiplexing, a technique that involves dividing the signal bandwidth into smaller subchannels and transmitting the data over these subchannels in parallel

Offboarding A policy or process related to terminating employee access or decommissioning a device from a production system

On-path attack (man-in-the-middle attack) An attack in which an attacker gets in the middle of a conversation between others in order to become the recipient of all information sent by victim computers

Onboarding A policy or process related to how a new employee or device is brought into an organization's IT systems

Open Authentication A null authentication that can enable any client to authenticate to an access point

Optical Ethernet Ethernet data running over a fiber link

Optical link budget A set of calculations used to verify that the proper received signal level (RSL) is received.

Optical spectrum Light frequencies from the infrared on up

Optical time-domain reflectometer (OTDR) A device that sends a light pulse down fiber and measures the reflected light, providing a measure of performance for the fiber

Organizationally unique identifier (OUI) The first 3 bytes of the MAC address, which identifies the manufacturer of the network hardware

OSH Act Occupational Safety and Health Act, 1970 legislation that created the Occupational Safety and Health Administration

OSHA Occupational Safety and Health Administration, an organization created to oversee and enforce safety standards in the workplace

OSI model Open Systems Interconnection model, a seven-layer model that describes network functions

OSPF Open Shortest Path First, a dynamic link state routing protocol that is supported by many vendors

OSPFv3 Open Shortest Path First version 3, the new OSPF version for IPv6

Outbound data traffic Data traffic leaving a network

Outsource To obtain goods or services from an outside source in place of an internal source

Overloading A process that involves translating a home network's private IP addresses to a single public IP address

Packet filtering Protection in which a limit is placed on the information that can enter the network

Packet shaper A device that sits between a campus network and an outside network that is configured with a set of rules that are used to prioritize data traffic for shaping the bandwidth

Packet sniffing An attack technique that involves watching the contents of data packets

Paging procedure A process used to establish and synchronize a connection between two Bluetooth devices

Pairing Setting up a Bluetooth device to connect to another Bluetooth device

PAP Password Authentication Protocol, a simple plaintext (unencrypted) authentication method that has been superseded by CHAP

Passkey A passphrase used in Bluetooth security to limit outsider access to pairing

Password cracking An attack in which the attacker tries to guess a user's password

Password policy A policy that sets the rules on the computing passwords for an entire organization

Patch cable A cable used to make a physical connection from a computer to a wall plate

PCI DSS Payment Card Industry Data Security Standard, a standard set by the Payment Card Industry that holds banks and merchants accountable for any credit card breach

PD Powered device

PDU Protocol data unit, information that is exchanged among the different layers of the OSI model

Peer A computer that uses and provides resources to a network

Peer-to-peer network A network in which all the computers provide similar services, including server functions

Penetration testing Testing that evaluates the security of a network

Permanent DoS (PDoS) A malicious attack that aims to sabotage hardware and render it useless

Physical access control device A device that is used to make sure personnel or visitors have adequate permission to access various facilities

Physical fiber map A map that shows the routing of fiber and also shows detail about the terrain, underground conduit, and entries into buildings

Physical layer Layer 1 of the OSI model, which provides the electrical and mechanical connection to the network

Physical layer cabling The media interconnecting networking devices

Piconet An ad hoc network of up to eight Bluetooth devices

ping A command that is used to test that a device on a network is reachable

Platform as a service (PaaS) A service that focuses on application development on any desired platform utilizing cloud computing

PoE+ A newer version of PoE, based on IEEE 802.3at

Point of presence (POP) The point where a customer connects network data traffic to a telecommunications carrier

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

Port A physical input/output interface to networking hardware

Port address translation (PAT) A technique that translates many IP addresses into a single public IP address or a handful of public IP addresses

Port-based VLAN A VLAN in which host computers connected to specific ports on a switch are assigned to a specific VLAN

Port forwarding (or port mapping) An application of NAT in which packets from one IP address/port number are redirected to another

Power over Ethernet (PoE) A technology developed to supply power over CAT5 or better network cabling

PPP Point-to-Point Protocol, the de facto protocol of dial-up networking

PPTP Point-to-Point Tunneling Protocol, a protocol developed jointly by Microsoft, 3Com, and Alcatel-Lucent that was designed to work in conjunction with PPP

Prefix length notation A shorthand technique for writing a subnet mask where class boundaries are not being crossed

Presentation layer Layer 6 of the OSI model, which accepts and structures the messages for the application

Private addresses IP addresses set aside for use in private intranets

Privileged mode A mode that enables configuration of router ports and routing features

Privileged user agreement An agreement that establishes expectations for the conduct of individuals granted privileged access to an organization's enterprise systems and services that may include computing systems, network, databases, data, user accounts, and user processes

Propagation delay A measure of the amount of time it takes for a signal to propagate from one end of a cable to the other

Protocol A set of rules established for users to exchange information

Protocol-based VLAN A VLAN in which connection to ports is based on the protocol being used

Proxy server A setup in which clients go through a proxy to communicate with secure systems

PSAACRF Power-sum alien attenuation to crosstalk ratio

PSANEXT Power-sum alien near-end crosstalk

PSE Power sourcing equipment

Pseudorandom A number sequence that appears random but actually repeats

PTR record (Pointer record) A record that maps an IP address to a hostname

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

Radio frequency identification (RFID) A technique that uses radio waves to track and identify people, animals, objects, and shipments

RADIUS Remote Authentication Dial-In User Service, a type of authentication that helps prevent unauthorized users from connecting to a network

range A command that makes it easier to apply the same security policy on a group of switch ports

Range extender A device that relays the wireless signal from an access point or wireless router into areas with a weak signal or no signal at all

Ranging A technique that cable modems use to determine the time it takes for data to travel to the cable headend

RAS Remote access server, a server that provides a way for an outside user to gain access to a network

RDP Remote Desktop Protocol port 3389

Received signal level (RSL) The input signal level to an optical receiver

Recovery Point Objective (RPO) The amount of data loss an organization can afford or tolerate in the event of an outage

Recovery Time Objective (RTO) The maximum downtime an organization can afford or tolerate to maintain its business continuity

Reflective/amplified DoS attack An attack that is carried out using spoofing and that is a combination of a reflection attack and an amplification attack

Refractive index The ratio of the speed of light in free space to its speed in a given material

Remote access VPN A VPN that is used to facilitate network access for users in remote office networks or remote users who travel a lot and need access to the network

Resistive power discovery The process of looking for devices that support PoE and have a 25kΩ resistor connected between the transmit and receive pairs

Return loss A measure of the ratio of power transmitted into a cable to the amount of power returned or reflected

Reverse DNS lookup (reverse lookup) Translation of an IP address to a name

RIP Routing Information Protocol; this is a dynamic routing protocol, which means the routers periodically exchange routes. RIP is classified as a distance vector protocol, and it uses router hop count as the metric

RIPng Routing Information Protocol Next Generation, a protocol used for RIP routing using IPv6

[rip_tag] A tag that is used to identify the RIP process

RIR Regional Internet registry, one of five organizations that are responsible for IP address allocation

RJ-45 The 8-pin modular connector used with CAT6/5e/5 cable

Roaming The term used to describe a user's ability to maintain network connectivity while moving through the workplace

Role-based access control (RBAC) Authorization based on a user's role and responsibilities

Rollover cable A cable with the signals reversed at each end

Root DNS servers A group of servers that use well-known IP addresses that have been programmed into DNS servers

Root Guard An STP feature that allows participation in spanning tree and BPDU messages as long as the attached device does not attempt to become the root bridge

Route flapping A situation in which intermittent routes go up and down, creating excessive LSA updates

route print A command used to obtain the routing table for a host PC computer

Routed network A network that uses layer 3 addressing for selecting routes to forward data packets

Router interface The physical connection where a router connects to a network

router ospf [process id] The command used to enable OSPF routing

Router uptime The amount of time a router has been running

Router# The prompt for a router's privileged EXEC mode

Router(config)# The prompt for a router's terminal configuration mode

Router(config-if)# A prompt which indicates that you are in the router's interface configuration mode

Router(config-line)# A prompt that indicates that you are in the router's line configuration mode

Routing loop A situation in which data is forwarded back to the router that sent the data packets

Routing table A table that keeps track of the routes to use for forwarding data to its destination

Routing table code C The router code for specifying a directly connected network

Routing table code S The router code for a static route

RR Resource record; defines the domain, its subdomains, and its host information

RS-232 A serial communications port

RSL Received signal level

RX Abbreviation for receive

SAN Storage area network, block-level data storage across a network

Sanitize device Wipe all information from a device

SC, ST, FC, LC, MT-RJ Typical optical fiber connectors

Scalability The ability of a system to expand the number of users and authentication

Scattering An attenuation factor caused by refractive index fluctuations, which accounts for 96% of attenuation loss

SDS Safety data sheets, documents that provide workers and emergency personnel with procedures for handling chemicals in a safe manner

Secure address An address with which a switch port automatically disables itself if a device with a different MAC address connects to the port

Serial port (S0/0, S0/1, S0/2, ...) The serial ports on a router

Service set identifier (SSID) A name that is used to identify a wireless network and is used by an access point or wireless router to establish an association

Session hijacking An attack that exploits web session control by stealing a session cookie and using it to establish a session with a remote server that thinks the session is valid

Session layer Layer 5 of the OSI model, which provides the control functions necessary to establish, manage, and terminate the connections

SFP Small form-factor pluggable

SFTP Secure File Transfer Protocol, one of the two main protocols available for secure FTP transfers

SHA Secure Hash Algorithm, a secure hash algorithm that includes cryptographic algorithms and secure protocols for the protection of sensitive, unclassified information

Shared-key authentication A type of authentication in which the client and the access point share a key called a pre-shared key (PSK)

show flash A command that lists the details of a router's flash memory

show ip interface brief (sh ip int brief) A command used to verify the status of a router's interfaces

show ip protocol (sh ip protocol) The command that displays the routing protocol running on the router

show ip route (sh ip route) The command that displays the routes and the routing address entries into the routing table

show ip route static (sh ip route static) The command that limits the routes displayed to only static ones

show running-config (sh run) The command that displays the router's running configuration

show startup-config (sh start) The command that displays the router's startup configuration

show version A command that lists the version of the Cisco IOS software running on the router

Single-mode fiber Fiber cables with core diameters of about 7–10 µm, in which light follows a single path

SIP Session Initiation Protocol, standard Voice over IP protocol using TCP/UDP ports 5060 and 5061

Site survey A process used to determine the best location(s) for placing the access point(s) to provide maximum RF coverage for wireless clients

Site-to-site VPN A VPN that is used to create a virtual link from one site to the other and essentially replaces the traditional WAN-type connection used in connecting typical sites

SLA Service-level agreement, a formal agreement typically between a service provider and a client or an end user, that defines the level of service expected from the service provider

Slotted Aloha A wireless network communications protocol technique similar to the Ethernet protocol

sm Single-mode

Smart device A device that is networkable and connected to the Internet

Smart doorbell A doorbell that can connect to the Internet and that can notify a user when someone is at the door

Smart locker A storage location that contains technology that can notify a user that a package or document is ready, provide access instructions, and send status notifications

Smart speaker A wireless speaker with an integrated voice assistant

SMB Server Message Block, Microsoft file sharing protocol using TCP port 445

SMTP Simple Mail Transfer Protocol, standard send mail protocol using TCP port 25

SNMP (SNMPv1) Simple Network Management Protocol (version 1), a connectionless protocol that uses UDP for the transmission of data to and from UDP port 161

SNMPv2 Simple Network Management Protocol version 2

SNMPv3 Simple Network Management Protocol version 3

SOA Start of Authority, a mandatory resource record for a zone that marks the start of the zone and provides the technical details of the zone

Social engineering A process by which an intruder obtains enough information from people to gain access to a network

Software as a service (SaaS) A service that focuses on application delivery

SOHO Small office/home office

SONET/SDH Synchronous Optical Network/ Synchronous Digital Hierarchy; protocol standards for optical transmission in long-haul communication

SOW Statement of work, a document often used in conjunction with an MSA that defines in detail the deliverables, schedules, and time lines, roles and responsibilities, and price agreed by all parties

Spanning Tree Protocol (STP) A link management protocol that prevents looping and controls data flow over possibly redundant data paths

SPF Sender Policy Framework

Spoof To insert a different IP address in place of an IP packet's source address to make it appear that a packet came from another network

Spot-the-difference approach A network trouble-shooting approach in which a comparison between working and non-working network environments or configurations is made

SRV Record (Service Record) A record that is used to identify a host (or hosts) that offers a specific type of service

SSH Secure Shell, a network protocol for securing services over an unsecured network

Standard operating procedure (SOP) A procedure document that describes the routine operations accompanied by step-by-step instructions for how to perform them

Star topology The most common networking topology in today's LANs, where all networking devices connect to a central switch or hub

Stateful firewall A type of firewall that keeps track of the data packet flow

Stateful packet inspection (SPI) A type of firewall that inspects incoming data packets to make sure they correspond to an outgoing request

Stateless address autoconfiguration (SLAAC) An IPv6 technique that enables serverless basic network configuration of IPv6 computers

Static assignment A process in which a MAC address has been manually assigned to a switch port

Static route A data traffic route that has been manually entered into either a router's or a computer's routing table

Static VLAN A port-based VLAN, with assignments created when ports are assigned to a specific VLAN

sticky A command option that causes the configured MAC address to appear in the running configuration of the switch and be saved in the startup configuration

Store-and-forward A mode in which an entire frame of data is received before any decision is made regarding forwarding the data packet to its destination

STP Shielded twisted-pair

Straight-through cable A cable in which the wire pairs in the cable connect to the same pin numbers on each end

STS Synchronous Transport Signal, an electrical signal used for transporting data in a fiber-optic transmission system

Stubby area An area that does not accept routes from the Internet

Subnet mask A number that identifies the network/subnet portion of an IP address

Subnet, NET A network segment

Supernetting A technique that allows multiple contiguous classful networks to be combined into one larger network

Surveillance Monitoring that often includes cameras watching a facility and the perimeter as well as notification systems such as sensors for intrusion detection

Switch A device that forwards a frame it receives directly out the port associated with its destination address

Switch latency The amount of time a data packet takes from the time it enters a switch until it exits

Switch port security (or port security) Switch commands used to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port

switch# The prompt for a switch's privileged EXEC mode

Switch(config)# The prompt for a switch's terminal configuration mode

Switch(config-line)# A prompt which indicates that you are in the switch's line configuration mode

SYN Synchronizing packet, a packet in the TCP three-way connection handshake

SYN ACK Synchronizing acknowledgment packet, a packet in the TCP three-way connection handshake

T568A Wire color guidelines specified in the TIA/EIA 568-A standard

T568B Wire color guidelines specified in the TIA/EIA 568-B standard

Tag-based VLAN A VLAN in which the VLAN ID is based on 802.1Q

TCL Transverse conversion loss

TCO Telecommunications outlet, the wall plate where the fiber or twisted-pair cable terminates in a room

TCP Transmission Control Protocol, Layer 4 protocol

TCP/IP Transmission Control Protocol/Internet Protocol, the protocol suite used for internetworks such as the Internet

TCTL Transverse conversion transfer loss

Telco The local telephone company

Telco cloud The telecommunications carrier's switched network, which is used to transport data to its destination; also, the interconnected networks on the Internet

Telecommunications closet The location of the cabling termination points that includes the mechanical terminations and the distribution frames

Telecommunications room (TR) Another name for the telecommunications closet

Telnet A virtual terminal connection that uses port 23

Terminated Describes where a cable connects to a jack in a wall plate, a patch panel, or an RJ-45 modular plug

Testing A procedure for evaluating a physical security system

TFTP Trivial File Transfer Protocol, UDP port 69

TIA Telecommunications Industry Association

TIA/EIA 568-B The standard that defines the six subsystems of a structured cabling system

TKIP Temporal Key Integrity Protocol, a protocol that provides key management for WPA

TLD Top-level domain

Token passing A technique in which an electrical token circulates around a network, and control of the token enables the user to gain access to the network

Token Ring hub A hub that manages the passing of the token in a Token Ring network

Token Ring network A network topology configured in a logical ring that complements the token passing protocol

Top-to-bottom (or top-down) approach A network troubleshooting approach that starts at the physical layer of the OSI model and works up to the application layer

Topology The architecture of a network

Topology Change Notification (TCN) A packet used to indicate that there has been a change in the switch

Topology Change Notification Acknowledgment (TCA) An acknowledgment from another switch that the TCN has been received

Totally stubby area An area that uses only a default route to reach destinations external to the autonomous system

Transceiver A transmit/receive unit

Translation bridge A bridge that is used to interconnect two LANs that are operating two different networking protocols

Transparent bridge A bridge that interconnects two LANs running the same type of protocol

transport input none A command that prevents remote access to the console port via reverse Telnet

Transport layer Layer 4 of the OSI model, which is concerned with message integrity between source and destination

Transport layer protocol A type of protocol that defines the type of connection established between hosts and how acknowledgments are sent

Tunable laser A laser in which the fundamental wavelength can be shifted a few nanometers, which is ideal for traffic routing in DWDM systems

TX Abbreviation for transmit

TXT record (Text record) A record that is used to hold arbitrary text information for the domain

Type 1 hypervisor A hypervisor that is loaded directly on hardware to abstract the hardware to the virtualization layer; commonly used on servers

Type 2 hypervisor A hypervisor that is loaded on an operating system and abstracts the virtualization layer through its host operating system and that's commonly used on personal computers

Type 5 A protection scheme that uses an MD5 hash for encryption

Type 7 A protection scheme that uses a Cisco encryption algorithm

UDP User Datagram Protocol

Unicast A transmission in which a packet has a fixed destination

Unicast address An address that is used to identify a single network interface address, with data packets sent directly to the computer that has the specified IPv6 address

U-NII Unlicensed National Information Infrastructure

Ultra-physical contact (UPC) A blue fiber connector whose endface is polished and has no angle

Uplink port A port that allows the connection of a switch to another switch without requiring a crossover cable

User EXEC mode A router mode that enables a user to check the router status

User mode Another term for user EXEC mode

User–Network Interface (UNI) The demarcation point between customer equipment and a service provider

UTP Unshielded twisted-pair

V.44/V.34 The standard for all analog modem connections with a maximum data rate of up to 34Kbps; V.44 provides improved data compression, smaller file sizes that provide faster file transfers, and improved web browsing

V.92/V.90 The standard for a combination analog and digital modem connection with a maximum data rate of 56Kbps; V.92 provides a quick-connect feature that cuts down on negotiation and handshake time compared to V.90

Variable-length subnet mask A subnet mask that better fits the needs of a network, thereby minimizing the waste of IP addresses when interconnecting subnets

Variable-length subnet masking (VLSM) A process in which routes can be configured using different subnet masks

Vertical cavity surface emitting laser (VCSEL) A laser that offers the simplicity of an LED and the performance of a laser

Virtualization A technology concept that involves creating a virtual computer

Virus A piece of malicious computer code that, when opened, can damage your hardware, software, or other files

Visual fault locator (VFL) A device that shines light down fiber to help locate broken glass

VLAN (virtual LAN) A group of host computers and servers that are configured as if they are in the same LAN, even if they reside across routers in separate LANs

VM Virtual machine, a virtual computer that lives inside a physical machine

VMM Virtual machine manager, software for managing and controlling the underlying physical hardware and associated virtual hardware

vMotion, XenMotion, Live Migration Different vendor options for moving a virtual machine to another host server in the event of a physical server failure

VPN Virtual private network, an extension of a private or trusted network over public infrastructure like the Internet; a secure network connection that helps protect a LAN's data from being observed by outsiders

VPN headend A device that handles multiple VPN connections (VPN tunnels) into a network

War chalking A process that involves leaving marks or symbols on the premises, outside the premises, or online to notify other hackers about the wireless vulnerabilities of the location

War driving A process in which attackers search for locations with open or weak wireless networks, so that they can gain more access to the network and collect information or data from connecting users

Warm site A not-yet-operational disaster recovery site with power, cooling, and rack space

Well-known ports Ports reserved by ICANN

WEP Wired Equivalent Privacy, a password protected security wireless protocol

Wide area network (WAN) A network that uses the telecommunications network to interconnect sites that are geographically distributed throughout a region, a country, or the world

Wi-Fi A term created and which is a trademark of the Wi-Fi Alliance to reference Wireless networks

Wi-Fi Alliance An organization that tests and certifies wireless equipment for compliance with the 802.11*x* standards

Wildcard bits The inverse mask bits used to match network IP addresses to interface IP addresses

WiMAX Worldwide Interoperability for Microwave Access, a broadband wireless system based on the IEEE 802.16e standard

Wire speed routing A situation in which data packets are processed as quickly as they arrive

Wired network A network that uses cables and connectors to establish network connections

Wireless network A network that uses radio signals to establish network connections

Wireless router A device used to interconnect wireless networking devices and to give access to

wired devices and establish the broadband Internet connection to the ISP

Wiremap A graphical or text description of the wire connections from pin to pin

Wireshark A protocol analyzer

WLAN Wireless local area network

Work area The location of computers and printers, patch cables, jacks, computer adapter cables, and fiber jumpers

Work area outlet (WO) Also called the telecommunications outlet (TO), the workstation used to connect devices (for example, PCs, printers, servers, phones, televisions, wireless access points) to the cable plant, typically with CAT5, CAT5e, CAT6, CAT6a, CAT7, CAT8, and various coaxial cables

Worm A type of virus that attacks computers, typically proliferates by itself, and can deny service to networks

WPA Wi-Fi Protected Access, a protocol that replaced WEP for securing wireless transfers

write memory (wr m) The command that saves configuration changes to memory

xDSL A generic representation of the various DSL technologies that are available

XENPAK, XPAK, X2, XFP, SFP+ 10 Gigabit interface adapters

Zero-day attack An exploit against a software vulnerability that is unknown to the developer

Zero-dispersion wavelength The point at which dispersion is zero

Z-Wave A wireless communications protocol developed for the home and garage access controls

INDEX

Symbols

? (help) command, 367

Numbers

3DES (Triple Data Encryption Standard), 651
3G wireless standard, 204
4G wireless standard, 204
4G/LTE, 204
5G wireless standard, 204
6to4 prefix, 335
8P8C connectors, 70–71
10BASE2 cabling, 41
10BASE5 cabling, 41
10BASE-FL cabling, 41
10BASE-T cabling, 41
10GBASE-LR cabling, 41
10GBASE-SR cabling, 41
10GBASE-T cabling, 41, 76, 97–98
AXT, 98
full-duplex transmissions, 100
F/UTP, 99
hybrid echo cancellation circuits, 100
IEEE 802.3an-2006, 98
performance, 100–101
PSAACRF, 98, 99
PSANEXT, 98, 99
signal transmission, 100–101
29 CFR 1910.1200 (Hazard Communication), 716
29 CFR 1910.157 (Portable Fire Extinguishers), 712–713
29 CFR 1910.160 (Fixed Extinguishing Systems), 713–714
29 CFR 1910.164 (Fire Detection Systems), 714–715
29 CFR 1910.165 (Employee Alarm Systems), 715–716
29 CFR 1910.36 (Design and Construction Requirements for Exit Routes), 709–710
29 CFR 1910.37 (Maintenance, Safeguards, and Operational Features for Exit Routes), 710
29 CFR 1910.38 (Emergency Action Plans), 710–711
29 CFR 1910.39 (Fire Prevention Plans), 711–712
32-bit CPU architectures, 679
40GBASE-T cabling, 41
64-bit CPU architectures, 679
100BASE-FX cabling, 41
100BASE-SX cabling, 41
100BASE-TX cabling, 41
802.1x (dot1x) wireless standard, 633
802.11 wireless standard, 175–176
ad hoc networks, 176, 177
AP, 177–178
BSS, 176, 177, 178
channel bonding, 179
CSMA/CD, 178
DSSS, 179
ESS, 178
FHSS, 180
frequency channels, 179
hand-offs, 178
hopping sequences, 180
ISM band, 179
MAC layer, 176
OFDM, 180
Open Authentication, 638
PHY layer, 176
pseudorandom numbering sequences, 180
roaming, 178
shared-key authentication, 638
transceivers, 177
transmit power, 180
WMN, 176
802.11a (Wi-Fi 2) wireless standard, 24, 180–181, 183
802.11ac (Wi-Fi 5) wireless standard, 24, 182, 183
802.11ax (Wi-Fi 6) wireless standard, 25, 182, 183
802.11b (Wi-Fi 1) wireless standard, 24, 181, 183
802.11g (Wi-Fi 3) wireless standard, 24, 181, 182, 183
802.11i wireless standard, 183
802.11n (Wi-Fi 4) wireless standard, 24, 181, 182, 183
802.11r wireless standard, 183
802.16a (WiMAX) wireless standard, 200
1000BASE-LX cabling, 41
1000BASE-SX cabling, 41
1000BASE-T cabling, 41

A

A records (Address records), 541–542
AAA (Authentication, Authorization, Accounting) frameworks, 623–624
AAAA records (Quad-A records), 545
A.B.C.D. values, 20–21
absorption, fiber-optic cabling, 136
access
BWA, 199–200
CDMA, 204

controlling, detection methods, 661–662
motion detection, 662
surveillance cameras, 662
controlling, physical security, 659, 660–661
access control vestibules (mantraps), 661
badge readers, 661
biometric scanners, 661
locking cabinets, 661
locking racks, 661
door access, 717
home access, home networks, 31
HSPA+204
NAC, 624
network access management, 623–624
public access, home networks, 31
RAS, 647
RBAC, 623
remote access security, 642
analog modems, 643–644
cable modems, 644
RAS, 647
xDSL modems, 644–646
routers, 626–628
TACACS+624
WPA, 215, 639
WPA2, 639–640
WPA3, 640
access control vestibules (mantraps), 661
access points (AP), 177–178, 186–187, 189–190
evil twin attacks, 598
home networks, 28
troubleshooting, 213
access/edge layer, LAN, 269
access-list permit ip any any command, 617
accounting, AAA framework, 623–624
ACK (Acknowledgement) packets, 297
ACL (Access Control Lists), 617–618
ACR (Attenuation to Crosstalk Ratios), 93, 95
PSAACRF, 98, 99
PSACR, 93, 95, 96
active/active disaster recovery architectures, 731
active/passive disaster recovery architectures, 731
active RFID tags, 202
ad hoc networks, 176, 177
adapter addresses. *See* MAC addresses
adaptive cut-through mode, switches, 247
addresses
adapter addresses. *See* MAC addresses
anycast addresses, 335
broadcast addresses, subnetting, 322
class network addresses, 467
classful addresses, 317, 467
DAD, 337
Ethernet addresses. *See* MAC addresses
gateway addresses, 265, 326–327, 359–361
HA, 302
hardware addresses. *See* MAC addresses
IPv4 addressing, 20, 312–313
6to4 prefix, 335
A.B.C.D. values, 20–21
APIPA, 532, 533
ARIN, 315
assigning, 315, 529–530
class network addresses, 467
classes, 313
classful addresses, 317
decimal/binary octets, 314
default gateway addresses, 359–361
dual stacks, 336
host IP addresses, 315
host numbers, 21
lease time, 532
managing with DHCP, 531–537
network/host bits, 314–315
network numbers, 21, 482
next hop addresses, 362
non-Internet-routable IP addresses, 316
Office LAN, 40
overloading, 35
private IP addresses, 21–22, 316
public IP addresses, 22
RIR, 315
structure of, 313
switches, 245
TCP/IP, 21–22
transitioning to IPv6, 335–337
wildcard bits, 482–483
IPv6 addressing, 333–335
6to4 prefix, 335
anycast addresses, 335
CIDR, 337–338
DAD, 337

defined, 333
dual stacks, 336
interface (host) identifiers, 335
IPng, 333
link-local addresses, 335, 336–337
multicast addresses, 335
routing, 499
routing, BGP, 501–502
routing, EIGRP, 501
routing, OSPF, 500–501
routing, RIP, 499–500
routing, static, 499
SLAAC, 336–337
transitioning to, 335–337
unicast addresses, 335
link-local addresses, 335, 336–337
logical addresses, 249
MAC addresses
CAM, 246
defined, 18
destination MAC addresses and sources, 17
filtering, 33
length of, 18
NIC, 18
Office LAN, 40
OUI, 18
sampling of, 18
spoofing attacks, 635
sticky command option, 634
multicast addresses, 303, 335
NAT, 34
defined, 34
private IP addresses, 34–35
public IP addresses, 35
NET addresses, 479
network addresses, 249, 322
next hop addresses, 362
PA, 301
physical addresses. *See* MAC addresses
secure addresses, switches, 243
unicast addresses, 335, 533
administrative distance, 461
administratively down, 390
ADSL (Asymmetric DSL), 645–646
advertising, routes, 466
AES (Advanced Encryption Standard), 640
aging time, 244
AH (Authentication Headers), 651
air interface (communications) portal, RFID tags, 203
alarms, CSU/DSU, 272
analog modems
asymmetric operations, 643
security, 643–644
V.44/V.34 modem standard, 643
V.92/V.90 modem standard, 643
analyzing network traffic, 552–565
ANDing, subnet masks, 361–362
ANT+ wireless technology, 183
antennas
dish (parabolic reflector) antennas, 209
EIRP, 210
multipoint distributions, 209–211
omnidirectional antennas, 208–209
placement of, point-to-multipoint WLAN case study, 207
ranges (wireless), extending, 214
remote installations, 211
RF site surveys, 209–211
selecting, 208–209
site surveys, 207
spatial diversity, 186
Yagi antennas, 209
antivirus/anti-malware software, 610–611
anycast addresses, 335
AP (Access Points), 177–178, 186–187, 189–190
evil twin attacks, 598
home networks, 28
troubleshooting, 213
APC connectors, 64, 146
APIPA (Automatic Private IP Addressing), 532, 533
appearance, home networks, 31
Application layer
OSI model, 13, 14
TCP/IP, 294, 295–296
applications (common) and port numbers, 295–296
Area 0, OSPF, 482
areas, OSPF, 477
ARIN (American Registry for Internet Numbers), 315, 529
ARP (Address Resolution Protocol), 301–303, 563
bridges, 233–235
caches, 233–235
caches, poisoning, 598
DAI, 635

expired entries, 235
replies, 563–564
spoofing attacks, 635
ARPANET (Advanced Research Projects Agency Network), 292
assembling Office LAN, 38–39
cabling, 40–43
client/server networks, 42–45
diagramming networks, 39–40
IP addressing, 40
MAC addresses, 40
network device connections, 40–43
peer-to-peer networks, 42, 43
asset disposal, 662
asset/inventory management, 728
assigning
IP addressing, 529–530
IPv4 addresses, 315
protocols, 529
associations, LAN interconnections, 233
associations, wireless connections, 186–187, 193
asymmetric operations, modems, 643
attacks, network security
ARP cache poisoning, 598
botnets, 608
brute-force attacks, 596
buffer overflow attacks, 599–600
coordinated DDoS attacks, 608
DDoS attacks, 608–609
deauthentication/disassociation attacks, 608
dictionary attacks, 596
directed broadcasts, 607
DoS attacks, 606–609
evil twin attacks, 598
intrusion attacks, 594–604
logic bombs, 604
malware, 602–604, 610–611
on-path attacks (man-in-the-middle attacks), 598
packet sniffing attacks, 597–599
password cracking attacks, 596–597
PDoS attacks, 607
ransomware attacks, 604
reflective/amplified DoS attacks, 608
session hijacking, 599
social engineering attacks, 595–596
software vulnerabilities, 599–604
spoofing attacks, 607, 635
viruses, 602–603, 610–611
VLAN hopping, 599
worms, 603
zero-day attacks, 604
attenuation (insertion loss), 92, 93–94
ACR, 93, 95
fiber-optic cabling, 127, 136–137, 142
PSAACRF, 98, 99
PSACR, 93, 95, 96
audits, IT, 728
AUP (Acceptable Use Policies), 725
authentication
AAA framework, 623–624
AH, 651
CCMP, 639–640
CHAP, 649, 650
deauthentication/disassociation attacks, 215
EAP, 640, 650
Kerberos, 623
LEAP, 640
MD5 hashing algorithm, 649, 650
Open Authentication, 638
PAP, 649–650
RADIUS, 624, 640
SHA, 649, 650
shared-key authentication, 638
authorization, AAA framework, 623–624
auto-negotiation, 383–386
AS (Autonomous Systems), 529
auxiliary input, routers, 250
AXT (Alien Crosstalk), 98

B

backbone
backbones
cabling, 67, 155
defined, 477
backscatter, 200
backups, 729–730
badge readers, 661
balanced mode, 74–75
bandwidth
fiber-optic cabling, 126
metrics, 461
multilevel encoding, 100

BD (Building Distribution) fiber, optical networking, 151–154
beacons, 638
beamforming, 182
best practices
asset/inventory management, 728
backups, 729–730
configuration standards, 727–728
documentation, 727
HA, 730–731
IT audits, 728
role separation, 728
BGP (Border Gateway Protocol), 496–498, 501–502
BiDi (Bidirectional) transceivers, 154
binary numbers
binary-to-decimal conversions, 306–307
decimal-to-binary conversions, 307–309
IPv4 addressing, 314
biometric scanners, 661, 717
BLE (Bluetooth Low Energy) technology, 197
blocked TCP/UDP ports, troubleshooting, 573
blocking state, STP, 423
Bluejacking, 641
Bluesnarfing, 641
Bluetooth
BLE technology, 197
enabling connections, 198–199
inquiry procedures, 197
output power classes, 197
paging procedures, 197
piconets, 197–198
security, 641
BNC connectors, 64
bonding, channel (Ethernet), 179
BOOTP (Bootstrap Protocol), 531
botnets, 608
bottlenecking (network congestion), 76, 252
bottom-to-top (bottom-up) troubleshooting approach, 569
BPDU (Bridge Protocol Data Units), 422–423
BPDU Filter, 636
BPDU Guard, 635–636
branching devices, 142
bridges
advantages/disadvantages of, 236
ARP caches, 233–235
associations, 233
broadcasts, 233
defined, 232
MAC addresses, 232–234
multiport bridges. *See* layer 2 switches
ports, 232–233
translation bridges, 235
transparent bridges, 235
wireless bridges, 187–189, 236
broadband modems/gateways, 28
broadcast addresses, subnetting, 322
broadcast domains, 246, 358
broadcasts
bridges, 233
broadcast storms, 233
defined, 9
directed broadcasts, 607
SSID broadcasts, turning off, 33
brute-force attacks, 596
BSS (Basic Service Sets), 176, 177, 178
buffer overflow attacks, 599–600
buffering/queuing, 252
building distributions, optical networking, 151–154
building entrances, structured cabling, 66–67
bus topologies, 8–9
business policies/procedures, 723
asset/inventory management, 728
AUP, 725
backups, 730
best practices, documentation, 727
configuration standards, 727–728
continuity/recovery policies/procedures, 729
MTBF, 729
MTTF, 729
MTTR, 729
HA, 730–731
incident response policies, 725
IT audits, 728
MLA, 724
MOU, 723–724
MSA, 724
NDA, 725
onboarding/offboarding policies, 727
password policies, 726
privileged user agreements, 726
role separation, 728
SLA, 724

SOP, 726–727
SOW, 725
business policies/procedures. ***See also*** **rules/regulations**
BWA (Broadband Wireless Access), 199–200
BYOD (Bring Your Own Device), 568

C

cabinets, locking, 661
cable modems
home networks, 28, 29
security, 644
cabling
8P8C connectors, 70–71
10BASE2 cabling, 41
10BASE5 cabling, 41
10BASE-FL cabling, 41
10BASE-T cabling, 41
10GBASE-LR cabling, 41
10GBASE-SR cabling, 41
10GBASE-T cabling, 41, 76, 97–98
AXT, 98
full-duplex transmissions, 100
F/UTP, 99
hybrid echo cancellation circuits, 100
IEEE 802.3an-2006, 98
performance, 100–101
PSAACRF, 98, 99
PSANEXT, 98, 99
signal transmission, 100–101
40GBASE-T cabling, 41
100BASE-FX cabling, 41
100BASE-SX cabling, 41
100BASE-TX cabling, 41
1000BASE-LX cabling, 41
1000BASE-SX cabling, 41
1000BASE-T cabling, 41
attenuation (insertion loss), 92, 93–94
backbone cabling, 67
balanced mode, 74–75
CAT5, patch cabling, CAT5, assembling, 87–90
CAT5e, test examples, 104–109
CAT6 cabling, 40
certification, 93–96
channel specifications, 93–96
coaxial cabling, 64
console cabling, 250, 255
crossover cabling, 41–42, 83
crosstalk, 94
ELFEXT, 93, 95
Ethernet LAN cabling, numerics, 41
Fast Ethernet, 76
fiber-optic cabling
absorption, 136
advantages of, 126–127
APC connectors, 146
attenuation (insertion loss), 127, 136–137
attenuators, 142
backbones, 155
bandwidth, 126
BD fiber, 151–154
branching devices, 142
building distributions, 151–154
campus networks, 154–157
chromatic dispersion, 137–138
cladding, 130
color-coding fiber, 156
components of, 126, 141–142
connectorization, 145–146
cores, 130
corrosion, 127
costs, 127
crosstalk, 127
CWDM, 142
detectors, 143–145
DFB lasers, 141
diplexers, 154
dispersion, 137–139
dispersion compensation, 139
dispersion shifted fibers, 138–139
DL, 141
DWDM, 130, 141
electrostatic interference, 126
Ethernet, 157
events, troubleshooting, 162
FC connectors, 145–146
fiber, 142
fiber Bragg grating, 139
fiber cross-connects, 151
fiber selection, 132–133
fiber-to-the-home/business, 130
FTTB, 149

FTTC, 149
FTTD, 149
FTTH, 149
fusion splicing, 144
GBIC, 152–153
glass, 142
graded-index fiber, 132, 133–134
IC fibers, 152
IDC, 152–153
index-matching gel, 144
IR (Infrared) radiation, 126
isolators, 142
LC connectors, 145–146
LED, 141
light pipes, 142
link budgets, 157–158
logical fiber maps, 154, 155
mechanical splicing, 144–145
microbending, 136–137
mm fibers, 155
modal dispersion, 137–138
mode field diameters, 134–135
MT-RJ connectors, 145–146
multimode fiber, 130, 132
numerical apertures, 131
optical connectors, 126
optical Ethernet, 149–150
optical networking, defined, 148–151
optical spectrum, 130–131
optical-line amplifiers, 143
OTDR, 162–163
photosensitive detectors, 126
physical fiber maps, 154, 156
polarization mode dispersion, 137, 139
pulse dispersions, 132–133
refraction of light, 129
refractive indexes, 129
RSL, 142
safety, 127, 160–161
SC connectors, 145–146
scattering, 136
security, 127
SFP, 152–153
SFP+153–154
"shooting the fiber", 162
single-mode fibers, 130, 134–135
sm fibers, 155
splitters, 142
ST connectors, 145–146
step-index fiber, 133
strands, 131–132
transceivers, 154
transmission strands, 126
troubleshooting, 162–163
tunable lasers, 141–142
"two-deep" rule, 152–153
unconnected fibers, 146
UPC connectors, 146
VCSEL, 141
VFL, 162
WDM, 130, 143
X2, 153–154
XENPAK, 153–154
XFP, 153–154
XPAK, 153–154
zero dispersion wavelengths, 138–139
full channels, 92
full-duplex cabling, 76
F/UTP, 99
Gigabit Ethernet, 76
HC, 68, 69
horizontal cabling, 67, 69–73, 83–87
hybrid echo cancellation circuits, 100
IC, 68, 69
links, 92
managing, 67
manufacturer's specifications, 102–104
MC, 68, 69
multilevel encoding, 100
NEXT, 92, 93, 94–95
patch cabling, 71–72, 82
performance, 110
physical layer cabling, 64
10 Gigabit Ethernet over Copper, 97–101
APC connectors, 64
BNC connectors, 64
cable testing/certification, 92–96
connectors, 64
fiber couplers, 64
structured cabling, 66–73
troubleshooting, 102–110
twisted-pair cabling, 74–77

twisted-pair cabling, terminating, 78–90
UPC connectors, 64
UTP couplers, 64
PSELFEXT, 93, 95, 96
PSNEXT, 93, 94
RJ-45 connectors, 40, 70–71, 75
rollover cabling, 255–256
STP cabling, 76–77
straight-through cabling, 82, 87–90
structured cabling
backbone cabling, 67
building entrances, 66–67
ER, 67
HC, 68, 69
horizontal cabling, 67, 69–73
IC, 68, 69
MC, 68, 69
STP cabling, 76–77
TCO, 67
telecommunications closets, 67, 69–70
TIA/EIA 568-A cabling standard, 66
TIA/EIA 568-B cabling standard, 66
TIA/EIA 569B cabling standard, 66–67
UTP cabling, 74–76
WO, 68
work areas, 67
T568A wiring standard
color maps, 78–80
defined, 78
pinouts, 79
T568B wiring standard
color maps, 78–80
defined, 78
pinouts, 79
TCO, 67
termination, 70
testing, 92–93
ACR, 93, 95
attenuation (insertion loss), 92, 93–94
channel specifications, 93–96
delay skew, 93, 96
ELFEXT, 93, 95
near-end testing, 94
NEXT, 92, 93, 94–95
propagation delay, 93, 96
PSACR, 93, 95, 96
PSELFEXT, 93, 95, 96
PSNEXT, 93, 94
Thin/Net cabling, bus topologies, 8
troubleshooting, 102
connectivity, 110
DTX-1800 certification reports, 103, 104
failures to meet manufacturer specifications, 102–104
multimeters, 110
performance, 110
stretching, 102
twisted-pair cabling
ELTCTL, 99
F/UTP, 99
LCL, 99
return loss, 93, 95–96
STP cabling, 76–77
TCL, 99
TCTL, 99
terminating, 78–80
UTP cabling, 74–76
UTP cabling, 76
CAT3, 75, 76
CAT5, 74, 75, 76
CAT5, patch cabling, 87–90
CAT5, straight-through cabling, 87–90
CAT5e, 74, 75, 76, 79–82
CAT5e, patch cabling, 87–90
CAT5e, straight-through cabling, 87–90
CAT5e, test examples, 104–109
CAT6, 74, 75, 76, 79–82, 83–87
CAT6a, 75, 76
CAT7, 74, 75, 79–82
CAT7a, 75
CAT8, 74, 75, 79–82
UTP, F/UTP, 99
wiremaps, 82
WLAN, troubleshooting, 215
WO, 68
work areas, 67
cache poisoning, ARP, 598
caches, virtualization, 679
CAM (Content-Addressable Memory), 246
cameras
IP security cameras, 662
surveillance, 662

campus networks
backbones, 477
defined, 230
hierarchical topologies, 69
optical networking, 154–157
CAN (Campus Area Networks), 5
captive portals, home networks, 32
Carrier Ethernet, 273–274
CAT3
twisted-pair cabling, 75
UTP cabling, 76
CAT5
patch cabling, 87–90
straight-through cabling, 87–90
UTP cabling, 74, 75, 76
CAT5e
patch cabling, 87–90
straight-through cabling, 87–90
test examples, 104–109
UTP cabling, 74, 75, 76, 79–82
CAT6
cabling, 40
horizontal cabling, terminating, 83–87
UTP cabling, 74, 75, 76, 79–82
CAT6a, UTP cabling, 75, 76
CAT7
STP cabling, 76–77
UTP cabling, 74, 75, 79–82
CAT7a, UTP cabling, 75
CAT8
STP cabling, 76–77
twisted-pair cabling, 75, 79–82
UTP cabling, 74
CBS (Committed Burst Size), 276
CCMP (Cipher Mode with Cipher Block Chaining Message Authentication Code Protocol), 639–640
ccTLD, 528
CDMA (Code-Division Multiple Access), 204
cellular (mobile) communications, 204
3G wireless standard, 204
4G wireless standard, 204
5G wireless standard, 204
CDMA, 204
EDGE, 204
geofencing, 204
HSPA+204
LTE/4G, 204
NFC, 204
certification
cabling, 93–96
DTX-1800 certification reports, 103, 104
CFR (Code of Federal Regulations), 709
change management policies, 624
changing
factory passwords, 33
SSID, 33
channel bonding, 179
channel specifications, cabling, 93–96
channel utilization (WLAN), troubleshooting, 214–215
CHAP (Challenge Handshake Authentication Protocol), 649, 650
check sequences, frames, 17
chromatic dispersion, 137–138
CIDR (Classless Interdomain Routing), 329
blocks, 330–331
IPv6 addressing, 337–338
notation, 329
subnet mask conversions, 329–330
CIR (Committed Information Rates), 276
Cisco, remote client VPN configurations, 653–657
cladding, fiber-optic cabling, 130
class network addresses, 467
classes, IPv4 addressing, 313
classful addresses, 317, 467
client/server networks, 42–45
client-to-site VPN, 648
cloud computing, 693–694
advantages/disadvantages of, 695–696
cloud services, 692–693
community clouds, 696
CSP, 696
DaaS, 695
defined, 692
elasticity, 696
email, 693
hybrid clouds, 696
IaaS, 694
infrastructures, 696–697
multitenancy, 695, 696
outsourcing, 692
PaaS, 695

private clouds, 696
public clouds, 696
SaaS, 695
scalability, 695–696
SDN, 696–697
security, 697
SLA, 693
cloud sites, disaster recovery, 731
CM-54 Beasley-Networking Essentials, 6e, 9780137455928, 5
CNA (Cisco Network Assistant), switches, 242–243
CNAME records (Canonical Name Records), 542–543, 693
coaxial cabling, 64
cold sites, disaster recovery, 731
cold/hot" aisles, 73
collision domains, isolating, 246
collisions, switches, 433
color maps, T568A/T568B wiring standards, 78–80
color-coding, fiber-optic cabling, 156
command prompt, Windows 10, 18
common applications and port numbers, 295–296
communications (air interface) portal, RFID tags, 203
community clouds, 696
compatibility (wireless), troubleshooting, 213
computer forensics, 621
configuration standards, 727–728
configure terminal (conf t) command, 374, 411
configuring (setting up)
BGP, 496–498
computers for LAN operation, 44
EIGRP, 488–494
FastEthernet interfaces, 376–377
firewalls, 611–617
interfaces, auto-negotiation, 383–386
IP addressing, switches, 245
OSPF, 481–485
PuTTY software, 256–259
routers
Privileged EXEC mode (Router#), 380–381
User EXEC mode (Router>), 369–371
SLAAC, 336–337
SNMP, 547–551
static routing, 454–458
static VLAN, 414–418
switches, 410, 419–420
configure terminal (conf t) command, 411
enable secret command, 412
hostname command, 411–412
line console passwords, 412–414
privileged mode, 411, 412
static VLAN configurations, 414–418
switch# prompt, 412
switch(config)# prompt, 411, 412
switch(config-line)# prompt, 413
VLAN subinterfaces, 418–419
virtualization, 682–690
WLAN, 185–195, 206–211
congestion (bottlenecking), networks, 76, 252
connection-oriented protocols, 297
connectivity
networks
home networks, 32
verifying with ping command, 240–241
ZTerm serial communications software, 259–261
troubleshooting, 110
connectorization, fiber-optic cabling, 145–146
connectors
8P8C connectors, 70–71
APC connectors, 64
BNC connectors, 64
DB-9 connectors, 254–255
DB-25 connectors, 254, 255
fiber couplers, 64
RJ-45 connectors, 70–71, 75, 255
UPC connectors, 64
UTP couplers, 64
console cabling, 255
console input/cabling, 250
console ports, routers
console cabling, 255
DB-9 connectors, 254–255
DB-25 connectors, 254, 255
PuTTY software, 256–259
RJ-45 connectors, 255
rollover cabling, 255–256
RS-232 serial communications ports, 254, 255
serial interfaces, 256
ZTerm serial communications software, 259–261
content filters, 620

contiguous networks, 467
continuity/recovery policies/procedures, 729
MTBF, 729
MTTF, 729
MTTR, 729
controllers, wireless, 189
controlling access, physical security, 659, 660–661
access control vestibules (mantraps), 661
badge readers, 661
biometric scanners, 661
locking cabinets, 661
locking racks, 661
convergence, dynamic routing protocols, 460
conversion loss, cabling
ELTCTL, 99
LCL, 99
TCL, 99
TCTL, 99
converting numbers
binary-to-decimal conversions, 306–307
decimal-to-binary conversions, 307–309
hexadecimal numbers, 309–311
coordinated DDoS attacks, 608
copper, 10GBASE-T cabling, 97–98
AXT, 98
full-duplex transmissions, 100
F/UTP, 99
hybrid echo cancellation circuits, 100
IEEE 802.3an-2006, 98
performance, 100–101
PSAACRF, 98, 99
PSANEXT, 98, 99
signal transmission, 100–101
copy running-configuration startup-configuration (copy run start) command, 457
core layer, LAN, 268
cores
fiber-optic cabling, 130
virtualization, 679
corrosion, fiber-optic cabling, 127
costs
fiber-optic cabling, 127
home networks, 30
metrics, 461
country domains, 539
couplers
fiber couplers, 64
UTP couplers, 64
CRC (Cyclic Redundancy Checksum) errors, 432
cross-connects
defined, 68, 69
fiber cross-connects, 151
HC, 68, 69
IC, 68, 69
MC, 68, 69
WO, 68
crossover cabling, 41–42, 83
crosstalk, 94
ACR, 93, 95
AXT, 98
fiber-optic cabling, 127
PSAACRF, 98, 99
PSACR, 93, 95, 96
crypto key generate rsa command, 628
CSMA/CD (Carrier-Sense Multiple Access/Collision Domains), 16, 178
CSP (Cloud Service Providers), 696
CSU/DSU (Channel Service Units/Data Service Units), 272
cut-through mode, switches, 247
CWDM (Coarse Wavelength Division Multiplexing), 142

D

DaaS (Infrastructure as a Service), 695
DAD (Duplicate Address Detection), 337
DAI (Dynamic ARP Inspection), 635
DARPA (Defense Advanced Research Projects Agency), 292
data, frames, 17
data centers
architectures, 269
“hot/cold” aisles, 73
racks
diagrams, 72
locks, 73
data channels, interconnecting LAN, 270–271
Data link layer, OSI model, 13
data packets
ACK packets, 297
ARP packets, 302–303

DHCP packets, 534
error thresholds, 247
filtering, 618
FTP data packets, 566–567
hello packets, 477
ICMP source-quench packets, 302
IGMP packets, 303–304
keepalive packets, 388
shaping, 253, 620
sniffing attacks, 597–599
SYN ACK packets, 297
SYN packets, 297
TCP packets
terminating connections, 299–300
transmitting, 298
UDP packet transfers, 300–301
WEP, 638–639
wire speed routing, 247
data rates
DS-0 to DS-3, 270
E1 to E3, 271
T1 to T3, 270
data speeds, home networks, 30
data transmissions, long hauls, 134
DB-9 connectors, 254–255
DB-25 connectors, 254, 255
DDoS (Distributed DoS) attacks, 608–609
deauthentication/disassociation attacks, 215, 608
decimal numbers
binary-to-decimal conversions, 306–307
decimal-to-binary conversions, 307–309
IPv4 addressing, 314
default gateways
addresses, 359–361
static routing, 448
delay metrics, 461
delay, propagation, 93, 96
delay skew, 93, 96
demarcation, lines of, 271
DES (Data Encryption Standard), 651
Design and Construction Requirements for Exit Routes (29 CFR 1910.36), 709–710
desktops, virtual vs remote, 695
destination MAC addresses and sources, defined, 17
detection methods, 661–662
motion detection, 662
surveillance cameras, 662
detectors, fiber-optic cabling, 143–145
deterministic networks, 7
device density, 189
DFB (Distributed Feedback) lasers, 141
DHCP (Dynamic Host Configuration Protocol)
data packets, 534
deploying, 535–537
DHCP ACK, 532
DHCP Discover, 532
DHCP Offer, 532
DHCP Request, 532
IP address management, 531–537
snooping, 572
troubleshooting, 216, 571–572
diagramming networks, 39–40
dialup modems, 644
dictionary attacks, 596
differential backups, 730
Diffie-Hellman key exchange, 651
dig command, 541
diplexers, 154
directed broadcasts, 607
disabled state, STP, 423
disassociation/deauthentication attacks, 215, 608
disaster recovery
active/active architectures, 731
active/passive architectures, 731
cloud sites, 731
cold sites, 731
hot sites, 731
policies/procedures, 729
MTBF, 729
MTTF, 729
MTTR, 729
RPO, 732
RTO, 732
sites, 731
virtualization, 681
warm sites, 731
dish (parabolic reflector) antennas, 209
dispersion, fiber-optic cabling, 137–138
dispersion compensation, 139
dispersion shifted fibers, 138–139

disposal of assets, 662
distance vector protocols, 463
hop count metrics, 463–464
RIP, 465
configuring, 466–468
IPv6, 499–500
link state protocols and, 477
[rip_tag] tags, 500
route configuration, 468–473
sh run command, 471–472
show ip protocol (sh ip protocol) command, 469–471
RIPv2, 474–475
configuring, 466–468
route configuration, 473–474
routing loops, 465
distance, WLAN, 189–190
distribution/aggregation layer, LAN, 269
divide-and-conquer troubleshooting approach, 569
DKIM (Domain Keys Identified Mail), 544
DL (Diode Lasers), 141
DMT (Discreet Multitone) modulation, 645–646
DMZ (Demilitarized Zones), 618
DNS (Domain Name Systems), 539
dig command, 541
forward DNS lookups, 539
nslookup command, 541
reverse DNS lookups, 539
root DNS servers, 539–540
RR, 541–546
tree hierarchies, 539–540
DOCSIS (Data Over Cable Service Interface Specification), 644
documentation
AUP, 725
best practices, 727
change management policies, 624
incident response policies, 725
MLA, 724
MOU, 723–724
MSA, 724
MSDS, 716
NDA, 725
onboarding/offboarding policies, 727
password policies, 726
privileged user agreements, 726
SDS, 716
security, 624
SLA, 724
SOP, 726–727
SOW, 725
domain names, managing, 528
domain registrars, 530
dongles, 682
door access, 717
doorbells, smart, 663
DoS (Denial-of-Service) attacks, 606–609
dot1x (802.1x) wireless standard, 633
down, administratively, 390
DS (Digital Signals), 270
DS-0 to DS-3 data rates, 270
DSL (Digital Subscriber Lines)
ADSL, 645–646
modems, home networks, 29–30
services, 645
xDSL
modems, 644–646
services, 645
DSSS (Direct-Sequence Spread Spectrum), 179
DTLS (Datagram Transport Layer Security) protocol, 598
DTX-1800 certification reports, 103, 104
dual stacks, 336
duplex operations. *See* building distributions
DWDM (Dense Wavelength Division Multiplexing), 130, 141
dynamic (private) ports, 295
dynamic assignments, 243
dynamic routing protocols, 460, 461
convergence, 460
load balancing, 460
metrics, 460, 461
path determination, 460
dynamic VLAN, 408

E

E1 to E3 data rates, 271
EAP (Emergency Action Plans), 710–711
EAP (Encryption Authentication Protocol), 640, 650
ease of implementation, home networks, 31
EBS (Excess Burst Size), 276
echo requests, 564–565

EDGE (Enhanced Data GSM Evolution), 204
education records, FERPA, 719
EF (Entrance Facilities), structured cabling, 67
EIA (Electronic Industries Alliance)
defined, 66
TIA/EIA 568-A cabling standard, 66
TIA/EIA 568-B cabling standard, 66
TIA/EIA 569B cabling standard, 66–67
EIGRP (Enhanced Interior Gateway Routing Protocol), 487–494, 501
EIR (Excess Information Rates), 276
EIRP (Effective Isotope Radiated Power), 210
E-LAN (Ethernet LAN) service, 275
elasticity, cloud computing, 696
electromagnetic wavelength spectrum, 131
electrostatic interference, fiber-optic cabling, 126
ELFEXT (Equal-Level FEXT), 93, 95
E-Line (Ethernet Service Line), 274, 275
ELTCTL (Equal Loss Transverse Conversion Transfer Loss), 99
email
cloud computing, 693
CNAME records, 693
MX records, 693
Emergency Action Plans (29 CFR 1910.38), 710–711
Employee Alarm Systems (29 CFR 1910.165), 715–716
enable command, routers, privileged mode, 373
enable secret command, 375, 412
encoding, multilevel, 100
encryption
3DES, 651
AES, 640
DES, 651
home networks, 33
Type 5 encryption algorithm, 627
Type 7 encryption algorithm, 627
wireless networks (Wi-Fi), 33
enterprise networks, 5, 262
enterprise storage
NAS, 700
SAN, 698–699
ER (Equipment Rooms), structured cabling, 67
error thresholds, 247
ESP (Encapsulating Security Protocols), 651
ESS (Extended Service Sets), 178
Ethernet
10GBASE-T cabling, 97–98
AXT, 98
full-duplex transmissions, 100
F/UTP, 99
hybrid echo cancellation circuits, 100
IEEE 802.3an-2006, 98
performance, 100–101
PSAACRF, 98, 99
PSANEXT, 98, 99
signal transmission, 100–101
bonding, 179
Carrier Ethernet, 273–274
Ethernet Service Definition, 274
EVC, 274
Fast Ethernet, 76
FastEthernet ports, 250
FCoE, 699
giants, 433
Gigabit Ethernet, 76
MEF, 274
MOE, 273–274
optical Ethernet, 149–150
optical networking, 157
PoE, 425–428
PoE+427
PoE++428
runts, 433
service attributes, 276–277
Ethernet addresses. *See* MAC addresses
Ethernet jumbo frames, preambles, 17
Ethernet LAN, 16
cabling, numerics, 41
CSMA/CD, 16
frames, 17
check sequences, 17
components of (overview), 17
data, 17
data structure of, 17
destination MAC addresses and sources, 17
jumbo frames, 17
length/type, 17
MAC addresses, 17, 18–20
NIC, 18
pads, 17

preambles, 17
start frame delimiters, 17
Ethernet packet frames, 17
check sequences, 17
components of (overview), 17
data, 17
data structure of, 17
destination MAC addresses and sources, 17
length/type, 17
MAC addresses, 17, 20
defined, 18
ipconfig/all command, 18–19
length of, 18
Linux, 20
macOS, 20
obtaining, 19–20
OUI, 18
sampling of, 18
Windows 10, 20
NIC
MAC addresses, 18
NIC, 18
teaming, 18
pads, 17
preambles, 17
start frame delimiters, 17
E-Tree (Ethernet Treet) service, 275–276
EVC (Ethernet Virtual Connections), 274
events, troubleshooting fiber-optic cabling, 162
evil twin attacks, 598
EXEC (privileged EXEC) passwords, 627
exit routes
Design and Construction Requirements for Exit Routes (29 CFR 1910.36), 709–710
Maintenance, Safeguards, and Operational Features for Exit Routes (29 CFR 1910.37), 710
export controls, international, 720–722
extending wireless ranges, 214

F

factory passwords, changing, 33
factory resets, 662
Fast Ethernet, 76
interface configurations, routers, 376–377
ports, 250, 263
fast-forward mode, switches, 247
FC (Fibre Channel), 699
FC connectors, fiber-optic cabling, 145–146
FCoE (Fibre Channel over Ethernet), 699
FERPA (Family Eductional Rights and Privacy Act), 719
FHRP (First Hop Redundancy Protocol), 730
FHSS (Frequency-Hopping Spread Spectrum), 180
fiber Bragg grating, 139
fiber couplers, 64
fiber cross-connects, 151
fiber transceivers, 154
fiber-optic cabling. *See also* physical layer cabling
absorption, 136
advantages of, 126–127
APC connectors, 146
attenuation (insertion loss), 127, 136–137
attenuators, 142
backbones, 155
bandwidth, 126
BD fiber, 151–154
branching devices, 142
building distributions, 151–154
campus networks, 154–157
chromatic dispersion, 137–138
cladding, 130
color-coding fiber, 156
components of, 126, 141–142
connectorization, 145–146
cores, 130
corrosion, 127
costs, 127
crosstalk, 127
CWDM, 142
detectors, 143–145
DFB lasers, 141
diplexers, 154
dispersion, 137–139
dispersion compensation, 139
dispersion shifted fibers, 138–139
DL, 141
DWDM, 130, 141
electrostatic interference, 126
Ethernet, 157
events, troubleshooting, 162
FC connectors, 145–146
fiber, defined, 142

fiber Bragg grating, 139
fiber cross-connects, 151
fiber selection, 132–133
fiber-to-the-home/business, 130
FTTB, 149
FTTC, 149
FTTD, 149
FTTH, 149
fusion splicing, 144
GBIC, 152–153
glass, 142
graded-index fiber, 132, 133–134
IC fibers, 152
IDC, 152–153
index-matching gel, 144
IR (Infrared) radiation, 126
isolators, 142
LC connectors, 145–146
LED, 141
light pipes, 142
link budgets, 157–158
logical fiber maps, 154, 155
mechanical splicing, 144–145
microbending, 136–137
mm fibers, 155
modal dispersion, 137–138
mode field diameters, 134–135
MT-RJ connectors, 145–146
multimode fiber, 130, 132
numerical apertures, 131
optical connectors, 126
optical Ethernet, 149–150
optical networking, defined, 148–151
optical spectrum, 130–131
optical-line amplifiers, 143
OTDR, 162–163
photosensitive detectors, 126
physical fiber maps, 154, 156
polarization mode dispersion, 137, 139
pulse dispersions, 132–133
refraction of light, 129
refractive indexes, 129
RSL, 142
safety, 127, 160–161
SC connectors, 145–146
scattering, 136
security, 127
SFP, 152–153
SFP+153–154
“shooting the fiber”, 162
single-mode fibers, 130, 134–135
sm fibers, 155
splitters, 142
ST connectors, 145–146
step-index fiber, 133
strands, 131–132
transceivers, 154
transmission strands, 126
troubleshooting, 162–163
tunable lasers, 141–142
“two-deep” rule, 152–153
unconnected fibers, 146
UPC connectors, 146
VCSEL, 141
VFL, 162
WDM, 130, 143
X2, 153–154
XENPAK, 153–154
XFP, 153–154
XPAK, 153–154
zero dispersion wavelengths, 138–139

fibers
BD fiber, 151–154
IC fibers, 152
mm fibers, 155
“shooting the fiber”, 162
sm fibers, 155
unconnected fibers, 146

fiber-to-the-home/business, 130

Fibre Channel (FC), 699

Fibre Channel over Ethernet (FCoE), 699

filtering
BPDU Filter, 636
content filters, 620
MAC addresses, 33
packets, 618
traffic, 268
web filters, 620

Fire Detection Systems (29 CFR 1910.164), 714–715

Fire Prevention Plans (29 CFR 1910.39), 711–712

firewalls, 34
ACL, 617–618
configuring, 611–617
deploying, 619

DMZ, 618
NGFW, 620
packet filtering, 618
personal firewalls, 610
proxy servers, 618
screened subnets, 618
SPI, 34
stateful firewalls, 618
FISMA (Federal Information Security Management Act), 719
Fixed Extinguishing Systems (29 CFR 1910.160), 713–714
flapping, route, 478
flash memory, 368
flat networks, 359
flooding, switches, 246
FLP (Fast Link Pulses), 383
forensics, computer, 621
forward DNS lookups, 539
forwarding, port, 35
forwarding state, STP, 423
FPP (Fire Prevention Plans), 711–712
fragment collisions, 247
fragment-free mode, switches, 247
frames, 17
check sequences, 17
components of (overview), 17
data, 17
data structure of, 17
destination MAC addresses and sources, 17
jumbo frames, 17
length/type, 17
MAC addresses, 17, 20
defined, 18
ipconfig/all command, 18–19
length of, 18
Linux, 20
macOS, 20
obtaining, 19–20
OUI, 18
sampling of, 18
Windows 10, 20
NIC, 18
MAC addresses, 18
teaming, 18
pads, 17
preambles, 17
start frame delimiters, 17
frequencies, interference, troubleshooting, 214
frequency bands, RFID tags, 203
frequency channels, WLAN, 179
FTP data packets, 566–567
FTTB (Fiber-To-The-Business), 149
FTTC (Fiber-To-The-Curb), 149
FTTD (Fiber-To-The-Desktop), 149
FTTH (Fiber-To-The-Home), 149
full backups, 730
full channels, 92
full-duplex cabling, 76
full-duplex mode, interfaces, 384–386
full-duplex transmissions, 100
fusion splicing, 144
F/UTP (Foil over Twisted-Pair Cabling), 99

G

gateways
addresses, 265, 326–327, 359–361
default gateways, static routing, 448
FHRP, 730
of last resort, 454
voice gateways, 251
gateways/broadband modems, 28
GBIC (Gigabit Interface Converters), 152–153
GDPR (General Data Protection Regulation), 719
geofencing, 204
giants, 433
Gigabit Ethernet, 76
glass, fiber-optic cabling, 142
GLBA (Gramm-Leach-Bliley Act), 719–720
graded-index fiber, 132, 133–134
GRE (Generic Routing Encapsulation), 648–649
gTLD, 528
guest machines, virtualization, 680

H

HA (Hardware Addresses), 302
HA (High Availability), 730–731
half-duplex mode, interfaces, 384–386
hand-offs, 178
handshakes, TCP, 298, 299
hardware addresses. *See* MAC addresses
hardware keys, 682

hashing algorithms
MD5, 649, 650
SHA, 649, 650
Hazard Communication (29 CFR 1910.1200), 716
HC (Horizontal Cross-Connects), 68, 69
HDLC (High-Level Data Link Control), 272, 273
headends, VPN, 647
headers
IP headers, 301
TCP, 296–297
UDP headers, 300–301
hello packets, 477
help (?) command, 367
hexadecimal numbers, 309–311
HF (High Frequency) RFID tags, 203
hierarchy data rates, SONET/SDH, 149
hijacking sessions, 599
HIPAA (Health Insurance Portability and Accountability Act), 720
home access, home networks, 31
home networks, 24
appearance, 31
captive portals, 32
connecting, 32
cost, 30
data speeds, 30
ease of implementation, 31
encryption, 33
home access, 31
hotspots, 32
public access, 31
range extenders, 32
security, 33–34
troubleshooting, 31–32
wired networks
access points (AP), 28
advantages/disadvantages of, 24
broadband modems/gateways, 28
cable modems, 28, 29
components of, 25–30
defined, 24
DSL modems, 29–30
example of, 25
hubs, 25
network adapters, 26
routers, 26–27
switches, 26
wireless routers, 28
wireless networks (Wi-Fi), 24
access points (AP), 28
advantages/disadvantages of, 24
broadband modems/gateways, 28
cable modems, 28, 29
components of, 25–30
defined, 24
DSL modems, 29–30
example of, 25
hubs, 25
IEEE wireless standards, 24–25
network adapters, 26
routers, 26–27
switches, 26
Wi-Fi Alliance, 24–25
wireless routers, 25, 28
hop count metrics, 461, 463–464
hopping sequences, 180
hopping, VLAN, 599
horizontal cabling, 67, 69–73, 83–87
host (interface) identifiers, 335
host IP addresses, 315
host machines, virtualization, 680
host numbers, IP addressing, 21
hostname command, 374–375, 411–412
hostnames, 366
hot sites, disaster recovery, 731
"hot/cold" aisles, 73
hotspots, 32, 641
HSPA+ (Evolved High-Speed Packet Access), 204
HSSI (High-Speed Serial Interfaces), 270
hub-and-spoke topologies. *See* star topologies
hubs
broadcasts, 9
defined, 9
home networks, 25
link light indicators, 42
switches and, 10, 239–242
Token Ring hubs, 7
wireless routers, home networks, 28
HVAC systems, 717
hybrid clouds, 696
hybrid echo cancellation circuits, 100
Hyper-V, 682–690
hypervisors, 680

I

IaaS (Infrastructure as a Service), 694
IANA (Internet Assigned Numbers Authority), 20, 528
IB (InfiniBand), 699
IC (Interconnect) fibers, 152
IC (Intermediate Cross-Connects), 68, 69
ICANN (Internet Corporation for Assigned Names and Numbers), 295, 529
ICMP (Internet Control Message Protocol), 46, 302–303
IDC (Intermediate Distribution Closets), 152–153
IDS (Intrusion Detection Systems), 619
IEEE (Institute of Electrical and Electronics Engineers), 7
802.1x (dot1x) wireless standard, 633
802.11 wireless standard, 175–176
ad hoc networks, 176, 177
AP, 177–178
BSS, 176, 177, 178
channel bonding, 179
CSMA/CD, 178
DSSS, 179
ESS, 178
FHSS, 180
frequency channels, 179
hand-offs, 178
hopping sequences, 180
ISM band, 179
MAC layer, 176
OFDM, 180
Open Authentication, 638
PHY layer, 176
pseudorandom numbering sequences, 180
roaming, 178
shared-key authentication, 638
transceivers, 177
transmit power, 180
WMN, 176
802.11a (Wi-Fi 2) wireless standard, 24, 180–181, 183
802.11ac (Wi-Fi 5) wireless standard, 24, 182, 183
802.11ax (Wi-Fi 6) wireless standard, 25, 182, 183
802.11b (Wi-Fi 1) wireless standard, 24, 181, 183
802.11g (Wi-Fi 3) wireless standard, 24, 181, 182, 183
802.11i wireless standard, 183
802.11n (Wi-Fi 4) wireless standard, 24, 181, 182, 183
802.11r wireless standard, 183
802.16a (WiMAX) wireless standard, 200
802.3an-2006, 98
Wi-Fi Alliance, 24–25
wireless standards, 24–25
IETF (Internet Engineering Task Force), 477
IGMP (Internet Group Management Protocol), 303–304
IKE (Internet Key Exchange), 651
implementing, home networks, 31
in-addr.arpa, 528
incident response policies, 725
incremental backups, 730
index-matching gel, 144
industry regulatory compliance, 718
FERPA, 718
FISMA, 719
GDPR, 719
GLBA, 719–720
HIPAA, 720
international export controls, 720–722
PCI DSS, 720
InfiniBand (IB), 699
infrastructure management
DHCP deployments, 535–537
DNS, 539
dig command, 541
forward DNS lookups, 539
nslookup command, 541
reverse DNS lookups, 539
root DNS servers, 539–540
RR, 541–546
tree hierarchies, 539–540
domain names, 528
FTP data packets, 566–567
IP address assignments, 529–530
IP addresses
assigning, 529–530
managing with DHCP, 531–537
IP networks, troubleshooting, 568–573
network management protocols, 546–551
network traffic analysis, 552–565
number resources, 529
protocol assignments, 529
scaling networks, 537–538
SFTP, 566
SNMP, 546–547
configuring, 547–551
MIB, 547

SNMPv2, 550
SNMPv3, 550
Wireshark, 560–565
inlays, RFID, 202
input errors, 432
input ports, 41
inquiry procedures, Bluetooth devices, 197
insertion loss (attenuation), 92, 93–94
ACR, 93, 95
fiber-optic cabling, 127, 136–137, 142
PSAACRF, 98, 99
PSACR, 93, 95, 96
.int, 528
interconnecting LAN
access/edge layer, 269
bridges
advantages/disadvantages of, 236
ARP caches, 233–235
associations, 233
broadcasts, 233
defined, 232
MAC addresses, 232–234
multiport bridges. See *layer 2 switches*
ports, 232–233
translation bridges, 235
transparent bridges, 235
wireless bridges, 236
Carrier Ethernet, 273–274
CSU/DSU, 272
data center architectures, 269
data channels, 270–271
distribution/aggregation layer, 269
E-LAN service, 275
E-Line, 274, 275
Ethernet service attributes, 276–277
Ethernet Service Definition, 274
E-Tree service, 275–276
EVC, 274
HDLC, 272, 273
lines of demarcation, 271
MEF, 274
MOE, 273–274
POP, 271
PPP, 272–273
routers, 262–266
auxiliary input, 250
console input/cabling, 250
console ports, 254–261
FastEthernet ports, 250, 263
gateway addresses, 265
higher-end routers, VoIP, 252–253
interfaces, 250–251
logical addresses, 249
MPLS, 252
network addresses, 249
packet shapers, 253
ports, 249–250
QoS, 251–253
routing tables, 265
segments, 265–266
serial interfaces, 251
serial ports, 264
USB interfaces, 250
VIC-4FXS/DID, 251
voice interface cards, 251
VoIP, 251
WIC2AM, 251
switches, 237–238, 239
adaptive cut-through mode, 247
aging time, 244
benefits of, 246
broadcast domains, 246
CNA, 242–243
cut-through mode, 247
dynamic assignments, 243
error thresholds, 247
fast-forward mode, 247
flooding, 246
fragment-free mode, 247
hubs and, 239–242
IP addressing, 245
isolating collision domains, 246
latency, 246
layer 2 switches, 238
managed switches, 242–247
MLS, 247
multicast messages, 239
ports, 243
secure addresses, 243
stacked switches, 243–244
static assignments, 243
store-and-forward mode, 246
wire speed routing, 247
traffic flows, 269

UNI, 274
WAN, 267–277
interfaces
auto-negotiation, 383–386
host interfaces, identifiers, 335
routers, 250–251
administratively down, 390
full-duplex mode, 384–386
half-duplex mode, 384–386
troubleshooting, 387–392
subinterfaces, VLAN, 418–419
UNI, 274
USB interfaces, 250
interference
fiber-optic cabling, 126
WLAN, troubleshooting, 214
international export controls, 720–722
Internet layer, TCP/IP, 294, 301
ARP, 301–303
ICMP, 302–303
IGMP, 303–304
IP, 301
intranets, 21, 316
intrusion attacks, 594–595
brute-force attacks, 596
dictionary attacks, 596
packet sniffing attacks, 597–599
password cracking attacks, 596–597
social engineering attacks, 595–596
inventory/asset management, 728
IoT (Internet of Things), 568, 662–663
IP (Internet Protocol)
addressing. *See* separate entry
ip helper command, 533
IP internetworks, 21–22
ip route command, 451
security cameras, 662
telephony, 251
troubleshooting, 568–573
tunnels, 648
IP (Internet Protocol), addressing
APIPA, 532, 533
assigning, 529–530
gateway addresses, 326–327
headers, 301
IANA, 20
IPAM, 546
IPSec, 598, 651
IPv4, 312–313
6to4 prefix, 335
ARIN, 315
assigning, 315
A.B.C.D. values, 20–21
class network addresses, 467
classes, 313
classful addresses, 317
decimal/binary octets, 314
default gateway addresses, 359–361
dual stacks, 336
host IP addresses, 315
host numbers, 21
network numbers, 21
network/host bits, 314–315
next hop addresses, 362
non-Internet-routable IP addresses, 316
private IP addresses, 21–22, 316
public IP addresses, 22
RIR, 315
structure of, 313
transitioning to IPv6, 335–337
IPv6, 333–335, 337
6to4 prefix, 335
anycast addresses, 335
CIDR, 337–338
defined, 333
dual stacks, 336
interface (host) identifiers, 335
IPng, 333
link-local addresses, 335, 336–337
multicast addresses, 335
routing, 499
routing, BGP, 501–502
routing, EIGRP, 501
routing, OSPF, 500–501
routing, RIP, 499–500
routing, static, 499
SLAAC, 336–337
transitioning to, 335–337
unicast addresses, 335
lease time, 532
managing with DHCP, 531–537
network numbers, 482
Office LAN, 40

overloading, 35
private IP addresses
APIPA, 532, 533
NAT, 34–35
public IP addresses, NAT, 35
switches, configuring, 245
TCP/IP, 21–22
troubleshooting, 570
VM, 682
wildcard bits, 482–483
IPAM (IP Address Management), 546
ipconfig command, LAN testing/troubleshooting, 47–48
ipconfig /release command, 532
ipconfig /renew command, 532
ipconfig/all command, 18–19, 39
IPng (IP Next Generation), 333
IPS (Intrusion Prevention Systems), 619
IPSec, 598, 651
IR (Infrared) radiation, 126, 130
ISAKMP (Internet Security Association and Key Management Protocol), 651
iSCSI (Internet Small Computer Systems Interface), 699
IS-IS (Intermediate System-to-Intermediate System), 478–479
ISM (Industrial, Scientific, Medical) band, 179
isolating
collision domains, 246
network problems, 14
isolators, fiber-optic cabling, 142
ISP (Internet Service Providers), defined, 21
IT audits, 728

J

jamming wireless networks, 638
jitter, 252
jumbo frames, 17

K

keepalive packets, 388
Kerberos authentication, 623
key exchanges
Diffie-Hellman key exchange, 651
IKE, 651
ISAKMP, 651
keys, hardware, 682

L

L2F (Layer 2 Forwarding) protocol, 650
L2TP (Layer 2 Tunneling Protocol), 650, 651
labeling, 71–72
port labeling, 72
system labeling, 72
LACP (Link Aggregation Control Protocol), 424
LAN (Local Area Networks), 5, 6. *See also* VLAN; WLAN
access/edge layer, 269
bridges
advantages/disadvantages of, 236
ARP caches, 233–235
associations, 233
broadcasts, 233
defined, 232
MAC addresses, 232–234
multiport bridges. See *layer 2 switches*
ports, 232–233
translation bridges, 235
transparent bridges, 235
wireless bridges, 236
Carrier Ethernet, 273–274
core layer, 268
CSU/DSU, 272
data center architectures, 269
data channels, 270–271
default gateway addresses, 359–361
distribution/aggregation layer, 269
E-LAN service, 275
E-Line, 274, 275
Ethernet LAN, 16
cabling, numerics, 41
CSMA/CD, 16
frames, 17
Ethernet service attributes, 276–277
Ethernet Service Definition, 274
E-Tree service, 275–276
EVC, 274
flat networks, 359
HDLC, 272, 273
interconnecting WAN, 267–277
layer 3 networks, 359–364
lines of demarcation, 271
MEF, 274
MOE, 273–274

Office LAN, assembling, 38–39
cabling, 40–43
client/server networks, 42–45
configuring computers for LAN operation, 44
diagramming networks, 39–40
IP addressing, 40
MAC addresses, 40
network device connections, 40–43
peer-to-peer networks, 42, 43
POP, 271
PPP, 272–273
routers
auxiliary input, 250
console input/cabling, 250
console ports, 254–261
FastEthernet ports, 250, 263
gateway addresses, 265
higher-end routers, VoIP, 252–253
interconnecting LAN, 262–266
interfaces, 250–251
logical addresses, 249
MPLS, 252
network addresses, 249
packet shapers, 253
ports, 249–250
QoS, 251–253
routing tables, 265
segments, 265–266
serial interfaces, 251
serial ports, 264
USB interfaces, 250
VIC-4FXS/DID, 251
voice interface cards, 251
VoIP, 251
WIC2AM, 251
switches, 237–238, 239
adaptive cut-through mode, 247
aging time, 244
benefits of, 246
broadcast domains, 246
CNA, 242–243
cut-through mode, 247
dynamic assignments, 243
error thresholds, 247
fast-forward mode, 247
flooding, 246
fragment-free mode, 247
hubs and, 239–242
IP addressing, 245
isolating collision domains, 246
latency, 246
layer 2 switches, 238
managed switches, 242–247
MLS, 247
multicast messages, 239
ports, 243
secure addresses, 243
stacked switches, 243–244
static assignments, 243
store-and-forward mode, 246
wire speed routing, 247
testing, 45–48
traffic flows, 269
troubleshooting, 45–48
UNI, 274
language table registries, 528
last resort, gateways of, 454
last-mile connections, 200
latency
metrics, 461
network latency, 252
switches, 246
layer 2 switches, 238
layer 3 networks, 359–364
LC connectors, fiber-optic cabling, 145–146
LCL (Longitudinal Conversion Loss), 99
LEAP (Lightweight Extensible Authentication Protocol), 640
learning state, STP, 423
lease time, 532
LED (Light-Emitting Diodes), 141
length/type, frames, 17
LF (Low Frequency) RFID tags, 203
licenses, MLA, 724
light
electromagnetic wavelength spectrum, 131
IR (Infrared) radiation, 126, 130
optical spectrum, 130–131
refraction of, 129
refractive indexes, 129
light detectors, fiber-optic cabling, 143–145
light pipes, defined, 142

line console passwords, 375–376, 412–414
line passwords, 626–627
lines of demarcation, 271
link budgets, 157–158
link integrity tests, 42
link light indicators, 42
link-local addresses, 335, 336–337
link (port) aggregation, 424
link pulses, 42
link state protocols, 476–477
EIGRP, 487–494, 501
IS-IS, 478–479
LSA, 477
NET addresses, 479
OSPF, 477, 483–486
advantages/disadvantages of, 478
Area 0, 482
areas, 477
configuring, 481–485
hello packets, 477
IPv6, 500–501
router ospf [process id] command, 481
VLSM, 478
RIP and, 477
route flapping, 478
links, cabling, 92
Linux
firewalls, 616–617
MAC addresses, obtaining, 20
listening state, STP, 423
Live Migration, 681
load balancing, dynamic routing protocols, 460
load issues (WLAN), troubleshooting, 215
load metrics, 461
lockers, smart, 663
locking cabinets, 661
locking racks, 661
locks, racks, 73
logging, routers, 630–631
logic bombs, 604
logical addresses, 249
logical fiber maps, 154, 155
long hauls, data transmissions, 134
lookups, DNS, 539
loopbacks, 448–449
loops, routing, 465
loss of association, WLAN, 193
LSA (Link State Advertisements), 477
LTE/4G, 204

M

MAC (Media Access Control) layer, 802.11 wireless standard, 176
MAC addresses, 20
aging time, 244
bridges, 232–234
CAM, 246
defined, 17, 18
destination MAC addresses and sources, 17
dynamic assignments, 243
filtering, 33
ipconfig/all command, 18–19
length of, 18
Linux, 20
macOS, 20
NIC, 18
obtaining, 19–20
Office LAN, 40
OUI, 18
sampling of, 18
spoofing attacks, 635
static assignments, 243
sticky command option, 634
Windows 10, 20
macOS
firewalls, 615–616
home networks, connecting, 32
MAC addresses, obtaining, 20
remote client VPN configurations, 652–653
ZTerm serial communications software, 259–261
magic numbers, subnetting, 323
Maintenance, Safeguards, and Operational Features for Exit Routes (29 CFR 1910.37), 710
malware
antivirus/anti-malware software, 610–611
logic bombs, 604
ransomware attacks, 604
viruses, 602–603
worms, 603
zero-day attacks, 604
MAN (Metropolitan Area Networks), 5

managed switches, 242–247
managing
asset/inventory management, 728
cabling, 67
change management policies, 624
domain names, 528
inventory/asset management, 728
IP addressing, IPAM, 546
network access, 623–624
network infrastructures
DHCP deployments, 535–537
DNS, 539–546
domain names, 528
FTP data packets, 566–567
IP address assignments, 529–530
IP address management with DHCP, 531–537
network management protocols, 546–551
number resources, 529
protocol assignments, 529
scaling networks, 537–538
SFTP, 566
SNMP, 546–551
traffic analysis, 552–565
troubleshooting IP networks, 568–573
Wireshark, 560–565
number resources, 529
man-in-the-middle attacks (on-path attacks), 598
mantraps (access control vestibules), 661
manufacturer's specifications, cabling, 102–104
mapping, ports, 35
maps
color maps, T568A/T568B wiring standards, 78–80
logical fiber maps, 154, 155
physical fiber maps, 154, 156
wiremaps, 82
MC (Main Cross-Connects), 68, 69
MD5 (Message Digest 5) hashing algorithm, 649, 650
mechanical splicing, 144–145
media converters, 262–263
MEF (Metro Ethernet Forum), 274
memory
CAM, 246
flash memory, 368
mesh topologies, 10–11
metrics, dynamic routing protocols, 460, 461
mGRE (Multipoint GRE), 649
MIB (Management Information Bases), 547
microbending, fiber-optic cabling, 136–137
MIMO (Multiple-Input Multiple-Output), 182
MLA (Master License Agreements), 724
MLS (Multilayer Switches), 247
mm (multimode) fibers, 155
mobile (cellular) communications, 204
3G wireless standard, 204
4G wireless standard, 204
5G wireless standard, 204
CDMA, 204
EDGE, 204
geofencing, 204
HSPA+204
LTE/4G, 204
NFC, 204
modal dispersion, 137–138
mode field diameters, 134–135
modems
ADSL modems, 645–646
analog modems
asymmetric operations, 643
security, 643–644
V.44/V.34 modem standard, 643
V.92/V.90 modem standard, 643
broadband modems/gateways, 28
cable modems
DSL modems, 29–30
home networks, 28, 29
security, 644
dialup modems, 644
xDSL modems, security, 644–646
MOE (Metro Optical Ethernet), 273–274
motion detection, 662
MOU (Memorandums of Understanding), 723–724
Mpbs (Megabits per second), 40
MPLS (Multiprotocol Label Switching), 252
MSA (Master Service Agreements), 724
MSDS (Material Safety Data Sheets), 716
MSTI (Multiple Spanning Tree Instances), 423–424
MSTP (Multiple Spanning Tree Protocol), 423–424
MT ACK, 534
MT Discover, 534
MT Offer, 534
MT Request, 534

MTBF (Mean Time Between Failures), 729
MT-RJ connectors, fiber-optic cabling, 145–146
MTTF (Mean Time To Failure), 729
MTTR (Mean Time To Recover/Repair), 729
multicast addresses, 335
multicast messages, 239
multicasting, 303
multilevel encoding, 100
multimeters, 110
multimode fiber, 130, 132
multiplexing, 271
CWDM, 142
DWDM, 130, 141
OFDM, 180, 200
WDM, 130
multipoint antenna distributions, 209–211
multiport bridges. *See* layer 2 switches
multiport repeaters. *See* hubs
multitenancy, cloud computing, 695, 696
MU-MIMO (Multiuser-MIMO), 182
MX records (Mail Exchange records), 543–544, 693

N

NAC (Network Access Control), 624
name resolution, troubleshooting, 571
NAS (Network Attached Storage), 700
NAT (Network Address Translation), 34
defined, 34
private IP addresses, 34–35
public IP addresses, 35
scaling networks, 537–538
NCP (Network Control Protocol), 292
NDA (Non-Disclosure Agreements), 725
near-end testing, 94
NET (Network Entity Title) addresses, 479
NET, subnet, 363
netstat -a command, 600
netstat -b command, 601
netstat -r command, 448
network adapters, home networks, 26
network addresses, 249, 322
network bridges. *See* bridges
Network interface layer, TCP/IP, 294, 304
Network layer, OSI model, 13
network numbers, IP addressing, 21, 482
network switches. *See* switches
network/host bits, IPv4 addressing, 314–315
networks
access management, 623–624
ad hoc networks, 176, 177
campus network hierarchical topologies, 69
campus networks
backbones, 477
defined, 230
optical networking, 154–157
CAN, 5
client/server networks, 42–45
congestion (bottlenecking), 76, 252
connections, verifying with ping command, 240–241
contiguous networks, 467
deterministic networks, 7
diagramming, 39–40
enterprise networks, 5, 262
flat networks, 359
home networks, 24
appearance, 31
captive portals, 32
connecting, 32
cost, 30
data speeds, 30
ease of implementation, 31
encryption, 33
home access, 31
hotspots, 32
NAT, 34–36
public access, 31
range extenders, 32
security, 33–34
troubleshooting, 31–32
infrastructure management
DHCP deployments, 535–537
DNS, 539–546
domain names, 528
FTP data packets, 566–567
IP address assignments, 529–530
IP address management with DHCP, 531–537
network management protocols, 546–551
number resources, 529
protocol assignments, 529
scaling networks, 537–538
SFTP, 566

traffic analysis, 552–565
troubleshooting IP networks, 568–573
Wireshark, 560–565
interfaces, auto-negotiation, 383–386
intranet, 21
IP internetworks, 21–22
IP networks, troubleshooting, 568–573
isolating problems, 14
LAN, 5, 6
assembling, 38–43
bridges, 232–236
configuring computers for LAN operation, 44
console port connections, 254–261
default gateway addresses, 359–361
Ethernet LAN, 16–23
flat networks, 359
routers, 249–253, 262–266
switches, 237–238
testing, 45–48
troubleshooting, 45–48
WAN interconnections, 267–277
latency, 252
layer 3 networks, 359–364
MAN, 5
management protocols, 546–551
NAS, 700
optical networking, 147–148
backbones, 155
BD fiber, 151–154
building distributions, 151–154
campus networks, 154–157
color-coding fiber, 156
defined, 148–151
diplexers, 154
Ethernet, 157
fiber cross-connects, 151
FTTB, 149
FTTC, 149
FTTD, 149
FTTH, 149
GBIC, 152–153
IC fibers, 152
IDC, 152–153
link budgets, 157–158
logical fiber maps, 154, 155
mm fibers, 155
optical Ethernet, 149–150
physical fiber maps, 154, 156
SFP, 152–153
SFP+153–154
sm fibers, 155
SONET/SDH, 148–149
transceivers, 154
“two-deep” rule, 152–153
X2, 153–154
XENPAK, 153–154
XFP, 153–154
XPAK, 153–154
OSI model, 12
Application layer, 13, 14
Data link layer, 13
layer numbers, 13
layers, summary of, 12–13
Network layer, 13
Physical layer, 13
Presentation layer, 13–14
Session layer, 13
Transport layer, 13
PAN, 4
peer-to-peer networks, 42, 43
PSTN, 251
SAN, 698–699
scaling, 537–538
SDN, 696–697
SD-WAN, 697
security
ARP cache poisoning, 598
brute-force attacks, 596
buffer overflow attacks, 599–600
dictionary attacks, 596
DoS attacks, 606–609
DTLS protocol, 598
evil twin attacks, 598
intrusion attacks, 594–604
IPSec, 598
malware, 602–604
on-path attacks (man-in-the-middle attacks), 598
packet sniffing attacks, 597–599
password cracking attacks, 596–597
session hijacking, 599
social engineering attacks, 595–596
software vulnerabilities, 599–604
SSL protocol, 597–598
TLS protocol, 598

TTLS protocol, 598
VLAN hopping, 599
segments, 265–266
defined, 246
subnet, NET, 363
slowdowns, 233
topologies, 7
bus topologies, 8–9
defined, 6
hub-and-spoke topologies. See *star topologies*
mesh topologies, 10–11
point-to-point topologies, 6
star topologies, 9, 10, 39
Token Ring topologies, 6, 7–8
traffic analysis, 552–565
troubleshooting
bottom-to-top (bottom-up) approach, 569
divide-and-conquer approach, 569
isolating problems, 14
spot-the-difference approach, 569
top-to-bottom (top-down) approach, 569
verifying settings, 570
VPN, 34
CHAP, 649, 650
client-to-site VPN, 648
EAP, 650
GRE, 648–649
headends, 647
IP tunnels, 648
IPSec, 651
L2F, 650
L2TP, 650
MD5 hashing algorithm, 649, 650
mGRE, 649
PAP, 649–650
PPP, 649
PPTP, 650
remote access VPN, 648
remote client configurations, 652–657
SHA, 649, 650
site-to-site VPN, 648
tunneling protocols, 648–651
WAN, 5
defined, 526
example of, 526
HSSI, 270
interconnecting LAN, 267–277
LAN interactions, 267–277
OC, 270
SD-WAN, 697
wired networks
access points (AP), 28
advantages/disadvantages of, 24
appearance, 31
broadband modems/gateways, 28
cable modems, 28, 29
components of, 25–30
cost, 30
data speeds, 30
defined, 24
DSL modems, 29–30
ease of implementation, 31
example of, 25
home access, 31
hubs, 25
network adapters, 26
public access, 31
routers, 26–27
switches, 26
troubleshooting, 31–32
wireless routers, 28
wireless networks (Wi-Fi), 24
access points (AP), 28
advantages/disadvantages of, 24
appearance, 31
broadband modems/gateways, 28
cable modems, 28, 29
captive portals, 32
components of, 25–30
connecting, 32
cost, 30
data speeds, 30
defined, 24
DSL modems, 29–30
ease of implementation, 31
encryption, 33
example of, 25
firewalls, 34
home access, 31
hotspots, 32
hubs, 25
IEEE wireless standards, 24–25

IP addressing, 34–36
NAT, 34–36
network adapters, 26
public access, 31
range extenders, 32
routers, 26–27
security, 33–34
switches, 26
troubleshooting, 31–32
VPN, 34
Wi-Fi Alliance, 24–25
wireless routers, 25, 28
wireless standards, 32
WMN, 176
WSN, ANT+ wireless technology, 183
NEXT (Near-End Crosstalk), 92, 93, 94–95; 98, 99
next hop addresses, 362
NFC (Near Field Communication), 204
NFPA (National Fire Protection Association), 709
NGFW (Next-Generation Firewalls), 620
NIC (Network Interface Cards)
defined, 18
MAC addresses, 18
teaming, 18
NLOS (Non-Line-Of-Sight), 200
nmap command, 601–602
no shutdown (no shut) command, 377
non-Internet-routable IP addresses, 316
NS records (Name Server records), 543
nslookup command, 541
NTP (Network Time Protocol), 630
number conversions
binary-to-decimal conversions, 306–307
decimal-to-binary conversions, 307–309
hexadecimal numbers, 309–311
number resources, managing, 529
numerical apertures, 131
numerics, Ethernet LAN cabling, 41

O

OC (Optical Carriers), 270
OFDM (Orthogonal Frequency-Division Multiplexing), 180, 200
offboarding/onboarding policies, 727
Office LAN, assembling, 38–39
cabling, 40–43
client/server networks, 42–45
configuring computers for LAN operation, 44
diagramming networks, 39–40
IP addressing, 40
MAC addresses, 40
network device connections, 40–43
peer-to-peer networks, 42, 43
omnidirectional antennas, 209
onboarding/offboarding policies, 727
on-path attacks (man-in-the-middle attacks), 598
Open Authentication, 638
optical beam splitters. ***See*** **WDM**
optical communications, fiber-optic cabling
absorption, 136
advantages of, 126–127
APC connectors, 146
attenuation (insertion loss), 127, 136–137
attenuators, 142
backbones, 155
bandwidth, 126
BD fiber, 151–154
branching devices, 142
building distributions, 151–154
campus networks, 154–157
chromatic dispersion, 137–138
cladding, 130
color-coding fiber, 156
components of, 126, 141–142
connectorization, 145–146
cores, 130
corrosion, 127
costs, 127
crosstalk, 127
CWDM, 142
detectors, 143–145
DFB lasers, 141
diplexers, 154
dispersion, 137–139
dispersion compensation, 139
dispersion shifted fibers, 138–139
DL, 141
DWDM, 130, 141
electrostatic interference, 126

Ethernet, 157
events, troubleshooting, 162
FC connectors, 145–146
fiber, defined, 142
fiber Bragg grating, 139
fiber cross-connects, 151
fiber selection, 132–133
fiber-to-the-home/business, 130
FTTB, 149
FTTC, 149
FTTD, 149
FTTH, 149
fusion splicing, 144
GBIC, 152–153
glass, 142
graded-index fiber, 132, 133–134
IC fibers, 152
IDC, 152–153
index-matching gel, 144
IR (Infrared) radiation, 126
isolators, 142
LC connectors, 145–146
LED, 141
light pipes, 142
link budgets, 157–158
logical fiber maps, 154, 155
mechanical splicing, 144–145
microbending, 136–137
mm fibers, 155
modal dispersion, 137–138
mode field diameters, 134–135
MT-RJ connectors, 145–146
multimode fiber, 130, 132
numerical apertures, 131
optical connectors, 126
optical Ethernet, 149–150
optical networking, defined, 148–151
optical spectrum, 130–131
optical-line amplifiers, 143
OTDR, 162–163
photosensitive detectors, 126
physical fiber maps, 154, 156
polarization mode dispersion, 137, 139
pulse dispersions, 132–133
refraction of light, 129
refractive indexes, 129
RSL, 142
safety, 127, 160–161
SC connectors, 145–146
scattering, 136
security, 127
SFP, 152–153
SFP+153–154
“shooting the fiber”, 162
single-mode fibers, 130, 134–135
sm fibers, 155
splitters, 142
ST connectors, 145–146
step-index fiber, 133
strands, 131–132
transceivers, 154
transmission strands, 126
troubleshooting, 162–163
tunable lasers, 141–142
“two-deep” rule, 152–153
unconnected fibers, 146
UPC connectors, 146
VCSEL, 141
VFL, 162
WDM, 130, 143
X2, 153–154
XENPAK, 153–154
XFP, 153–154
XPAK, 153–154
zero dispersion wavelengths, 138–139
optical connectors, 126
optical Ethernet, 149–150
optical link budgets, 157–158
optical networking, 147–148
backbones, 155
BD fiber, 151–154
building distributions, 151–154
campus networks, 154–157
color-coding fiber, 156
defined, 148–151
diplexers, 154
Ethernet, 157
fiber cross-connects, 151
FTTB, 149
FTTC, 149
FTTD, 149
FTTH, 149

GBIC, 152–153
IC fibers, 152
IDC, 152–153
link budgets, 157–158
logical fiber maps, 154, 155
mm fibers, 155
optical Ethernet, 149–150
physical fiber maps, 154, 156
SFP, 152–153
SFP+153–154
sm fibers, 155
SONET/SDH, 148
hierarchy data rates, 149
STS, 149
transceivers, 154
"two-deep" rule, 152–153
X2, 153–154
XENPAK, 153–154
XFP, 153–154
XPAK, 153–154
optical spectrum, light, 130–131
optical transceivers, 154
optical-line amplifiers, fiber-optic cabling, 143
OSH (Occupational Safety and Health) Act, 708–709
OSHA (Occupational Safety and Health Administration), 708–709
OSI (Open Systems Interconnection) model, 12
Application layer, 13, 14
Data link layer, 13
layers
numbers, 13
summary of, 12–13
Network layer, 13
Physical layer, 13
Presentation layer, 13–14
Session layer, 13
Transport layer, 13
OSPF (Open Shortest Path First), 477, 483–486
advantages/disadvantages of, 478
Area 0, 482
areas, 477
configuring, 481–485
hello packets, 477
IPv6, 500–501
router ospf [process id] command, 481
VLSM, 478
OTDR (Optical Time-Domain Reflectometers), 162–163
OUI (Organizationally Unique Identifiers), 18, 304
outsourcing, cloud computing, 692
overloading, 35

P

PA (Protocol Addresses), 301
PaaS (Platform as a Service), 695
packet frames, 17
check sequences, 17
components of (overview), 17
data, 17
data structure of, 17
destination MAC addresses and sources, 17
jumbo frames, 17
length/type, 17
MAC addresses, 17, 20
defined, 18
ipconfig/all command, 18–19
length of, 18
Linux, 20
macOS, 20
obtaining, 19–20
OUI, 18
sampling of, 18
Windows 10, 20
NIC
MAC addresses, 18
NIC, 18
teaming, 18
pads, 17
preambles, 17
start frame delimiters, 17
packet shapers, 253, 620
packets
ACK packets, 297
ARP packets, 302–303
DHCP packets, 534
error thresholds, 247
filtering, 618
FTP data packets, 566–567
hello packets, 477
ICMP source-quench packets, 302
IGMP packets, 303–304
keepalive packets, 388

shaping, 620
sniffing attacks, 597–599
SYN ACK packets, 297
SYN packets, 297
TCP packets
terminating connections, 299–300
transmitting, 298
UDP packet transfers, 300–301
WEP, 638–639
wire speed routing, 247
pads, defined, 17
paging procedures, Bluetooth devices, 197
PAN (Personal Area Networks), 4
PAP (Password Authentication Protocol), 649–650
parabolic reflector (dish) antennas, 209
passing tokens, 7
passive RFID tags, 201–202
passwords
brute-force attacks, 596
cracking attacks, 596–597
dictionary attacks, 596
EXEC (privileged EXEC) passwords, 627
factory passwords, changing, 33
line console passwords, 375–376, 412–414
line passwords, 626–627
packet sniffing attacks, 597–599
PAP, 649–650
policies, 726
PAT (Port Address Translation), 35, 538
patch cabling, 71–72, 82, 87–90
path determination, dynamic routing protocols, 460
PBX (Private Branch Exchanges), 251
PCI DSS (Payment Card Industry Data Security Standard), 720
PD (Powered Devices), 426, 427
PDoS (Permanent DoS) attacks, 607
PDU (Protocol Data Units), 730–731
peer-to-peer networks, 42, 43
penetration testing, 602
performance
10GBASE-T cabling, 100–101
cabling, 110
slowdowns, network, 233
personal firewalls, 610
photodetectors. *See* detectors
photosensitive detectors, fiber-optic cabling, 126
PHY (Physical) layer, 802.11 wireless standard, 176
physical addresses. *See* MAC addresses
physical fiber maps, 154, 156
physical layer cabling, 64. *See also* fiber-optic cabling; twisted-pair cabling
APC connectors, 64
BNC connectors, 64
connectors, 64
fiber couplers, 64
structured cabling
backbone cabling, 67
building entrances, 66–67
ER, 67
HC, 68, 69
horizontal cabling, 67, 69–73
IC, 68, 69
MC, 68, 69
TCO, 67
telecommunications closets, 67, 69–70
TIA/EIA 568-A cabling standard, 66
TIA/EIA 568-B cabling standard, 66
TIA/EIA 569B cabling standard, 66–67
WO, 68
work areas, 67
UPC connectors, 64
UTP couplers, 64
Physical layer, OSI model, 13
physical security, 659, 660
access control, 659, 660–661
access control vestibules (mantraps), 661
badge readers, 661
biometric scanners, 661
locking cabinets, 661
locking racks, 661
asset disposal, 662
biometric scanners, 661, 717
control devices, 660
detection methods, 661–662
motion detection, 662
surveillance cameras, 662
door access, 717
surveillance, 659
testing, 659
piconets, 197–198

ping command, 14, 45–47, 240–241, 302–303
pinouts, T568A/T568B wiring standards, 79
PoE (Power over Ethernet), 425–428
PoE+427
PoE++428
point-to-point topologies, 6
poisoning ARP caches, 598
polarization mode dispersion, 137, 139
POP (Points of Presence), 271
port (link) aggregation, 424
Portable Fire Extinguishers (29 CFR 1910.157), 712–713
port-based VLAN, 407
ports
bridges, 232–233
common applications and port numbers, 295–296
console ports, routers
console cabling, 255
DB-9 connectors, 254–255
DB-25 connectors, 254, 255
PuTTY software, 256–259
RJ-45 connectors, 255
rollover cabling, 255–256
RS-232 serial communications ports, 254, 255
serial interfaces, 256
ZTerm serial communications software, 259–261
defined, 9
FastEthernet ports, 250, 263
forwarding, 35
input ports, 41
labeling, 72
mapping, 35
PAT, 35
private (dynamic) ports, 295
registered ports, 295
routers, 249–250
RS-232 serial communications ports, 254, 255
serial ports, 264
straight-through ports, 42
switches, 243, 431–432, 633–635
TCP ports, 573
TCP/IP, 295
trunk ports, 408–409
UDP ports, 573
uplink ports, 42
VLAN port assignments, 431
well-known (reserved) ports, 295
PPP (Point-to-Point Protocol), 272–273, 649
PPTP (Point-to-Point Tunneling Protocol), 650
preambles, defined, 17
Presentation layer, OSI model, 13–14
printers, wireless printers, troubleshooting, 216
private clouds, 696
private (dynamic) ports, 295
private IP addresses, 21–22, 316
APIPA, 532, 533
NAT, 34–35
Privileged EXEC mode (Router#), 373–381
privileged mode
routers, 373
switches, 411, 412
privileged user agreements, 726
propagation delay, 93, 96
protocol-based VLAN, 408
protocols
assigning, 529
defined, 6
ICMP, 46
proxy servers, 618
PSAACRF (Power-Sum Alien ACRF), 98, 99
PSACR (Power-Sum Attenuation to Crosstalk Ratios), 93, 95, 96
PSANEXT (Power-Sum Alien NEXT), 98, 99
PSE (Power Sourcing Equipment), 426–427
PSELFEXT (Power-Sum ELFEXT), 93, 95, 96
pseudorandom numbering sequences, 180
PSNEXT (Power-Sum NEXT), 93, 94
PSTN (Public-Switched Telephone Networks), 251
PTR records (Pointer records), 542
public access, home networks, 31
public clouds, 696
public IP addresses, 22, 35
pulse dispersions, 132–133
PuTTY software, configuring, 256–259
PVST (Per-VLAN Spanning Tree), 423–424

Q - R

QoS (Quality of Service), VoIP, 251–253
queuing/buffering, 252
racks
diagrams, 72
locks, 73, 661

RADIUS (Remote Authentication Dial-In User Service), 624, 640
range command, 633
ranges (wireless), extending, 32, 195, 214
ranging, cable modems, 644
ransomware attacks, 604
RAS (Remote Access Servers), 647
RBAC (Role-Based Access Control), 623
readers, RFID, 201
recovery/continuity policies/procedures, 729
MTBF, 729
MTTF, 729
MTTR, 729
redundancy
circuits, 730
FHRP, 730
reflective/amplified DoS attacks, 608
refraction of light, 129
refractive indexes, 129
registered ports, 295
reliability metrics, 461
remote access security, 642
analog modems, 643–644
cable modems, 644
RAS, 647
xDSL modems, 644–646
remote access VPN, 648
remote antenna installations, 211
remote client VPN configurations, 652–657
remote desktops, 695
replies, ARP, 301–303
requests, ARP, 301–302
reserved (well-known) ports, 295
resets, factory, 662
return loss, testing, 93, 95–96
reverse DNS lookups, 539
RF signal strength, WLAN, 191–195, 209–211
RFID (Radio Frequency Identification), 200, 201
backscatter, 200
block diagram, 200–201
inlays, 202
readers, 201
tags, 200
active tags, 202
communications (air interface) portal, 203
frequency bands, 203
HF tags, 203
LF tags, 203
passive tags, 201–202
semi-active tags, 202
Slotted Aloha, 203
UHF tags, 203
RIP (Routing Information Protocol), 465
configuring, 466–468
IPv6, 499–500
link state protocols and, 477
[rip_tag] tags, 500
route configuration, 468–473
sh run command, 471–472
show ip protocol (sh ip protocol) command, 469–471
RIPng (RIP Next Generation), 499–500
[rip_tag] tags, 500
RIPv2 (Routing Information Protocol version 2), 474–475
configuring, 466–468
route configuration, 473–474
RIR (Regional Internet Registries), 315, 529
RJ-45 connectors, 40, 70–71, 75, 255
roaming, WLAN connectivity, 178
role separation, 728
rollover cabling, 255–256
root DNS servers, 539–540
Root Guard, 636
route flapping, 478
route print command, 448
router ospf [process id] command, 481
routers
access, 626–628
administrative distance, 461
auto-negotiation, 383–386
auxiliary input, 250
configure terminal (conf t) command, 374
configuring
Privileged EXEC mode (Router#), 380–381
User EXEC mode (Router>), 369–371
console input/cabling, 250
console ports
console cabling, 255
DB-9 connectors, 254–255
DB-25 connectors, 254, 255
PuTTY software, 256–259
RJ-45 connectors, 255
rollover cabling, 255–256

RS-232 serial communications ports, 254, 255
serial interfaces, 256
ZTerm serial communications software, 259–261
enable command, 373
enable secret command, 375
EXEC (privileged EXEC) passwords, 627
FastEthernet interface configurations, 376–377
FastEthernet ports, 250, 263
fundamentals of, 358–364
gateway addresses, 265
higher-end routers, VoIP, 252–253
home networks, 26–27
hostname command, 374–375
interconnecting LAN, 262–266
interfaces, 250–251
administratively down, 390
auto-negotiation, 383–386
full-duplex mode, 384–386
troubleshooting, 387–392
ip helper command, 533
line console passwords, 375–376
line passwords, 626–627
logging, 630–631
logical addresses, 249
MPLS, 252
network addresses, 249
no shutdown (no shut) command, 377
packet shapers, 253
ports, 249–250
Privileged EXEC mode (Router#), 373–381
privileged mode, 373
QoS, 251–253
Router (config-if)# prompt, 377
routing tables, 265
RSA keys, 627–628
security, 626
access, 626–628
logging, 630–631
services, 628–630
segments, 265–266
serial interfaces, 251, 377–380
serial ports, 264
services, 628–630
show ip interface brief (sh ip int brief) command, 377, 387–392, 430
uptime, 369
USB interfaces, 250
User EXEC mode (Router>), 366–371
VIC-4FXS/DID, 251
voice interface cards, 251
VoIP, 251
WIC2AM, 251
wireless routers, 25, 28, 213
routing
advertising, 466
BGP, 496–498, 501–502
CIDR, 329
blocks, 330–331
IPv6 addressing, 337–338
notation, 329
subnet mask conversions, 329–330
distance vector protocols, 463
hop count metrics, 463–464
RIP, 465
RIP, [rip_tag] tags, 500
RIP, configuring, 466–468
RIP, IPv6, 499–500
RIP, route configuration, 468–473
RIP, sh run command, 471–472
RIP, show ip protocol (sh ip protocol) command, 469–471
RIP and link state protocols, 477
RIPv2, 474–475
RIPv2, configuring, 466–468
RIPv2, route configuration, 473–474
routing loops, 465
dynamic routing protocols, 460, 461
convergence, 460
load balancing, 460
metrics, 460, 461
path determination, 460
EIGRP, 487–494, 501
GRE, 648–649
IPv6 routing, 499
BGP, 501–502
EIGRP, 501
OSPF, 500–501
RIP, 499–500
static routing, 499
link state protocols, 476–477
configuring, 481–485
EIGRP, 487–494

EIGRP, IPv6, 501
IS-IS, 478–479
LSA, 477
NET addresses, 479
OSPF, 477, 483–486
OSPF, advantages/disadvantages of, 478
OSPF, Area 0, 482
OSPF, areas, 477
OSPF, hello packets, 477
OSPF, IPv6, 500–501
OSPF, router ospf [process id] command, 481
OSPF, VLSM, 478
RIP and, 477
route flapping, 478
loops, 465
OSPF, 477
advantages/disadvantages of, 478
areas, 477
hello packets, 477
VLSM, 478
RIP, 465
RIPng, 499–500
static routing, 447–448, 458
commands (overview), 457
configuring, 454–458
copy running-configuration startup-configuration (copy run start) command, 457
default gateways, 448
gateways of last resort, 454
ip route command, 451
IPv6, 499
loopbacks, 448–449
netstat -r command, 448
route print command, 448
routing tables, code C, 453
routing tables, code S, 453
setting, 449–451
show ip route (sh ip route) command, 451–454
show ip route static (sh ip route static) command, 456
show running-config (sh run) command, 456–457
show startup-config (sh start) command, 457
subnet masks, 451
VLSM, 451
write memory (wr m) command, 457
wire speed routing, 247
routing tables
code C, 453
code S, 453
defined, 265
RPO (Recovery Point Objectives), 732
RR (Resource Records), DNS, 541–546
RS-232 serial communications ports, 254, 255
RSA keys, 627–628
RSL (Received Signal Levels), fiber-optic cabling, 142
RSSI (Received Signal Strength Indicators), 214
RSTP (Rapid Spanning Tree Protocol), 423–424
RTO (Recovery Time Objectives), 732
rules/regulations
industry regulatory compliance, 718
FERPA, 718
FISMA, 719
GDPR, 719
GLBA, 719–720
HIPAA, 720
international export controls, 720–722
PCI DSS, 720
safety codes/standards
biometric scanners, 717
CFR, 709–716
Design and Construction Requirements for Exit Routes (29 CFR 1910.36), 709–710
door access, 717
Emergency Action Plans (29 CFR 1910.38), 710–711
Employee Alarm Systems (29 CFR 1910.165), 715–716
Fire Detection Systems (29 CFR 1910.164), 714–715
Fire Prevention Plans (29 CFR 1910.39), 711–712
Fixed Extinguishing Systems (29 CFR 1910.160), 713–714
Hazard Communication (29 CFR 1910.1200), 716
HVAC systems, 717
Maintenance, Safeguards, and Operational Features for Exit Routes (29 CFR 1910.37), 710
MSDS, 716
NFPA, 709
OSH Act, 708–709
OSHA, 708–709
Portable Fire Extinguishers (29 CFR 1910.157), 712–713
SDS, 716
runts, 433

S

SaaS (Software as a Service), 695
safety
codes/standards
biometric scanners, 717
CFR, 709–716
Design and Construction Requirements for Exit Routes (29 CFR 1910.36), 709–710
door access, 717
Emergency Action Plans (29 CFR 1910.38), 710–711
Employee Alarm Systems (29 CFR 1910.165), 715–716
Fire Detection Systems (29 CFR 1910.164), 714–715
Fire Prevention Plans (29 CFR 1910.39), 711–712
Fixed Extinguishing Systems (29 CFR 1910.160), 713–714
Hazard Communication (29 CFR 1910.1200), 716
HVAC systems, 717
Maintenance, Safeguards, and Operational Features for Exit Routes (29 CFR 1910.37), 710
MSDS, 716
NFPA, 709
OSH Act, 708–709
OSHA, 708–709
Portable Fire Extinguishers (29 CFR 1910.157), 712–713
SDS, 716
fiber-optic cabling, 127, 160–161
SAN (Storage Area Networks), 698–699
FC, 699
FCoE, 699
IB, 699
iSCSI, 699
sanitizing devices for disposal, 662
SC connectors, fiber-optic cabling, 145–146
scalability, cloud computing, 695–696
scaling networks, 537–538
scanners, biometric, 661, 717
scattering, fiber-optic cabling, 136
screened subnets, 618
SDN (Software-Defined Networking), 696–697
SDS (Safety Data Sheets), 716
SD-WAN (Software-Defined Wide Area Networks), 697
secure addresses, switches, 243
security
3DES, 651
access control, 659, 660–661
access control vestibules (mantraps), 661
badge readers, 661
biometric scanners, 661
locking cabinets, 661
locking racks, 661
AH, 651
analog modems, 643–644
antivirus/anti-malware software, 610–611
ARP cache poisoning, 598
Bluetooth, 641
botnets, 608
brute-force attacks, 596
buffer overflow attacks, 599–600
cable modems, 644
change management policies, 624
cloud computing, 697
computer forensics, 621
content filters, 620
coordinated DDoS attacks, 608
DAI, 635
DDoS attacks, 608–609
deauthentication/disassociation attacks, 608
DES, 651
dictionary attacks, 596
Diffie-Hellman key exchange, 651
directed broadcasts, 607
documentation, 624
DoS attacks, 606–609
DTLS protocol, 598
encryption, 33
ESP, 651
evil twin attacks, 598
EXEC (privileged EXEC) passwords, 627
fiber-optic cabling, 127
firewalls, 34
ACL, 617–618
configuring, 611–617
deploying, 619
DMZ, 618
NGFW, 620

packet filtering, 618
personal firewalls, 610
proxy servers, 618
screened subnets, 618
SPI, 34
stateful firewalls, 618
home networks, 33–34
IDS, 619
IKE, 651
intrusion attacks, 594–604
IoT, 662–663
IP security cameras, 662
IPS, 619
IPSec, 598, 651
ISAKMP, 651
Kerberos authentication, 623
locks, racks, 73
logic bombs, 604
MAC addresses, filtering, 33
malware, 602–604, 610–611
modems
analog modems, 643–644
cable modems, 644
xDSL modems, 644–646
NAC, 624
NAT, 34
defined, 34
private IP addresses, 34–35
public IP addresses, 35
network access management, 623–624
on-path attacks (man-in-the-middle attacks), 598
packet sniffing attacks, 597–599
passwords
changing factory passwords, 33
cracking attacks, 596–597
PDoS attacks, 607
physical security, 659, 660
access control, 659, 660–661
access control vestibules (mantraps), 661
asset disposal, 662
badge readers, 661
biometric scanners, 661, 717
control devices, 660
detection methods, 661–662
door access, 717
locking cabinets, 661
locking racks, 661
motion detection, 662
surveillance, 659
surveillance cameras, 662
testing, 659
RADIUS, 624
ransomware attacks, 604
RAS, 647
RBAC, 623
reflective/amplified DoS attacks, 608
remote access security, 642
analog modems, 643–644
cable modems, 644
RAS, 647
xDSL modems, 644–646
routers, 626
access, 626–628
logging, 630–631
services, 628–630
RSA keys, 627–628
session hijacking, 599
smart doorbells, 663
smart lockers, 663
smart speakers, 663
smart thermostats, 663
social engineering attacks, 595–596
software
buffer overflow attacks, 599–600
netstat -a command, 600
netstat -b command, 601
nmap command, 601–602
penetration testing, 602
vulnerabilities, 599–604
SPI, 34
spoofing attacks, 607, 635
SSID
changing default SSID, 33
turning off SSID broadcasts, 33
SSL protocol, 597–598
switches, 631–633
BPDU Filter, 636
BPDU Guard, 635–636
DAI, 635
ports, 633–635
Root Guard, 636
STP, 635–636

TACACS+624
TLS protocol, 598
TTLS protocol, 598
Type 5 encryption algorithm, 627
Type 7 encryption algorithm, 627
UTM, 624
viruses, 602–603, 610–611
VLAN hopping, 599
VPN, 34
CHAP, 649, 650
client-to-site VPN, 648
EAP, 650
GRE, 648–649
headends, 647
IP tunnels, 648
IPSec, 651
L2F, 650
L2TP, 650
MD5 hashing algorithm, 649, 650
mGRE, 649
PAP, 649–650
PPP, 649
PPTP, 650
remote access VPN, 648
remote client configurations, 652–657
SHA, 649, 650
site-to-site VPN, 648
tunneling protocols, 648–651
web filters, 620
wireless networks (Wi-Fi), 637
AES, 640
Bluetooth, 641
CCMP, 639–640
EAP, 640, 650
guidelines, 640–641
hotspots, 641
jamming, 638
LEAP, 640
Open Authentication, 638
RADIUS, 640
shared-key authentication, 638
SSID, 638
TKIP, 639
war chalking, 641
war driving, 641
war flying, 641
WEP, 638–639
WPA, 639
WPA2, 639–640
WPA3, 640
WLAN, 637
AES, 640
Bluetooth, 641
CCMP, 639–640
EAP, 640, 650
guidelines, 640–641
hotspots, 641
jamming, 638
LEAP, 640
Open Authentication, 638
RADIUS, 640
shared-key authentication, 638
SSID, 638
TKIP, 639
war chalking, 641
war driving, 641
war flying, 641
WEP, 638–639
WPA, 639
WPA2, 639–640
WPA3, 640
worms, 603
xDSL modems, 644–646
zero-day attacks, 604
segments, 265–266
defined, 246
subnet, NET, 363
semi-active RFID tags, 202
serial interfaces
console ports, routers, 256
HSSI, 270
routers, 251, 377–380
serial ports, 264
servers
proxy servers, 618
RAS, 647
root DNS, 539–540
service attributes, Ethernet, 276–277
services
cloud services, 692–693
DaaS, 695
DSL, 645

IaaS, 694
MSA, 724
PaaS, 695
routers, 628–630
SaaS, 695
xDSL, 645
session hijacking, 599
Session layer, OSI model, 13
setting up (configuring)
BGP, 496–498
computers for LAN operation, 44
EIGRP, 488–494
FastEthernet interfaces, 376–377
firewalls, 611–617
interfaces, auto-negotiation, 383–386
IP addressing, switches, 245
OSPF, 481–485
PuTTY software, 256–259
routers
Privileged EXEC mode (Router#), 380–381
User EXEC mode (Router>), 369–371
SLAAC, 336–337
SNMP, 547–551
static routing, 454–458
static VLAN, 414–418
switches, 410, 419–420
configure terminal (conf t) command, 411
enable secret command, 412
hostname command, 411–412
line console passwords, 412–414
privileged mode, 411, 412
static VLAN configurations, 414–418
switch# prompt, 412
switch(config)# prompt, 411, 412
switch(config-line)# prompt, 413
VLAN subinterfaces, 418–419
virtualization, 682–690
WLAN, 185–195, 206–211
SFP (Small Form-Factor Pluggables), 152–153
SFP+153–154
SFTP (Secure File Transfer Protocol), 566
sh run command, 471–472
SHA (Secure Hash Algorithm), 649, 650
shared-key authentication, 638
"shooting the fiber", 162
show flash command, 368
show interface status (sh int status) command, 430–431
show ip interface brief (sh ip int brief) command, 377, 387–392, 430
show ip protocol (sh ip protocol) command, 469–471
show ip route (sh ip route) command, 451–454
show ip route static (sh ip route static) command, 456
show mac address-table command, 433–434
show running-config command, 429–430
show running-config (sh run) command, 456–457
show startup-config (sh start) command, 457
show version command, 368–369, 434
signal strength, WLAN, 191–195
RF site surveys, 209–211
RSSI, 214
troubleshooting, 214
signal transmission, 10GBASE-T cabling, 100–101
single-mode fibers, 130, 134–135
site surveys, 190–195, 207, 209–211
site-to-site VPN, 648
SLA (Service-Level Agreements), 693, 724
SLAAC (Stateless Address Autoconfiguration), 336–337
Slotted Aloha, 203
slowdowns, network, 233
sm (single-mode) fibers, 155
smart devices, 568
smart doorbells, 663
smart lockers, 663
smart speakers, 663
smart thermostats, 663
snapshots
virtualization, 681
WLAN, 192–193
SNMP (Simple Network Management Protocol), 546–547
configuring, 547–551
MIB, 547
SNMPv2, 550
SNMPv3, 550
snooping, DHCP, 572
SOA (Start of Authority) resource records, 541
social engineering attacks, 595–596
software
antivirus/anti-malware software, 610–611
botnets, 608
buffer overflow attacks, 599–600
coordinated DDoS attacks, 608
DDoS attacks, 608–609

deauthentication/disassociation attacks, 608
directed broadcasts, 607
DoS attacks, 606–609
logic bombs, 604
malware, 602–604
PDoS attacks, 607
ransomware attacks, 604
reflective/amplified DoS attacks, 608
SDN, 696–697
security
netstat -a command, 600
netstat -b command, 601
nmap command, 601–602
penetration testing, 602
spoofing attacks, 607
viruses, 602–603
vulnerabilities, 599–604
worms, 603
zero-day attacks, 604
SONET/SDH (Synchronous Optical Networks/ Synchronous Digital Hierarchy), 148
hierarchy data rates, 149
STS, 149
SOP (Standard Operating Procedures), 726–727
source-quench packets, 302
SOW (Statements of Work), 725
spatial diversity, 186
speakers, smart, 663
speeds, data, home networks, 30
SPF (Sender Policy Frameworks), 544
SPI (Stateful Pack Inspection), 34
splicing
connectorization, 146
fusion splicing, 144
index-matching gel, 144
mechanical splicing, 144–145
splitters, fiber-optic cabling, 142
spoofing attacks, 607, 635
spot-the-difference troubleshooting approach, 569
SRV records (Service records), 544
SSID (Service Set Identifiers), 186, 638
broadcasts, turning off, 33
changing, 33
defined, 33
troubleshooting, 215
SSL (Secure Socket Layer) protocol, 597–598
ST connectors, fiber-optic cabling, 145–146
stacked switches, 243–244
star topologies, 9, 10, 39
start frame delimiters, defined, 17
stateful firewalls, 618
static assignments, 243
static routing, 447–448, 458
commands (overview), 457
configuring, 454–458
copy running-configuration startup-configuration (copy run start) command, 457
default gateways, 448
gateways of last resort, 454
ip route command, 451
IPv6, 499
loopbacks, 448–449
netstat -r command, 448
route print command, 448
routing tables
code C, 453
code S, 453
setting, 449–451
show ip route (sh ip route) command, 451–454
show ip route static (sh ip route static) command, 456
show running-config (sh run) command, 456–457
show startup-config (sh start) command, 457
subnet masks, 451
VLSM, 451
write memory (wr m) command, 457
static VLAN, 408, 414–418
step-index fiber, 133
sticky command option, 634
storage
NAS, 700
SAN, 698–699
store-and-forward mode, switches, 246
STP (Shielded Twisted-Pair) cabling, 76–77
STP (Spanning Tree Protocol), 422–424
BPDU Filter, 636
BPDU Guard, 635–636
Root Guard, 636
straight-through cabling, 82, 87–90
straight-through ports, 42
strands, fiber-optic cabling, 131–132

stretching cable, 102
structured cabling
backbone cabling, 67
building entrances, 66–67
ER, 67
HC, 68, 69
horizontal cabling, 67, 69–73
IC, 68, 69
MC, 68, 69
STP cabling, 76–77
TCO, 67
telecommunications closets, 67, 69–70
TIA/EIA 568-A cabling standard, 66
TIA/EIA 568-B cabling standard, 66
TIA/EIA 569B cabling standard, 66–67
twisted-pair cabling, 74, 78–80
UTP cabling, 74–76
WO, 68
work areas, 67
STS (Synchronous Transport Signals), 149
subinterfaces, VLAN, 418–419
subnet masks
ANDing, 361–362
applying, 318
CIDR-subnet mask conversions, 329–330
classful addresses, 317
creating, 321
defined, 317
examples of, 324–326
magic numbers, 323
original/default subnet masks, 319
static routing, 451
subnetting process, 319–323
troubleshooting, 570–571
VLSM, 331–332, 451, 478
subnetting
broadcast addresses, 322
classful addresses, 317
defined, 318–319
magic numbers, 323
NET, 363
network addresses, 322
network numbers, 482
process of, 319–323
VLSM, 331–332
supernetting, 328–329
CIDR, 329–330
CIDR blocks, 330–331
VLSM, 331–332
surveillance
cameras, 662
physical security, 659
switches, 9, 237–238, 239, 410
adaptive cut-through mode, 247
aging time, 244
benefits of, 246
BPDU, 422–423
broadcast domains, 246
CNA, 242–243
collisions, 433
configure terminal (conf t) command, 411
configuring, 411, 412, 419–420
connections, 10
CRC errors, 432
cut-through mode, 247
dynamic assignments, 243
enable secret command, 412
error thresholds, 247
fast-forward mode, 247
flooding, 246
fragment-free mode, 247
giants, 433
home networks, 26
hostname command, 411–412
hubs and, 10, 239–242
input errors, 432
IP addressing, 245
isolating collision domains, 246
latency, 246
layer 2 switches, 238
line console passwords, 412–414
link light indicators, 42
managed switches, 242–247
MLS, 247
multicast messages, 239
PD, 426, 427
PoE, 425–428
PoE+427
PoE++428
ports, 243, 431–432, 633–635
privileged mode, 411, 412

PSE, 426–427
runts, 433
secure addresses, 243
security, 631–633
BPDU Filter, 636
BPDU Guard, 635–636
DAI, 635
ports, 633–635
Root Guard, 636
STP, 635–636
show interface status (sh int status) command, 430–431
show mac address-table command, 433–434
show running-config command, 429–430
show version command, 434
stacked switches, 243–244
static assignments, 243
static VLAN, configuring, 414–418
store-and-forward mode, 246
STP, 422–424
switch# prompt, 412
switch(config)# prompt, 411, 412
switch(config-line)# prompt, 413
troubleshooting, 429–434
VLAN
security, 634
subinterfaces, 418–419
wire speed routing, 247
SYN (Synchronizing) packets, 297
SYN ACK (Synchronizing Acknowledgement) packets, 297
system labeling, 72

T

T1 to T3 data rates, 270
T568A wiring standard
color maps, 78–80
defined, 78
pinouts, 79
T568B wiring standard
color maps, 78–80
defined, 78
pinouts, 79
TACACS+ (Terminal Access Controller Access-Control System Plus), 624
tag-based VLAN, 408
tags
RFID, 200
active tags, 202
communications (air interface) portal, 203
frequency bands, 203
HF tags, 203
LF tags, 203
passive tags, 201–202
semi-active tags, 202
Slotted Aloha, 203
UHF tags, 203
[rip_tag] tags, 500
VLAN tags, 277
TCL (Transverse Conversion Loss), 99
TCO (Telecommunications Outlets), 67
TCP (Transmission Control Protocol), 292
defined, 297
headers, 296–297
packets
terminating connections, 299–300
transmitting, 298
ports, 573
three-packet TCP handshakes, 298, 299
TCP/IP (Transmission Control Protocol/Internet Protocol), 21–22
Application layer, 294, 295–296
defined, 292
gateway addresses, 326–327
Internet layer, 294, 301
ARP, 301–303
ICMP, 302–303
IGMP, 303–304
IP, 301
IPv4 addressing, 312–313
6to4 prefix, 335
ARIN, 315
assigning, 315
classes, 313
classful addresses, 317
decimal/binary octets, 314
dual stacks, 336
host IP addresses, 315
network/host bits, 314–315
non-Internet-routable IP addresses, 316
private IP addresses, 316
RIR, 315

structure of, 313
transitioning to IPv6, 335–337
IPv6 addressing, 333–335
6to4 prefix, 335
anycast addresses, 335
CIDR, 337–338
DAD, 337
defined, 333
dual stacks, 336
interface (host) identifiers, 335
IPng, 333
link-local addresses, 335, 336–337
multicast addresses, 335
SLAAC, 336–337
transitioning to, 335–337
unicast addresses, 335
layers of, summary, 294
Network interface layer, 294, 304
number conversions
binary-to-decimal conversions, 306–307
decimal-to-binary conversions, 307–309
hexadecimal numbers, 309–311
ports, 295
subnet masks
ANDing, 361–362
applying, 318
CIDR-subnet mask conversions, 329–330
classful addresses, 317
creating, 321
defined, 317
examples of, 324–326
magic numbers, 323
original/default subnet masks, 319
subnetting process, 319–323
subnetting
broadcast addresses, 322
classful addresses, 317
defined, 318–319
magic numbers, 323
network addresses, 322
process of, 319–323
VLSM, 331–332
supernetting, 328–329
CIDR, 329–330
CIDR blocks, 330–331
VLSM, 331–332
Transport layer, 294, 296–301
TCTL (Transverse Conversion Transfer Loss), 99
TE (Telecommunications Enclosures), structured cabling, 67
teaming, NIC, 18
telco, defined, 270
telco clouds, 270–271
telecommunications closets
components of, 69–70
structured cabling, 67
terminating
cabling, 70
CAT6 horizontal cabling, 83–87
TCP connections, 299–300
twisted-pair cabling, 78–80
DTX-1800 certification reports, 103, 104
testing
cabling, 92–93
ACR, 93, 95
attenuation (insertion loss), 92, 93–94
channel specifications, 93–96
delay skew, 93, 96
ELFEXT, 93, 95
near-end testing, 94
NEXT, 92, 93, 94–95
propagation delay, 93, 96
PSACR, 93, 95, 96
PSELFEXT, 93, 95, 96
PSNEXT, 93, 94
return loss, 93, 95–96
LAN, 45–48
near-end testing, 94
physical security, 659
thermostats, smart, 663
Thin/Net cabling, bus topologies, 8
three-packet TCP handshakes, 298, 299
TIA (Telecommunications Industry Alliance)
defined, 66
TIA/EIA 568-A cabling standard, 66
TIA/EIA 568-B cabling standard, 66
TIA/EIA 569B cabling standard, 66–67
ticks metrics, 461
time, aging, 244
TKIP (Temporal Key Integrity Protocol), 639
TLD (Top-Level Domains), 539
TLS (Transport Layer Security) protocol, 598
Token Ring hubs, 7
Token Ring topologies, 6, 7–8

tokens, passing, 7
topologies, 7
bus topologies, 8–9
campus network hierarchical topologies, 69
defined, 6
hub-and-spoke topologies. *See* star topologies
mesh topologies, 10–11
point-to-point topologies, 6
star topologies, 9, 10, 39
Token Ring topologies, 6, 7–8
top-to-bottom (top-down) troubleshooting approach, 569
TR (Telecommunications Rooms), structured cabling, 67
traffic analysis, 552–565
traffic filtering, 268
traffic flows
CBS, 276
CIR, 276
EBS, 276
EIR, 276
LAN, 269
transceivers
optical networking, 154
WLAN, 177
translation bridges, 235
transmission strands, fiber-optic cabling, 126
transmit power
802.11a (Wi-Fi 2) wireless standard, 181
WLAN, 180
transmitting data, long hauls, 134
transparent bridges, 235
transport input none command, 627
Transport layer
OSI model, 13
protocol, 296
TCP/IP, 294, 296–301
tree hierarchies, DNS, 539–540
troubleshooting
AP, 213
bottom-to-top (bottom-up) approach, 569
cabling, 102
DTX-1800 certification reports, 103, 104
failures to meet manufacturer specifications, 102–104
multimeters, 110
performance, 110
stretching, 102
WLAN, 215
channel utilization, WLAN, 214–215
compatibility (wireless), 213
connectivity, 110
deauthentication/disassociation attacks, 215
DHCP, 216, 571–572
divide-and-conquer approach, 569
fiber-optic cabling, 162–163
gateways, 571
home networks, 31–32
IP addresses, 570
IP networks, 568–573
LAN, 45–48
load issues (WLAN), 215
name resolution, 571
networks
bottom-to-top (bottom-up) approach, 569
divide-and-conquer approach, 569
isolating problems, 14
spot-the-difference approach, 569
top-to-bottom (top-down) approach, 569
ping command, 14
printers, 216
router interfaces, 387–392
signal strength, WLAN, 214
spot-the-difference approach, 569
SSID, 215
subnet masks, 570–571
switches, 429–434
TCP ports, 573
top-to-bottom (top-down) approach, 569
UDP ports, 573
wired networks, 31–32
wireless networks (Wi-Fi), 31–32, 213
AP, 213
cabling, 215
channel utilization, 214–215
compatibility, 213
deauthentication/disassociation attacks, 215
DHCP, 216
extending wireless ranges, 214
frequencies, 214
interference, 214
load issues, 215
signal strength, 214
SSID, 215
wireless printers, 216

wireless routers, 213
WPA, 215
wireless printers, 216
wireless routers, 213
WLAN. *See* wireless networks (Wi-Fi)
trunk ports, 408–409
TTLS (Tunneled Transport Layer Security) protocol, 598
tunable lasers, 141–142
tunneling protocols
L2F, 650
L2TP, 650, 651
PPTP, 650
VPN, 648–651
turning off SSID broadcasts, 33
twisted-pair cabling. *See also* physical layer cabling
ELTCTL, 99
F/UTP, 99
LCL, 99
return loss, 93, 95–96
STP cabling, 76–77
TCL, 99
TCTL, 99
terminating, 78–80
UTP cabling
CAT3, 75, 76
CAT5, 74, 75, 76
CAT5e, 74, 75, 76, 79–82
CAT6, 74, 75, 76, 79–82
CAT6a, 75, 76
CAT7, 74, 75, 79–82
CAT7a, 75
CAT8, 74, 75, 79–82
"two-deep" rule, optical networking, 152–153
TXT records (Text records), 544
Type 1 hypervisors, 680
Type 2 hypervisors, 680
Type 5 encryption algorithm, 627
Type 7 encryption algorithm, 627

U

UDP (User Datagram Protocol)
defined, 300
headers, 300–301
packet transfers, 300–301
ports, 573
UHF (Ultra-Hugh Frequency) RFID tags, 203
unconnected fibers, fiber-optic cabling, 146
UNI (User-Network Interfaces), 274
unicast addresses, 335, 533
U-NII (Unlicensed-National Information Infrastructure), 802.11a (Wi-Fi 2) wireless standard, 180–181
UPC connectors, 64, 146
uplink ports, 42
uptime, routers, 369
USB interfaces, 250
User EXEC mode (Router>), 366–371
UTM (Unified Threat Management), 624
UTP (Unshielded Twisted-Pair) cabling
CAT3, 75, 76
CAT5, 74, 75, 76
patch cabling, 87–90
straight-through cabling, 87–90
CAT5e, 74, 75, 76, 79–82
patch cabling, 87–90
straight-through cabling, 87–90
test examples, 104–109
CAT6, 74, 75, 76, 79–82, 83–87
CAT6a, 75, 76
CAT7, 74, 75, 79–82
CAT7a, 75
CAT8, 74, 75, 79–82
F/UTP, 99
UTP couplers, 64

V

V.44/V.34 modem standard, 643
V.92/V.90 modem standard, 643
VCSEL (Vertical Cavity Surfacd Emitting Lasers), 141
verifying
network connections with ping command, 240–241
network settings, 570
VFL (Visual Fault Locators), 162
VIC-4FXS/DID, 251
virtual desktops, remote desktops and, 695
virtualization, 679, 682
32-bit CPU architectures, 679
64-bit CPU architectures, 679
advantages/disadvantages of, 680–681
caches, 679
cores, 679

defined, 679
disaster recovery, 681
dongles, 682
guest machines, 680
hardware keys, 682
host machines, 680
Hyper-V, 682–690
hypervisors, 680
Live Migration, 681
SD-WAN, 697
setting up, 682–690
snapshots, 681
VM, 680, 681–682
vMotion, 681
XenMotion, 681
viruses, 602–603, 610–611
VLAN (Virtual Local Area Networks), 407. ***See also*** **LAN**
assigning memberships, 408
dynamic VLAN, 408
hopping, 599
port assignments, 431
port-based VLAN, 407
protocol-based VLAN, 408
PVST, 423–424
static VLAN, 408, 414–418
subinterfaces, 418–419
switch security, 634
tag-based VLAN, 408
tags, 277, 408–409
trunk ports, 408–409
VSTP, 423–424
VTP, 409
VLSM (Variable-Length Subnet Masking), 331–332
OSPF, 478
static routing, 451
VM (Virtual Machines), 680, 681–682
vMotion, 681
voice gateways, 251
voice interface cards, 251
VoIP (Voice Over Internet Protocol)
jitter, 252
networks
congestion (bottlenecking), 252
latency, 252
QoS, 251–253
queuing/buffering, 252
routers, 251, 252–253
VPN (Virtual Private Networks), 34
CHAP, 649, 650
client-to-site VPN, 648
EAP, 650
GRE, 648–649
headends, 647
IP tunnels, 648
IPSec, 651
L2F, 650
L2TP, 650
MD5 hashing algorithm, 649, 650
mGRE, 649
PAP, 649–650
PPP, 649
PPTP, 650
remote access VPN, 648
remote client configurations, 652–657
SHA, 649, 650
site-to-site VPN, 648
tunneling protocols, 648–651
VSTP (VLAN Spanning Tree Protocol), 423–424
VTP (VLAN Trunking Protocol), 409

W

WAN (Wide Area Networks), 5
defined, 526
example of, 526
HSSI, 270
interconnecting LAN, 267–277
OC, 270
SD-WAN, 697
war chalking, 641
war driving, 641
war flying, 641
warm sites, disaster recovery, 731
WDM (Wavelength Division Multiplexing), 130, 143
diplexers, 154
transceivers, 154
web filters, 620
well-known (reserved) ports, 295
WEP (Wired Equivalent Privacy), 638–639
whois command, 530
WIC2AM (WAN Interface Cards), 251

Wi-Fi 1 (802.11b) wireless standard, 24, 181, 183
Wi-Fi 2 (802.11a) wireless standard, 24, 180–181, 183
Wi-Fi 3 (802.11g) wireless standard, 24, 181, 182, 183
Wi-Fi 4 (802.11n) wireless standard, 24, 181, 182, 183
Wi-Fi 5 (802.11ac) wireless standard, 24, 182, 183
Wi-Fi 6 (802.11ax) wireless standard, 25, 182, 183
Wi-Fi Alliance, 24–25, 183
Wi-Fi networks. *See* wireless networks (Wi-Fi)
wildcard bits, 482–483
WiMAX (Worldwide Interoperability for Microwave Access), 199–200
Windows 10
command prompt, 18
firewalls, 611–615
home networks, connecting, 32
MAC addresses, obtaining, 20
PuTTY software, 256–259
remote client VPN configurations, 652
wire speed routing, 247
wired networks
access points (AP), 28
advantages/disadvantages of, 24
appearance, 31
broadband modems/gateways, 28
cable modems, 28, 29
components of, 25–30
cost, 30
data speeds, 30
defined, 24
DSL modems, 29–30
ease of implementation, 31
example of, 25
home access, 31
hubs, 25
network adapters, 26
public access, 31
routers, 26–27
switches, 26
troubleshooting, 31–32
wireless routers, 28
wireless bridges, 187–189, 236
wireless controllers, 189
wireless LAN adapters, 185
wireless networks (Wi-Fi), 24, 174
3G wireless standard, 204
4G wireless standard, 204
5G wireless standard, 204
802.11 wireless standard, 175–176
MAC layer, 176
PHY layer, 176
802.11a (Wi-Fi 2) wireless standard, 180–181, 183
802.11ac (Wi-Fi 5) wireless standard, 182, 183
802.11ax (Wi-Fi 6) wireless standard, 182, 183
802.11b (Wi-Fi 1) wireless standard, 181, 183
802.11g (Wi-Fi 3) wireless standard, 181, 182, 183
802.11i wireless standard, 183
802.11n (Wi-Fi 4) wireless standard, 181, 182, 183
802.11r wireless standard, 183
802.16a (WiMAX) wireless standard, 200
access points (AP), 28
ad hoc networks, 176, 177
advantages/disadvantages of, 24
AES, 640
ANT+ wireless technology, 183
antennas, 186
dish (parabolic reflector) antennas, 209
EIRP, 210
extending wireless ranges, 214
multipoint distributions, 209–211
omnidirectional antennas, 208–209
placement of, 207
remote installations, 211
RF site surveys, 209–211
selecting, 208–209
site surveys, 207
Yagi antennas, 209
AP, 177–178, 186–187, 189–190
appearance, 31
associations, 186–187, 193
basic setup, 185–186
beacons, 638
beamforming, 182
Bluetooth
BLE technology, 197
enabling connections, 198–199
inquiry procedures, 197
output power classes, 197
paging procedures, 197
piconets, 197–198
security, 641
broadband modems/gateways, 28
BSS, 176, 177, 178
BWA, 199–200
cable modems, 28, 29

cabling, troubleshooting, 215
captive portals, 32
CCMP, 639–640
CDMA, 204
channel bonding, 179
channel utilization, 214–215
components of, 25–30
configuring, 185–195, 206–211
connecting, 32
cost, 30
CSMA/CD, 178
data speeds, 30
deauthentication/disassociation attacks, 215
defined, 24, 174
device density, 189
DHCP, 216
distance, 189–190
DSL modems, 29–30
DSSS, 179
EAP, 640, 650
ease of implementation, 31
EDGE, 204
encryption, 33
ESS, 178
example of, 25
FHSS, 180
firewalls, 34
frequencies, troubleshooting, 214
frequency channels, 179
geofencing, 204
hand-offs, 178
home access, 31
hopping sequences, 180
hotspots, 32, 641
HSPA+204
hubs, 25
IEEE wireless standards, 24–25
interference, troubleshooting, 214
IP addressing, 34–36
ISM band, 179
last-mile connections, 200
LEAP, 640
load issues, troubleshooting, 215
loss of association, 193
LTE/4G, 204
MIMO, 182
mobile (cellular) communications, 204
MU-MIMO, 182
NAT, 34
defined, 34
private IP addresses, 35
public IP addresses, 35
network adapters, 26
NFC, 204
OFDM, 180
point-to-multipoint WLAN configuration case study, 206–211
printers, 216
pseudorandom numbering sequences, 180
public access, 31
RADIUS, 640
ranges (wireless), extending, 32, 195, 214
RFID, 200, 201
backscatter, 200
block diagram, 200–201
inlays, 202
readers, 201
tags, 200, 201–203
roaming, 178
routers, 26–27
RSSI, 214
security, 33–34, 637
AES, 640
Bluetooth, 641
CCMP, 639–640
EAP, 640, 650
guidelines, 640–641
hotspots, 641
jamming, 638
LEAP, 640
Open Authentication, 638
RADIUS, 640
shared-key authentication, 638
SSID, 638
TKIP, 639
war chalking, 641
war driving, 641
war flying, 641
WEP, 638–639
WPA, 639
WPA2, 639–640
WPA3, 640

signal strength, 191–195, 214
site surveys, 190–195, 207, 209–211
snapshots, 192–193
spatial diversity, 186
SSID, 186, 215
switches, 26
transceivers, 177
transmit power, 180
troubleshooting, 31–32, 213
AP, 213
cabling, 215
channel utilization, 214–215
compatibility, 213
deauthentication/disassociation attacks, 215
DHCP, 216
extending wireless ranges, 214
frequencies, 214
interference, 214
load issues, 215
signal strength, 214
SSID, 215
wireless printers, 216
wireless routers, 213
WPA, 215
VPN, 34
war chalking, 641
war driving, 641
war flying, 641
Wi-Fi Alliance, 24–25, 183
WiMAX, 199–200
wireless bridges, 187–189
wireless controllers, 189
wireless LAN adapters, 185
wireless routers, 25, 28
wireless standards, 32
WLC, 189–190
WMN, 176
WPA, 215, 639
WPA2, 639–640
WPA3, 640
Z-Wave wireless technology, 183
wireless printers, troubleshooting, 216
wireless routers, 25, 28
home networks, 28
troubleshooting, 213
wireless standards
802.1x (dot1x) wireless standard, 633
802.11 wireless standard, 175–176
ad hoc networks, 176, 177
AP, 177–178
BSS, 176, 177, 178
channel bonding, 179
CSMA/CD, 178
DSSS, 179
ESS, 178
FHSS, 180
frequency channels, 179
hand-offs, 178
hopping sequences, 180
ISM band, 179
MAC layer, 176
OFDM, 180
Open Authentication, 638
PHY layer, 176
pseudorandom numbering sequences, 180
roaming, 178
shared-key authentication, 638
transceivers, 177
transmit power, 180
WMN, 176
802.11a (Wi-Fi 2) wireless standard, 24, 180–181, 183
802.11ac (Wi-Fi 5) wireless standard, 24, 182, 183
802.11ax (Wi-Fi 6) wireless standard, 25, 182, 183
802.11b (Wi-Fi 1) wireless standard, 24, 181, 183
802.11g (Wi-Fi 3) wireless standard, 24, 181, 182, 183
802.11i wireless standard, 183
802.11n (Wi-Fi 4) wireless standard, 24, 181, 182, 183
802.11r wireless standard, 183
802.16a (WiMAX) wireless standard, 200
wireless networks (Wi-Fi), 32
wiremaps, 82
Wireshark, network traffic analysis, 560–565
wiring standards
T568A wiring standard
color maps, 78–80

defined, 78
pinouts, 79
T568B wiring standard
color maps, 78–80
defined, 78
pinouts, 79
WLAN (Wireless Local Area Networks), 174. ***See also*** **LAN**
3G wireless standard, 204
4G wireless standard, 204
5G wireless standard, 204
802.11 wireless standard, 175–176
MAC layer, 176
PHY layer, 176
802.11a (Wi-Fi 2) wireless standard, 180–181, 183
802.11ac (Wi-Fi 5) wireless standard, 182, 183
802.11ax (Wi-Fi 6) wireless standard, 182, 183
802.11b (Wi-Fi 1) wireless standard, 181, 183
802.11g (Wi-Fi 3) wireless standard, 181, 182, 183
802.11i wireless standard, 183
802.11n (Wi-Fi 4) wireless standard, 181, 182, 183
802.11r wireless standard, 183
802.16a (WiMAX) wireless standard, 200
ad hoc networks, 176, 177
AES, 640
ANT+ wireless technology, 183
antennas, 186
dish (parabolic reflector) antennas, 209
EIRP, 210
extending wireless ranges, 214
multipoint distributions, 209–211
omnidirectional antennas, 208–209
placement of, 207
remote installations, 211
RF site surveys, 209–211
selecting, 208–209
site surveys, 207
Yagi antennas, 209
AP, 177–178, 186–187, 189–190
associations, 186–187, 193
basic setup, 185–186
beacons, 638
beamforming, 182
Bluetooth
BLE technology, 197
enabling connections, 198–199
inquiry procedures, 197
output power classes, 197
paging procedures, 197
piconets, 197–198
security, 641
BSS, 176, 177, 178
BWA, 199–200
cabling, troubleshooting, 215
CCMP, 639–640
CDMA, 204
channel bonding, 179
channel utilization, 214–215
configuring, 185–195, 206–211
CSMA/CD, 178
deauthentication/disassociation attacks, 215
defined, 174
device density, 189
DHCP, 216
distance, 189–190
DSSS, 179
EAP, 640, 650
EDGE, 204
ESS, 178
FHSS, 180
frequencies, troubleshooting, 214
frequency channels, 179
geofencing, 204
hand-offs, 178
hopping sequences, 180
hotspots, 641
HSPA+204
interference, troubleshooting, 214
ISM band, 179
last-mile connections, 200
LEAP, 640
load issues, troubleshooting, 215
loss of association, 193
LTE/4G, 204
MIMO, 182

mobile (cellular) communications, 204
MU-MIMO, 182
NFC, 204
OFDM, 180
point-to-multipoint WLAN configuration case study, 206–211
printers, 216
pseudorandom numbering sequences, 180
RADIUS, 640
range extenders, 195
ranges (wireless), extending, 214
RFID, 200, 201
backscatter, 200
block diagram, 200–201
inlays, 202
readers, 201
tags, 200, 201–203
roaming, 178
RSSI, 214
security, 637
AES, 640
Bluetooth, 641
CCMP, 639–640
EAP, 640, 650
guidelines, 640–641
hotspots, 641
jamming, 638
LEAP, 640
Open Authentication, 638
RADIUS, 640
shared-key authentication, 638
SSID, 638
TKIP, 639
war chalking, 641
war driving, 641
war flying, 641
WEP, 638–639
WPA, 639
WPA2, 639–640
WPA3, 640
signal strength, 191–195, 214
site surveys, 190–195, 207, 209–211
snapshots, 192–193
spatial diversity, 186
SSID, 186, 215
transceivers, 177
transmit power, 180
troubleshooting, 213
AP, 213
cabling, 215
channel utilization, 214–215
compatibility, 213
deauthentication/disassociation attacks, 215
DHCP, 216
extending wireless ranges, 214
frequencies, 214
interference, 214
load issues, 215
signal strength, 214
SSID, 215
wireless printers, 216
wireless routers, 213
WPA, 215
war chalking, 641
war driving, 641
war flying, 641
Wi-Fi Alliance, 183
WiMAX, 199–200
wireless bridges, 187–189
wireless controllers, 189
wireless LAN adapters, 185
WLC, 189–190
WMN, 176
WPA, 215, 639
WPA2, 639–640
WPA3, 640
Z-Wave wireless technology, 183
WLC (Wireless LAN Controllers), 189–190
WMN (Wireless Mesh Networks), 176
WO (Work-Area Outlets), 68
work areas, 67
worms, 603
WPA (Wi-Fi Protected Access), 215, 639
WPA2 (Wi-Fi Protected Access version 2), 639–640
WPA3 (Wi-Fi Protected Access version 3), 640
write memory (wr m) command, 457
WSN (Wireless Sensor Networks), ANT+ wireless technology, 183

X

X2, 153–154
xDSL
modems, security, 644–646
services, 645
XenMotion, 681
XENPAK, 153–154
XFP, 153–154
XPAK, 153–154

Y

Yagi antennas, 209

Z

zero-day attacks, 604
zero dispersion wavelengths, 138–139
ZTerm serial communications software, configuring, 259–261
Z-Wave wireless technology, 183

Exclusive Offer – 40% OFF

Pearson IT Certification Video Training

livelessons

pearsonitcertification.com/video

Use coupon code **PITCVIDEO40** during checkout.



Video Instruction from Technology Experts



Advance Your Skills

Get started with fundamentals, become an expert, or get certified.



Train Anywhere

Train anywhere, at your own pace, on any device.



Learn

Learn from trusted author trainers published by Pearson IT Certification.

Try Our Popular Video Training for FREE!

pearsonitcertification.com/video

Explore hundreds of **FREE** video lessons from our growing library of Complete Video Courses, LiveLessons, networking talks, and workshops.

PEARSON
IT CERTIFICATION

pearsonitcertification.com/video

ALWAYS LEARNING

PEARSON



REGISTER YOUR PRODUCT at PearsonITcertification.com/register

Access Additional Benefits and SAVE 35% on Your Next Purchase

- Download available product updates.
- Access bonus material when applicable.
- Receive exclusive offers on new editions and related products. (Just check the box to hear from us when setting up your account.)
- Get a coupon for 35% for your next purchase, valid for 30 days. Your code will be available in your PITC cart. (You will also find it in the Manage Codes section of your account page.)

Registration benefits vary by product. Benefits will be listed on your account page under Registered Products.

PearsonITcertification.com–Learning Solutions for Self-Paced Study, Enterprise, and the Classroom

Pearson is the official publisher of Cisco Press, IBM Press, VMware Press, Microsoft Press, and is a Platinum CompTIA Publishing Partner–CompTIA's highest partnership accreditation.

At **PearsonITcertification.com** you can

- Shop our books, eBooks, software, and video training.
- Take advantage of our special offers and promotions (pearsonitcertifcation.com/promotions).
- Sign up for special offers and content newsletters (pearsonitcertifcation.com/newsletters).
- Read free articles, exam profiles, and blogs by information technology experts.
- Access thousands of free chapters and video lessons.

Connect with PITC – Visit PearsonITcertifcation.com/community

Learn about PITC community events and programs.

PEARSON IT CERTIFICATION

Addison-Wesley • Cisco Press • IBM Press • Microsoft Press • Pearson IT Certification • Prentice Hall • Que • Sams • VMware Press

To receive your 10% off Exam Voucher, register your product at:

www.pearsonitcertification.com/register

and follow the instructions.

10percent_ad.indd 1

Networking Essentials, Sixth Edition, Companion Website

Access interactive study tools on this book's companion website, including Net-Challenge Simulation Software, Wireshark Network Protocol Analyzer Software capture examples, standalone Network+ quizzes, and flashcards helping you master key terms.

To access the companion website, simply follow these steps:

1. Go to **www.pearsonITcertification.com/register**.
2. Enter the print book ISBN: **9780137455928**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

If you have any issues accessing the companion website, you can contact our support team by going to **http://pearsonitp.echelp.org.**

Pearson

Where are the companion content files?



Register this digital version of
Networking Essentials, Sixth Edition
to access important downloads.

Register this eBook to unlock the companion files. Follow these steps:

1. Go to **pearsonITcertification.com/account** and log in or create a new account.
2. Enter the ISBN: **9780137455928** (NOTE: Please enter the print book ISBN provided to register the eBook you purchased.)
3. Answer the challenge question as proof of purchase.
4. Click on the "Access Bonus Content" link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

This eBook version of the print title does not contain the practice test software that accompanies the print book.

You May Also Like—Premium Edition eBook and Practice Test. To learn about the Premium Edition eBook and Practice Test series, visit **pearsonITcertification.com/practicetest**

The Professional and Personal Technology Brands of Pearson

Addison Wesley · Cisco Press · informIT · PEARSON IT Certification · que · SAMS