PEARSON IT

CYBERSECURITY CURRICULUM

FIFTH EDITION

NETWORKING ESSENTIALS

A CompTIA Network+ N10-007 Textbook

JEFFREY S. BEASLEY
PIYASAT NILKAEW

TABLE OF CONTENTS

Introduction xxii

CHAPTER 1 Introduction to Computer Networks 2

Chapter Outline 3
Objectives 3
Key Terms 3
1-1 Introduction 5
1-2 Network Topologies 7
Section 1-2 Review 11
Test Your Knowledge 11
1-3 The OSI Model 12
Section 1-3 Review 14
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 37
1-6 Assembling an Office LAN 38
Section 1-6 Review 43
Test Your Knowledge 43
1-7 Testing and Troubleshooting a LAN 44
Section 1-7 Review 47
Test Your Knowledge 47
Summary 48
Questions and Problems 48
Certification Questions 56

CHAPTER 2 Physical Layer Cabling: Twisted-Pair 60

Chapter Outline 61
Objectives 61
Key Terms 61

2-1 Introduction 63
2-2 Structured Cabling 64
Horizontal Cabling 67
Section 2-2 Review 70
Test Your Knowledge 70
2-3 Unshielded Twisted-Pair Cable 71
Shielded Twisted-Pair Cable 74
Section 2-3 Review 75
Test Your Knowledge 75
2-4 Terminating CAT6/5e/5 UTP Cables 76
Computer Communication 78
Straight-through and Crossover Patch Cables 80
Section 2-4 Review 87
Test Your Knowledge 88
2-5 Cable Testing and Certification 89
Section 2-5 Review 93
Test Your Knowledge 93
2-6 10 Gigabit Ethernet over Copper 94
Overview 94
Alien Crosstalk 95
Signal Transmission 96
Section 2-6 Review 97
Test Your Knowledge 97
2-7 Troubleshooting Cabling Systems 98
Installation 98
Cable Stretching 99
Cable Failing to Meet Manufacturer Specifications 99
CAT5e Cable Test Examples 100
Section 2-7 Review 106
Test Your Knowledge 106
Summary 107
Questions and Problems 107
Certification Questions 115

CHAPTER 3 Physical Layer Cabling: Fiber Optics 118

Chapter Outline 119
Objectives 119
Key Terms 119
3-1 Introduction 120

3-2 The Nature of Light 123
Graded-Index Fiber 127
Single-Mode Fibers 127
Section 3-2 Review 128
Test Your Knowledge 129
3-3 Fiber Attenuation and Dispersion 129
Attenuation 129
Dispersion 131
Dispersion Compensation 132
Section 3-3 Review 133
Test Your Knowledge 133
3-4 Optical Components 134
Intermediate Components 135
Detectors 136
Fiber Connectorization 138
Section 3-4 Review 139
Test Your Knowledge 140
3-5 Optical Networking 140
Defining Optical Networking 141
Building Distribution 143
Campus Distribution 147
Section 3-5 Review 150
Test Your Knowledge 150
3-6 Safety 151
Section 3-6 Review 152
Test Your Knowledge 152
Summary 153
Questions and Problems 153
Certification Questions 156

CHAPTER 4 Wireless Networking 158

Chapter Outline 159
Objectives 159
Key Terms 159
4-1 Introduction 160
4-2 The IEEE 802.11 Wireless LAN Standard 161
Section 4-2 Review 169
Test Your Knowledge 170

4-3 802.11 Wireless Networking 170
Section 4-3 Review 180
Test Your Knowledge 181
4-4 Bluetooth, WiMAX, RFID, and Mobile Communications 181
Bluetooth 181
WiMAX 184
Radio Frequency Identification 185
Mobile (Cellular) Communications 188
Section 4-4 Review 189
Test Your Knowledge 189
4-5 Configuring a Point-to-Multipoint Wireless LAN: A Case Study 190
Step 1. Conducting an Antenna Site Survey 191
Step 2. Establishing a Point-to-Point Wireless Link to the Home Network 191
Steps 3 and 4. Configuring the Multipoint Distribution and Conducting an RF Site Survey 192
Step 5. Configuring the Remote Installations 194
Section 4-5 Review 195
Test Your Knowledge 195
Summary 196
Questions and Problems 196
Critical Thinking 200
Certification Questions 201

CHAPTER 5 Interconnecting the LANs 204

Chapter Outline 205
Objectives 205
Key Terms 205
5-1 Introduction 206
5-2 The Network Bridge 207
Section 5-2 Review 212
Test Your Knowledge 213
5-3 The Network Switch 213
Hub and Switch Comparison 216
Managed Switches 218
Multilayer Switches 223
Section 5-3 Review 224
Test Your Knowledge 224
5-4 The Router 225
The Router Interface: Cisco 2800 Series 226
Section 5-4 Review 229
Test Your Knowledge 230

5-5 Interconnecting LANs with the Router 230
Gateway Address 233
Network Segments 233
Section 5-5 Review 233
Test Your Knowledge 234
5-6 Configuring the Network Interface: Auto-negotiation 234
Auto-negotiation Steps 235
Full-Duplex/Half-Duplex 235
Section 5-6 Review 237
Test Your Knowledge 237
5-7 The Console Port Connection 238
Configuring the HyperTerminal Software (Windows) 240
Configuring the ZTerm Serial Communications Software (Mac) 242
Section 5-7 Review 244
Test Your Knowledge 244
Summary 245
Questions and Problems 245
Critical Thinking 250
Certification Questions 251

CHAPTER 6 TCP/IP 254

Chapter Outline 255
Objectives 255
Key Terms 255
6-1 Introduction 256
6-2 The TCP/IP Layers 257
The Application Layer 258
The Transport Layer 260
The Internet Layer 264
The Network Interface Layer 266
Section 6-2 Review 267
Test Your Knowledge 267
6-3 Number Conversion 268
Binary-to-Decimal Conversion 268
Decimal-to-Binary Conversion 270
Hexadecimal Numbers 271
Section 6-3 Review 274
Test Your Knowledge 274
6-4 IPv4 Addressing 274
Section 6-4 Review 278
Test Your Knowledge 278

6-5 Subnet Masks 278
Section 6-5 Review 285
Test Your Knowledge 286
6-6 CIDR Blocks 286
Section 6-6 Review 289
Test Your Knowledge 289
6-7 IPv6 Addressing 290
IPv6 CIDR 294
Section 6-7 Review 295
Test Your Knowledge 295
Summary 296
Questions and Problems 296
Critical Thinking 305
Certification Questions 306

CHAPTER 7 Introduction to Switch Configuration 310

Chapter Outline 311
Objectives 311
Key Terms 311
7-1 Introduction 312
7-2 Introduction to VLANs 313
Virtual LANs 313
Section 7-2 Review 315
Test Your Knowledge 315
7-3 Introduction to Switch Configuration 316
Hostname 316
Enable Secret 317
Setting the Line Console Passwords 317
Static VLAN Configuration 319
Networking Challenge: Switch Configuration 323
Section 7-3 Review 323
Test Your Knowledge 324
7-4 Spanning-Tree Protocol 324
Section 7-4 Review 326
Test Your Knowledge 327
7-5 Network Management 327
Configuring SNMP 328
Section 7-5 Review 331
Test Your Knowledge 331

7-6 Power over Ethernet 332
Section 7-6 Review 334
Test Your Knowledge 335
7-7 Switch Security 335
Switch Port Security 337
STP Special Features 338
Section 7-7 Review 340
Test Your Knowledge 340
Summary 341
Questions and Problems 341
Critical Thinking 348
Certification Questions 348

CHAPTER 8 Introduction to Router Configuration 352

Chapter Outline 353
Objectives 353
Key Terms 353
8-1 Introduction 354
8-2 Router Fundamentals 355
Layer 3 Networks 356
Section 8-2 Review 362
Test Your Knowledge 362
8-3 The Router's User EXEC Mode (Router>) 363
The User EXEC Mode 363
Router Configuration Challenge: User EXEC Mode 366
Section 8-3 Review 368
Test Your Knowledge 369
8-4 The Router's Privileged EXEC Mode (Router#) 369
Hostname 371
Enable Secret 371
Setting the Line Console Passwords 372
FastEthernet Interface Configuration 373
Serial Interface Configuration 374
Router Configuration Challenge: Privileged EXEC Mode 376
Section 8-4 Review 378
Test Your Knowledge 379
Summary 380
Questions and Problems 380
Critical Thinking 385
Certification Questions 387

CHAPTER 9 Routing Protocols 390

Chapter Outline 391
Objectives 391
Key Terms 391
9-1 Introduction 392
9-2 Static Routing 393
Gateway of Last Resort 400
Configuring Static Routes 400
Networking Challenge: Static Routes 403
Section 9-2 Review 404
Test Your Knowledge 404
9-3 Dynamic Routing Protocols 405
Section 9-3 Review 406
Test Your Knowledge 407
9-4 Distance Vector Protocols 407
Section 9-4 Review 410
Test Your Knowledge 410
9-5 Configuring RIP and RIPv2 410
Configuring Routes with RIP 412
Configuring Routes with RIPv2 417
Networking Challenge: RIPv2 418
Section 9-5 Review 419
Test Your Knowledge 420
9-6 Link State Protocols 420
Section 9-6 Review 423
Test Your Knowledge 423
9-7 Configuring the Open Shortest Path First (OSPF) Routing Protocol 424
Networking Challenge: OSPF 429
Section 9-7 Review 430
Test Your Knowledge 430
9-8 Advanced Distance Vector Protocol: Configuring Enhanced Interior Gateway Routing Protocol (EIGRP) 430
Configuring Routes with EIGRP 431
Networking Challenge: EIGRP 436
Section 9-8 Review 437
Test Your Knowledge 437
9-9 IPv6 Routing 438
IPv6 Static Routing 438
RIP for IPv6 438
OSPF for IPv6 439

EIGRP for IPv6 440
Section 9-9 Review 440
Test Your Knowledge 440
Summary 442
Questions and Problems 442
Critical Thinking 455
Certification Questions 456

CHAPTER 10 Internet Technologies: Out to the Internet 458

Chapter Outline 459
Objectives 459
Key Terms 459
10-1 Introduction 461
10-2 The Line Connection 463
Data Channels 464
Point of Presence 465
Section 10-2 Review 468
Test Your Knowledge 468
10-3 Remote Access 468
Analog Modem Technologies 469
Cable Modems 470
xDSL Modems 470
Remote Access Server 472
Section 10-3 Review 475
Test Your Knowledge 475
10-4 Metro Ethernet/Carrier Ethernet 476
Ethernet Service Types 477
Service Attributes 479
Section 10-4 Review 479
Test Your Knowledge 480
10-5 Network Services: DHCP and DNS 480
The DHCP Data Packets 482
DHCP Deployment 483
Network Services: DNS 485
Internet Domain Names 486
Section 10-5 Review 491
Test Your Knowledge 492
10-6 Internet Routing: BGP 492
Section 10-6 Review 495
Test Your Knowledge 495

10-7 Analyzing Internet Data Traffic 495
Utilization/Errors Strip Chart 497
Network Layer Matrix 497
Network Layer Host Table 498
Frame Size Distribution 498
Section 10-7 Review 499
Test Your Knowledge 500
Summary 501
Questions and Problems 501
Certification Questions 507

CHAPTER 11 Troubleshooting 510

Chapter Outline 511
Objectives 511
Key Terms 511
11-1 Introduction 512
11-2 Analyzing Computer Networks 514
Using Wireshark to Inspect Data Packets 514
Using Wireshark to Capture Packets 517
Section 11-2 Review 519
Test Your Knowledge 519
11-3 Analyzing Computer Networks: FTP Data Packets 519
Section 11-3 Review 520
Test Your Knowledge 521
11-4 Analyzing Campus Network Data Traffic 521
Section 11-4 Review 524
Test Your Knowledge 524
11-5 Troubleshooting the Router Interface 525
Section 11-5 Review 529
Test Your Knowledge 529
11-6 Troubleshooting the Switch Interface 530
Section 11-6 Review 534
Test Your Knowledge 534
11-7 Troubleshooting Fiber Optics: The OTDR 535
Section 11-7 Review 537
Test Your Knowledge 537
11-8 Troubleshooting Wireless Networks 537
Hardware Issues 537
Signal Strength Problems 538

Frequency Interference Problems 538
Load Issues 538
DHCP Issues 538
SSID Issues 538
Securing Wi-Fi Issues 538
Wireless Printer Issues 538
Wireless Router Issues 539
Extending the Wireless Range 539
Selecting Wireless Channels 539
Wireless Compatibility 539
Cable Issues 540
Switch Uptime 540
Section 11-8 Review 540
Test Your Knowledge 540
11-9 Troubleshooting IP Networks 541
Verifying Network Settings 543
Investigating IP Address Issues 543
Finding Subnet Mask Issues 544
Looking for Gateway Issues 544
Identifying Name Resolution Issues 544
Investigating DHCP Issues 545
Checking for Blocked TCP/UDP Ports 546
Section 11-9 Review 546
Test Your Knowledge 547
Summary 548
Questions and Problems 548
Certification Questions 555

CHAPTER 12 Network Security 558

Chapter Outline 559
Objectives 559
Key Terms 559
12-1 Introduction 560
12-2 Intrusion: How Attackers Gain Control of a Network 562
Social Engineering 562
Password Cracking 563
Packet Sniffing 564
Vulnerable Software 566
Preventing Vulnerable Software Attacks 567

Viruses and Worms 569
Section 12-2 Review 570
Test Your Knowledge 571
12-3 Denial of Service 571
Distributed Denial of Service Attacks 574
Section 12-3 Review 574
Test Your Knowledge 574
12-4 Security Software and Hardware 575
Antivirus Software 575
Personal Firewalls 575
Configuring Firewall Settings for Windows 10 576
Configuring Firewall Settings for Mac OS X 580
Configuring Firewall Settings for Linux 581
Firewalls 582
Other Security Appliances 584
Computer Forensics 585
Section 12-4 Review 586
Test Your Knowledge 587
12-5 Managing Network Access 587
Section 12-5 Review 589
Test Your Knowledge 589
12-6 Introduction to Virtual Private Networks 590
VPN Tunneling Protocols 591
Configuring a Remote Access VPN Server 593
Configuring a Remote Client's VPN Connection 593
Windows 10/8/7 VPN Client 593
Mac OS X VPN Client 594
Cisco VPN Client 595
Section 12-6 Review 599
Test Your Knowledge 599
12-7 Wireless Security 600
Section 12-7 Review 604
Test Your Knowledge 604
Summary 605
Questions and Problems 605
Critical Thinking 610
Certification Questions 611

CHAPTER 13 Cloud Computing and Virtualization 614

Chapter Outline 615
Objectives 615
Key Terms 615
13-1 Introduction 616
13-2 Virtualization 617
Setting Up Virtualization on Windows 8 or 10 620
Section 13-2 Review 628
Test Your Knowledge 628
13-3 Cloud Computing 629
Infrastructure as a Service (IaaS) 631
Platform as a Service (PaaS) 632
Software as a Service (SaaS) 632
Cloud Infrastructures 632
Section 13-3 Review 633
Test Your Knowledge 634
13-4 Enterprise Storage 634
Section 13-4 Review 635
Test Your Knowledge 635
Summary 637
Questions and Problems 637
Certification Questions 640

CHAPTER 14 Codes and Standards 642

Chapter Outline 643
Objectives 643
Key Terms 643
14-1 Introduction 644
14-2 Safety Standards and Codes 645
Design and Construction Requirements for Exit Routes (29 CFR 1910.36) 645
Maintenance, Safeguards, and Operational Features for Exit Routes (29 CFR 1910.37) 646
Emergency Action Plans (29 CFR 1910.38) 647
Fire Prevention Plans (29 CFR 1910.39) 647
Portable Fire Extinguishers (29 CFR 1910.157) 648
Fixed Extinguishing Systems (29 CFR 1910.160) 648
Fire Detection Systems (29 CFR 1910.164) 650
Employee Alarm Systems (29 CFR 1910.165) 650
Hazard Communication (29 CFR 1910.1200) 651

HVAC Systems 652
Door Access 652
Section 14-2 Review 652
Test Your Knowledge 653
14-3 Industry Regulatory Compliance 653
FERPA 653
FISMA 653
GLBA 654
HIPAA 654
PCI DSS 654
International Export Controls 654
Section 14-3 Review 656
Test Your Knowledge 656
14-4 Business Policies, Procedures, and Other Best Practices 657
Memorandum of Understanding 657
Service Level Agreement 658
Master Service Agreement 658
Master License Agreement 658
Non-Disclosure Agreement 659
Statement of Work 659
Acceptable Use Policy 659
Incident Response Policy 659
Password Policy 660
Privileged User Agreement 660
Standard Operating Procedure 660
Other Best Practices 661
Asset Management 661
Section 14-4 Review 662
Test Your Knowledge 662
14-5 Business Continuity and Disaster Recovery 663
Section 14-5 Review 664
Test Your Knowledge 665
Summary 666
Questions and Problems 666
Certification Questions 672

Glossary 674

Index 692

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 the Ethernet frame
- Define the function of the network interface card
- Describe the purpose of the 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 of configuring a home network
- Discuss the issue of assembling an office LAN

Key Terms

local area network (LAN)
protocol
topology
Token Ring topology
token passing
IEEE
deterministic
Token Ring hub
bus topology
star topology
hub
multiport repeater
broadcast
switch
ports
mesh topology
OSI
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, physical, hardware, 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
wireless router
range extender
hotspot
service set identifier (SSID)
firewall protection
stateful packet inspection (SPI)
virtual private network (VPN)
network address translation (NAT)
overloading
port address translation (PAT)

Key Terms continued

port forwarding (port mapping)
CAT6 (category 6)
RJ-45
Mbps
numerics
ports
crossover
straight-through
uplink port
link light
link integrity test
link pulses
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 maybe checking the current price of an auction item on the Internet. All this requires computers to access multiple networks and share their resources. The multiple networks required to accomplish this are the local area network (LAN), the enterprise network, the campus area network (CAN), the metropolitan area network (MAN), Metro Ethernet, the personal area network (PAN), and the wide area network (WAN).

This text introduces the essentials for implementing modern computer networks. Each chapter steps you through the various modern networking technologies. The accompanying textbook web-link comes with the Net-Challenge simulator software developed specifically for this text. This software provides the reader with invaluable insight into the inner workings of computer networking and with the experience of configuring the router and switch for use in computer networks.

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

The ease of connecting to the Internet and the dramatic decrease in computer systems' cost has led to an explosion in their usage. Organizations such as corporations, colleges, and government agencies have acquired large numbers of single-user computer systems. These 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 these locally distributed computer networks allows users to exchange information (data) with other network members. It also allows resource sharing of expensive equipment such as file servers and high-quality graphics printers or access to more powerful computers for tasks too complicated for the local computer to process. The network commonly used to accomplish this interconnection is called a **local area network (LAN)**, which is a network of users that share computer resources in a limited area.

Table 1-1 outlines the CompTIA Network+ objectives 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 aid in your understanding of key concepts before you advance to the next section of the chapter. The end of the chapter includes a complete set of questions as well as sample certification exam-type questions.

1-2 NETWORK TOPOLOGIES

Local area networks are 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 ring, bus, and star, as illustrated in Figure 1-1.

Figure 1-2 shows an example of a LAN configured using the **Token Ring topology**. In this topology, a "token" (shown as a T) 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 is called **token passing** and is based on the **IEEE** 802.5 Token-Ring Network standard. A Token Ring network is a **deterministic** network, meaning each station connected to the network is ensured access for transmission of its messages at regular or fixed time intervals.

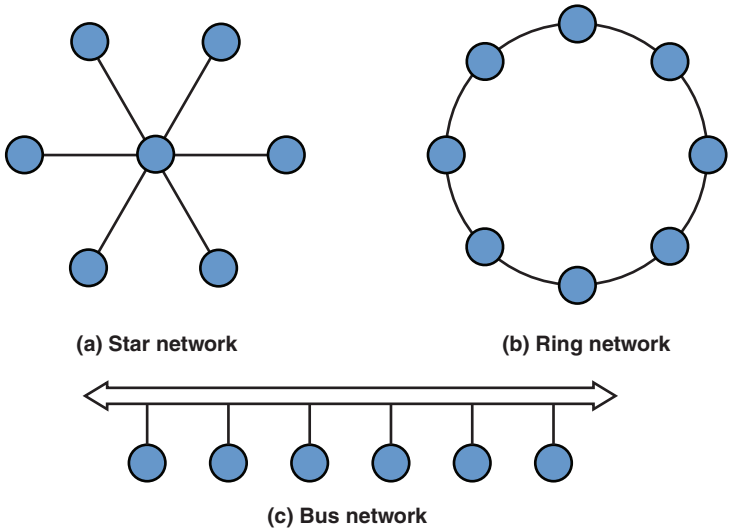

FIGURE 1-1 Network topologies. (From *Modern Electronic Communication* 9/e, by G. M. Miller & J. S. Beasley, 2008 Copyright © 2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

One disadvantage of the Token Ring system is that if an error changes the token pattern, it can cause the token to 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. Another disadvantage of the Token Ring network is from a troubleshooting and maintenance point of view. The Token Ring path must be temporarily broken (path interrupted) if a computer or any device connected to the network is to be removed or added to the network. This results in downtime for the network. A fix to

Protocol
Set of rules established for users to exchange information

Topology
Architecture of a network

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

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

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

this is to attach all the computers to a central **Token Ring hub**. Such a device manages the passing of the token rather than relying on individual computers to pass it, which improves the reliability of the network. It is important to note that the Token Ring network has become a "legacy" now in computer networking. Ethernet technology has replaced it in almost all modern computer networks.

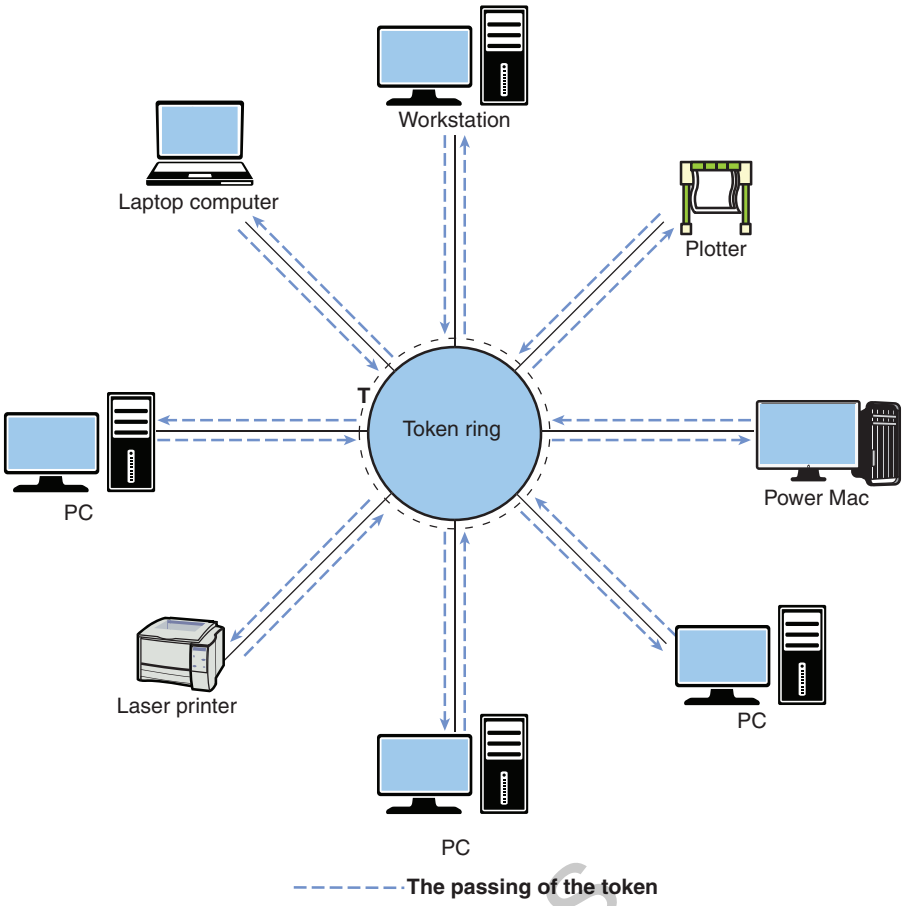

FIGURE 1-2 The Token Ring network topology.

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

Figure 1-3 illustrates a **bus topology**. In a bus system, 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. Referring to Figure 1-3, 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.

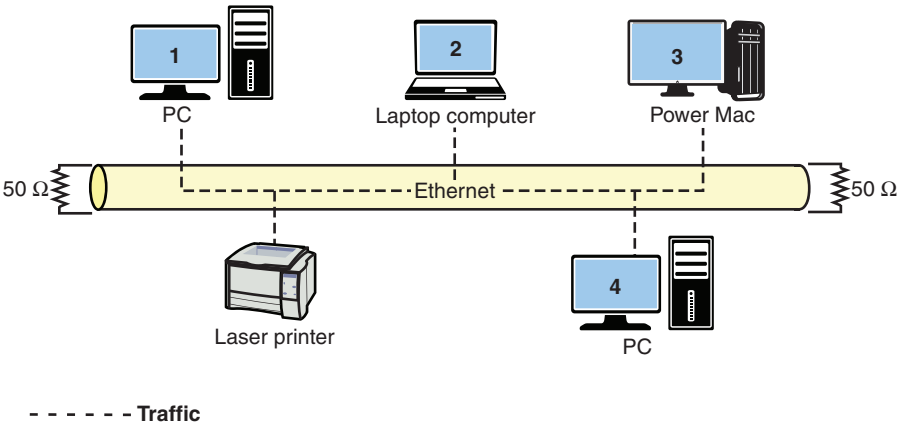

FIGURE 1-3 The bus topology.

The **star topology**, shown in Figure 1-4, is the most common networking topology in today's LANs. Twisted-pair cables (see Chapter 2, "Physical Layer Cabling: Twisted-Pair") with modular plugs are used to connect the computers and other networking devices. At the center of a star network is either a switch or a hub. This connects the network devices and facilitates the transfer of data. For example, if computer 1 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**, meaning 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 interconnected in the star network. The data traffic path for this is shown in the solid black arrowed lines going to all networking devices in Figure 1-4. This is similar to the bus topology in that all data traffic on the LAN is being seen by all computers. The fact that the hub broadcasts all data traffic to the devices connected to its network ports makes these devices of limited use in large networks.

To minimize unnecessary data traffic and isolate sections of the network, a **switch** can be used 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
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

Ports
The physical input/output interfaces to networking hardware

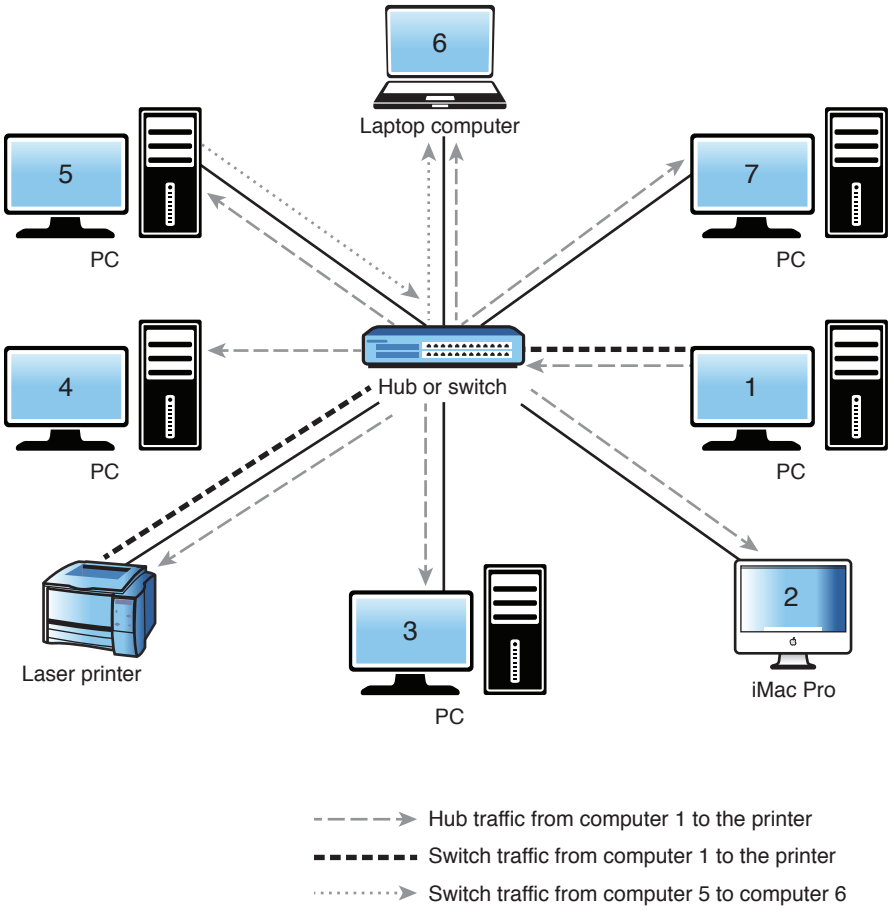

FIGURE 1-4 The star topology.

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 traffic path for the switched network is shown in the dotted lines in Figure 1-4. 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 shown in the dashed line in Figure 1-4. For 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

Another topology is the **mesh topology**, shown in Figure 1-5. In this topology, 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 cabling costs and the networking hardware cost (for example, the expense of 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.

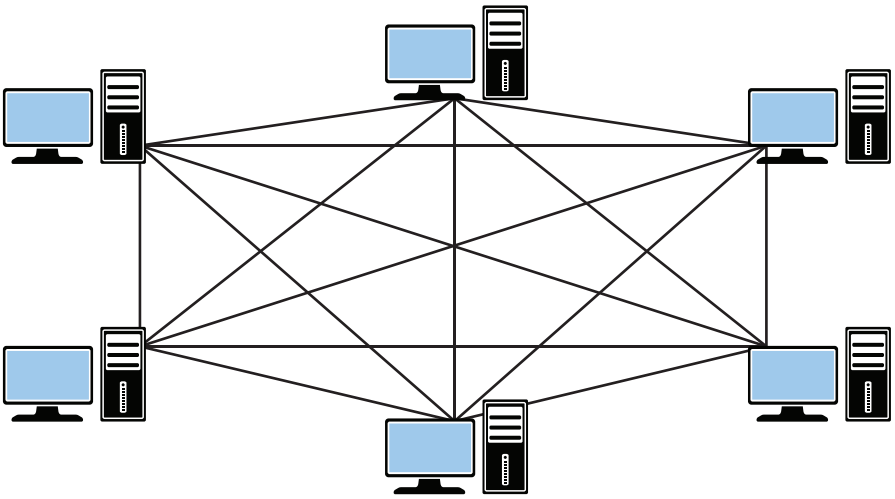

FIGURE 1-5 The mesh topology.

Section 1-2 Review

This section covers the following **Network+** exam objectives.

1.5 Compare and contrast the characteristics of network topologies, types, and technologies

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.

2.2 Given a scenario, determine the appropriate placement of networking devices and install/configure them

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 have developed an understanding that data from a hub is replicated out all ports. This means that 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. The term deterministic means
    a. access to the network is provided at random time intervals.
    b. access to the network is provided using CSMA/CD.
    c. access to the network is provided at fixed time intervals.
    d. None of these answers is 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

OSI
Open Systems Interconnection

OSI 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 to enable different types of networks to be linked together. The model contains seven layers, as shown in Figure 1-6. These layers describe networking functions from the physical network interface to the software applications interfaces. 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.

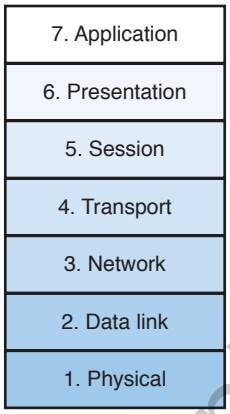

FIGURE 1-6 The seven layers of the OSI reference model.

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

Layer	Function	Examples
7. Application	Support for applications	HTTP, FTP, SMTP (email)
6. Presentation	Protocol conversion, data translation	ASCII, JPEG
5. Session	Establishes, manages, and terminates sessions	NFS, SQL
4. Transport	Ensures error-free packets	TCP, UDP
3. Network	Provides routing decisions	IP, IPX
2. Data link	Provides for the flow of data	MAC addresses
1. Physical	Signals and media	NICs, twisted-pair cable, fiber

Briefly, the OSI model consists of the following layers:

1. **Physical layer:** Provides the 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, UTP, fiber, and network interface cards (NICs).
2. **Data link layer:** Handles error recovery, flow control (synchronization), and sequencing (which terminals are sending and which are receiving). It is considered the "media access control layer" and is where media access control (MAC) addressing is defined. The Ethernet 802.3 standard is defined in this area, which is why the MAC address is sometimes called the Ethernet address.
3. **Network layer:** Accepts outgoing messages and combines messages or segments into packets, adding a header that includes routing information. It acts as the network controller. Examples of protocols working in this layer are Internet Protocol (IP) and Internetwork Packet Exchange (IPX).
4. **Transport layer:** Is concerned with message integrity between source and destination. It also segments/reassembles (the 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:** Provides the control functions necessary to establish, manage, and terminate the connections as required to satisfy the user request. Examples of technologies working in this layer are Network File System (NFS) and Structured Query Language (SQL).
6. **Presentation layer:** Accepts and structures the messages for the application. It translates the message from one code to another, if necessary. This layer is responsible for data compression and encryption. Examples of technologies working in this layer are American Standard Code for Information Interchange (ASCII) and Joint Photographic Experts Group (JPEG).
7. **Application layer:** Interacts with application programs that incorporate a communication component such as your Internet browser and email. This layer is responsible for logging the message in, interpreting the request, and determining what information is needed to support the request. Examples are Hypertext Transfer

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 your Internet browser and email

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 describe networking problems by layer number. For example, a physical link problem is described as a layer 1 problem; a router problem is a layer 3 issue; and so on.

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

Step 1 Is the connection to the machine down? (layer 1)
Step 2 Is the network down? (layer 3)
Step 3 Is a service on a specific machine down? (layer 7)

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 the network problem occurs.

For example, assume 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. (Note: 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 case of "request timed out," 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 do get knocked loose or break.

Section 1-3 Review

This section covers the following **Network+** exam objectives.

1.2 Explain devices, applications, protocols and services at their appropriate OSI layers

A network administrator needs to have a good understanding of all seven layers of the OSI model. Knowledge of the layers can help in isolating 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? (layer 1)
2. Is the network down? (layer 3)
3. Is a service on a specific machine down? (layer 7)

5.1 Explain the network troubleshooting methodology

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.

5.2 Given a scenario, use the appropriate tool

*This section presents 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 in which layer of the OSI model?
    a. Layer 7
    b. Layer 6
    c. Layer 5
    d. Layer 2
    e. None of these answers is correct.
4. The 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: The network address is another name for a layer 4 address.
   a. True
   b. False

1-4 THE ETHERNET LAN

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 via a joint effort among Xerox, Digital Equipment Corporation, and Intel. Basically, for a computer to "talk" on the 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).

Frame
A format that provides grouping of information for transmission

The information in an Ethernet network is exchanged in a **frame** format. The frame provides grouping of the information for transmission that includes the header, data, and trailer. The header consists of the preamble, start frame delimiter, destination and source addresses, and 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 structure of the Ethernet packet frame is shown in Figure 1-7 and described in Table 1-3.

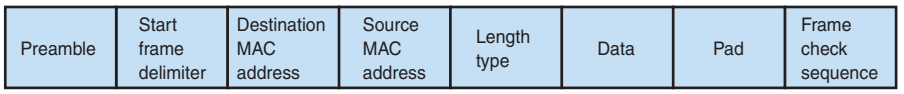

FIGURE 1-7 The data structure for the Ethernet frame. (From *Modern Electronic Communication* 9/e, by G. M. Miller & J. S. Beasley, 2008. Copyright © 2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

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

Preamble	An alternating pattern of 1s and 0s used for synchronization.
Start frame delimiter	A binary 8-bit sequence of 1 0 1 0 1 0 1 1 that 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 and IPX.)
Data	The variable length of data being transferred from the source to the destination.
Pad	A field used to bring the total number of bytes up to the minimum of 64 if the data field is less than 64 bytes.
Frame check sequence	A 4-byte CRC value used for error detection. The CRC is performed on the bits from the destination MAC address through the Pad fields. If an error is detected, the frame is discarded.

The minimum length of the 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.

How are the destination and source addresses for the 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 in what is called *NIC teaming*. The objective of teaming is to provide 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.

The NIC contains a unique network address called the **MAC address**. MAC stands for media access control. The MAC address is 6 bytes, or 48 bits, in length. The address is displayed in 12 hexadecimal 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.

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

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 that identifies the manufacturer of the network hardware

Ethernet, Physical, Hardware, 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

The MAC address, also called the **Ethernet**, **physical**, **hardware**, or **adapter address**, can be obtained from computers operating under Microsoft Windows by typing the **ipconfig /all** command while in the command mode or at the MS-DOS prompt. The following is an example of obtaining the MAC address for a computer operating under Windows 7 and Windows 10.

In Windows 7, you can enter **cmd** at the search field of the **Start** menu or find it by selecting **Start > Programs > Accessories > cmd**. In Windows 10, you can search for **command prompt** or **cmd** in the search field of the **Start** menu, as shown in Figure 1-8, or find it under **Start > Windows System**.

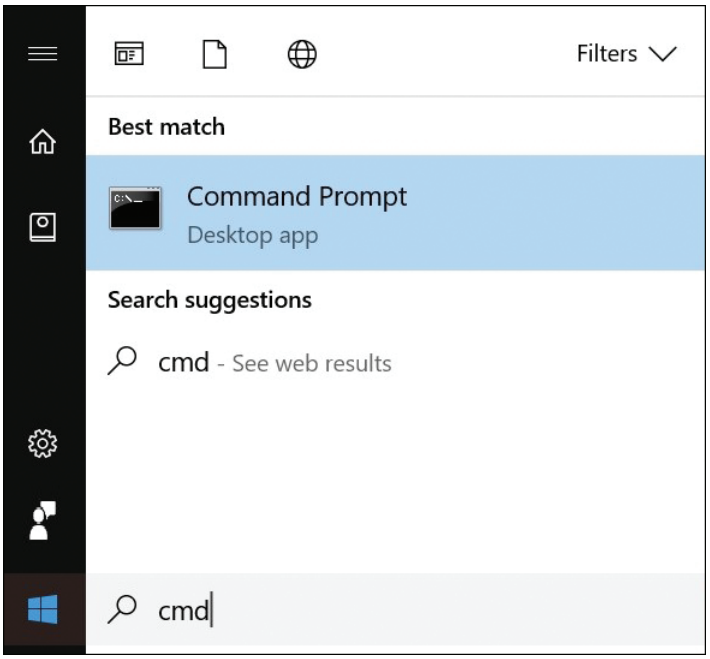

FIGURE 1-8 The command prompt in Windows 10.

At the command prompt, enter the **ipconfig /all** command, as shown in Figure 1-9. The **/all** switch on the command enables the MAC address information to be displayed—for this example, the information for computer 1. Note in this example that the **Host Name** for the computer is **COMPUTER-1**. This information is typically established when the computer's operating system is installed, but it can be changed 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** of **00-10-A4-13-99-2E** is the actual MAC address for the computer.

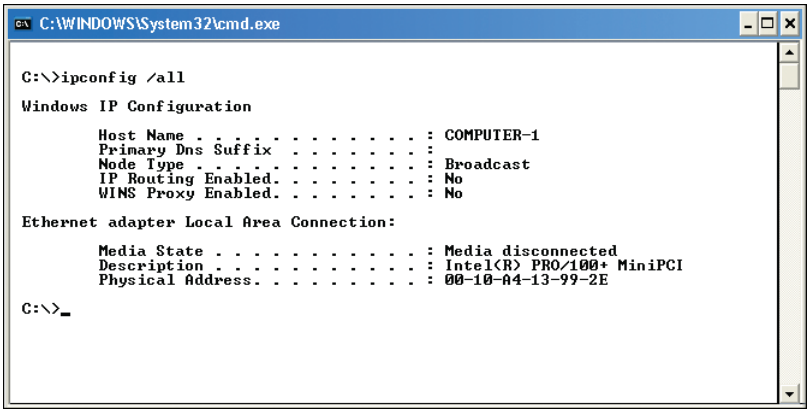

FIGURE 1-9 A typical text screen result when entering the ***ipconfig /all*** command in the command window.

Table 1-4 lists how the MAC address can be obtained for various computer operating systems.

TABLE 1-4 **Commands for Obtaining the MAC Address for Various Operating Systems**

Operating System	Command Sequence	Comments
Windows 98	Click **Start** > **Run**, type **winipcfg**, and press **Enter**.	The adapter address is the MAC address.
Windows NT	Click **Start** > **Run** and type **winipcfg**. At the command prompt, type **ipconfig /all** and press **Enter**.	The physical address is the MAC address.
Windows 2000	Click **Start** > **Run** and type **cmd**. At the command prompt, type **ipconfig /all** and then press **Enter**.	The physical address is the MAC address.
Windows Vista/XP	In Windows XP and Vista, enter the command window by selecting **Start** and then **Run**. At the command prompt, type **ipconfig /all** and then press **Enter**.	The physical address is the MAC address.
Windows 7, 8, 10	In Windows 7, 8, 10 the text **cmd** can be entered at the search field of the **Start** menu. In the command prompt, type **ipconfig/all**, and then press **Enter**.	The physical address is the MAC address.
Linux	At the command prompt, type **ifconfig**.	The HWaddr line contains the MAC address.