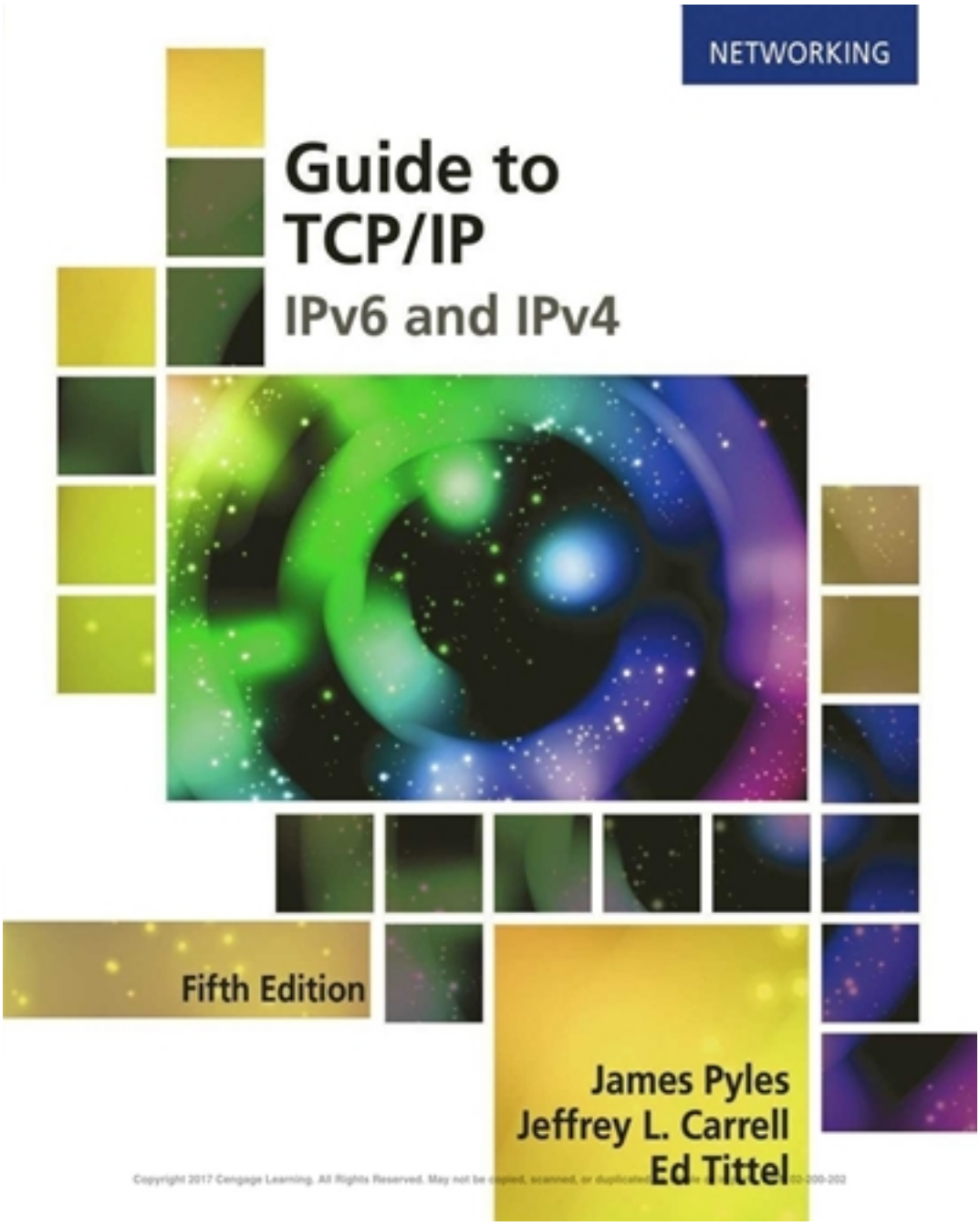
Solutions for Guide to TCP IP IPv6 and IPv4 5th Edition by Pyles

CLICK HERE TO ACCESS COMPLETE Solutions



Solutions

Guide to TCP/IP: IPv6 and IPv4, Fifth Edition
ISBN 978-1-305-94695-8

Chapter 1 Solutions

Answers to Review Questions

1. a, b, c, d
2. d
3. c
4. d
5. a
6. c
7. c, a, d, b
8. False
9. d, b, c, g, f, e, a
10. a, b, c, d
11. a, b
12. a, c, d
13. a
14. b
15. c
16. c, d
17. c
18. b
19. True
20. c
21. d
22. a, b, c, d, e
23. b
24. a, c
25. a, b, c

Hands-on Projects Discussion

Hands-On Project 1-1
In this project, the students install the Wireshark protocol analyzer software on their computer for use throughout the course. It's important to make sure that the software installs properly.

Hands-On Project 1-2
In this project, the students explore the capabilities of the protocol analyzer. First, they perform basic protocol analyzer tasks, such as capturing basic packet traffic and observing basic display and analysis capabilities on the trace buffer, including protocols observed to be in use, a list of conversations observed on the network while data capture is underway, the MAC address of a source (sender) computer, packet size distribution, and general statistics.

It's important for the students to understand how a protocol analyzer works, what it can do, and the various interface controls in Wireshark. This project is intended to familiarize students with this important network diagnostic and analysis tool so that they can use it properly to perform specific tasks in later projects. Make sure they spend the time necessary to become comfortable with the interface and familiar with the program's capabilities.

Note: If students encounter any difficulties running Wireshark, be sure to offer assistance or get help from a qualified network technician. If the protocol analyzer won't work, make sure the network interface controller (NIC) in the computer can indeed run in promiscuous mode. (If the NIC won't make that switch, the software won't work, period.)

Hands-On Project 1-3
In this project, students learn to perform basic tasks that are absolutely necessary to understanding how to use a protocol analyzer on the job (or at least, on a real network). In this project, students select a protocol filter to learn

how to limit the amount of data that the protocol analyzer captures and stores. Because the protocol analyzer can capture data only until the trace buffer is full (or older data must be overwritten with newer data to keep going), students should learn how to reduce the amount of data they capture to the precise focus of their inquiries or interests.

Hands-On Project 1-4
In this project, students learn how to create a display filter. A display filter reduces the amount of information that Wireshark displays from a trace file. This is helpful when a student wants to view only specific traffic captured in a trace file, especially if the trace file has tens or hundreds of packets.

Be sure to emphasize the difference between capture filters (used in the previous Hands-On Project) and display filters. It's sometimes best to capture all data for a short period of time and then use a display filter to view only certain packets in the trace file. Other times, it's best to limit the amount of data captured initially. Every situation is different. You could give some examples from your own experience.

Hands-On Project 1-5
In this project, students examine the contents of captured packets, as decoded and displayed by the protocol analyzer software. This gives students their first looks into the precise data structures and organizations that ultimately define what TCP/IP is and how it works. Students build on this foundation, and learn how to read more into such decodes throughout the rest of this course.

Case Projects Discussion

Case Project 1
The correct answer to this question is “at the hub.” On a hub-based network, such as the one described in this Case Project, all network traffic must transit through the hub as it’s transmitted by any single machine, and then forwarded to all other machines. Because the hub is the center of this particular networking environment, it’s the best place to attach the protocol analyzer. Modern networks are more likely to use switches, and to require use of devices called network taps to capture traffic targeted at specific switch ports. Hubs make network monitoring convenient but they no longer represent common practice on today’s networks.

From our experience, based on the scenario described, what’s probably happening is that everyone is attempting to log on at more or less the same time, and the server is probably choking on downloading all 11 user profiles, logon scripts, and other startup information, all at once. If the hub itself is congested, one solution is to install a second hub and a second NIC in the server, then divide the users into two groups—a group of five and a group of six—to more evenly balance the load between the two groups. If the server is overloaded, it may be necessary to beef up that machine, or add another machine (if the cost can be justified) to balance the load in that way.

The simplest solution, however, is to encourage users to arrive at staggered intervals so that all users do not attempt to log on at the same exact moment!

Case Project 2
The best arguments for switching to IPv6 (or for supporting dual-stack environments where IPv4 and IPv6 coexist) include the following factors: improved security, a larger and more flexible address space, and more room to grow in the future. IPv6 includes numerous enhancements that boost its security across the board as compared to IPv4, with enhanced support for encryption, stronger authentication, and a richer and more diverse set of security features. Of course, with 128-bit addresses, and a staggering increase in the addresses routinely made available on a per-organization basis—remember that the IPv6 addresses issued to most organizations are /64, so that by themselves they include 4 billion times as many addresses as are available for all of IPv4, organizations do not need to worry about outgrowing their address allocations. And finally, with IPv4 addresses exhausted, the only room for future IP network growth lies with IPv6. These are compelling reasons to include support for IPv6 on today’s networks, and to start planning for migration to IPv6 networks in the future.

Case Project 3
One obvious method is to check the protocols list in a protocol analyzer that’s set up to run for a day or longer on the network during normal load and activity conditions. Even if administrators do not capture much data, the

statistics analysis will compile a list of all the TCP/IP protocols it observes in use on the network. By carefully reviewing this list, and augmenting it with any other protocols that are only seldom used, administrators can easily build a minimal protocol list for their UNIX machines with ease.

Case Project 4

Excessive errors on a network render what would ordinarily be usable bandwidth completely unusable. Thus, overall effective utilization of the network usually decreases, even as measured utilization of the network may actually increase. Because errors still consume bandwidth, even though they're not communicating anything useful, they are considered "bandwidth stealers" that should be located and corrected as soon as possible. For that reason, network monitors and protocol analyzers normally set alarm thresholds at the point where errors consume 2% of network bandwidth. Although that level may occasionally be reached without an underlying pathology, if that level is reached with any kind of regularity, it's usually an indication that something is amiss on a network. Likewise, because all stations on a cable segment must read broadcast traffic, on the off chance that they must reply or respond to its content, excessive broadcasts have the same effect on network utilization— they steal what would otherwise be usable bandwidth for no real benefits. As with errors, the same 2% threshold for broadcast traffic is a good place to set an alarm. In fact, there is a severe pathology, known as a "broadcast storm" (normally caused by a failing network interface of some kind), in which all available network bandwidth is consumed by bogus broadcasts. Single this essentially makes a network unusable, locating and repairing such a problem is a high priority!

Case Project 5

1. Requests for Comments (RFCs) were established in 1969 as a series of notes or memos intended to be an informal fast distribution way to share ideas with other network researchers.
2. RFCs were originally informal notes or memos printed on paper and distributed to network researchers as a method of sharing ideas about network development within this body of professionals. Over time, RFCs have become a collection of official protocol standards that are used as documents of record in the Internet engineering and standards community.
3. Internet Protocol (IP) is used to specify unique address space and Transmission Control Protocol/Internet Protocol (TCP/IP) is the form of communication that the Internet must support.

Chapter 1

Introducing TCP/IP

At a Glance

Instructor's Manual Table of Contents

Lecture Notes

Overview

This chapter introduces the background and history of the collection of networking protocols known as TCP/IP, which is an abbreviation for Transmission Control Protocol/Internet Protocol. In addition, this chapter covers the Open Systems Interconnection (OSI) reference model and the TCP/IP networking model, various ways of identifying specific protocols and services, how TCP/IP standards are defined and managed, and which elements of the TCP/IP collection are most noteworthy. The chapter concludes with an overview of the art and science of protocol analysis, which uses special tools to gather data directly from a network itself, characterize a network's traffic and behavior, and examine the details inside the data that's moving across a network at any given point in time.

Chapter Objectives

- Describe TCP/IP's origins and history
- Explain the process by which TCP/IP standards and other documents, called Requests for Comments (RFCs), are created, debated, and formalized (where appropriate)
- Describe the "huge difference" between IPv4 and IPv6 and explain why a switch to IPv6 is both necessary and inevitable
- Describe the Open Systems Interconnection network reference model, often used to characterize network protocols and services, and how it relates to TCP/IP's own internal networking model
- Define the terms involved and explain how TCP/IP protocols, sockets, and ports are identified
- Describe data encapsulation and how it relates to the four layers of the TCP/IP protocol stack
- Describe and apply the basic practices and principles that underlie network protocol analysis

Teaching Tips

What Is TCP/IP?

1. This section introduces the basic definition of TCP/IP. While most students taking this class have likely heard of TCP/IP, many will not be able to define what a "protocol" is. Begin by defining a protocol as "a formal description of the sets of information that describe how data is exchanged on a network." The glossary defines protocol as "a precise set of standards that governs communications between computers on a network. Many protocols function in one or more layers of the OSI reference model."

2. Point out that TCP/IP is both a combination of two protocols and an entire protocol suite. It is important not to confuse the two.

3. TCP/IP is the de facto protocol of the Internet and is used in the majority of local area networks (LANs) and wide area networks (WANs) currently in operation. This has not always been true and is ironically a prime reason why TCP/IP has become so popular. We will see this clearly as the chapter progresses.

4. The history of TCP/IP is about 40 years old. Work on TCP/IP began in 1973, and Internet Protocol version 4 (IPv4) was developed in 1978. Point out that most of your students were born into a world where TCP/IP was already in use.

The Origins and History of TCP/IP

1. Like many devices, utilities, and services we currently enjoy, TCP/IP was initially created for military purposes. The Department of Defense (DoD) funded the research that led to the development of TCP/IP, and several other products we use were also developed by the military—often in wartime. Many medical and technological advances were first created by the Armed Forces, NASA, or other government agencies.

TCP/IP's Design Goals

1. Point out that the development of TCP/IP resulted from the need to give dissimilar networks the ability to communicate under certain conditions and further to use the existing telco network—a network that still commonly transports network communication—to communicate over thousands of miles.

2. One could argue that TCP/IP exists as it does because of how computer and communication systems were constructed at that time. Current networks are now designed to accommodate the structure of the TCP/IP protocol stack.

TCP/IP Chronology

1. Emphasize the difference between the "Internet" and an "internetwork." While an internetwork may use the Internet, it is not required to do so; many commercial enterprises use packet-switched or circuit-switched WANs to communicate with various offices and bureaus around the world.

2. Note that 1983 was an important year in the development of TCP/IP and the Internet. With the split between MILNET and ARPANET, two distinct "arms" of the Internet—the military and the public arms—were created, opening the door for the development of the Internet we know today.

3. While the development of TCP/IP and UNIX BSD go hand in hand, UNIX as an operating system and a concept may be somewhat elusive to most of your students. They will associate it with Linux but will most likely lack historical knowledge. While

it is not important for them to know about the development of UNIX in detail, you might consider assigning a small research project to familiarize the students in this area.

4. Previous editions of the textbook listed a full chronology of the history of networking; the fifth edition moved the bulk of that chronology to a Case Project. Open a Web browser on your computer and go to *www.isoc.org/internet/history/brief.shtml*. It might be helpful to have the students associate each year mentioned in the history with some sort of personal or more interesting historical event. While it may not increase their knowledge of TCP/IP per se, students may better connect to and recall key events in network development. Here is a short list of historical events to give you an idea.

    a. 1983: Michael Jackson's "Thriller" goes to number one; the final episode of M*A*S*H is watched by 125,000,000 viewers; Disneyland Tokyo opens; Pioneer 10 becomes the first man-made object to leave the solar system; Arnold Schwarzenegger (the former governor of California) became a U.S citizen; and President Reagan signed a bill establishing Martin Luther King Day.

    b. 1986: The Space Shuttle Challenger Disaster occurs; Clint Eastwood is elected Mayor of Carmel, CA; IBM produces the first megabit chip; and the world's worst nuclear plant disaster occurs at Chernobyl, USSR.

    c. 1989: The "Friday the 13th" virus strikes hundreds of computers in Great Britain; Michael Jordan scores his 1,000th NBA point in his 5th season; Oliver North goes to trial during the Iran-Contra hearings; the movies "Indiana Jones and the Last Crusade," "Star Trek V," "Ghostbusters II," and "Batman" premiere; and Mel Blanc (the voice of "Bugs Bunny" and other Warner Bros cartoon characters) dies.

Who "Owns" TCP/IP?

1. Note that even though TCP/IP and related protocols fall under the purview of some specific standards-making bodies, TCP/IP falls squarely into the public domain because it has been funded with public monies since its inception.

Standards Groups That Oversee TCP/IP

1. Facts about standards groups, such as events and dates, may seem a little dry. Emphasize why each are important.

2. As with the previous section, have students each take a standards organization and do a brief search on them. Have them find out why each might be important to a network technician or systems administrator. Can students join these? Do any host Internet forums? What can they learn by participating in these organizations?

IPv4 and IPv6

1. Explain the main differences between the 32-bit address space of IPv4 versus the 128-bit model of IPv6.

2. For IP address space comparison, the IPv4 vs. IPv6: Everything You Need to Know infographic at *www.telx.com/blog/ipv4-vs-ipv6-everything-you-need-to-know-infographic/* has you think of the IPv4 address space as the size of a postage stamp and the IPv6 address space the size of the solar system. Consider browsing some of the other information in the infographic with the students.

Quick Quiz 1

1. The term _____ refers to a single logical network composed of multiple physical networks, which may all be at a single physical location or spread among multiple physical locations.
   Answer: internetwork

2. True or False: The entire IPv6 address space is occupied.
   Answer: False

3. The _____ is the parent organization for all the various Internet boards and task forces.
   Answer: Internet Society (ISOC)

4. The _____ is the group responsible for drafting, testing, proposing, and maintaining official Internet Standards, in the form of RFCs, through the agencies of multiple working groups under its purview.
   Answer: Internet Engineering Task Force (IETF)

TCP/IP Standards and RFCs

1. Most students will not know what a "Request for Comment" is or what it means. The following definition should prove helpful: "A document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all (actually, very few) RFCs describe Internet standards, but all Internet standards are written up as RFCs."

2. A quick exercise you can assign students during the lecture is to have them use different search methods to locate the same RFC. As RFC 5000 is specifically mentioned in the textbook, have one student search the Internet for "RFC 5000"; have another open a Web browser, type "RFC 5000" directly into the address field, and press Enter; and have a third search for "Internet Official Protocol Standards" and drill down from there. They will find that RFC 5000 obsoleted RFC 3700 and has been obsoleted itself by RFC 7100. This will also demonstrate the idea of a "historic standard" as mentioned in this part of the text.

3. Discuss the purpose of RFC 2026 and process of RFC adoption.

4. Another source of information mentioned in the text is *http://www.faqs.org/rfcs/*. Encourage your students to visit this site. Introductory and overview chapters can be somewhat slow for many students and the more you are able to involve them in the lecture process, the more likely they will find interest in, learn, and retain the knowledge.

Teaching ***Tip***	Point your students to *http://tools.ietf.org/html/rfc1180* for an RFC containing a TCP/IP tutorial.

OSI Network Reference Model Overview

1. Few concepts are more basic or more vital than the OSI reference model. Virtually any conversation between techs or admins regarding the description or troubleshooting of a network will be expressed in terms of this model. Any school or certification program involving computer networking will require a thorough knowledge of OSI. Your students will learn more about the details of this model as the class progresses, but start building this critical knowledge base now.

2. Explain that a model is just that—a model. It is not "real life" any more than the scale models of jet aircraft or sailing ships are the "real thing." Emphasize that this does not mean that the OSI model or any other model have no worth; the layers and processes give us a conceptual understanding of what networks do.

Teaching ***Tip***	Read more about the OSI reference model at *http://docwiki.cisco.com/wiki/Open_System_Interconnection_Protocols*.

Breaking Networking Into Layers

1. Why is "layering" information or systems a good idea? Give some examples of other ways complex information is broken down into more manageable, "bite-sized" pieces.

2. We teach small children compound words by showing them the "smaller" words inside the "larger" ones. "Roadmap" is really "road" and "map." The same is true of larger, complex math problems. We break them down into smaller problems to make them more solvable.

3. Models are created when people do not easily understand the true nature of a system. Meteorologists create "weather models" because the dynamics of our planetary weather system are not truly known. This gives us the ability to at least approximately predict the weather days ahead of time and to understand weather trends over longer time spans.

4. Explain the concepts of "peer layers" and the "reversibility" of encapsulation. For example, an item is packaged, layer by layer at its origin, and then upon arriving at its destination, it is unpackaged in the exact reverse order.

5. Note the idea of a different "expertise" for each OSI layer. It is true that an expert in the Physical layer will likely possess a different skill set than an expert in the Transport layer. Extend this concept to career goals. It is premature to discuss career outcomes of students just beginning to learn basic networking, but it is quite likely that one of the overall goals of your students in pursuing this line of study is to get a job. As students study the OSI model, they can at least start thinking about which areas seem more attractive (of course, they will still have to become familiar with them all).

The ISO/OSI Network Reference Model Layers

1. Beginning networking students may find that learning about the seven OSI layers and their functions is a bit daunting. Teaching your students a few mnemonics will be enormously helpful. You might insert a little humor here as well.

From top to bottom:	
All	(**A**pplication)
People	(**P**resentation)
Seem	(**S**ession)
To	(**T**ransport)
Need	(**N**etwork)
Data	(**D**ata Link)
Processing	(**P**hysical)

From bottom to top:	
Please	(**P**hysical)
Do	(**D**ata Link)
Not	(**N**etwork)
Take	(**T**ransport)
Sally's	(**S**ession)
Pizza	(**P**resentation)
Anymore	(**A**pplication)

2. Ask if any of the students can come up with original mnemonics of their own. Often the ones they create will be more memorable to them.

How Protocol Layers Behave

1. Examples of a protocol "stack" might be a stack of dishes or books. Often teachers will demonstrate this concept on a board or present it as part of a PowerPoint presentation. You might also literally stack books, perhaps different colored books, of different sizes to represent the different functions and characteristics of each layer.

Physical Layer

1. This is a great opportunity to display all of the objects that are representative of this layer. Gather some lengths of Cat 5 patch cable, RJ-45 connectors, an Ethernet hub, a fiber media converter (if available), among other items you want to share with the students. All of these are layer 1 devices. One type of media often overlooked and certainly harder to see in such a demonstration is wireless networking media. The media involved is radio waves in the 2.4 GHz and 5 GHz bands. The most common Wi-Fi standards available today are IEEE 802.11g, 802.11n, and 802.11ac. 802.11g operates in the 2.4-GHz frequency, 802.11ac operates in the 5 GHz frequency, and 802.11n operates in both frequencies. For a demonstration, an access point will do. A unit of information at this layer is usually an electrical impulse.

Data Link Layer

1. Examples of devices at this layer would be a switch and possibly a network interface controller (NIC). The Media Access Control (MAC) or physical address of a computer is burned onto its NIC; usually (but not always), the only way to modify this is to change the NIC.

2. A unit of information at this layer is usually called a datagram or a frame.

Network Layer

1. The device that represents this layer is a router. If a MAC is the physical address of a computer at the Data Link layer, then an IP address is the logical address of a computer at this layer and this address is very changeable.

2. IP addressing, Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS) are all described more in detail later in the textbook but are introduced briefly here. These are so common in the world of networking that many non-technical computer users are aware of them as well.

3. The idea of multiple network connections will be visited more in detail when you discuss ports and sockets later in the chapter.

Transport Layer

1. The concept of “segmentation” is important for your students to understand. Breaking down the cars in a long freight train into two or more trains to make them lighter and smaller for more difficult terrain is an example of this. You may also share the example of a person traveling most of a journey in a large, commercial jet and then transferring to a smaller aircraft to make the remainder of the journey.

Session Layer

1. Your students are likely familiar with the setting up and tearing down of a communications link. This happens every time they make a phone call or access the Internet with a slow connection.

Presentation Layer

1. Redirectors (Microsoft) versus network shell (UNIX) can be a difficult concept for some. Basically, requests come in for services to a device. The service is provided by either the local machine or the network. The redirector does just that . . . redirects the request to the appropriate provider. Naturally, this is an "in-a-nutshell" description and would need to be expanded significantly in a more detailed discussion.

Application Layer

1. This is most commonly thought of as the user interface layer. The user initially inputs the information that is transmitted down the OSI stack and across the network, such as a request for a Web page or sending an e-mail attachment. This is the layer with which, without realizing it, your students are most familiar.

Quick Quiz 2

1. The _____ layer includes the physical transmission medium (cables or wireless media) that any network must use to send and receive the signals that constitute the physical expression of networked communications.
   Answer: Physical

2. The _____ layer is situated between the Data Link layer and the Transport layer in the reference model.
   Answer: Network

3. Data Link layer PDUs are called _____.
   Answer: frames or data frames

4. _____ define the last point up to which successful communications are known to have occurred, and define the last known point to which a conversation must be rolled back for missing or damaged elements to be replayed to recover from the effects of missing or damaged data.
   Answer: Checkpoints

The TCP/IP Networking Model

1. Explain that the OSI model and the TCP/IP networking model are very close in terms of mapping; however, it is important to remember that they are not identical stacks that have been simply renamed and relayered.

Most network technicians use the OSI model on a day-to-day basis. It may be more difficult for some students to remember the layers of the TCP/IP stack. Even though there are only four layers, some of the layers contain a great deal of data, particularly the Application layer.

TCP/IP Network Access Layer

1. Note that the text formally introduces the IEEE and a portion of the 802 project.

Teaching ***Tip***	A complete list of 802 standards can be found at any number of places on the Internet, such as *http://www.ieee802.org/* and *http://standards.ieee.org/getieee802/*.

2. Encourage your students to make use of the many resources on the Internet to become familiar with the IEEE and the 802 project during this introductory chapter, as it will prepare them for more detail in later chapters.

3. Emphasize that Fast Ethernet and Gigabit Ethernet have largely replaced Token Ring, and relatively few organizations still use this topology. Token ring networks follow the 802.5 Token Ring standard, which is no longer updated.

TCP/IP Network Access Layer Protocols

1. High-Level Data Link Control (HDLC), frame relay, and Asynchronous Transfer Mode (ATM) are all considered Layer 2 protocols, which can be confusing to beginning networking students. The OSI model Data Link layer focuses on Layer 2 LAN technology. Point out that much of the Internet actually operates at Layer 2. Telco WAN switching is basically like LAN switching. These concepts will be discussed more in detail when routing is addressed.

Teaching ***Tip***	*http://whatis.techtarget.com* is an excellent resource for explaining technical terms and concepts and should be in every student's list of favorites.

2. Point-to-Point Protocol (PPP) is the common transport protocol of the Internet. When your students surf the Web, they use PPP, though most are unaware of it. For more information, they can look up RFC 1661.

TCP/IP Internet Layer Functions

1. The concept of fragmentation was covered previously. Make a connection between the OSI model and the TCP/IP model here.

2. IP addressing will be covered in Chapter 2. If students seem overwhelmed at this point, remind them that this chapter is an overview of what is coming in later chapters. They can think of the overview as a "protocol stack" and each chapter as a "layer" in the stack (yet another example of why layering is beneficial).

TCP/IP Internet Layer Protocols

1. This section provides a more detailed description of protocols.

2. RIP, OSPF, and BGP are all routing protocols. Reinforce the idea of a routing versus a routed protocol here.

TCP/IP Transport Layer Functions

1. A host is any networked device. Your students will typically think of a host as a PC but it can be any networked device, from a mainframe to a network printer.

TCP/IP Transport Layer Protocols

1. You can point out that the Transport layer of the OSI and TCP/IP stacks map more or less identically.

2. Explain the high-level differences between TCP and User Datagram Protocol (UDP), if you didn't cover the information previously.

TCP/IP Application Layer

1. This layer is like the OSI Application layer in that it is a user interface layer. In many other ways, the two layers are quite different.

2. File Transfer Protocol (FTP) and Telnet are introduced here. FTP is an older, well-known protocol. Since information can commonly be downloaded from HTTP sites today, many students have not had the experience of downloading by FTP, so a few words of introduction could be useful here. Likewise, although Telnet is a well-known application, discuss its functionality.

3. Voice over IP or VoIP (usually pronounced "voyp") uses UDP for the same reasons as streaming audio and video. Reliable delivery that is guaranteed by TCP requires the capacity to retransmit dropped packets. This is acceptable in most kinds of data transfer, but would be hopelessly frustrating and disruptive in a phone conversation.

4. The term "daemon" (pronounced "day-mon") will be familiar to those students who have some knowledge of Linux. Ask for a show of hands from students who have a Linux background.

5. This section introduces the idea of port numbers, which will become clearer with the detailed description of the next section.

Quick Quiz 3

1. Devices that operate on the Internet are generically identified as _____.
   Answer: hosts

2. The TCP/IP Application layer is also known as the _____ layer because this is where the protocol stacks interfaces with applications or processes on a host machine.
   Answer: Process

3. Each TCP/IP service has an associated _____ that uses a 16-bit number to identify a specific process or service.
   Answer: port address

4. Any _____ or listener process essentially hangs around, listening for attempts to connect on the well-known port address (or addresses) associated with its services.
   Answer: daemon

TCP/IP Protocols, Services, Sockets, and Ports

1. The text mentions how common it is to have multiple applications and services open at the same time. Demonstrate this by asking how many students have a browser open and are surfing the Web, checking e-mail, and using a messaging application in class. Then use the situation to discuss why ports are necessary.

2. Well-known ports can be found on the Web at *http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml*. If you have Internet access and your PC uses a projector, you can go to this site and show the class the list. Alternately, you could have students look up the site.

TCP/IP Protocol Numbers

1. Explain that the protocol number in an IP datagram header appears in the 10th byte. Students will learn more about protocol numbers in Chapter 3 but should browse the protocol information at *www.iana.org/assignments/protocol-numbers* as a preview.

TCP/IP Port Numbers

1. You can describe a series of source port numbers and destination port numbers as a group if cables are attached to various physical ports from one PC to the ports on another PC. Your class may be too young to remember the old-fashioned telephone operator who manually created and tore down circuits by plugging cables into a board

all day long; yet, that operator kept track of conversations much in the same way as ports do on modern networks.

Teaching ***Tip***	Another great resource for locating listings of port numbers and ranges of port numbers is *http://www.sockets.com/services.htm*.

TCP/IP Sockets

1. Sockets are somewhat difficult to understand. Many people get ports and sockets confused or just assume they are the same thing. For the record, a socket is defined by three elements: the IP address of the host, the type of protocol (TCP or UDP), and the port number.

Quick Quiz 4

1. Breaking up an incoming data stream so separate portions may be delivered to the correct applications is called _____.
   Answer: demultiplexing

2. TCP/IP application processes are sometimes called _____ and are identified by port numbers.
   Answer: network services

3. Regarding network services, the _____ port number identifies the process that sends data.
   Answer: source

4. All port addresses below 1024 represent well-known services, and there are many so-called _____ ports associated with specific application services in the range from 1024 to 65535.
   Answer: registered

Data Encapsulation in TCP/IP

1. Draw a simple “box car” made up of a header, payload, and trailer to demonstrate data encapsulation. Another idea would be to draw a rocket with a guidance system (header), payload, and motor (trailer).

Protocol Analysis

1. This last section is the most “practical” and least “theoretical” of the sections and, ironically, probably one that will be the most difficult for your students to understand—at least at first.

2. Point out not only how protocol analyzers are used but also how they can be misused. Caution your students from using this tool to analyze the traffic of other students unless it is specifically part of a lab. If your classroom LAN has access to the larger campus network and to the Internet, remind your student that any attempt to monitor network traffic outside of a specific lab is an invasion of privacy at best. If your students have signed your school's computer lab and Internet access policies and use statement, remind them of that fact.

Useful Roles Protocol Analysis

1. Explain that protocol analyzers are a vital tool in establishing baseline functioning, network utilization, and troubleshooting of a network.

2. Explain that the textbook uses the Wireshark protocol analyzer in its examples and associated exercises. However, analyzers are available from many different vendors. Students should be aware that they may encounter various analyzers in the real world but that most analyzers work similarly.

Protocol Analyzer Elements

1. The term *promiscuous mode* sounds a little off color and perhaps difficult to understand. It is best explained as the state of a network card when it is not filtering traffic at all so that every frame that the NIC encounters on the network is recorded. A PC or laptop using a network analyzer will need an NIC in promiscuous mode in order to properly detect and capture packets. Most over-the-counter network cards or built-in network interfaces and drivers run in promiscuous mode.

2. Most modern LANs either make minimal use of or have completely done away with hubs in favor of switches. Since Layer 2 switches create a point-to-point link between the sender and receiver, only those two nodes comprise a "collision domain." In a production environment, they might not encounter collisions as frequently as they would have 10 years ago. Having said that, like Token Ring, there are still plenty of older, "legacy" networks that use hubs and have relatively large collision domains.

3. The text defines packet fragments as "runts," but it would be good to mention that oversized packets are called "giants." Some analyzers use these terms when expressing statistical information.

4. Note that the material in this section will make more sense to your class once they start using the Wireshark tool.

5. Describe a packet filter as sort of a screen or net designed to capture and separate just one item. In this case, some of the "things" they capture are source data link address, destination IP address, and so on. A packet filter works very much like a filter on an e-commerce Web site that allows you to narrow your choices. An older analogy of filters is the nineteenth century gold prospectors who used a boxed screen to "pan" a river for gold.

6. If any of your students have used Microsoft Excel, Microsoft Access, or another database program, they are probably familiar with filtering. Ask the class if any of them have used spreadsheet or database filters.

7. Note that the packets in the trace buffer can be viewed immediately after they are captured or saved for viewing at a later time.

8. Note that decodes are applied to the packets that are captured into the trace buffer. These decodes enable you to see the packets in a readable format with the packet fields and values interpreted for you.

9. Note that alarms notify the network technician of an event on the network requiring immediate attention.

10. Explain that statistics are used to create baselines. A baseline is the measure of a network's initial or optimum functioning. Statistics are then used to compare the network's current functioning against the baseline to determine if the usage is changing or to indicate unusual events. Periodic monitoring of network changes can sometimes help in anticipating in upcoming problem.

Placing a Protocol Analyzer on a Network

1. Remind the class of how differently Layer 1 devices (hubs) and Layer 2 devices (switches) behave.

2. A quick example of the difference between half duplex and full duplex is the difference between a walkie-talkie and a cell phone.

3. The text may make it seem like the protocol analyzer is a special device that is attached to a network at some point, but most commonly, it is a laptop with the analyzer software loaded and plugged into a hub or switch in the server room of a network. The technician can move to different switches analyzing different portions of the network.

Quick Quiz 5

1. True or False: You can use a protocol analyzer to test a network either passively or actively.
   Answer: True

2. On a network, collisions increase in frequency as traffic volumes increase/decrease (choose one).
   Answer: increase

3. _____ is the process of tapping into the network communications system, capturing packets that cross the network, gathering network statistics, and decoding the packets into readable form.

Answer: Protocol analysis

4. True or False: A card that runs in promiscuous mode can capture broadcast packets.
Answer: True

Class Discussion Topics

1. Have the class describe any of the concepts presented in class that are applicable to their personal use of the Internet.

2. Have the class compare and contrast the OSI reference model with the TCP/IP networking model. Which one do they think is more useful when working with and describing networks? Why?

3. Discuss some ways in which a dishonest person could misuse a protocol analyzer.

Additional Projects

1. This chapter introduces the basic definition of TCP/IP. While most students have likely heard of TCP/IP, many will not be able to define exactly what a "protocol" is. Ask students to write a report with a general definition of "protocol" (e.g., "A formal description of the sets of information that describe how data is exchanged on a network") and then apply this definition to the details of the TCP/IP protocols.

2. While connected to the Internet at school or at home, ask students to right-click the network connection indicator in the system tray and open the Network and Sharing Center (assuming they are using a computer running Windows 7 or Windows 10). They should click the link for the active connection, and then record the status and details for that connection. Have them discuss how the information relates to what they've learned in class.

3. Have students do an Internet search for "protocol analyzers." How many can they find? Are there any shareware or freeware analyzers?

Additional Resources

1. The paper "An Overview of TCP/IP Protocols and the Internet" was first submitted to InterNIC in August 1994. This paper is continuously updated and can be found at *http://www.garykessler.net*. Click "Articles, Papers, URL Lists, and Utilities" link, and then scroll down to find the article.

2. For another brief history of TCP/IP, read "Introduction to TCP/IP" at *http://www.yale.edu/pclt/COMM/TCPIP.HTM*.

3. The text refers to UNIX BSD and TCP/IP development. For background information, go to *http://minnie.tuhs.org*, click on "seminars and presentations," scroll down and click on "FreeBSD" in the "1995" section, and then click the "A Brief History of Unix, BSD and FreeBSD" link.

Key Terms

- **4.2 BSD** The version of the Berkeley Software Distribution (BSD) of UNIX that was the first to include a TCP/IP implementation.
- **addressing** A method of assigning a unique symbolic name or numerical identifier to an individual network interface on a network segment to make every such interface uniquely identifiable (and addressable).
- **Advanced Research Projects Agency (ARPA)** An agency within the U.S. Department of Defense that funded forward-thinking research in computing technology.
- **alarm** Notification of events or errors on the network.
- **anycast packet** An IPv6 multicast method that permits multiple recipients to be designated for a single message, usually for a single cable segment or broadcast domain.
- **Application layer** The uppermost layer of the ISO/OSI network reference model (and the TCP/IP model) where the interface between the protocol suite and actual applications resides.
- **application process** A system process that represents a specific type of network application or service.
- **ARPANET** An experimental network, funded by ARPA, designed to test the feasibility of a platform-neutral, long-distance, robust, and reliable internetwork that provided the foundation for what we know today as the Internet.
- **Best Current Practice (BCP)** A specific type of Internet RFC document that outlines the best ways to design, implement, and maintain TCP/IP-based networks.
- **broadcast** A specific type of network transmission (and address) meant to be noticed and read by all recipients on any cable segment where that transmission appears; a way of reaching all addresses on any network.
- **broadcast packet** A type of network transmission intended for delivery to all devices on the network. The Ethernet broadcast address is 0xff-ff-ff-ff-ff-ff for IPv6 and 255.255.255.255 for IPv4.
- **cable segment** Any single collection of network media and attached devices that fits on a single piece of network cable, within a single network device such as a hub, or in a virtual equivalent such as a local area network emulation environment on a switch.
- **capture filter** A method used to identify specific packets that should be captured into a trace buffer based on some packet characteristic, such as source or destination address.
- **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** A formal name for Ethernet's contention management approach. CSMA means "listen before attempting to send" (to make sure no later message tramples on an earlier one) and "listen while sending" (to make sure messages sent at roughly the same time don't collide with one another).

- **checkpoint** A point in time at which all system state and information is captured and saved so that, after a subsequent failure in systems or communications, operations can resume at that point in time, with no further loss of data or information.
- **checksum** A special mathematical value that represents the contents of a message so precisely that any change in the contents will cause a change in the checksum—calculated before and after network transmission of data, and then compared. If transmitted and calculated checksums agree, the assumption is that the data arrived unaltered.
- **congestion control** A TCP mechanism, also available from other protocols, that permits network hosts to exchange information about their ability to handle traffic volumes and thereby causes senders to decrease or increase the frequency and size of their upcoming communications.
- **connectionless** A type of networking protocol does not require network senders and receivers to exchange information about their availability or ability to communicate; also known as "best-effort delivery."
- **connection-oriented** A type of networking protocol that relies on explicit communications and negotiations between sender and receiver to manage delivery of data between the two parties.
- **daemon** Taken from James Clerk Maxwell's famous physics idea, a daemon is a computer process whose job is to "listen" in on connection attempts for one or more specific network services and to hand off all valid attempts to temporary connections known as sockets attempts.
- **data frame** The basic PDU at the Data Link layer, which represents what is transmitted or received as a pattern of bits on a network interface.
- **Data Link layer** Layer 2 of the ISO/OSI network reference model. The Data Link layer is responsible for enabling reliable transmission of data through the Physical layer at the sending end and for checking such reliability upon reception at the receiving end.
- **data segment** The basic PDU for TCP at the Transport layer. *See also* segment.
- **datagram** The basic protocol data unit at the TCP/IP Network Access layer. Used by connectionless protocols at the Transport layer, a datagram simply adds a header to the PDU, supplied from whichever Application layer protocol or service uses a connectionless protocol, such as UDP; hence, UDP is also known as a datagram service.
- **decode** The interpreted value of a PDU, or a field within a PDU, performed by a protocol analyzer or similar software package.
- **decoding** The process of interpreting the fields and contents of a packet, and presenting the packet in a readable format.
- **Defense Information Systems Agency (DISA)** The DoD agency that took over operation of the Internet when ARPA surrendered its control in 1983.
- **demultiplexing** The process of breaking up a single stream of incoming packets on a computer and directing its components to the various active TCP/IP processes based on socket addresses in the TCP or UDP headers.
- **destination port number** A port address for an incoming TCP/IP communication that identifies a target application or service process.
- **display filters** Filters that are applied to the packets that reside in a trace buffer, for the purpose of viewing only the packets of interest.
- **divide and conquer** A computer design approach that consists of decomposing a big, complex problem into a series of smaller, less complex, and interrelated problems, each of which can be solved more or less independently of the others.

- **Draft Standard** A Standard RFC that has gone through the draft process, that has been approved, and for which two reference implementations must be shown to work together before it can move on to Internet Standard status.
- **dynamically assigned port address** A temporary TCP or UDP port number allocated to permit a client and server to exchange data with each other only as long as their connection remains active.
- **encapsulation** Enclosure of data from an upper-layer protocol between a header and a trailer (the trailer is optional) for the current layer to identify sender and receiver and, possibly, include data integrity check information.
- **Ethernet** A network access protocol based on carrier sense, multiple access, and collision detection.
- **Ethernet collision fragments** The garbled traffic on a network produced when two packets transmitted at about the same time collide, resulting in a hodgepodge of signals.
- **fragmentation** The process of dividing a packet into multiple smaller packets to cross a link that supports an MTU than the link where the packet originated.
- **frame** The basic Data Link layer PDU of the ISO/OSI reference model.
- **header** That portion of a PDU that precedes the actual content for the PDU and usually identifies sender and receiver, protocols in use, and other information necessary to establish context for senders and receivers.
- **Historic Standard** An Internet RFC that was superseded by a newer, more current version.
- **host** TCP/IP terminology for any computer with one or more valid TCP/IP addresses (hence, reachable on a TCP/IP-based network). A host also can be a computer that offers TCP/IP services to clients.
- **IEEE 802** A project undertaken by the IEEE in 1980 that covers Physical and Data Link layers for networking technologies in general (802.1 and 802.2), plus specific networking technologies, such as Ethernet (802.3).
- **Institute of Electrical and Electronic Engineers (IEEE)** An international organization that sets standards for electrical and electronic equipment, including network interfaces and communications technologies.
- **International Organization for Standardization (ISO)** An international standards organization based in Geneva, Switzerland, that sets standards for information technology and networking equipment, protocols, and communications technologies.
- **International Organization for Standardization Open Systems Interconnection** *See* International Organization for Standardization and Open Systems Interconnection.
- **Internet Architecture Board (IAB)** The organization within the Internet Society that governs the actions of both the IETF and the IRTF, and has final approval authority for Internet Standards.
- **Internet Corporation for Assigned Names and Numbers (ICANN)** The organization within the Internet Society responsible for proper assignment of all domain names and numeric IP addresses for the global Internet. ICANN works with private companies called name registrars to manage domain names and with ISPs to manage assignment of numeric IP addresses.
- **Internet Engineering Task Force (IETF)** The organization within the Internet Society that's responsible for all currently used Internet Standards, protocols, and services as well as for managing the development and maintenance of Internet Requests for Comments (RFCs).

- **Internet Protocol (IP)** The primary Network layer protocol in the TCP/IP suite. IP manages routing and delivery for traffic on TCP/IP-based networks.
- **Internet Protocol version 4 (IPv4)** The original version of IP that's still in widespread public use, although IPv6 is currently fully specified and moving into global deployment and use.
- **Internet Protocol version 6 (IPv6)** The latest version of IP that's moving into global deployment and use (IPv4 remains the predominant TCP/IP version in use but will slowly be supplanted by IPv6).
- **Internet Research Task Force (IRTF)** The forward-looking research and development arm of the Internet Society. The IRTF reports to the IAB for direction and governance.
- **Internet Society (ISOC)** The parent organization under which the rest of the Internet governing bodies fall. ISOC is a user-oriented, public-access organization that solicits end-user participation and input to help set future Internet policy and direction.
- **Internet Standard** An RFC document that specifies the rules, structure, and behavior of a current Internet protocol or service. Also called a Standard RFC.
- **internetwork** Literally, a "network of networks," an internetwork is better understood as a collection of multiple interconnected physical networks that together behave as a single logical network (of which the Internet is the prime example).
- **ISO/OSI network reference model** The official name for the seven-layer network reference model used to describe how networks operate and behave.
- **layer** A single component or facet in a networking model that handles one particular aspect of network access or communications.
- **local area network (LAN)** A single network cable segment, subnet, or logical network community that represents a collection of machines that can communicate with one another more or less directly (using MAC addresses).
- **maximum transmission unit (MTU)** The biggest single chunk of data that can be transferred across any particular type of network medium—for example, 1,518 bytes is the MTU for conventional Ethernet.
- **media flow control** The management of data transmission rates between two devices across a local network medium that guarantees the receiver can accept and process input before it arrives from the sender.
- **multicast packet** A packet sent to a group of devices, often multiple routers.
multiplexing The process whereby multiple individual data streams from Application layer processes are joined together for transmission by a specific TCP/IP transport protocol through the IP protocol.
- **network analysis** Another term for protocol analysis.
- **Network File System (NFS)** A TCP/IP-based, network-distributed file system that permits users to treat files and directories on machines elsewhere on a network as an extension of their local desktop file systems.
- **network interface controller (NIC)** A hardware device used to permit a computer to attach to and communicate with a local area network.
- **Network layer** Layer 3 of the ISO/OSI network reference model. The Network layer handles logical addresses associated with individual machines on a network by correlating human-readable names for such machines with unique, machine-readable numeric addresses. It uses addressing information to route a PDU from a sender to a receiver when the source and destination do not reside on the same physical network segment.

- **network reference model** *See* ISO/OSI network reference model.
- **network services** A TCP/IP term for a protocol/service combination that operates at the Application layer in the TCP/IP network model.
- **Open Systems Interconnection (OSI)** The name of an open-standard internetworking initiative undertaken in the 1980s, primarily in Europe, and originally intended to supersede TCP/IP. Technical and political problems prevented this anticipated outcome from materializing, but the ISO/OSI reference model is a legacy of this effort.
- **oversized packets** Packets that exceed the MTU for the network and usually point to a problem with a NIC or its driver software.
- **packet** A generic term for a PDU at any layer in a networking model. The term is properly applied to PDUs at Layer 3 or the TCP/IP Internet layer.
- **packet filter** A specific collection of inclusion or exclusion rules that is applied to a stream of network packets and determines what is captured (and what is ignored) from the original input stream.
- **packet header** *See* header.
- **packet trailer** *See* trailer.
- **packet-switched network** A network in which data packets may take any usable path between sender and receiver, where sender and receiver are identified by unique network addresses and there's no requirement that all packets follow the same path in transit (although they often do).
- **payload** That portion of a PDU that contains information intended for delivery to an application or to a higher-layer protocol (depending on where in the stack the PDU is situated).
- **pcap** A generic term (short for "protocol capture") for a special network interface driver designed to permit capture of all network traffic in promiscuous mode while running. Though originally associated with the tcpdump open source command-line protocol analyzer, pcap is widely used in protocol analyzers today, including the one chosen as a teaching tool for this book, the Wireshark protocol analyzer.
- **pcapng** A packet capture driver used in Wireshark beginning with version 1.8 and developed to overcome limitations in the libpcap format. The term pcapng is short for "PCAP Next Generation."
- **peer layers** Analogous layers in the protocol stacks on a sender and a receiver; the receiving layer usually reverses whatever operations the sending layer performs (which is what makes those layers peers).
- **Physical layer** Layer 1 in the ISO/OSI network reference model. The Physical layer is where connections, communications, and interfaces—hardware and signaling requirements—are handled.
- **Point-to-Point Protocol (PPP)** A Layer 2 or TCP/IP Network Interface layer protocol that permits a client and a server to establish a communications link that can accommodate a variety of higher-layer protocols, including IP. Today's most widely used serial line protocol for making Internet connections.
- **point-to-point transmission** A type of network communication in which pairs of devices establish a communications link to exchange data with one another; the most common type of connection used when communicating with an Internet service provider.
- **Point-to-Point Tunneling Protocol (PPTP)** A Layer 2 or TCP/IP Network Interface layer protocol that allows a client and a server to establish a secure, encrypted communications link for just about any kind of PPP traffic.

- **port number** A 16-bit number that identifies either a well-known application service or a dynamically assigned port number for a transitory sender-receiver exchange of data through TCP or UDP. Also referred to as a port address.
- **pre-filter** A type of data filter applied to a raw input stream in a protocol analyzer that selects only packets that meet its criteria for capture and retention. Because it is applied before data is captured, it's called a pre-filter.
- **Presentation layer** Layer 6 of the ISO/OSI reference model. The Presentation layer is where generic network data formats are translated into platform-specific data formats for incoming data and vice versa for outgoing data. This is also the layer where optional encryption or compression services may be applied (or reversed).
- **Process layer** A synonym for the TCP/IP Application layer, where high-level protocols and services, such as FTP and Telnet, operate.
- **promiscuous mode operation** Network interface card and driver operation used to capture broadcast packets, multicast packets, packets sent to other devices, and error packets.
- **Proposed Standard** An intermediate step for standards-level RFCs in which a Draft Standard goes through initial review, with two or more reference implementations to demonstrate interoperability between those implementations.
- **protocol** A precise set of standards that governs communications between computers on a network. Many protocols function in one or more layers of the OSI reference model.
- **protocol analysis** The process of capturing packets off the network for the purpose of gathering communication statistics, observing trends, and examining communication sequences.
- **protocol data unit (PDU)** At any layer in a networking model, a PDU represents the package for data at that layer, including a header, a payload, and, in some cases, a trailer.
- **protocol number** An 8-bit numeric identifier associated with some specific TCP/IP protocol.
- **protocol stack** A specific implementation of a protocol suite on a computer, including a network interface, necessary drivers, and whatever protocol and service implementations are necessary to enable the computer to use a specific protocol suite to communicate across the network.
- **protocol suite** A named family of networking protocols, such as TCP/IP, where each such family enables computers to communicate across a network.
- **reassembly** The process applied at the Transport layer in which messages segmented into multiple chunks for transmission across the network are put back together in the proper order for delivery to an application on the receiving end. The IP Fragment Offset field (discussed in Chapter 3) is used to identify the order of the fragments for reassembly.
- **registered port** A TCP or UDP port number in the range from 1024 to 65535 and associated with a specific Application layer protocol or service. IANA maintains a registered port number list at *www.iana.org*.
- **Remote Monitoring (RMON)** A TCP/IP Application layer protocol designed to support remote monitoring and management of networking devices, such as hubs, servers, and routers.

- **Request for Comments (RFCs)** IETF standards documents that specify or describe best practices, provide information about the Internet, or specify an Internet protocol or service.
- **routing** The process whereby a packet makes its way from a sender to a receiver based on known paths (or routes) from the sending network to the receiving network.
- **runts** *See* undersized packets.
- **segment** The name of the PDU for the TCP protocol in a TCP/IP environment.
- **segmentation** The process whereby TCP takes a message larger than an underlying network medium's MTU and breaks it up into a numbered sequence of chunks less than or equal to the MTU in size.
- **session** A temporary, but ongoing, exchange of messages between a sender and a receiver on a network.
- **Session layer** Layer 5 in the ISO/OSI reference model. The Session layer handles setup, maintenance, and teardown of ongoing exchanges of messages between pairs of hosts on a network.
- **socket** *See* socket address.
- **socket address** A numeric TCP/IP address that concatenates a network host's numeric IP address (first 4 bytes) with the port address for some specific process or service on that host (last two bytes) to uniquely identify that process across the entire Internet.
- **source port number** The sender's port address for a TCP or UDP PDU.
- **statistics** Short- or long-term historical information regarding network communications and performance, captured by a protocol analyzer or other similar software.
- **TCP/IP** *See* Transmission Control Protocol/Internet Protocol.
- **trace buffer** An area of memory or hard disk space set aside for the storage of packets captured off the network by a protocol analyzer.
- **trailer** An optional, concluding portion of a PDU that usually contains data integrity check information for the preceding content in that PDU.
- **Transmission Control Protocol (TCP)** A robust, reliable, connection-oriented protocol that operates at the Transport layer in both the TCP/IP and ISO/OSI reference models and that gives TCP/IP part of its name.
- **Transmission Control Protocol/Internet Protocol (TCP/IP)** The name of the standard protocols and services in use on the Internet, denoted by the names of the two key constituent protocols: the Transmission Control Protocol, or TCP, and the Internet Protocol, or IP.
- **Transport layer** Layer 4 of the ISO/OSI network reference model and the third layer of the TCP/IP network model. The Transport layer handles delivery of data from sender to receiver.
- **undersized packets** Packets that are below minimum packet size requirements and point to potential hardware or driver problems.
- **unicast packet** A packet sent to a single device on the network.
- **Uniform Resource Locator (URL)** Web terminology for an address that specifies the protocol (http://), location (domain name), directory (/directory-name/), and filename (example.html) so that a browser can access a resource.
- **Virtual Private Network (VPN)** A network connection (containing one or more packaged protocols) between a specific sender and receiver in which information sent is often encrypted. A VPN uses public networks—like the Internet—to deliver secure, private information from sender to receiver.

- **well-known port number** A 16-bit number that identifies a preassigned value associated with some well-known Internet protocol or service that operates at the TCP/IP Application layer. Most well-known port numbers fall in the range from 0 to 1024, but IANA (see *www.iana.org*) also documents registered port numbers above that range that behave likewise. Also called a well-known port address.
- **well-known protocol** An 8-bit number in the header of an IP packet that identifies the protocol in use, as per IANA (at *www.iana.org*).
- **well-known service** A synonym for a recognizable TCP/IP protocol or service; these assignments are documented at the IANA site (*www.iana.org*).

Technical Notes for Hands-On Projects

The lab setup for Chapter 1 includes the following elements:

HANDS-ON PROJECT	NETWORK DEVICES REQUIRED	WORKSTATION OPERATING SYSTEM REQUIRED	OTHER RESOURCES REQUIRED
1-1	Network adapter, network connection	Windows 7 Professional or Windows 10 Pro	Wireshark v2.0.0 (installation file available in student and instructor resources for *Guide to TCP/IP: IPv6 and IPv4* at *cengagebrain.com* or at *www.wireshark.org*)
1-2	Network adapter, network connection	Windows 7 Professional or Windows 10 Pro	Wireshark software installed on workstation
1-3	Network adapter, network connection	Windows 7 Professional or Windows 10 Pro	Wireshark software installed on workstation
1-4	Network adapter, network connection	Windows 7 Professional or Windows 10 Pro	Wireshark software installed on workstation
1-5	Network adapter, network connection	Windows 7 Professional or Windows 10 Pro	Wireshark software installed on workstation

Note: Each chapter is accompanied by a set of Hands-On Project (HOP) assessment questions, some of which require access to files used in the HOPs. Have the students save personal data files while performing HOP activities, even if saving files is not part of the instructions in the HOPs.