PEARSON IT

CYBERSECURITY CURRICULUM

FIFTH EDITION

NETWORKING ESSENTIALS

A CompTIA Network+ N10-007 Textbook

JEFFREY S. BEASLEY
PIYASAT NILKAEW

NETWORKING ESSENTIALS, FIFTH EDITION A COMPTIA NETWORK+ N10-007 TEXTBOOK

JEFFREY S. BEASLEY AND PIYASAT NILKAEW

Pearson
800 East 96th Street
Indianapolis, Indiana 46240 USA

Networking Essentials, Fifth Edition

ISBN-13: 978-0-7897-5874-3
ISBN-10: 0-7897-5874-1

Library of Congress Control Number: 2017957345

Printed in the United States of America

01 18

EDITOR-IN-CHIEF
Mark Taub

PRODUCT LINE MANAGER
Brett Bartow

DEVELOPMENT EDITOR
Marianne Bartow

MANAGING EDITOR
Sandra Schroeder

PROJECT EDITOR
Mandie Frank

COPY EDITOR
Kitty Wilson

INDEXER
Ken Johnson

PROOFREADER
Debbie Williams

TECHNICAL EDITOR
Sean Wilkins

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

PUBLISHING COORDINATOR
Vanessa Evans

DESIGNER
Chuti Prasertsith

COMPOSITOR
Tricia Bronkella

CONTENTS AT A GLANCE

TABLE OF CONTENTS

ABOUT THE AUTHORS

Jeff Beasley is a professor in the Information and Communications Technology program at New Mexico State University, where he teaches computer networking and many related topics. He is coauthor of *Modern Electronic Communication*, 9th edition, author of *Networking*, 2nd edition, and coauthor of *Networking Essentials*, 4th edition, and *Practical Guide to Advanced Networking.*

Piyasat Nilkaew is the director of Telecommunications and Networking at New Mexico State University. He has more than 20 years of experience in network management and consulting. He has extensive expertise in deploying and integrating multi-protocol and multi-vendor data, voice, and video network solutions. He is coauthor of *Networking Essentials*, 4th edition, and *Practical Guide to Advanced Networking.*

DEDICATIONS

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

This book is dedicated to my family, Boonsong, Pariya, June, Ariya, and Atisat —Piyasat Nilkaew

ACKNOWLEDGMENTS

I am grateful to the many people who have helped with this text. My sincere thanks go to the following technical consultants: Danny Bosch and Matthew Peralta, for sharing their expertise with optical networks and unshielded twisted-pair cabling, and Don Yates, for his help with the initial Net-Challenge software.

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

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

Your efforts are greatly appreciated.

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

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

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

—Jeffrey S. Beasley and Piyasat Nilkaew

ABOUT THE TECHNICAL REVIEWER

Sean Wilkins (@Sean_R_Wilkins) is an accomplished networking consultant and writer for infoDispersion (www.infodispersion.com). He has been in the IT field for more than 20 years, working with several large enterprises. Sean holds certifications with Cisco (CCNP/CCDP), Microsoft (MCSE), and CompTIA (A+ and Network+). He spends most of his time writing articles and books for various clients, including Cisco Press, Pearson, Tom's IT Pro, and PluralSight, and he is an active video training author for PluralSight.

Sean maintains various online social media accounts, including Facebook (https://www.facebook.com/infoDispersion), Twitter (@Sean_R_Wilkins), and LinkedIn (http://www.linkedin.com/in/swilkins/en), and maintains a website for centrally organizing his content across multiple clients (http://www.idisperse.info).

WE WANT TO HEAR FROM YOU!

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

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

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

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

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

READER SERVICES

Register your copy of ***Networking Essentials*** at www.pearsonitcertification.com for convenient access to the book's companion website as well as downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account. Enter the product ISBN, 9780789758743, and click Submit. Once the process is complete, you will find any available bonus content under Registered Products.

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

INTRODUCTION

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

In our years of teaching, we have observed that technology students prefer to learn "how to swim" after they have gotten wet and taken in a little water. Then they are ready for more challenges. In this book, we therefore show you the technology, how it is used, and why, and you can take the applications of the technology to the next level. Allowing you to experiment with the technology helps you develop a greater understanding.

ORGANIZATION OF THE TEXT

This book has been thoroughly updated to reflect the latest version of the CompTIA Network+ exam. *Networking Essentials,* 5th edition, is a practical, up-to-date, and hands-on guide to the basics of networking. Written from the viewpoint of the network administrator, it requires absolutely no previous experience with either network concepts or day-to-day network management. Throughout the text, you will gain an appreciation of how basic computer networks and related hardware are interconnected to form a network. You will come to understand the concepts of twisted-pair cable, fiber optics, LANs interconnection, TCP/IP configuration, subnet masking, basic router configuration, switch configuration and management, wireless networking, and network security.

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

Key Pedagogical Features

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

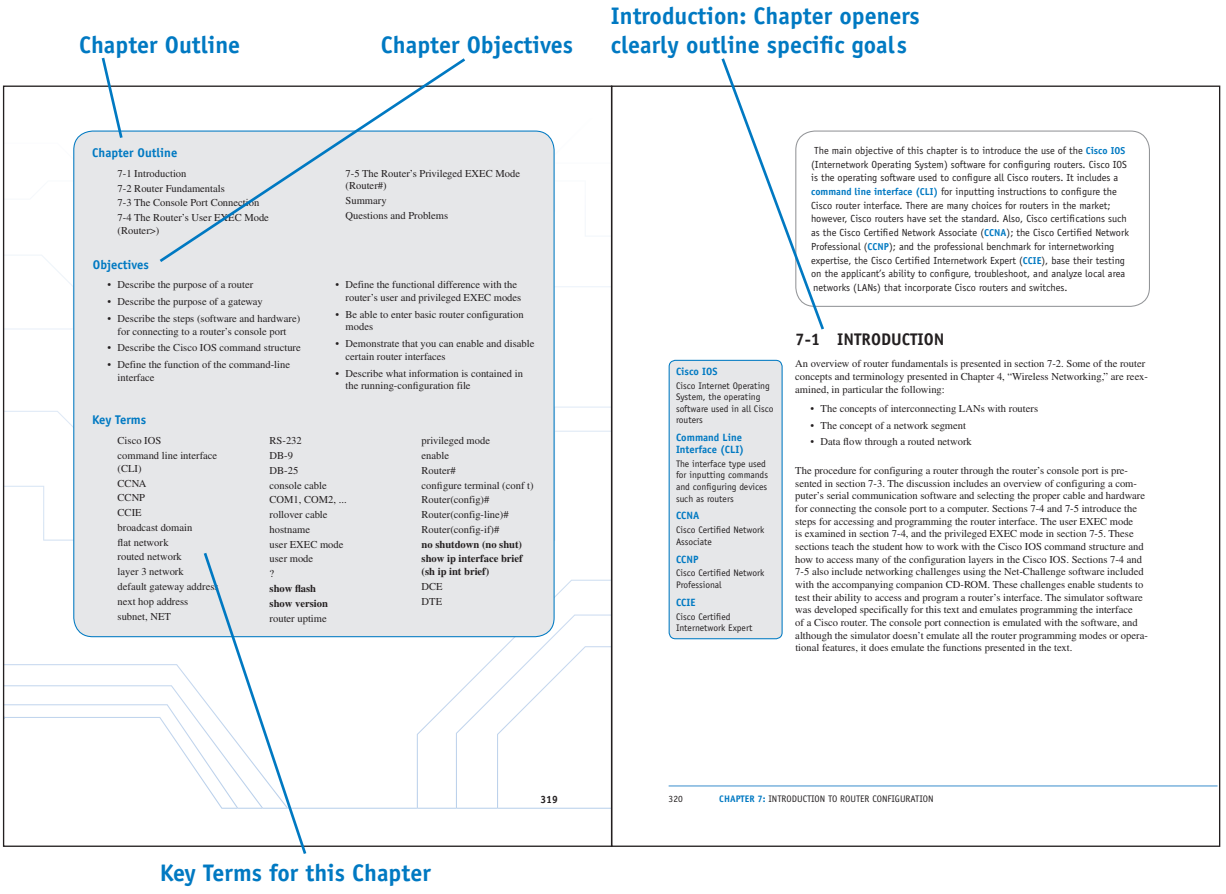


FIGURE I-1

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

Net-Challenge exercises are found throughout the text where applicable

Exercises challenge readers to undertake certain tasks

The status of the serial interfaces can be checked using the **sh ip int brief** command as demonstrated here:

```
Router# sh ip int brief
Interface        IP-Address      OK?   Method     Status     Protocol
FastEthernet0    10.10.20.250    YES   manual     up         up
FastEthernet1    10.10.200.1     YES   manual     up         up
FastEthernet2    10.10.100.1     YES   manual     up         up
Serial0          10.10.128.1     YES   manual     up         up
Serial1          10.10.64.1      YES   manual     up         up
```

Router Configuration Challenge: The Privileged EXEC Mode

Use the Net-Challenge software included with the companion CD-ROM to complete this exercise. Place the CD-ROM in your computer's drive. The software is located in the *NetChallenge* folder on the CD-ROM. Open the folder and click the *Net-ChallengeV4.exe* file. The program will open on your desktop with the screen shown previously in Figure 7-15. The Net-Challenge software is based on a three-router campus network setting. The topology for the network can be viewed by clicking the **View Topology** button. The network topology used in the software is shown in Figure 7-20. The software allows the user to configure each of the three routers and to configure the network interface for computers in the LANs attached to each router. Clicking one of the router symbols in the topology will enable you to view the IP address for the router required for the configuration.

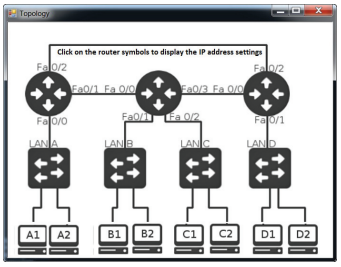


FIGURE 7-20 The network topology for Net-Challenge. The arrows indicate where to click to display the router IP address configurations.

Connection to each router is provided by clicking one of the three router buttons shown previously in Figure 7-17. An arrow is pointing to the buttons used to establish a console connection. Clicking a button connects the selected router to a terminal console session, enabling the simulated console terminal access to all three routers. The routers are marked with their default hostnames of Router A, Router B, and Router C. This challenge tests your ability to use router commands in the privileged EXEC mode, also called the enable mode. Click the *Net-ChallengeV4.exe* file to start the software. Next, click the **Select Challenge** button to open a list of challenges available with the software. Select the **Chapter 7 - Privileged EXEC Mode** challenge to open a check box screen. Each challenge will be checked when the task has been successfully completed:

1. Make sure you are connected to Router A by clicking the appropriate selection button.
2. Demonstrate that you can enter the router's privileged EXEC mode. The router screen should display **Router#**. The password is **Chile**.
3. Place the router in the terminal configuration mode [**Router(config)#**].
4. Use the **hostname** command to change the router hostname to RouterA.
5. Set the **enable secret** for the router to **Chile**.
6. Set the vty password to ConCarne.
7. Configure the three FastEthernet interfaces on RouterA as follows:

```
FastEthernet0/0     (fa0/0)     10.10.20.250        255.255.255.0
FastEthernet0/1     (fa0/1)     10.10.200.1         255.255.255.0
FastEthernet0/2     (fa0/2)     10.10.100.1         255.255.255.0
```

8. Enable each of the router FastEthernet interfaces using the **no shut** command.
9. Use the **sh ip interface brief** (**sh ip int brief**) command to verify that the interfaces have been configured and are functioning. For this challenge, the interfaces on Router B and Router C have already been configured.
10. Configure the serial interfaces on the router. Serial interface 0/0 is the DCE. The clock rate should be set to 56000. (use clock rate 56000) The IP addresses and subnet masks are as follows:

```
Serial 0/0      10.10.128.1      255.255.255.0
Serial 0/1      10.10.64.1       255.255.255.0
```

11. Use the **sh ip int brief** command to verify that the serial interfaces are properly configured. For this challenge, the interfaces on Router B and Router C have already been configured.
12. Use the **ping** command to verify that you have a network connection for the following interfaces:

```
RouterA FA0/1 (10.10.200.1) to RouterB FA0/2 (10.10.200.2)
RouterA FA0/2 (10.10.100.1) to RouterC FA0/2 (10.10.100.2)
```


FIGURE I-2

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

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

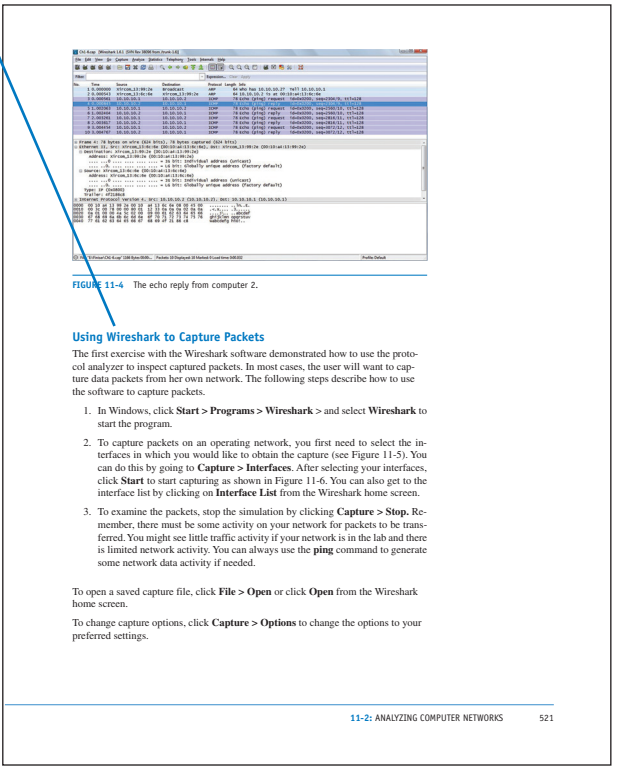


FIGURE 11-4 The echo reply from computer 2.

Using Wireshark to Capture Packets

The first exercise with the Wireshark software demonstrated how to use the protocol analyzer to inspect captured packets. In most cases, the user will want to capture data packets from her own network. The following steps describe how to use the software to capture packets.

1. In Windows, click **Start > Programs > Wireshark** > and select **Wireshark** to start the program.
2. To capture packets on an operating network, you first need to select the interfaces in which you would like to obtain the capture (see Figure 11-5). You can do this by going to **Capture > Interfaces**. After selecting your interfaces, click **Start** to start capturing as shown in Figure 11-6. You can also get to the interface list by clicking on **Interface List** from the Wireshark home screen.
3. To examine the packets, stop the simulation by clicking **Capture > Stop.** Remember, there must be some activity on your network for packets to be transferred. You might see little traffic activity if your network is in the lab and there is limited network activity. You can always use the **ping** command to generate some network data activity if needed.

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

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

FIGURE I-3

- *Key Terms* and their definitions are highlighted in the margins to foster inquisitiveness and ensure retention. Illustrations and photos are used throughout to aid in understanding the concepts discussed (see Figure I-4).

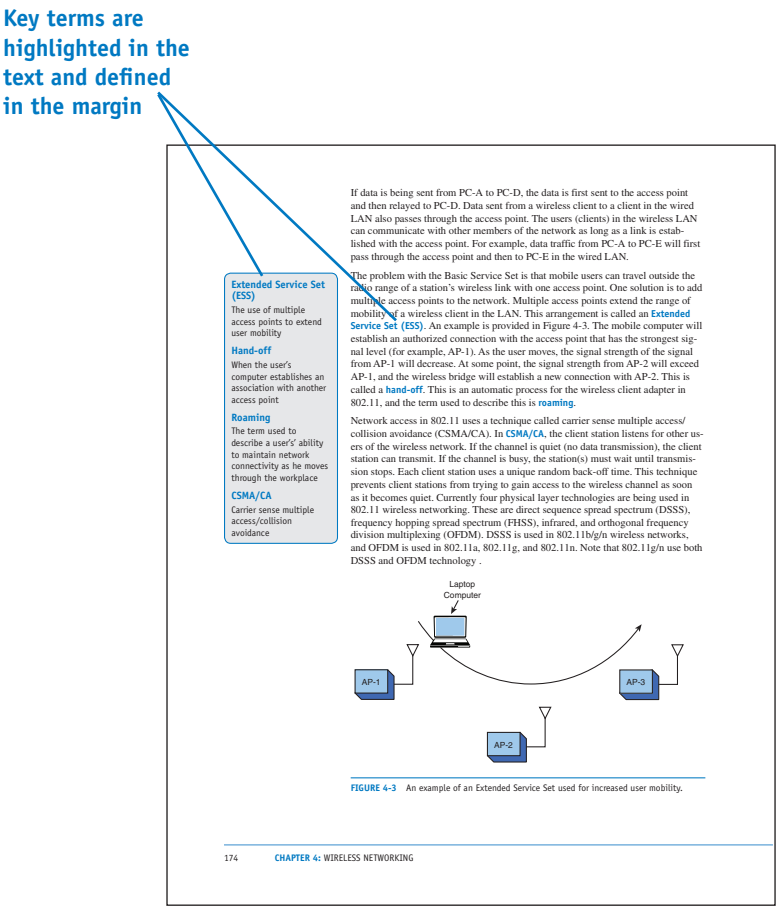


FIGURE I-4

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

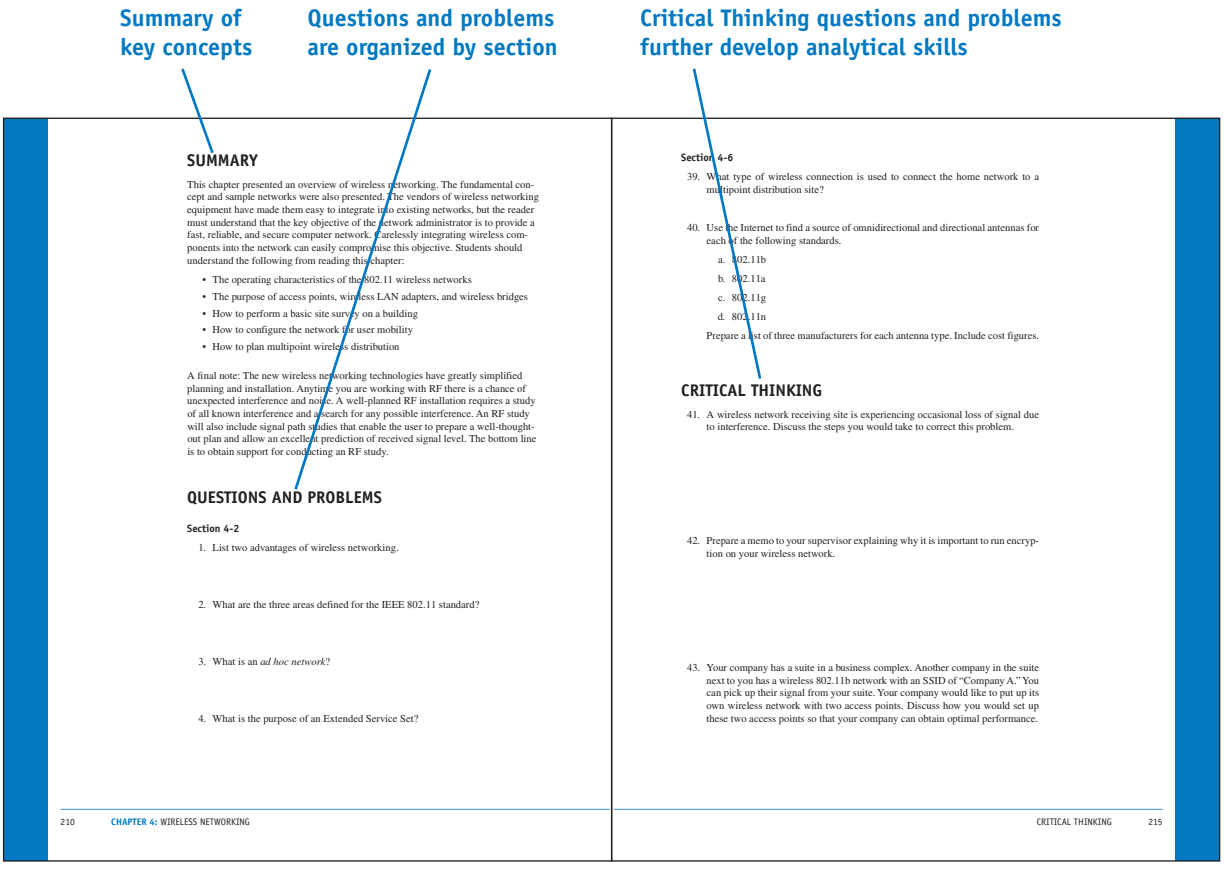
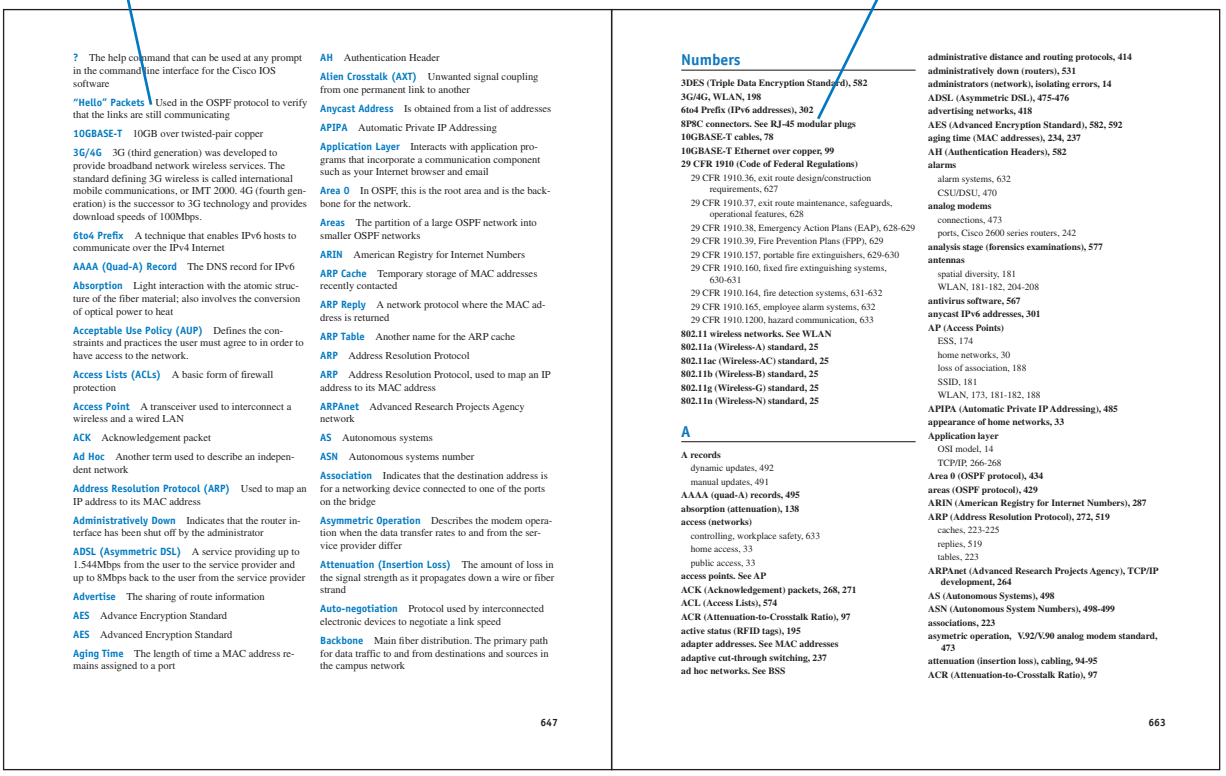


FIGURE I-5

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

Complete Glossary of terms and acronyms provide quick reference

Exhaustive Index provides quick reference



? The help command that can be used at any prompt in the command line interface for the Cisco IOS software

"Hello" Packets Used in the OSPF protocol to verify that the links are still communicating

10GBASE-T 10GB over twisted-pair copper

3G/4G 3G (third generation) was developed to provide broadband network wireless services. The standard defining 3G wireless is called international mobile communications, or IMT 2000. 4G (fourth generation) is the successor to 3G technology and provides download speeds of 100Mbps.

6to4 Prefix A technique that enables IPv6 hosts to communicate over the IPv4 Internet

AAAA (Quad-A) Record The DNS record for IPv6

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

Acceptable Use Policy (AUP) Defines the constraints and practices the user must agree to in order to have access to the network.

Access Lists (ACLs) A basic form of firewall protection

Access Point A transceiver used to interconnect a wireless and a wired LAN

ACK Acknowledgement packet

Ad Hoc Another term used to describe an independent network

Address Resolution Protocol (ARP) Used to map an IP address to its MAC address

Administratively Down Indicates that the router interface has been shut off by the administrator

ADSL (Asymmetric DSL) A service providing up to 1.544Mbps from the user to the service provider and up to 8Mbps back to the user from the service provider

Advertise The sharing of route information

AES Advance Encryption Standard

AES Advanced Encryption Standard

Aging Time The length of time a MAC address remains assigned to a port

AH Authentication Header

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

Anycast Address Is obtained from a list of addresses

APIPA Automatic Private IP Addressing

Application Layer Interacts with application programs that incorporate a communication component such as your Internet browser and email

Area 0 In OSPF, this is the root area and is the backbone for the network.

Areas The partition of a large OSPF network into smaller OSPF networks

ARIN American Registry for Internet Numbers

ARP Cache Temporary storage of MAC addresses recently contacted

ARP Reply A network protocol where the MAC address is returned

ARP Table Another name for the ARP cache

ARP Address Resolution Protocol

ARP Address Resolution Protocol, used to map an IP address to its MAC address

ARPAnet Advanced Research Projects Agency network

AS Autonomous systems

ASN Autonomous systems number

Association Indicates that the destination address is for a networking device connected to one of the ports on the bridge

Asymmetric Operation Describes the modem operation when the data transfer rates to and from the service provider differ

Attenuation (Insertion Loss) The amount of loss in the signal strength as it propagates down a wire or fiber strand

Auto-negotiation Protocol used by interconnected electronic devices to negotiate a link speed

Backbone Main fiber distribution. The primary path for data traffic to and from destinations and sources in the campus network

647

Numbers

3DES (Triple Data Encryption Standard), 582
3G/4G, WLAN, 198
6to4 Prefix (IPv6 addresses), 302
8P8C connectors. See RJ-45 modular plugs
10GBASE-T cables, 78
10GBASE-T Ethernet over copper, 99
29 CFR 1910 (Code of Federal Regulations)
29 CFR 1910.36, exit route design/construction requirements, 627
29 CFR 1910.37, exit route maintenance, safeguards, operational features, 628
29 CFR 1910.38, Emergency Action Plans (EAP), 628-629
29 CFR 1910.39, Fire Prevention Plans (FPP), 629
29 CFR 1910.157, portable fire extinguishers, 629-630
29 CFR 1910.160, fixed fire extinguishing systems, 630-631
29 CFR 1910.164, fire detection systems, 631-632
29 CFR 1910.165, employee alarm systems, 632
29 CFR 1910.1200, hazard communication, 633
802.11 wireless networks. See WLAN
802.11a (Wireless-A) standard, 25
802.11ac (Wireless-AC) standard, 25
802.11b (Wireless-B) standard, 25
802.11g (Wireless-G) standard, 25
802.11n (Wireless-N) standard, 25

A

A records
dynamic updates, 492
manual updates, 491
AAAA (quad-A) records, 495
absorption (attenuation), 138
access (networks)
controlling, workplace safety, 633
home access, 33
public access, 33
access points. See AP
ACK (Acknowledgement) packets, 268, 271
ACL (Access Lists), 574
ACR (Attenuation-to-Crosstalk Ratio), 97
active status (RFID tags), 195
adapter addresses. See MAC addresses
adaptive cut-through switching, 237
ad hoc networks. See BSS
administrative distance and routing protocols, 414
administratively down (routers), 531
administrators (network), isolating errors, 14
ADSL (Asymmetric DSL), 475-476
advertising networks, 418
AES (Advanced Encryption Standard), 582, 592
aging time (MAC addresses), 234, 237
AH (Authentication Headers), 582
alarms
alarm systems, 632
CSU/DSU, 470
analog modems
connections, 473
ports, Cisco 2600 series routers, 242
analysis stage (forensics examinations), 577
antennas
spatial diversity, 181
WLAN, 181-182, 204-208
antivirus software, 567
anycast IPv6 addresses, 301
AP (Access Points)
ESS, 174
home networks, 30
loss of association, 188
SSID, 181
WLAN, 173, 181-182, 188
APIPA (Automatic Private IP Addressing), 485
appearance of home networks, 33
Application layer
OSI model, 14
TCP/IP, 266-268
Area 0 (OSPF protocol), 434
areas (OSPF protocol), 429
ARIN (American Registry for Internet Numbers), 287
ARP (Address Resolution Protocol), 272, 519
caches, 223-225
replies, 519
tables, 223
ARPAnet (Advanced Research Projects Agency), TCP/IP development, 264
AS (Autonomous Systems), 498
ASN (Autonomous System Numbers), 498-499
associations, 223
asymetric operation, V.92/V.90 analog modem standard, 473
attenuation (insertion loss), cabling, 94-95
ACR (Attenuation-to-Crosstalk Ratio), 97

663

FIGURE I-6

Companion Website

The companion website includes the captured data packets used in the text. It also includes the Net-Challenge software, which was developed specifically for this text. A new addition to the fifth edition is the Network+ quiz software. This quiz bank includes more than 450+ quiz questions to help the student better learn the CompTIA terms featured in Network+ N10-007. The companion website also includes sample videos on network virtualization from the CompTIA Network+ N10-007 Complete Video Course. See the special offer for a discount on the full version of this product in the sleeve in the back of the book.

To access the companion website, go to: www.pearsonitcertification.com/register to register your book ISBN (9780789758743). Once you answer the challenge questions, your book will appear in the Registered Products tab on your account page. Simply click the Access Bonus Content link to access the companion website and download the digital assets that come with this book.

CHAPTER 1

INTRODUCTION TO COMPUTER NETWORKS

Chapter Outline

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.

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

Domain/ Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	**Networking Concepts**	
1.2	Explain devices, applications, protocols and services at their appropriate OSI layers	1-3
1.3	Explain the concepts and characteristics of routing and switching	1-3, 1-4, 1-5
1.4	Given a scenario, configure the appropriate IP addressing components	1-4, 1-6
1.5	Compare and contrast the characteristics of network topologies, types, and technologies	1-1, 1-2
1.6	Given a scenario, implement the appropriate wireless technologies and configurations	1-5
1.8	Explain the function of network services	1-7
2.0	**Infrastructure**	
2.1	Given a scenario, deploy the appropriate cabling solution	1-6
2.2	Given a scenario, determine the appropriate placement of networking devices on a network and install/ configure them	1-2, 1-4, 1-5
2.5	Compare and contrast WAN technologies	1-4, 1-5
3.0	**Network Operations**	
3.2	Compare and contrast business continuity and disaster recovery concepts	1-4
3.4	Given a scenario, use remote access methods	1-5
4.0	**Network Security**	
4.3	Given a scenario, secure a basic wireless network	1-5
4.4	Summarize common networking attacks	1-5
5.0	**Network Troubleshooting Tools**	
5.1	Explain the network troubleshooting methodology	1-3
5.2	Given a scenario, use the appropriate tool	1-3, 1-4, 1-7
5.4	Given a scenario, troubleshoot common wireless connectivity and performance issues	1-5

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.

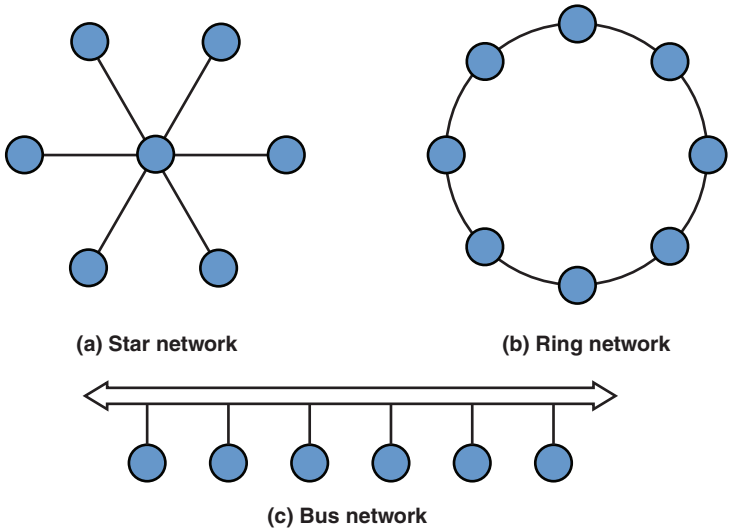


FIGURE 1-1 Network topologies. (From *Modern Electronic Communication* 9/e, by G. M. Miller & J. S. Beasley, 2008 Copyright © 2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

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

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

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.

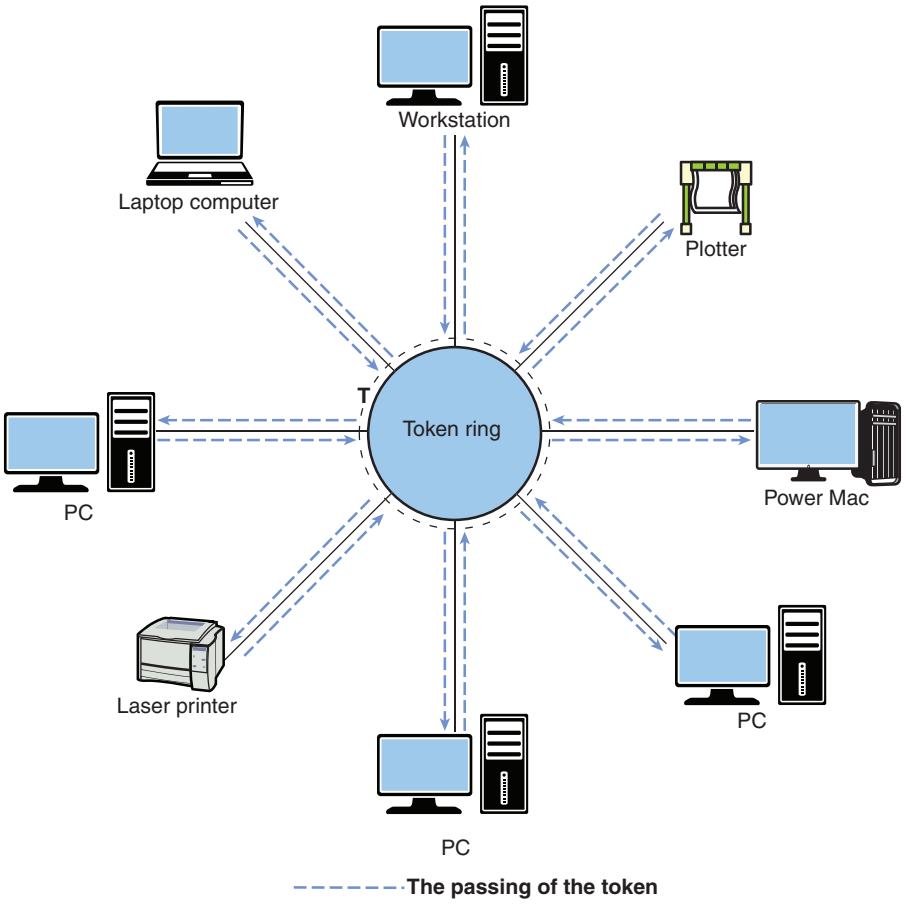


FIGURE 1-2 The Token Ring network topology.

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.

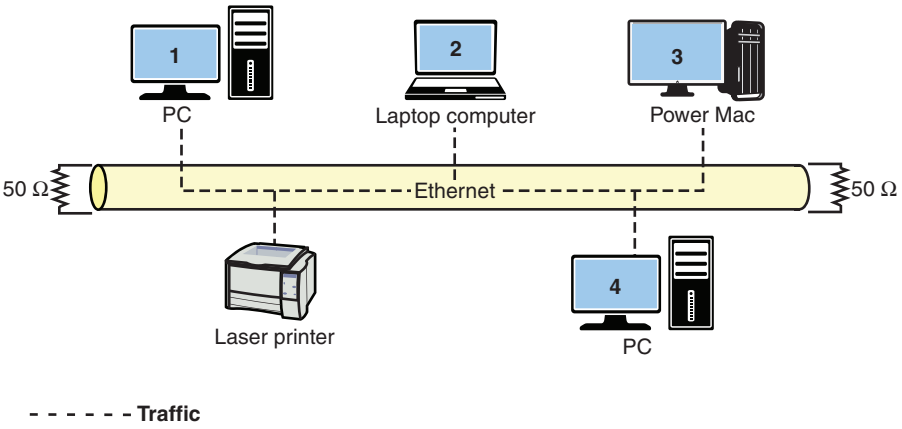


FIGURE 1-3 The bus topology.

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

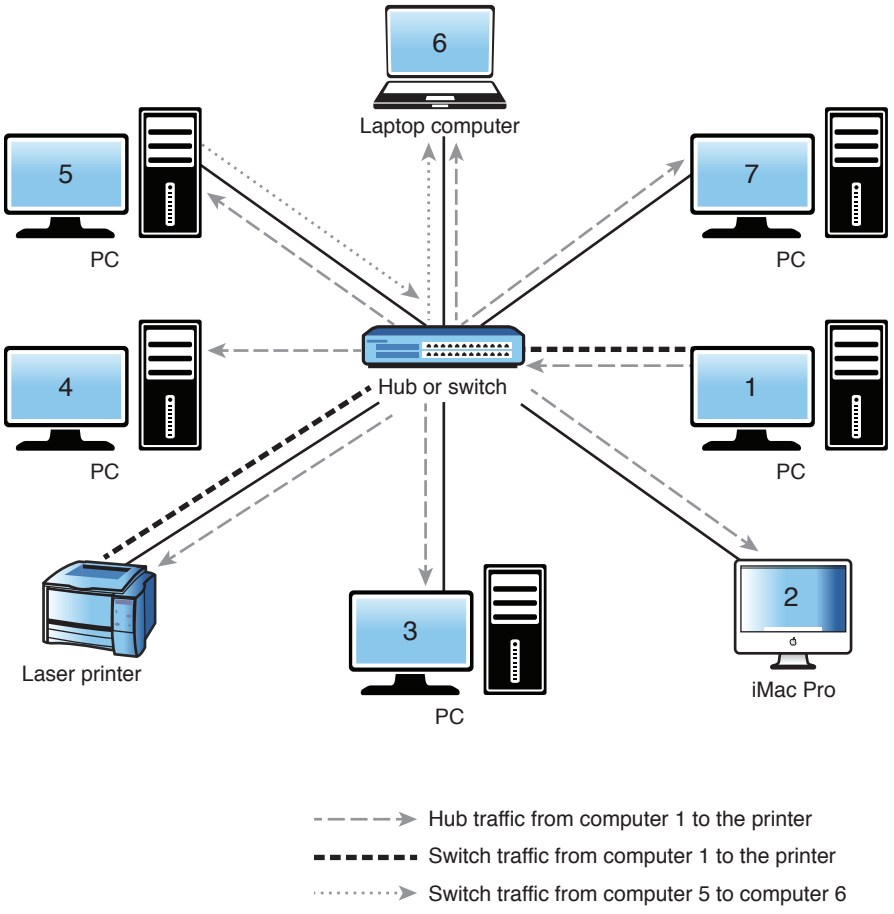


FIGURE 1-4 The star topology.

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.

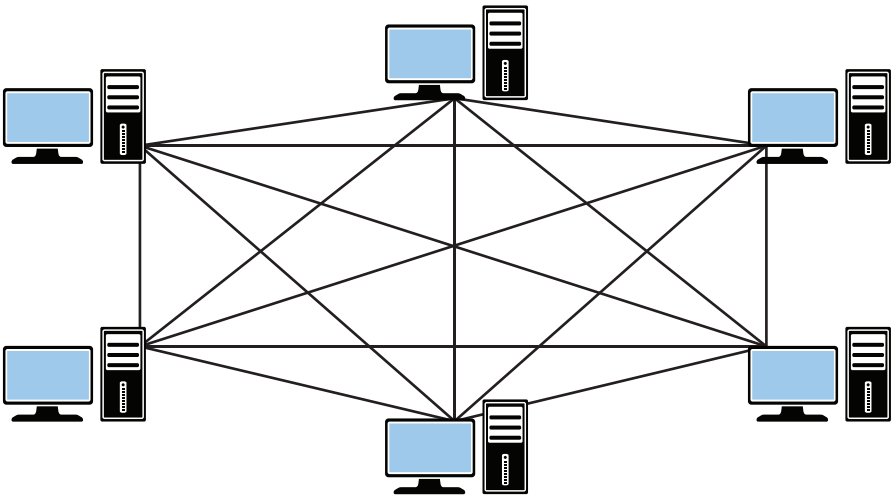


FIGURE 1-5 The mesh topology.

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.

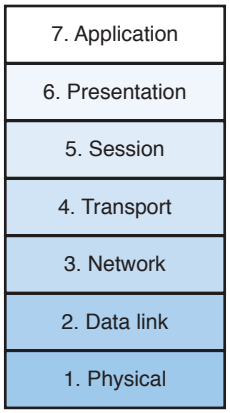


FIGURE 1-6 The seven layers of the OSI reference model.

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.

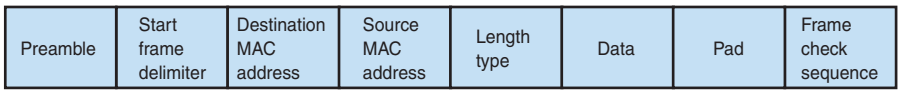


FIGURE 1-7 The data structure for the Ethernet frame. (From *Modern Electronic Communication* 9/e, by G. M. Miller & J. S. Beasley, 2008. Copyright © 2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

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**.

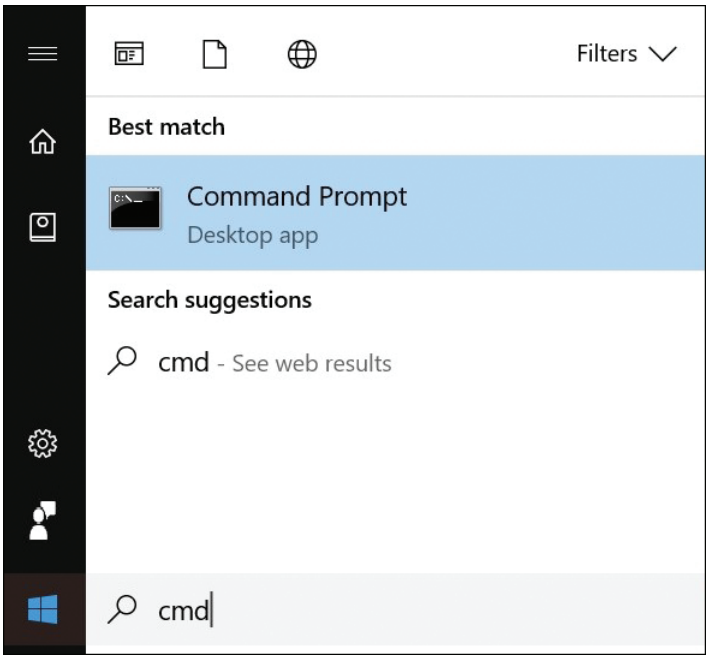


FIGURE 1-8 The command prompt in Windows 10.

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.

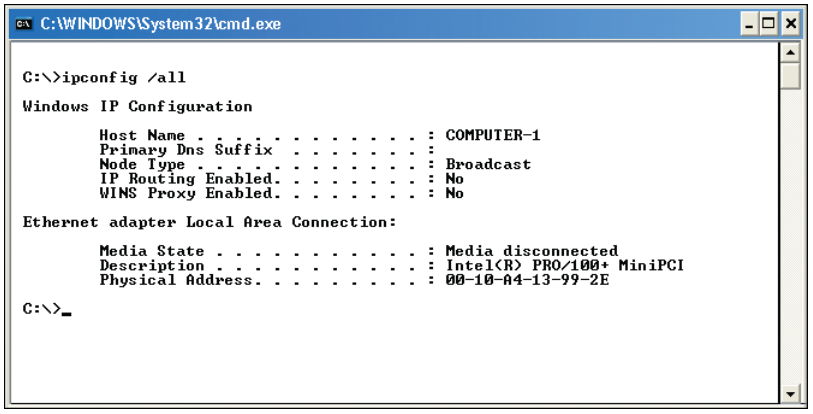


FIGURE 1-9 A typical text screen result when entering the ***ipconfig /all*** command in the command window.

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.

Operating System	Command Sequence	Comments
Mac OS (9.x and older)	Click the **Apple icon** and then select **Control Panels > AppleTalk** and click the **Info** button.	The hardware address is the MAC address.
Mac OS X	Click **Apple icon > About This MAC > More Info > Network > Built-in Ethernet**.	The hardware address is the MAC address.

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

MAC addresses are listed in hexadecimal (base-16). The complete MAC address consists of 12 hexadecimal digits. The first 6 digits identify the vendor. The last 6 form a serial number assigned by the manufacturer of the network interface card. A searchable database of IEEE OUI and company ID assignments is available at http://standards-oui.ieee.org/oui.txt. Large companies may have many OUI numbers assigned to them. For example, the OUI 00-AA-00 is only one of Intel's many OUIs. Table 1-5 lists a few examples of MAC addresses.

TABLE 1-5 **A Sample of MAC Addresses**

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

IP Addressing

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

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

IP addresses are classified as either IPv4 or IPv6. IP version 4 (IPv4) is the current TCP/IP addressing technique being used on the Internet. Address space for IPv4 is quickly running out due to the rapid growth of the Internet and the development of new Internet-compatible technologies. However, both IPv4 and IPv6 are being supported by manufacturers of networking equipment and the latest computer operating systems. The details about IPv6 are addressed in Chapter 6, "TCP/IP." IPv4 is currently the most common method for assigning IP addresses. This text refers to IPv4 addressing as "IP addressing." The **IP address** is a 32-bit address that identifies on which network a computer is located and differentiates the computer from all other devices on that network. The address is divided into four 8-bit parts. The format for the IP address is:

A.B.C.D

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

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

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

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

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

Class A	0.0.0.0 to 127.255.255.255
Class B	128.0.0.0 to 191.255.255.255
Class C	192.0.0.0 to 223.255.255.255
Class D	224.0.0.0 to 239.255.255.255

Examples of network addresses also are shown in Table 1-6. The decimal numbers indicate the **network number**, which is the portion of the IP address that defines which network the IP packet is originating from or being delivered to. The x entries for each class represent the **host number**, which is the portion of the IP address that defines the address of the networking device connected to the network. The host number is also called the **host address**. The network number provides sufficient information for routing the data to the appropriate destination network. A device

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

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

Host Address
Another term for host number

ISP
Internet service provider

Private Addresses
IP addresses set aside for use in private intranets

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

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

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

on the destination network then uses the remaining information (the x portion) to direct the packet to the destination computer or host. The x portion of the address is typically assigned by the local network system administrator or is dynamically assigned when users need access outside their local networks. For example, your Internet service provider (**ISP**) dynamically assigns an IP address to your computer when you log on to the Internet. Remember that you can check the IP address assigned to your computer by your ISP by using the **ipconfig** command at the command prompt.

This book uses a group of IP addresses called **private addresses** for assigning IP addresses to networks. Private addresses are IP addresses set aside for use in private **intranets**. An intranet is an internal internetwork that provides file and resource sharing. Private addresses are not valid addresses for Internet use because they have been reserved for internal use and are not routable on the Internet. However, these addresses can be used within a private LAN (intranet) to create an **IP internetwork**. An IP internetwork uses IP addressing to identify devices connected to the network and is also the addressing scheme used in **TCP/IP** networks. TCP/IP stands for Transmission Control Protocol/Internet Protocol and is the protocol suite used for internetworks such as the Internet. The three address blocks for the private IP addresses are as follows:

10.0.0.0–10.255.255.255
172.16.0.0–172.31.255.255
192.168.0.0–192.168.255.255

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

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

Section 1-4 Review

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

1.3 Explain the concepts and characteristics of routing and switching

This section introduces CSMA/CD. Make sure you understand how this protocol manages network access from multiple devices.

1.4 Given a scenario, configure the appropriate IP addressing components

It is important that you understand the structure of the IPv4 address and what bits define the network address and which bits are the host bits. Make sure you understand the structure of both the MAC address and the IPv4 address and know how to get this information from many types of computers. You should also make sure you have an understanding of the concept of private versus public IP addresses.

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

This section presents the concept of the networking hub and switch and how to use the **ipconfig /all** *command to verify connectivity.*

2.5 Compare and contrast WAN technologies

This section presents the concept of public versus private IP addresses. Make sure you know the address range for each.

3.2 Compare and contrast business continuity and disaster recovery concepts

This section introduces the concept of NIC teaming. Sometimes more than one NIC is installed on a computer. The purpose of NIC 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.

5.2 Given a scenario, use the appropriate tool

Remember that you can check the IP address assigned to your computer by your ISP by using the **ipconfig** *command at the command prompt. Issuing the* **ipconfig /all** *command enables a network administrator to determine whether the network interface card is connected to a network and to determine the MAC and IP addresses of a networking device.*

Test Your Knowledge

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

1-5 HOME NETWORKING

Wired Network
A network that uses cables and connectors to establish the network connection

Wireless Network
A network that uses radio signals to establish the network connection

Most students have at some point set up a home network. This is an exciting opportunity for the student to demonstrate his/her knowledge of computer networks, but setting up a home network can be quite a challenge. One of the first issues to determine is whether to set up a wired or wireless home network. A **wired network** uses cabling and connectors to establish the network connections. A **wireless network** uses radio signals to establish the network connection.

Section 1-6, "Assembling an Office LAN," discusses setting up wired networks for both office and home networks; however, the home networking technologies are presented in this section.

A wireless home network is probably the most common home network configuration in use today.

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

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

	Advantages	Disadvantages
Wired network	Faster network data transfer speeds (within the LAN).	The cable connections typically require the use of specialized tools.
	Relatively inexpensive to set up.	The cable installation can be labor-intensive and expensive.
	The network is not susceptible to outside interference.	
Wireless network	User mobility.	Security issues.
	Simple installations.	The data transfer speed within the LAN can be slower than in wired networks.
	No cables.	

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

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

- **802.11a (Wireless-A):** This standard can provide data transfer rates up to 54Mbps and an operating range up to 75 feet. It operates at 5GHz.
- **802.11b (Wireless-B):** This standard can provide data transfer rates up to 11Mbps, with ranges of 100–150 feet. It operates at 2.4GHz.
- **802.11g (Wireless-G):** This standard can provide data transfer rates up to 54Mbps up to 150 feet. It operates at 2.4GHz.

- **802.11n (Wireless-N):** This standard provides data transfer rates up to 4 × 802.11g speeds (200+Mbps). It operates either at 2.4GHz or 5GHz.
- **802.11ac (Wireless-AC):** This is the latest wireless standard. It provides single-station data transfer rates of 1.3Gbps and operates in the 5GHz frequency band.

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

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

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

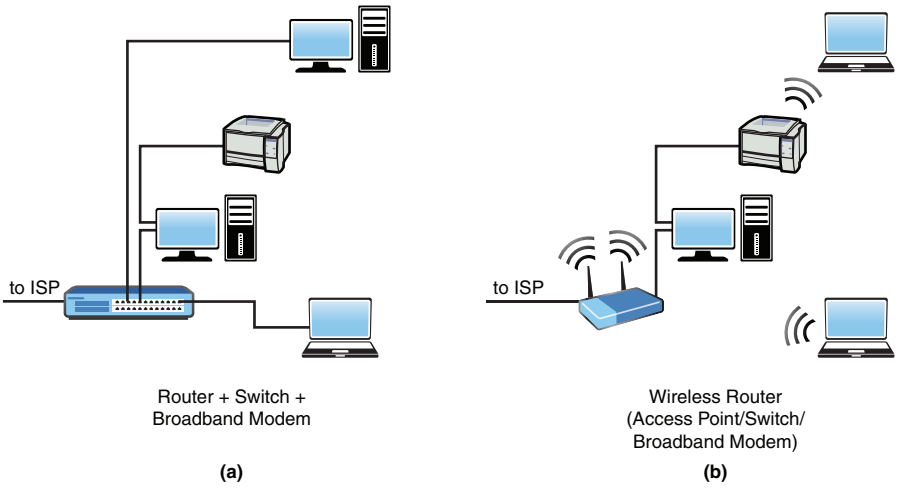


FIGURE 1-10 Examples of (a) wired and (b) wireless Wi-Fi home networks.

A home network can include the following components:

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

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

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

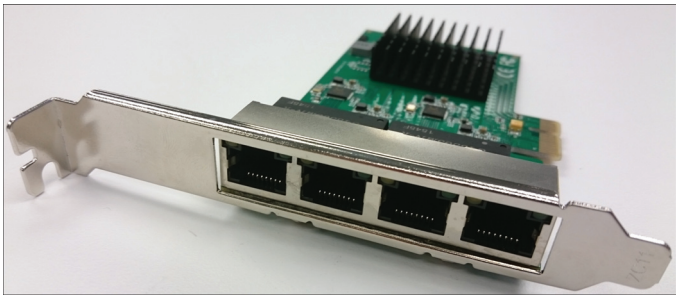


FIGURE 1-12 A 4-port PCI Express Gigabit Ethernet card.

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

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

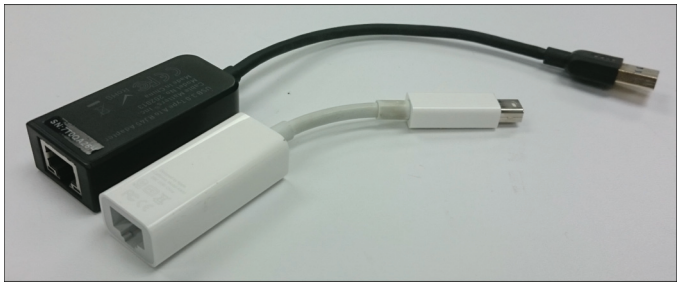


FIGURE 1-13 A USB Ethernet adapter and Thunderbolt Ethernet adapter.

FIGURE 1-14 A Netgear wireless router.

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

FIGURE 1-15 A Linksys Wireless-N access point.

- **Wireless router:** This device uses RF to connect to the networking devices. A wireless router typically contains a router, switch, and wireless access point and is probably the most common way to interconnect wireless LANs to the ISP's access device. Note that these devices also have wired network connections available on the system. Figure 1-16 provides an image of a wireless router.

FIGURE 1-16 A TP-Link wireless router.

- **Cable modem:** This device is used to make a broadband network connection from your home network to the ISP, using your cable connection. This setup requires a splitter to separate the cable TV from the home network. Access to the Internet is typically provided by the cable TV service provider. Figure 1-17 provides an image of a cable modem.

FIGURE 1-17 A Surfboard cable modem.

- **Broadband modem/gateway:** This type of device is used to provide high-speed data access via your cable connection or via a telephone company's DSL connection. A gateway combines a modem and a router into one network box. Figure 1-18 provides an image of a broadband modem/gateway.
- **DSL modem:** This device is used to make a broadband network connection from your home network to the ISP using the telephone line. Broadband access to the Internet is provided via the phone company or a separate ISP. The DSL connection requires the placement of filters on all telephone lines except the one going into the modem to prevent interference. Figure 1-19 provides an image of a DSL modem.

FIGURE 1-18 An ActionTec cable modem.

FIGURE 1-19 A Zoom DSL wireless router.

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

- **Data speed:** The data speed is determined by whether you chose to implement a wired or wireless home network. Wired networks offer the best data transfer rate inside the home network, up to 10Gbps. The best data transfer rates for a wireless home network can be obtained using 802.11ac (Wireless-ac) technology. This is the next generation of high-speed wireless connectivity, providing single-station data transfer rates of 1.3Gbps.
- **Cost:** Implementing a high-speed wired network can be quite expensive. With the networking hardware, cabling, and related hardware, you can incur unexpected additional costs in implementing a high-speed wired home network. The cost of switching to or implementing a Wireless-ac network is minimal, and such a network is a suitable alternative to a wired network. But remember that the maximum data rate for a Wireless-ac network is still much lower than the possible maximum data rate with a wired LAN.
- **Ease of implementation:** A wireless home network is probably the easiest to implement if the cabling and connectors for a wired network are not already installed. The time required to install a wireless home network is usually minimal as long as unexpected problems do not surface.
- **Appearance:** A wireless home network offers the best choice in regard to appearance because there won't be cables and networking hardware scattered around the house. The wireless home network requires a wireless router and an external wired connection to the ISP (refer to Figure 1-10(b)).
- **Home access:** The choice of wired or wireless technology does not affect home access. However, while a wired network offers the best data transfer speed internal to the network, a wireless network offers the best choice for mobility.
- **Public access:** The choice of wired or wireless technology does not impact public access. The data rate for the connection to/from the ISP is the limiting factor for the data transfer rate for public access.

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

Step 1 Check to ensure that the proper lights for your networking device that connects you to your ISP are properly displayed. Incorrect lights can indicate a connection problem with your cable modem, DSL modem, or telephone connection. Your ISP might also be having a problem, and you might need to call the ISP to verify your connection.

Step 2 Next, to fix basic connection problems to the ISP, you should reboot the host computer (the computer connected to the router) and reboot the router. This usually fixes the problem, and the correct lights should be displayed. In some cases, you might also have to power down/up your broadband modem. (Note that the broadband modem might be integrated with the router.) Once again, check to see whether the correct lights are being displayed.

Step 3 Verify that your hardware cable or phone connection is in place and has not been pulled loose. Make corrections as needed. You should also verify that all wireless units have network connections. The following are steps to verify wireless connectivity for Windows 10/8/7, and Mac OS X:

- **Windows 10/8/7:** Go to **Control Panel > Network and Sharing Center**. The wireless connection appears as enabled if there is a wireless connection.
- **Mac OS X:** Click the **Apple icon > System Preferences > Network**. Look for the following indicators:
  - If you are connected, the Wi-Fi status displays "Connected" with a green indicator.
  - If the wireless Wi-Fi is on but is not connected to a network, the Wi-Fi status displays "On" with an amber indicator.
  - If the Wi-Fi is off, the Wi-Fi status displays "Off" with a red indicator.

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

Step 4 Sometimes you might need to verify your network settings. This can happen if your computer has lost the data for the settings. In this case, follow the steps provided by the manufacturer of your broadband modem or your ISP.

The following are the basic steps for establishing a wireless connection for a wireless notebook computer running Windows 10/8/7 or Mac OS X:

- **Windows 10/8: Go to Control Panel > Network and Sharing Center—Set Up a New Connection or Network**. You need to choose the **Connect to the Internet** option and then select **Wireless** to establish a wireless connection.
- **Windows 7:** Click **Start > Control Panel > Network and Sharing Center—Set Up a New Connection or Network**. You need to choose the **Connect to the Internet** option and then select **Wireless** to establish a wireless connection.
- **Mac OS X:** Click the **Apple icon > System Preferences > Network**, select the **Wi-Fi** connection, and then click the **Turn Wi-Fi On** button. The available wireless networks appear under the **Network Name** drop-down menu. Select a desired wireless network and enter the WEP/WPA/WPA2 password for when prompted. If you are connected, a radio wave should appear at the top of the screen in the menu bar, indicating that the network is connected.

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

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

In some cases, the wireless signal might not be reaching all the areas that need coverage. In such a case, a device called a wireless **range extender** can be used. This device relays the wireless signals from an access point or wireless router into areas with a weak signal or no signal at all. This improves the wireless remote access

from all points in the home. This same technology can also be used to improve connectivity in stores and warehouses and can also be used to provide excellent connectivity in public places such as **hotspots**. A hotspot is a limited geographic area that provides wireless access for the public. A captive portal is a web page that the user of a public access network is obliged to view and interact with before access is granted. Captive portals are typically used in business centers, airports, hotel lobbies, coffee shops, libraries, schools, and other venues that offer free Wi-Fi hotspots for Internet users.

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

Securing a Home Network

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

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

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

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

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

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

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

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

- **Network address translation (NAT):** With NAT, an outsider sees only the router's IP address because the IP addresses of the internal networking devices are not provided on the Internet. Only the ISP-assigned IP address of the router is provided. The home network typically uses a private address that is not routable on the Internet. (Private IP addresses are blocked by the ISP.)
- **Firewall protection:** A common practice is to turn on **firewall protection**. The purpose of a firewall is to prevent unauthorized access to your network. Firewall protection is available in both the Windows and MAC operating environments. A type of firewall protection is **stateful packet inspection (SPI)**. This type of protection inspects incoming data packets to make sure they correspond to an outgoing request. For example, if you are exchanging information with a website, data packets that are not requested may be rejected. The topic of firewalls is covered in more detail in Chapter 12, "Network Security."
- VPN connections for transferring sensitive information: A **virtual private network (VPN)** establishes a secure network connection and helps protect your LAN's data from being observed by outsiders. The VPN connection capability is available with Windows 10, Windows 8, Windows 7, and Mac OS X. A VPN connection enables a remote or mobile user to access the network as if he or she were actually physically at the network. In addition, the VPN connection is encrypted, providing privacy for the data packets being transmitted.

IP Addressing in a Home Network

How is IP addressing handled for all the computers connected to the Internet? A home network typically has only one connection to the ISP, but multiple computers can be connected to the Internet at the same time. IP addressing for a home network is managed by the router or wireless router that connects to the ISP. The ISP issues an IP address to the router from an available pool of IP addresses managed by the ISP. The computers in the home network should be issued private IP addresses (applicable ranges are 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, and 192.168.0.0–192.168.255.255) using a technique called **network address translation (NAT)**.

Figure 1-20 provides an example. A routable public IP address is issued by the ISP for the wireless router. This public IP address enables all computers in the home network access to the Internet. The wireless router issues private addresses to all computers connected to the network.

FIGURE 1-20 A home network using a wireless router connected to the ISP.

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

Overloading
A process in which NAT translates a home network's private IP addresses to a single public IP address

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

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

For example, if computer 1 establishes a connection to a website on the Internet, the data packets from the website are sent back to computer 1 using the home network's routable public IP address. First, the network enables the data packet to be routed back to the home network. Next, the router uses the NAT lookup table and port number to translate the destination for the data packet back to the computer 1 private IP address and original port number, which might be different. Figure 1-21 shows an example of the NAT translation process for a home network. The home network has been assigned Class C private IP addresses (192.168.0.x) by the router. The x is a unique number (from 1 to 254) assigned to each computer. The router translates the private IP addresses to the public routable IP address assigned by the ISP. In addition, the router tracks a port number with the public IP address to identify the computer. For example, the computer with the private IP address 192.168.0.64 is assigned the public IP address 128.123.246.55:1962, where 1962 is the port number tracked by the router.

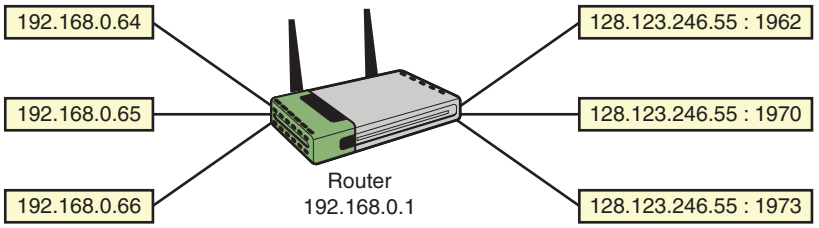


FIGURE 1-21 NAT translation using PAT.

Section 1-5 Review

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

1.3 Explain the concepts and characteristics of routing and switching

This section presents an overview of both NAT (network address translation) and PAT (port address translation). It also presents the concept of port forwarding.

1.6 Given a scenario, implement the appropriate wireless technologies and configurations.

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

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

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

2.5 Compare and contrast WAN technologies

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

3.4 Given a scenario, use remote access methods

The most common broadband connections to the ISP are via cable modem and DSL. In some cases, the router, switch, and broadband modem are separate devices, but most often they are integrated into one device.

4.3 Given a scenario, secure a basic wireless network

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

4.4 Summarize common networking attacks

Wi-Fi Protected Setup (WPS) simplifies the configuration process, enabling the user to set up WPA PSK without having to enter a long string of symbols, random numbers, or letters. Although WPS helps protect wireless networks, it is susceptible to brute-force attacks.

5.4 Given a scenario, troubleshoot common wireless connectivity and performance issues

This section introduces the concept of interference with wireless versus wired connections. You always need to make sure that your area is not subject to outside radio interference. You also need to be aware of possible interference issues with poorly installed DSL connections.

Test Your Knowledge

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

1-6 ASSEMBLING AN OFFICE LAN

This section presents an example of assembling an office-type LAN. In this example, the Ethernet protocol is used for managing the exchange of data in the network, and the networking devices are interconnected in a star topology. There are many options for assembling and configuring a LAN, but this example presents a networking approach that is simple and consistent with modern computer networking. It also provides a good introduction to the networking topics presented in the text.

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

Step 1 Document the devices to be connected in the network and prepare a simple sketch of the proposed network. Each device's MAC and IP addresses should be included in the network drawing documentation.
Figure 1-22 provides an example of a small office LAN. The desired IP addresses and the actual MAC addresses for each computer and printer are listed. Remember that each NIC contains a unique MAC address, and the IP addresses are locally assigned by the network administrator. The MAC addresses were obtained by entering the **ipconfig /all** command from the command prompt in Windows 7. Repeat this step for all computing devices connected to the LAN. Table 1-9 provides the results of the MAC address inquiries. Each networking device should be assigned an IP address, and Table 1-9 also lists the planned IP addresses of the devices used in this office LAN.

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

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

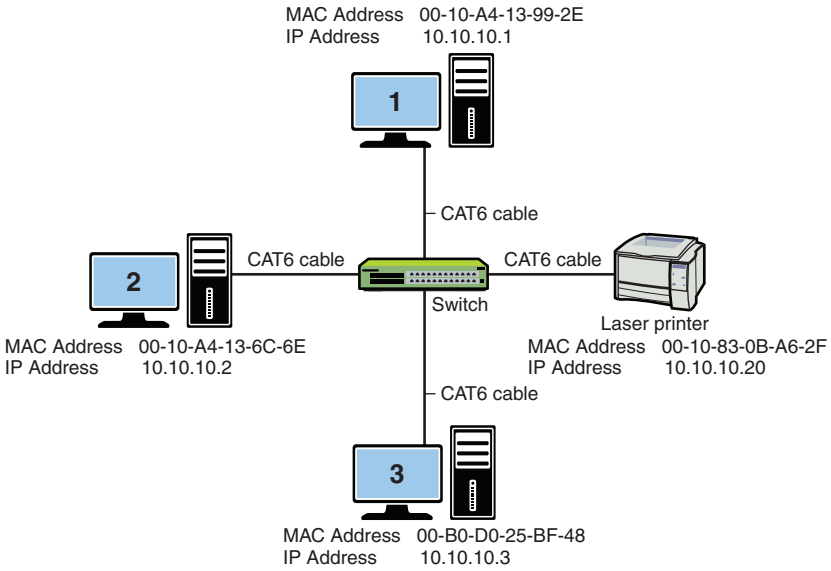


FIGURE 1-22 An example of a small office LAN star topology.

Note

In this text, you will function as the network administrator. The network administrator must know how to obtain all IP and MAC address information for devices connected to the network. The network administrator must therefore keep good documentation of the network.

Step 2 Connect all the networking devices using the star topology shown in Figure 1-22. At the center of this star topology network is a switch or hub. Recall that either a switch or a hub can be used to connect the networking devices. The switch is the best choice in this case because the hub broadcasts data it receives to all devices connected to its ports, and the switch enables the devices to communicate directly. Although hubs are not as sophisticated as switches and are not reflective of modern computer networking, hubs are still suitable for use in small networks.

The connections from the switch to the computers and the printer are made using premade twisted-pair patch cables. The cable type used here is **CAT6 (category 6)** twisted-pair cable. CAT6 twisted-pair cables have **RJ-45** modular connectors on each end, as shown in Figure 1-23, and are capable of carrying 1000**Mbps** (1 gigabit) or more of data up to a length of 100 meters; this is the typical speed and distance requirements for CAT6. Chapter 2 covers the twisted-pair media and its various category specifications, as well as issues associated with the proper cabling. If the network hardware and software are properly set up, all computers can access the printer and other computers.

CAT6 (category 6)
Twisted-pair cable capable of carrying up to 1000Mbps (1 gigabit) of data up to a length of 100 meters

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

Mbps
Megabits per second

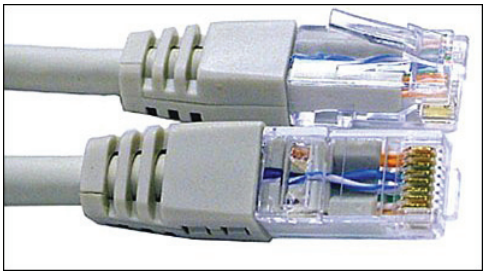


FIGURE 1-23 The RJ-45 twisted-pair patch cables (courtesy of StarTech.com).

Numerics
Numerical representations

The media used for transporting data in a modern computer network are either wireless, twisted-pair, or fiber-optic cables. The principles behind selecting, installing, and testing twisted-pair cabling are presented in Chapter 2. Table 1-10 lists the common **numerics** used to describe the data rates for the twisted-pair media and the older-style copper coaxial cable used in a LAN. Common numerics for fiber-optic LANs are also listed. Numerics provide an alphanumeric description of a technology. For example, 100BaseT means that this is a 100Mbps baseband, twisted-pair technology.

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

Numeric	Description
10Base2	10Mbps over coaxial cable up to 185 m, also called Thinnet (seldom used anymore)
10Base5	10Mbps over coaxial cable up to 500 m, also called Thicknet (seldom used anymore)
10BaseT	10Mbps over twisted-pair
10BaseF	10Mbps over multimode fiber-optic cable
10BaseFL	10Mbps over 850 nm multimode fiber-optic cable
100BaseT	100Mbps over twisted-pair (also called Fast Ethernet)
100BaseFX	100Mbps over fiber
1000BaseT	1000Mbps over twisted-pair
1000BaseFX	1000Mbps over fiber
1000BaseLS	1000Mbps over fiber
1000BaseSX	1000Mbps over fiber
1000BaseLX	1000Mbps over fiber
10GE	10GB (10GBaseT) Ethernet

The RJ-45 plugs connect to the switch inputs via the RJ-45 jacks. Figure 1-24 shows a simple 8-port switch. The inputs to the switch are also called the input **ports**, and they are the interfaces for the networking devices. The switch inputs marked with an "x" (or "uplink"), as shown in Figure 1-24(b), indicate that these devices are cross-connected, meaning the transmit and receive pairs on the twisted-pair cable are crossed to properly align each for data communication. The term for a cable that has cross-connected TX/RX data lines is **crossover**. Some of the switches might have the port labeled "uplink," which indicates the cross-connect capability. Furthermore, some newer switches are equipped with automatic crossover detection, so you don't have to worry about whether to use a straight-through cable or a crossover cable. Examples of straight-through and crossover cables are presented in Chapter 2.

Ports
Interfaces for networking devices

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

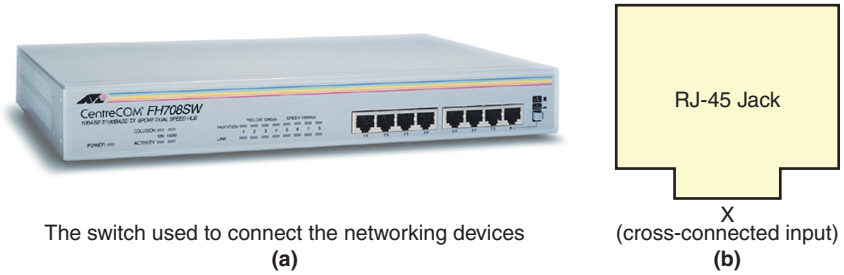


FIGURE 1-24 (a) The switch used to connect the networking devices; (b) close-up view of "x" input, indicating an uplink port (courtesy of Anixter, Inc.).

Figure 1-25(a) provides an example of this cross-connected concept. Switches usually have at least one port that can be switched or selected for use as either a cross-connected or **straight-through** input. A straight-through port is also called an **uplink port**. The uplink port allows for the connection of a switch to a switch or hub without the use of a special cable. Devices requiring cross-connected input ports are computers, printers, and routers. Devices requiring a straight-through connection are uplink connections to other switches or hubs. Figure 1-25(b) provides a block diagram explaining the concept of a straight-through input.

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

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

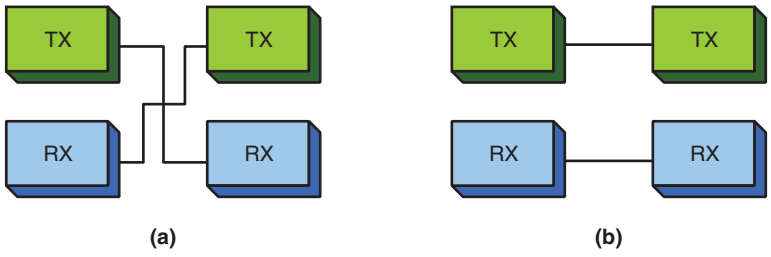


FIGURE 1-25 (a) An example of the wiring on an "x" type input on a switch; (b) an example of straight-through wiring.

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

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

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

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

Step 3 Configure the IP address settings on each computer according to the assigned addresses provided in Table 1-9. Configuring the computers to operate on the LAN requires that each computing device be assigned an IP address. To configure the computers in the office LAN using Windows 10/8/7 or Mac OS X, use the IP addresses from Table 1-9 and the following procedures:

- **Windows 10/8:** Go to **Control Panel > Network and Internet—Network and Sharing Center.** Click **Local Area Connection** and select **Properties** and then click **Continue**. In the Local Area Connection Properties menu, double-click **Internet Protocol Version 4 (TCP/IPv4)**. From the Properties menu, select **Use the Following IP Address**, enter the IP address and subnet mask, and click **OK**.
- **Windows 7:** Click **Start > Control Panel > Network and Internet—Network and Sharing Center.** Click **Local Area Connection** and select **Properties** and then click **Continue**. In the Local Area Connection Properties menu, double-click **Internet Protocol Version 4 (TCP/IPv4)**. From the Properties menu, select **Use the Following IP Address**, enter the IP address and subnet mask, and click **OK**.
- **Mac OS X:** Click the **Apple icon > System Preferences > Network** and select the **Ethernet** or **USB Ethernet** connection. From the Configure IPv4 drop-down menu, select **Manually**. This option lets you manually set the IP address and subnet mask. Fields should now be displayed for inputting both the IP address and subnet mask. Enter the desired IP address and subnet mask and click **Apply**.

As shown in Table 1-9, the IP address for computer 1 is 10.10.10.1, and in this example, a subnet mask of 255.255.0.0 is being used. Chapter 6 examines subnet masking in detail. For now, leave the remaining fields empty; their purposes are discussed later in the text. Your network configuration for computer 1 should now be complete, and you can repeat these steps for computers 2 and 3 in this LAN example.

Section 1-6 Review

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

1.4 Given a scenario, configure the appropriate IP addressing components

This section presents examples that demonstrate how to manually configure subnet masks on the computer.

2.1 Given a scenario, deploy the appropriate cabling solution

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

Test Your Knowledge

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

1-7 TESTING AND TROUBLESHOOTING A LAN

When the network configurations on the computers are completed and the cable connections are in place, you need to test and possibly troubleshoot the network. First, you need to verify that the computers are properly connected on the network. Do this by verifying that you have link lights on each switch port connected to a computer or other networking device. Figure 1-26 shows an example of a switch with the link light activated.

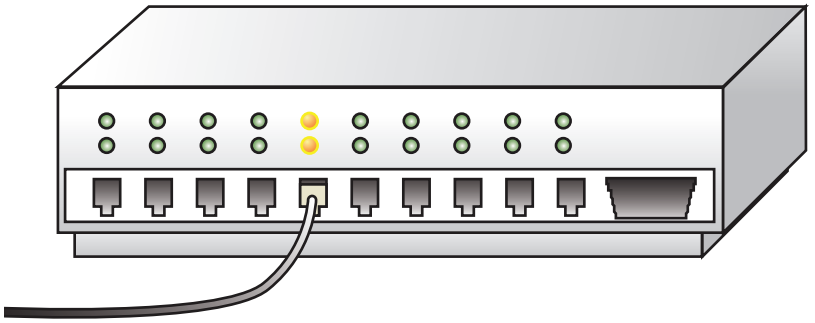


FIGURE 1-26 An example of the link light on a hub.

ping
Command used to test that a device on the network is reachable

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

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

```
Usage ping[-t][-a][-n count)[-1 size][-f -i TTL][-v TOS]  [-r count][-s
  count]
[[-j host-list]:[-k host-list][-w timeout] destination-list
Options
-t Ping the specified host until stopped
 To see statistics and continue, type Control-Break
 To stop, type Control-C
```

```
-a Resolve addresses to host-names
-n count Number of echo requests to send
-1 size Send buffer size
-f Set Don't Fragment flag in packet
-I
TTL Time To Live v
TOS Type Of Service
r count Record route for count hops
s count Timestamp for count hops
j host-list Loose source route along host-list
k host-list Strict source route along host-list
w timeout in milliseconds to wait for each reply
```

For example, you can use the command **ping 10.10.10.1** to ping the IP address for computer 1 because the IP address 10.10.10.1 is the destination address. Another example would be the destination IP address for computer 3; in this case, you would use **ping 10.10.10.3**. (Refer to Table 1-9 and Figure 1-22 for the IP addresses of the computers in the sample network.)

The following is an example of pinging another computer on the network to verify that the computers are communicating. In this example, computer 1 is used to ping computer 2. Remember that the **ping** command is executed from the command window:

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

The text shows that 32 bytes of data is being sent to the computer with the IP address 10.10.10.2. **"Reply from 10.10.10.2"** indicates that computer 2 received the message. If the computer at IP address 10.10.10.2 did not respond, the message **"Request timed out."** is displayed:

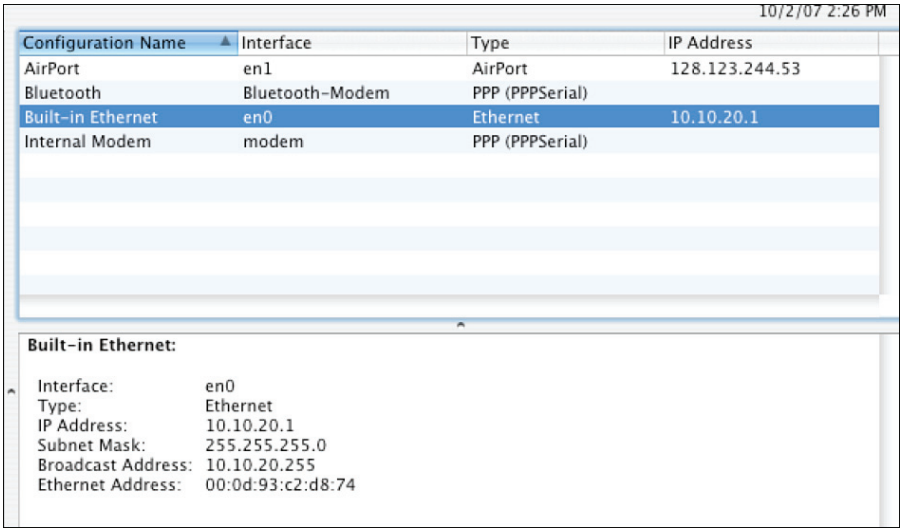
```
ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.10.10.2:
 Packets: Sent = 4, Received = 0, Lost= 4
(100% loss),
```

ipconfig
A command used to display a computer's address

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

```
Windows IP Configuration
Ethernet adapter Local Area Connection:
      Connection-specific DNS Suffix .:
      IP Address.....: 10.10.10.1
      Subnet Mask.....:  255.255.0.0
      Default Gateway .....:
```

(a)



(b)

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

Section 1-7 Review

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

1.8 Explain the function of network services

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

5.2 Given a scenario, use the appropriate tool

This section introduces the important step of verifying network connectivity using the ***ping*** *command. It presents several examples of using* ***ping*** *to troubleshoot a network.*

Test Your Knowledge

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

SUMMARY

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

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

QUESTIONS AND PROBLEMS

Section 1-1

1. State whether each of the following network descriptions describes a MAN, a WAN, or a LAN:

   a. A network of users who share computer resources in a limited area

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

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

2. Expand the acronym *NIC*.

3. Expand the acronym *MAC*.

4. Expand the acronym *LAN*.

5. Expand the acronym *WAN*.

Section 1-2

6. Define the term *protocol*.

7. Define the term *topology*.

8. Define the term *deterministic*.

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

   a. Router

   b. Multiport repeater

   c. Token passer

   d. Token-ring hub

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

    a. Mesh

    b. Bus

    c. Ring

    d. Star

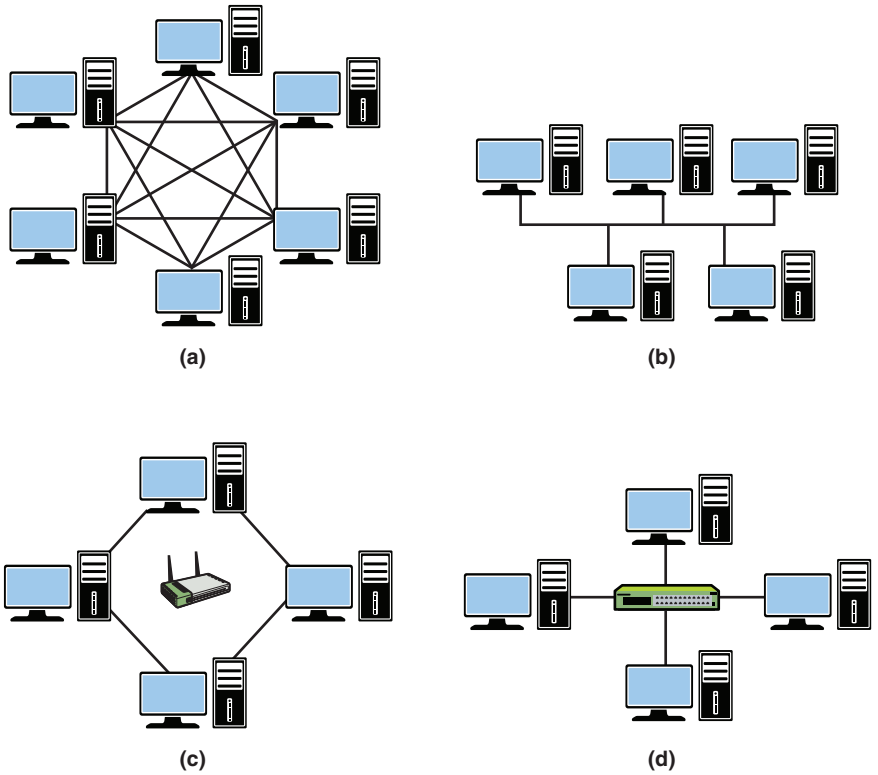


FIGURE 1-28 The networks for question 10.

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

Section 1-3

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

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

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

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

16. At what layer does a router work?

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

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

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

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

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

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

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

Section 1-4

24. Expand the acronym *CSMA/CD*. What protocol uses CSMA/CD?

25. What information is not included in an Ethernet frame?
    a. Frame size
    b. Source MAC address
    c. Pad
    d. Frame check sequence

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

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

    a. a bad frame.

    b. a jumbo frame.

    c. an MTU.

    d. All of the above

    e. None of the above

28. Expand the acronym *OUI.* Where is the OUI used?

29. What does the OUI represent?

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

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

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

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

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

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

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

    a. 46.39.42.05____

    b. 220.244.38.168____

    c. 198.1.0.4____

    d. 126.87.12.34____

    e. 99.150.200.251____

    f. 128.64.32.16____

33. Expand the acronym *TCP/IP.*

Section 1-5

34. What are three advantages of a wireless network?

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

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

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

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

39. What is the purpose of a range expander?

40. What is a hotspot?

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

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

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

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

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

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

47. What is stateful packet inspection?

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

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

50. What is port address translation (PAT)?

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

Section 1-6

52. Which of the following is not a step in building an office LAN?
    a. Obtaining proper government permits
    b. Configuring the network settings
    c. Connecting the devices together
    d. Network documentation
53. What is *RJ-45*?
    a. A 45-pin connector for CAT6
    b. An IEEE standard for data speed
    c. An 8-pin modular connector for twisted-pair Ethernet
    d. A protocol used to verify a communications link
54. What is an *uplink port*?
55. What is the maximum speed and length for Category 6 cabling?
56. What do the link lights on a hub indicate?
57. What does *cross-connected* mean?
58. DOCUMENTATION: Draw a network diagram similar to Figure 1-29, consisting of three computers, a switch, and a printer. Use the MAC addresses given in Table 1-9. Assign each network device an IP address from the private address space 192.168.5.x network. You are the network administrator and may choose the host address for each device.

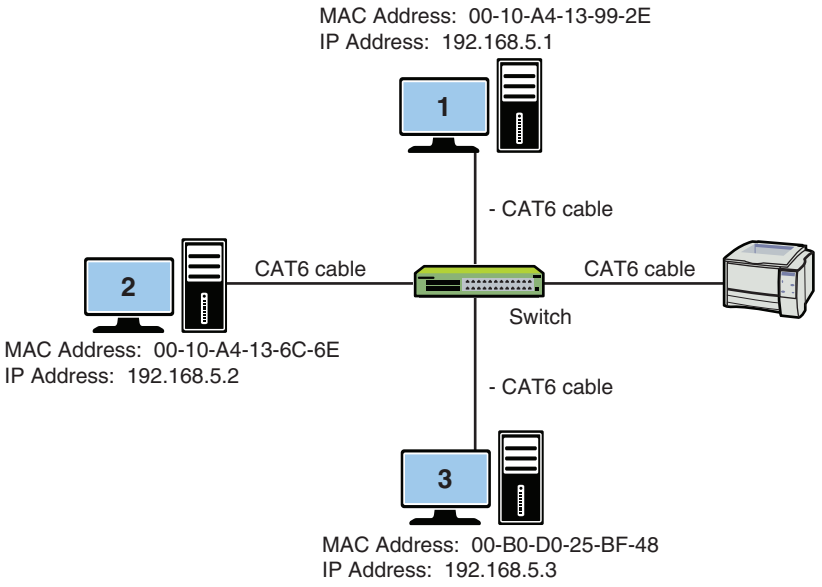


FIGURE 1-29 The sample network diagram for question 58.

Section 1-7

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

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

61. Expand the acronym *TTL*.

Certification Questions

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

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

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

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

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

63. What networking protocol does Ethernet use?

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

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

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

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

64. A network interface card has the MAC address 00-00-86-15-7A. From this information, specify the OUI.

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

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

    c. The OUI is 86-00-00.

    d. The OUI is 00-00-86.

65. An IP address for a computer is assigned by the

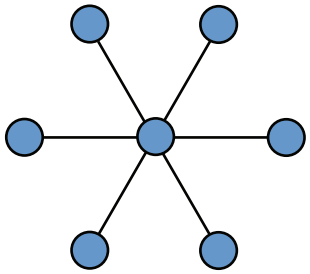
    a. Internet Assigned Numbers Authority.

    b. local network administrator.

    c. user of the computer.

    d. Internet Address Numbers Authority.

66. Which network topology is shown here?



    a. Star

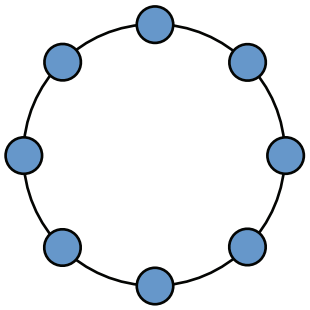
    b. Token Ring

    c. Bus

    d. Mesh

    e. None of these answers is correct.

67. Which network topology is shown here?



a. Star

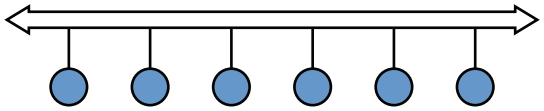
b. Token Ring

c. Bus

d. Mesh

e. None of these answers is correct.

68. Which network topology is shown here?



a. Star

b. Token Ring

c. Bus

d. Mesh

e. None of these answers is correct.

69. The pad field in an Ethernet packet

a. is used to bring the total number of bytes up to 46 if the data file is less than 46 bytes.

b. is used to bring the total number of bytes up to 64 if the data file is less than 64 bytes.

c. is not required with CSMA/CD.

d. provides grouping of the information for transmission.

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

a. A Class A address

b. A Class B address

c. A private IP address

d. A routable IP address

e. A nonroutable Internet IP address

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

    a. It uses class E addressing.

    b. It is used in high-speed (Gigabit) Ethernet.

    c. It is an internal network that provides file and resource sharing.

    d. It enables Fast Ethernet connections.

    e. It is not accessed from the Internet.

INDEX

Numbers

A

B

C

D

E

F

G

H

I

J-L

M

N

0

P

Q-R

S

T

U

V

W

X

Y-Z