PEARSON IT

CYBERSECURITY CURRICULUM

SIXTH EDITION

NETWORKING ESSENTIALS

A CompTIA® Network+ N10-008 Textbook

JEFFREY S. BEASLEY
PIYASAT NILKAEW

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

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.

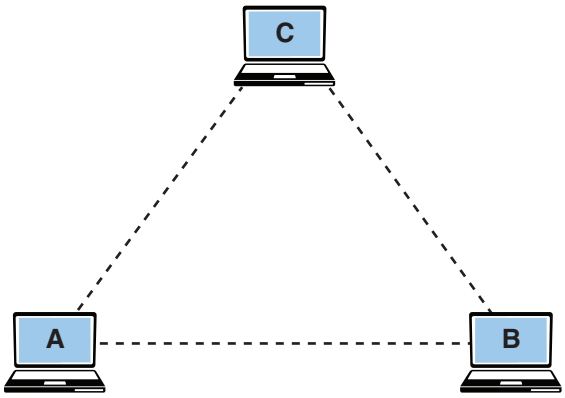

FIGURE 4-1 An example of an independent basic service set, or ad hoc, network.

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

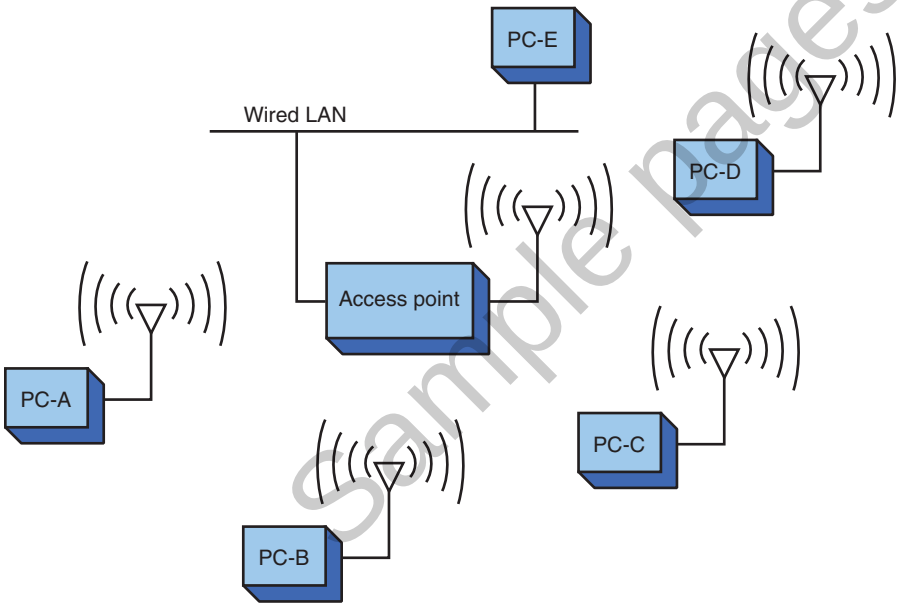

FIGURE 4-2 Adding an access point to a basic service set.

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.

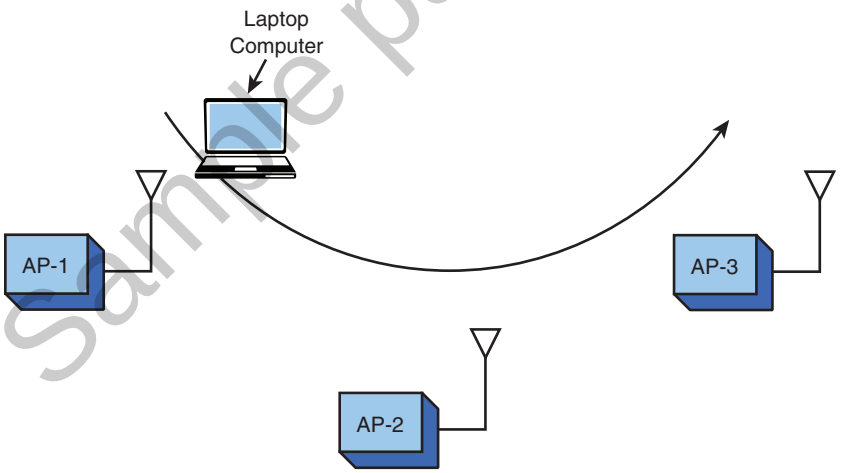

FIGURE 4-3 An example of an extended service set used for increased user mobility.

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

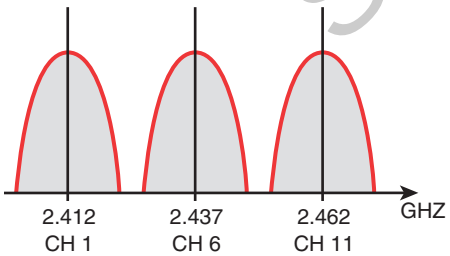

FIGURE 4-4 An example of the three channels in the DSSS spectrum.

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.

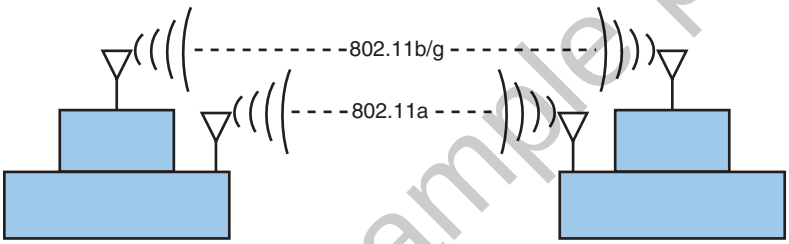

FIGURE 4-5 An example of an 802.11a installation and an 802.11b link running alongside each other.

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