chapter 2

Networking Standards and the OSI Model

After reading this chapter and completing the exercises, you will be able to:

- Identify organizations that set standards for networking
- Describe the purpose of the OSI model and each of its layers
- Explain specific functions belonging to each OSI model layer
- Understand how two network nodes communicate through the OSI model
- Discuss the structure and purpose of data packets and frames
- Describe the two types of addressing covered by the OSI model

On the Job

When new technologies emerge, it's valuable to establish standards before the technology is widely deployed. To do so requires getting many parties involved early—the technology developers, equipment suppliers, service providers, end users, marketers, and even organizations that set standards for different, but related, technologies.

For years I've worked on a technology called Metro Ethernet, which uses ubiquitous Ethernet to deliver high-speed data networking services directly to businesses over metropolitan area networks (MANs). This streamlined service bypasses the traditional voice-oriented telephone network often seen as a bottleneck for efficient data communications. My partners and I founded a company in July 1999 and first offered Metro Ethernet in February 2000. It rapidly became clear that this technology was hot. But at that time, no one in the industry agreed on exactly what Metro Ethernet included and how the services should be supplied. That's why I and others founded the Metro Ethernet Forum (MEF) in 2001. The MEF is a nonprofit organization with over 60 member companies working to create and accelerate the adoption of Metro Ethernet standards worldwide. Our members include traditional telephone companies, new types of network service providers, networking equipment manufacturers, electronic component suppliers, and other organizations.

Generating standards that are meaningful and lasting requires significant time and effort. The MEF relies on volunteers from its membership to participate in the work of our Technical or Marketing committees. In each, they review issues, draft recommendations, submit straw ballots, collaborate to achieve consensus, and craft and vote on subsequent ballots that gradually define our implementation agreements and standards. Finally, a letter ballot is submitted to the membership for review and a vote on acceptance at a quarterly meeting. Approximately 80 percent of proposed standards are accepted.

MEF is now working with other standards organizations, such as IEEE, IETF, and ITU, to foster national and international adoption of Metro Ethernet standards. The MEF has created liaisons with these organizations, sharing research and proposing specifications so that other standards bodies need not duplicate our efforts. Wishing to contribute to worldwide cooperation, in July 2003 the MEF hosted in San Francisco the ITU Forum Summit—the largest gathering to date of telecom forum leaders.

Ron Young CEO, MetNet Communications, Inc. and Founding Chairman of the Board of the Metro Ethernet Forum

When trying to grasp a new theoretical concept, it often helps to form a picture of that concept in your mind. In the field of chemistry, for example, even though you can't see a water molecule, you can represent it with a simple drawing of two hydrogen atoms and one oxygen atom. Similarly, in the field of networking, even though you can't see the communication that occurs between two nodes on a network, you can use a model to depict how the communication takes place. The model commonly used to describe network communications is called the OSI (Open Systems Interconnection) model.

In this chapter, you will learn about the standards organizations that have helped create the various conventions (such as the OSI model) used in networking. Next, you'll be introduced to the seven layers of the OSI model and learn how they interact. You will then take a closer look at what goes on in each layer. Finally, you will learn to apply those details to a practical networking environment. Granted, learning the OSI model is not the most exciting part of becoming a networking expert. Thoroughly understanding it, however, is essential to proficient network design and troubleshooting.

Networking Standards Organizations

Standards are documented agreements containing technical specifications or other precise criteria that stipulate how a particular product or service should be designed or performed. Many different industries use standards to ensure that products, processes, and services suit their purposes. Because of the wide variety of hardware and software in use today, standards are especially important in the world of networking. Without standards, it would be very difficult to design a network because you could not be certain that software or hardware from different manufacturers would work together. For example, if one manufacturer designed a network cable with a 1-centimeter-wide plug and another company manufactured a wall plate with a 0.8-centimeter-wide opening, you would not be able to insert the plug into the wall plate.

When purchasing networking equipment, therefore, you want to verify that equipment meets the standards your network requires. However, bear in mind that standards define the *minimum* acceptable performance of a product or service—not the ideal. So, for example, you might purchase two different network cables that comply with the minimum standard for transmitting at a certain speed, but one cable might exceed that standard, allowing for better network performance. In the case of network cables, exceeding minimum standards often follows from the use of quality materials and careful production techniques.

Because the computer industry grew so quickly out of several technical disciplines, many different organizations evolved to oversee its standards. In some cases, a few organizations are responsible for a single aspect of networking. For example, both ANSI and IEEE are involved in setting standards for wireless networks. Whereas ANSI prescribes the kind of NIC (network interface card) that the consumer needs to accept a wireless connection, IEEE prescribes, among other things, how the network will ensure that different parts of a communication sent through the atmosphere arrive at their destination in the correct sequence.

A complete list of the standards that regulate computers and networking would fill an encyclopedia. Although you don't need to know the fine points of every standard, you should be familiar with the groups that set networking standards and the critical aspects of standards required by your network.

ANSI

ANSI (**American National Standards Institute**) is an organization composed of more than a thousand representatives from industry and government who together determine standards for the electronics industry and other fields, such as chemical and nuclear engineering, health and safety, and construction. ANSI also represents the United States in setting international standards. This organization does not dictate that manufacturers comply with its standards, but requests voluntarily compliance. Of course, manufacturers and developers benefit from compliance, because compliance assures potential customers that the systems are reliable and can be integrated with an existing infrastructure. New electronic equipment and methods must undergo rigorous testing to prove they are worthy of ANSI's approval.

You can purchase ANSI standards documents online from ANSI's Web site (*www.ansi.org*) or find them at a university or public library. You need not read complete ANSI standards to be a competent networking professional, but you should understand the breadth and significance of ANSI's influence.

EIA and TIA

Two related standards organizations are EIA and TIA. **EIA** (**Electronic Industries Alliance**) is a trade organization composed of representatives from electronics manufacturing firms across the United States. EIA not only sets standards for its members, but also helps write ANSI standards and lobbies for legislation favorable to the growth of the computer and electronics industries.

In 1988, one of the EIA's subgroups merged with the former United States Telecommunications Suppliers Association (USTSA) to form **TIA** (**Telecommunications Industry Association**). TIA focuses on standards for information technology, wireless, satellite, fiber optics, and telephone equipment. Both TIA and EIA set standards, lobby governments and industry, and sponsor conferences, exhibitions, and forums in their areas of interest.

Probably the best known standards to come from the TIA/EIA alliance are its guidelines for how network cable should be installed in commercial buildings, known as the "TIA/EIA 568-B Series." You can find out more about TIA from its Web site, *www.tiaonline.org*, and EIA from its Web site, *www.eia.org*.

IEEE

The **IEEE** (**Institute of Electrical and Electronics Engineers**), or "I-triple-E," is an international society composed of engineering professionals. Its goals are to promote development and education in the electrical engineering and computer science fields. To this end, IEEE hosts numerous symposia, conferences, and local chapter meetings and publishes papers designed to educate members on technological advances. It also maintains a standards board that establishes its own standards for the electronics and computer industries and contributes to the work of other standards-setting bodies, such as ANSI.

IEEE technical papers and standards are highly respected in the networking profession. Among other places, you will find references to IEEE standards in the manuals that accompany NICs. You can purchase IEEE documents online from IEEE's Web site (*www.ieee.org*) or find them in a university or public library.

ISO

ISO (**International Organization for Standardization**), headquartered in Geneva, Switzerland, is a collection of standards organizations representing 157 countries. ISO's goal is to establish international technological standards to facilitate global exchange of information and barrier-free trade. Given the organization's full name, you might expect it to be called *IOS*, but ISO is not meant to be an acronym. In fact, *iso* is the Greek word for *equal*. Using this term conveys the organization's dedication to standards.

ISO's authority is not limited to the information-processing and communications industries. It also applies to the fields of textiles, packaging, distribution of goods, energy production and utilization, shipbuilding, and banking and financial services. The universal agreements on screw threads, bank cards, and even the names for currencies are all products of ISO's work. In fact, fewer than 3000 of ISO's more than 17,000 standards apply to computer-related products and functions. You can find out more about ISO at its Web site: *www.iso.org*.

ITU

The **ITU** (**International Telecommunication Union**) is a specialized United Nations agency that regulates international telecommunications, including radio and TV frequencies, satellite and telephony specifications, networking infrastructure, and tariffs applied to global communications. It also provides developing countries with technical expertise and equipment to advance those nations' technological bases.

The ITU was founded in Paris in 1865. It became part of the United Nations in 1947 and relocated to Geneva, Switzerland. Its standards arm contains members from 191 countries and publishes detailed policy and standards documents that can be found on its Web site: *www.itu.int*. Typically, ITU documents pertain more to global telecommunications issues than to industry technical specifications. However, the ITU is deeply involved with the implementation of worldwide Internet services. As in other areas, the ITU cooperates with several different standards organizations, such as ISOC (discussed next), to develop these standards.

ISOC

ISOC (**Internet Society**), founded in 1992, is a professional membership society that helps to establish technical standards for the Internet. Some current ISOC concerns include the rapid growth of the Internet and keeping it accessible, information security, and the need for stable addressing services and open standards across the Internet. ISOC's membership consists of thousands of Internet professionals and companies from 90 chapters around the world.

ISOC oversees groups with specific missions, such as the **IAB** (**Internet Architecture Board**). IAB is a technical advisory group of researchers and technical professionals interested in overseeing the Internet's design and management. As part of its charter, IAB is responsible for Internet growth and management strategy, resolution of technical disputes, and standards oversight.

Another ISOC group is the **IETF** (**Internet Engineering Task Force**), the organization that sets standards for how systems communicate over the Internet—in particular, how protocols operate and interact. Anyone can submit a proposed standard for IETF approval. The standard then undergoes elaborate review, testing, and approval processes. On an international level, IETF works with the ITU to help give technical standards approved in the United States international acceptance.

You can learn more about ISOC and its member organizations, IAB and IETF, at their Web site: *www.isoc.org*.

IANA and ICANN

You have learned that every computer on a network must have a unique address. On the Internet, this is especially important because millions of different computers must be available to transmit and receive data at any time. Addresses used to identify computers on the Internet and other TCP/IP-based networks are known as **IP (Internet Protocol) addresses**. To ensure that every Internet-connected device has a unique IP address, organizations across the globe rely on centralized authorities.

In early Internet history, a nonprofit group called the **IANA (Internet Assigned Numbers Authority)** kept records of available and reserved IP addresses and determined how addresses were doled out. Starting in 1997, IANA coordinated its efforts with three **RIRs (Regional Internet Registries)**: ARIN (American Registry for Internet Numbers), APNIC (Asia Pacific Network Information Centre), and RIPE (Réseaux IP Européens). An RIR is a not-for-profit agency that manages the distribution of IP addresses to private and public entities. In the late 1990s, the United States Department of Commerce (DOC), which funded IANA, decided to overhaul IP addressing and domain name management. The DOC recommended the formation of **ICANN (Internet Corporation for Assigned Names and Numbers)**, a private, nonprofit corporation. ICANN is now ultimately responsible for IP addressing and domain name management. Technically speaking, however, IANA continues to perform the system administration.

Individuals and businesses do not typically obtain IP addresses directly from an RIR or IANA. Instead, they lease a group of addresses from their **ISP (Internet service provider)**, a business that provides organizations and individuals with access to the Internet and often, other services, such as e-mail and Web hosting. An ISP, in turn, arranges with its RIR for the right to use certain IP addresses on its network. The RIR obtains its right to dole out those addresses from ICANN. In addition, the RIR coordinates with IANA to ensure that the addresses are associated with devices connected to the ISP's network.

You can learn more about IANA and ICANN at their Web sites, *www.iana.org* and *www.icann.org*, respectively.

The OSI Model

Net+ 4.1

In the early 1980s, ISO began work on a universal set of specifications that would enable computer platforms across the world to communicate openly. The result was a helpful model for understanding and developing computer-to-computer communications over a network. This model, called the **OSI (Open Systems Interconnection) model**, divides network communications into seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. At each layer, protocols perform services unique to that layer. While performing those services, the protocols also interact with protocols in the layers directly above and below. In addition, at the top of the OSI model, Application layer protocols interact with the software you use (such an e-mail or spreadsheet program). At the bottom, Physical layer services act on the networking cables and connectors to issue and receive signals.

You have already learned that protocols are the rules by which computers communicate. A protocol is simply a set of instructions written by a programmer to perform a function or

Net+ 4.1

group of functions. Some protocols are included with a computer's operating system. Others are files installed with software programs. Chapter 4 covers protocols in depth; however, some protocols are briefly introduced in the following sections to better explain what happens at each layer of the OSI model.

The OSI model is a theoretical representation of what happens between two nodes communicating on a network. It does not prescribe the type of hardware or software that should support each layer. Nor does it describe how software programs interact with other software programs or how software programs interact with humans. Every process that occurs during network communications can be associated with a layer of the OSI model, so you should be familiar with the names of the layers and understand the key services and protocols that belong to each.

Networking professionals often devise a mnemonic way of remembering the seven layers of the OSI model. One strategy is to make a sentence using words that begin with the same first letter of each layer, starting with either the lowest (Physical) or the highest (Application) layer. For example, you might choose to remember the phrase "Programmers Dare Not Throw Salty Pretzels Away." Quirky phrases are often easiest to remember.

The path that data takes from one computer to another through the OSI model is illustrated in Figure 2-1. First, a user or device initiates a data exchange through the Application layer. The Application layer separates data into **PDUs** (**protocol data units**), or discrete amounts of data. From there, Application layer PDUs progress down through OSI model layers 6, 5, 4, 3,

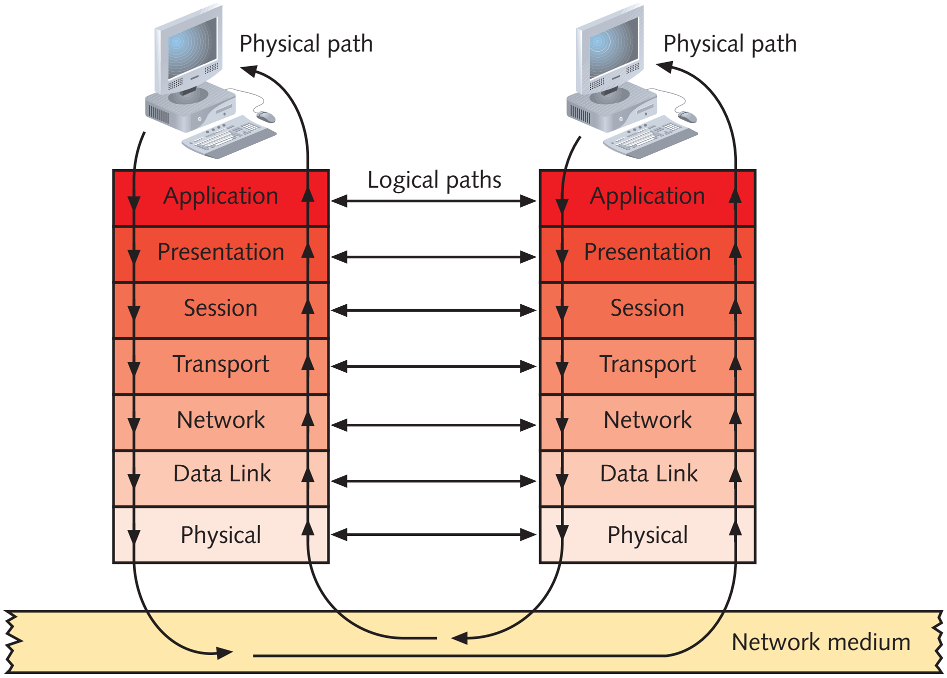


Figure 2-1 Flow of data through the OSI model

Net+ 4.1 2, and 1 before being issued to the network medium—for example, the wire. The data traverses the network until it reaches the second computer's Physical layer. Then at the receiving computer the data progresses up the OSI model until it reaches the second computer's Application layer. This transfer of information happens in milliseconds.

Logically, however, each layer communicates with the same layer from one computer to another. In other words, the Application layer protocols on one computer exchange information with the Application layer protocols of the second computer. Protocols from other layers do not attempt to interpret Application layer data. In the following sections, the OSI model layers are discussed from highest to lowest, beginning with the Application layer, where the flow of information is initiated.

Bear in mind that the OSI model is a generalized and sometimes imperfect representation of network communication. In some cases, network functions can be associated with more than one layer of the model, and in other cases, network operations do not require services from every layer.

Application Layer

Net+ 4.1 The top, or seventh, layer of the OSI model is the **Application layer**. Contrary to what its name implies, the Application layer does not include software applications, such as Microsoft Word or Firefox. Instead, Application layer services facilitate communication between software applications and lower-layer network services so that the network can interpret an application's request and, in turn, the application can interpret data sent from the network. Through Application layer protocols, software applications negotiate their formatting, procedural, security, synchronization, and other requirements with the network.

Net+ 1.1 4.1 For example, when you choose to open a Web page in Firefox, an Application layer protocol called **HTTP** (**Hypertext Transfer Protocol**) formats and sends your request from your client's browser (a software application) to the server. It also formats and sends the Web server's response back to your client's browser.

Suppose you choose to view the Exhibits page at the Library of Congress's Web site. You type "www.loc.gov/index.html" in Firefox and press Enter. At that point, Firefox's **API** (**application program interface**), a set of routines that make up part of the software, transfers your request to the HTTP protocol. HTTP prompts lower-layer protocols to establish a connection between your computer and the Web server. Next, HTTP formats your request for the Web page and sends the request to the Web server. One part of the HTTP request includes a command that begins with "GET" and tells the server what page you want to retrieve. Other parts of the request indicate what version of HTTP you're using, what types of graphics and what language your browser can accept, and what browser version you're using, among other things.

After receiving your computer's HTTP request, the Web server responsible for *www.loc.gov* responds, also via HTTP. Its response includes the text and graphics that make up the Web page, plus specifications for the content contained in the page, the HTTP version used, the type of HTTP response, and the length of the page. However, if the Web page is unavailable, the host, *www.loc.gov*, sends an HTTP response containing an error message, such as "Error 404 – File Not Found."

After receiving the Web server's response, your workstation uses HTTP to interpret this response so that Firefox can present the *www.loc.gov/index.html* Web page in a format

Net+ 1.1 4.1 you'll recognize, with neatly arranged text and images. Note that the information issued by one node's HTTP protocol is designed to be interpreted by the other node's HTTP protocol. However, as you will learn in later sections, HTTP requests cannot traverse the network without the assistance of lower-layer protocols.

Presentation Layer

Net+ 4.1 Protocols at the **Presentation layer** accept Application layer data and format it so that one type of application and host can understand data from another type of application and host. In other words, the Presentation layer serves as a translator. If you have spent any time working with computer graphics, you have probably heard of the GIF, JPG, and TIFF methods of compressing and encoding graphics. MPEG and QuickTime are two popular methods of compressing and encoding audio and video data. The popular audio format MP3, for example, uses MPEG compression. It can turn a music track that would require 30 MB of space on a CD into a file no larger than 3 MB – or even smaller, if lower quality were acceptable. Two well-known methods of encoding text are ASCII and EBCDIC. In each of these examples, it is the Presentation layer protocols that perform the coding and compression. They also interpret coded and compressed formats in data received from other computers. In the previous example of requesting a Web page, the Presentation layer protocols would interpret the JPG files transmitted within the Web server's HTTP response.

Presentation layer services also manage data encryption (such as the scrambling of passwords) and decryption. For example, if you look up your bank account status via the Internet, you are using a secure connection, and Presentation layer protocols will encrypt your account data before it is transmitted. On your end of the network, the Presentation layer will decrypt the data as it is received.

Session Layer

Net+ 4.1 Protocols in the **Session layer** coordinate and maintain communications between two nodes on the network. The term **session** refers to a connection for ongoing data exchange between two parties. Historically, it was used in the context of terminal and mainframe communications, in which the **terminal** is a device with little (if any) of its own processing or disk capacity that depends on a host to supply it with software and processing services. Today, the term *session* is often used in the context of a connection between a remote client and an access server or between a Web browser client and a Web server.

Among the Session layer's functions are establishing and keeping alive the communications link for the duration of the session, keeping the communication secure, synchronizing the dialogue between the two nodes, determining whether communications have been cut off, and, if so, figuring out where to restart transmission, and terminating communications. Session layer services also set the terms of communication by deciding which node communicates first and how long a node can communicate. Finally, the Session layer monitors the identification of session participants, ensuring that only the authorized nodes can access the session.

When you initiate a connection with your ISP, for example, the Session layer services at your ISP's server and on your computer negotiate the connection. If your data cable accidentally falls out of the wall jack, Session layer protocols on your end will detect the loss of a connection and initiate attempts to reconnect. If they cannot reconnect after a certain period of time, they will close the session and inform your client software that communication has ended.

Transport Layer

Net+ 1.1 4.1

Protocols in the **Transport layer** accept data from the Session layer and manage end-to-end delivery of data. That means they can ensure that the data is transferred from point A to point B reliably, in the correct sequence, and without errors. Without Transport layer services, data could not be verified or interpreted by its recipient. Transport layer protocols also handle **flow control**, which is the process of gauging the appropriate rate of transmission based on how fast the recipient can accept data. Dozens of different Transport layer protocols exist, but most modern networks, such as the Internet, rely on only a few. In the example of retrieving a Web page, a Transport layer protocol called TCP (Transmission Control Protocol) takes care of reliably transmitting the HTTP protocol's request from client to server and vice versa. You will learn more about this significant protocol later in this book.

Some Transport layer protocols take steps to ensure that data arrives exactly as it was sent. Such protocols are **connection oriented**, because they establish a connection with another node before they begin transmitting data. TCP is one example of a connection-oriented protocol. In the case of requesting a Web page, the client's TCP protocol first sends a **SYN** (**synchronization**) packet request for a connection to the Web server. The Web server responds with a **SYN-ACK** (**synchronization-acknowledgment**) packet, or a confirmation, to indicate that it's willing to make a connection. Then, the client responds with its own **ACK** (**acknowledgment**). Through this three-step process, also known as a handshake, a connection is established. Only after TCP establishes this connection does it transmit the HTTP request for a Web page.

Acknowledgments are also used in subsequent communications to ensure that data was properly delivered. For every data unit a node sends, its connection-oriented protocol expects an acknowledgment from the recipient. For example, after a client's TCP protocol issued an HTTP request, it would expect to receive an acknowledgment from the Web server proving that the data arrived. If data isn't acknowledged within a given time period, the client's protocol assumes the data was lost and retransmits it.

To ensure data integrity further, connection-oriented protocols such as TCP use a checksum. A **checksum** is a unique character string that allows the receiving node to determine if an arriving data unit exactly matches the data unit sent by the source. Checksums are added to data at the source and verified at the destination. If at the destination a checksum doesn't match what the source predicted, the destination's Transport layer protocols ask the source to retransmit the data. As you will learn, protocols at other layers of the OSI model also use checksums.

Not all Transport layer protocols are concerned with reliability. Those that do not establish a connection before transmitting and make no effort to ensure that data is delivered free of errors are called **connectionless** protocols. A connectionless protocol's lack of sophistication makes it more efficient than a connection-oriented protocol and renders it useful in situations in which data must be transferred quickly, such as live audio or video transmissions over the Internet. In these cases, connection-oriented protocols—with their acknowledgments, checksums, and flow control mechanisms—would add overhead to the transmission and potentially bog it down. In a video transmission, for example, this could result in pictures that are incomplete or aren't updated quickly enough to coincide with the audio.

In addition to ensuring reliable data delivery, Transport layer protocols break large data units received from the Session layer into multiple smaller units, called **segments**. This process is known as **segmentation**. On certain types of networks, segmentation increases data transmission efficiency. In some cases, segmentation is necessary for data units to match a

Net+ 1.1 4.1 network's **MTU** (**maximum transmission unit**), the largest data unit it will carry. Every network type specifies a default MTU (though its size can be modified to some extent by a network administrator). For example, by default, Ethernet networks cannot accept packets with data payloads larger than 1500 bytes. Suppose an application wants to send a 6000-byte unit of data. Before this data unit can be issued to an Ethernet network, it must be segmented into units no larger than 1500 bytes. To learn a network's MTU size (and thereby determine whether it needs to segment packets), Transport layer protocols perform a discovery routine upon establishing a connection with the network. Thereafter, the protocols will segment each data unit as necessary until closing the connection.

Segmentation is similar to the process of breaking down words into recognizable syllables that a child uses when learning to read. **Reassembly** is the process of reconstructing the segmented data units. To continue the reading analogy, when a child understands the separate syllables, he can combine them into a word—that is, he can reassemble the parts into a whole. To learn how reassembly works, suppose that you asked this question in history class: "Ms. Jones? How did poor farming techniques contribute to the Dust Bowl?" but that the words arrived at Ms. Jones's ear as "poor farming techniques Ms. Jones? how did to the Dust Bowl? contribute." On a network, the Transport layer recognizes this kind of disorder and rearranges the data pieces so that they make sense.

Sequencing is a method of identifying segments that belong to the same group of subdivided data. Sequencing also indicates where a unit of data begins, as well as the order in which groups of data were issued and, therefore, should be interpreted. While establishing a connection, the Transport layer protocols from two devices agree on certain parameters of their communication, including a sequencing scheme. For sequencing to work properly, the Transport layer protocols of two nodes must synchronize their timing and agree on a starting point for the transmission.

Figure 2-2 illustrates the concept of segmentation and reassembly.

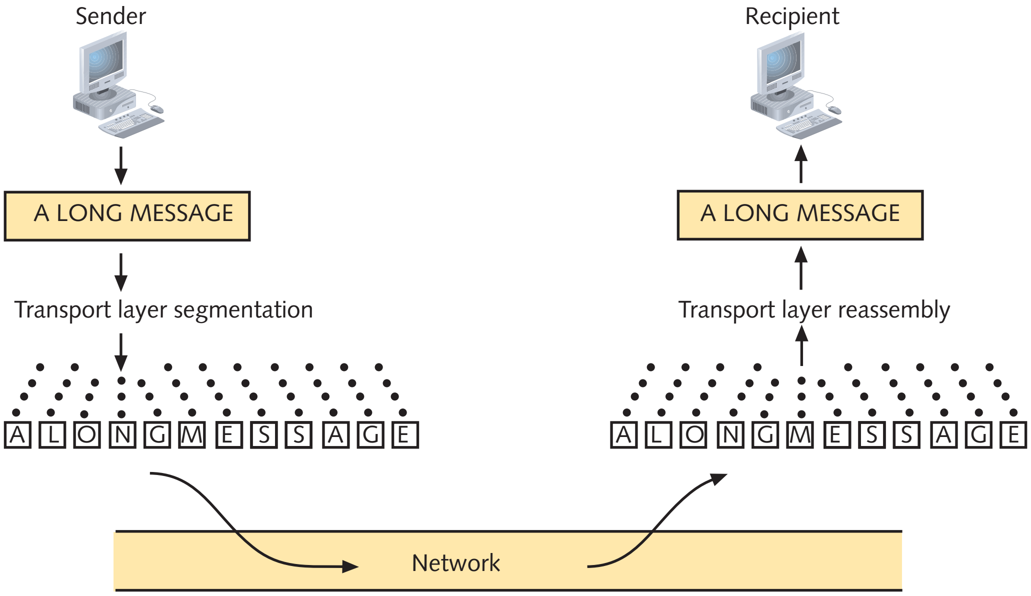
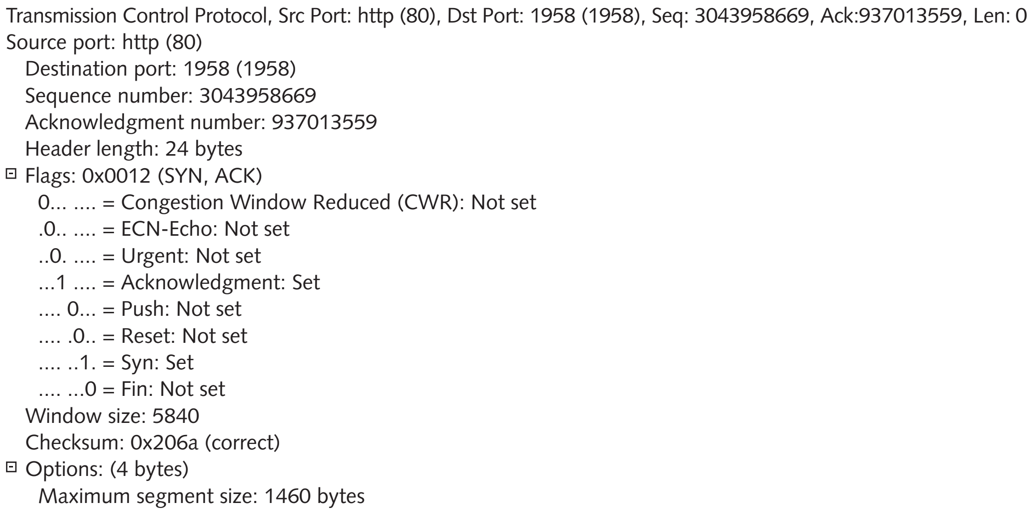


Figure 2-2 Segmentation and reassembly

Net+
1.1
4.1

Figure 2-3 depicts the information contained in an actual TCP segment used to request the Web page *www.loc.gov/index.html*. After reading this section, you should recognize much of the segment's contents. After learning more about protocols later in this book, you will understand the meaning of everything contained in a TCP segment.



```
Transmission Control Protocol, Src Port: http (80), Dst Port: 1958 (1958), Seq: 3043958669, Ack:937013559, Len: 0
Source port: http (80)
   Destination port: 1958 (1958)
   Sequence number: 3043958669
   Acknowledgment number: 937013559
   Header length: 24 bytes
⊟ Flags: 0x0012 (SYN, ACK)
     0... .... = Congestion Window Reduced (CWR): Not set
     .0.. .... = ECN-Echo: Not set
     ..0. .... = Urgent: Not set
     ...1 .... = Acknowledgment: Set
     .... 0... = Push: Not set
     .... .0.. = Reset: Not set
     .... ..1. = Syn: Set
     .... ...0 = Fin: Not set
   Window size: 5840
   Checksum: 0x206a (correct)
⊟ Options: (4 bytes)
     Maximum segment size: 1460 bytes
```

Figure 2-3 A TCP segment

Net+
1.3
4.1

Network Layer

The primary function of protocols at the **Network layer**, the third layer in the OSI model, is to translate network addresses into their physical counterparts and decide how to route data from the sender to the receiver. Addressing is a system for assigning unique identification numbers to devices on a network. Each node has two types of addresses.

One type of address is called a network address. **Network addresses** follow a hierarchical addressing scheme and can be assigned through operating system software. They are hierarchical because they contain subsets of data that incrementally narrow down the location of a node, just as your home address is hierarchical because it provides a country, state, ZIP code, city, street, house number, and person's name. Network layer address formats differ depending on which Network layer protocol the network uses. Network addresses are also called **network layer addresses**, **logical addresses**, or **virtual addresses**. The second type of address assigned to each node is called a physical address, discussed in detail in the next section.

For example, a computer running on a TCP/IP network might have a network layer address of 10.34.99.12 and a physical address of 0060973E97F3. In the classroom example, this addressing scheme is like saying that "Ms. Jones" and "United States citizen with Social Security number 123-45-6789" are the same person. Even though there may be other people named "Ms. Jones" in the United States, only one person has the Social Security number 123-45-6789. Within the confines of your classroom, however, there is only one Ms. Jones, so you can be certain the correct person will respond when you say, "Ms. Jones?" There's no need to use her Social Security number.

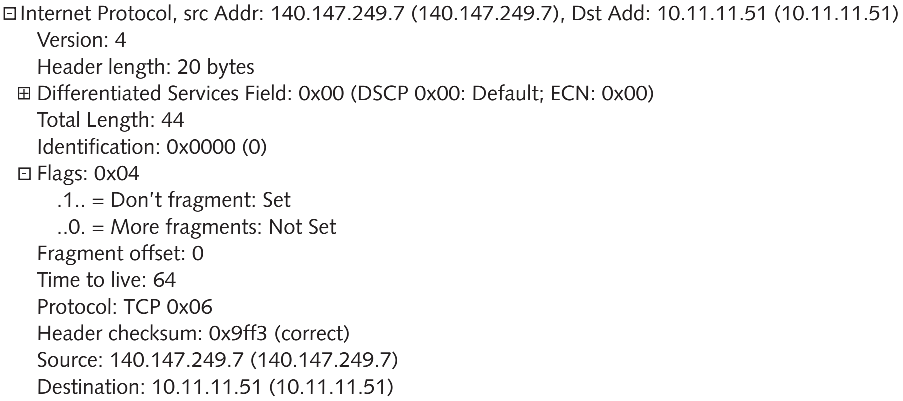
Net+ 4.1 Network layer protocols accept the Transport layer segments and add logical addressing information in a network header. At this point, the data unit becomes a packet. Network layer protocols also determine the path from point A on one network to point B on another network by factoring in:

- Delivery priorities (for example, packets that make up a phone call connected through the Internet might be designated high priority, whereas a mass e-mail message is low priority)
- Network congestion
- Quality of service (for example, some packets may require faster, more reliable delivery)
- Cost of alternative routes

The process of determining the best path is known as routing. More formally, to **route** means to intelligently direct data based on addressing, patterns of usage, and availability. Because the Network layer handles routing, **routers**—the devices that connect network segments and direct data—belong in the Network layer.

Net+ 1.1 4.1 Although there are numerous Network layer protocols, one of the most common, and the one that underlies most Internet traffic, is the **IP** (**Internet Protocol**). In the example of requesting a Web page, IP is the protocol that instructs the network where the HTTP request is coming from and where it should go. Figure 2-4 depicts the data found in an IP packet used to contact the Web site *www.loc.gov/index.html*. Notice the Network layer addresses, or IP addresses, in the first line of the packet. The first, labeled "src Addr" reveals the unique IP address of the computer issuing the transmission. The next, labeled "DST Add" indicates the unique IP address of the receiving computer.

On TCP/IP-based networks (such as the Internet), Network layer protocols can perform an additional function called fragmentation. In **fragmentation**, a Network layer protocol (such as IP) subdivides the segments it receives from the Transport layer into smaller packets. If this process sounds familiar, it's because fragmentation accomplishes the same task at the Network layer that segmentation performs at the Transport layer. It ensures that packets issued to the network are no larger than the network's maximum transmission unit size.



```
⊟Internet Protocol, src Addr: 140.147.249.7 (140.147.249.7), Dst Add: 10.11.11.51 (10.11.11.51)
   Version: 4
   Header length: 20 bytes
 ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
   Total Length: 44
   Identification: 0x0000 (0)
 ⊟ Flags: 0x04
     .1.. = Don't fragment: Set
     ..0. = More fragments: Not Set
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP 0x06
   Header checksum: 0x9ff3 (correct)
   Source: 140.147.249.7 (140.147.249.7)
   Destination: 10.11.11.51 (10.11.11.51)
```

Figure 2-4 An IP packet

Net+ 1.1 4.1

However, if a Transport layer protocol performs segmentation, fragmentation may not be necessary. For greater network efficiency, segmentation is preferred. Not all Transport layer protocols are designed to accomplish segmentation. If a Transport layer protocol cannot perform segmentation, Network layer protocols will perform fragmentation, if needed.

Net+ 4.1

Data Link Layer

The primary function of protocols in the second layer of the OSI model, the **Data Link layer**, is to divide data they receive from the Network layer into distinct frames that can then be transmitted by the Physical layer. A **frame** is a structured package for moving data that includes not only the raw data, or "payload," but also the sender's and receiver's network addresses, and error checking and control information. The addresses tell the network where to deliver the frame, whereas the error checking and control information ensure that the frame arrives without any problems.

To understand the function of the Data Link layer fully, pretend for a moment that computers communicate as humans do. Suppose you are in Ms. Jones's large classroom, which is full of noisy students, and you need to ask the teacher a question. To get your message through, you might say, "Ms. Jones? Can you explain more about the effects of railroads on commerce in the mid-nineteenth century?" In this example, you are the sender (in a busy network) and you have addressed your recipient, Ms. Jones, just as the Data Link layer addresses another computer on the network. In addition, you have formatted your thought as a question, just as the Data Link layer formats data into frames that can be interpreted by receiving computers.

What happens if the room is so noisy that Ms. Jones hears only part of your question? For example, she might receive "on commerce in the late-nineteenth century?" This kind of error can happen in network communications as well (because of wiring problems, for example). The Data Link layer protocols find out that information has been dropped and ask the first computer to retransmit its message—just as in a classroom setting Ms. Jones might say, "I didn't hear you. Can you repeat the question?" The Data Link layer accomplishes this task through a process called error checking.

Error checking is accomplished by a 4-byte **FCS** (**frame check sequence**) field, whose purpose is to ensure that the data at the destination exactly matches the data issued from the source. When the source node transmits the data, it performs an algorithm (or mathematical routine) called a **CRC** (**cyclic redundancy check**). CRC takes the values of all of the preceding fields in the frame and generates a unique 4-byte number, the FCS. When the destination node receives the frame, its Data Link layer services unscramble the FCS via the same CRC algorithm and ensure that the frame's fields match their original form. If this comparison fails, the receiving node assumes that the frame has been damaged in transit and requests that the source node retransmit the data. Note that the receiving node, and not the sending node, is responsible for detecting errors.

In addition, the sender's Data Link layer waits for acknowledgment from the receiver's Transport layer that data was received correctly. If the sender does not get this acknowledgment within a prescribed period of time, its Data Link layer gives instruction to retransmit the information. The Data Link layer never tries to figure out what went wrong. Similarly, as in a busy classroom, Ms. Jones will probably say, "Pardon me?" rather than, "It sounds as if you might have a question about railroads, and I heard only the last part of it, which dealt with commerce, so I assume you are asking about commerce and railroads; is that correct?" Obviously, the former method is more efficient.

Net+ 4.1

Another communications mishap that might occur in a noisy classroom or on a busy network is a glut of communication requests. For example, at the end of class, 20 people might ask Ms. Jones 20 different questions at once. Of course, she can't pay attention to all of them simultaneously. She will probably say, "One person at a time, please," then point to one student who asked a question. This situation is analogous to what the Data Link layer does for the Physical layer. One node on a network (a Web server, for example) may receive multiple requests that include many frames of data each. The Data Link layer controls the flow of this information, allowing the NIC to process data without error.

In fact, the IEEE has divided the Data Link layer into two sublayers, as shown in Figure 2-5. The reason for this change was to allow higher layer protocols (for example, those operating in the Network layer) to interact with Data Link layer protocols without regard for Physical layer specifications.

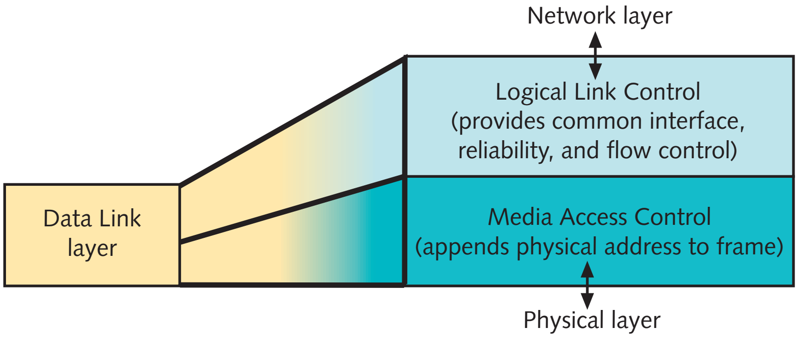

Network layer
Logical Link Control
(provides common interface,
reliability, and flow control)
Data Link
layer
Media Access Control
(appends physical address to frame)
Physical layer

Figure 2-5 The Data Link layer and its sublayers

Net+ 1.3 4.1

The upper sublayer of the Data Link layer, called the **LLC (Logical Link Control)** sublayer, provides an interface to the Network layer protocols, manages flow control, and issues requests for transmission for data that has suffered errors. The **MAC (Media Access Control)** sublayer, the lower sublayer of the Data Link layer, manages access to the physical medium. It appends the **physical address** of the destination computer onto the data frame. The physical address is a fixed number associated with a device's NIC; it is initially assigned at the factory and stored in the NIC's on-board memory. Because this address is appended by the MAC sublayer of the Data Link layer, it is also known as a **MAC address** or a **Data Link layer address**. Sometimes, it's also called a **hardware address**.

You can find a NIC's MAC address through your computer's protocol configuration utility or by simply looking at the NIC. The MAC address will be stamped directly onto the NIC's circuit board or on a sticker attached to some part of the NIC, as shown in Figure 2-6. In Hands-on Project 2-3 at the end of this chapter, you will have a chance to discover your computer's NIC using both these methods.

MAC addresses contain two parts: a block ID and a device ID. The **block ID** is a six-character sequence unique to each vendor. IEEE manages which block IDs each manufacturer can use. For example, a series of Ethernet NICs manufactured by the 3Com Corporation begins with the six-character sequence "00608C," while a series of Ethernet NICs manufactured by Intel begins with "00AA00." Some manufacturers have several different block IDs. The remaining six characters in the MAC address are added at the factory, based on the NIC's model and manufacture date, and collectively form the **device ID**. An example of a device ID assigned by

Net+
1.3
4.1

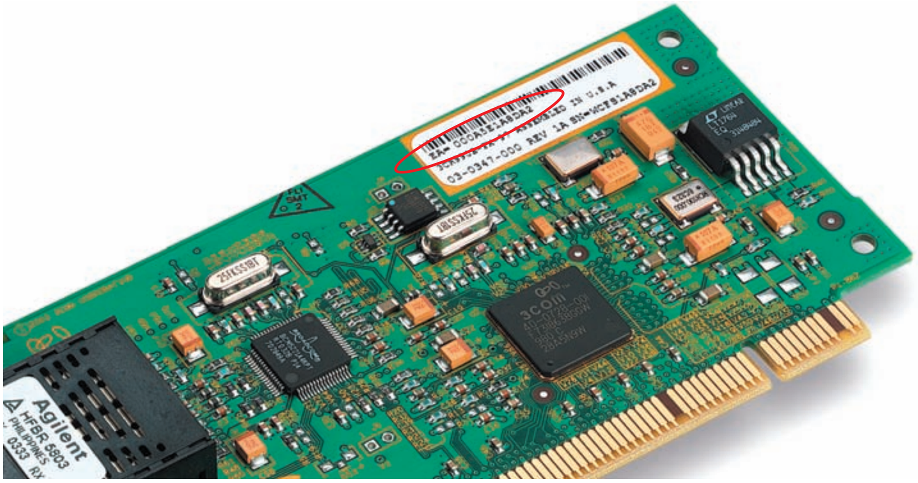


Figure 2-6 A NIC's MAC address

a manufacturer might be 005499. The combination of the block ID and device ID result in a unique, 12-character MAC address of 00608C005499. MAC addresses are also frequently depicted in their hexadecimal format—for example, 00:60:8C:00:54:99.

TIP

Hexadecimal, or base 16, is a numeral system that uses 0 through 9 to represent its first 10 numbers, then uses the letters A through F to represent the next six numbers. (The system we use for everyday counting is base 10, or decimal, notation.) In hexadecimal notation, the decimal number 12 is represented by the letter C, for example. Starting with the decimal number 16, hexadecimal notation uses a 1 to represent the previous 15 digits and begins counting again at 0. In other words, a decimal number 16 is represented as 10 in hexadecimal and a decimal number 32 is represented as 20 in hexadecimal. In computer science, hexadecimal notation (sometimes called, simply, "hex") is used as a shorter, readable version of the binary numbers that computers interpret. You won't often be asked to convert hexadecimal notation to decimal or binary notation, but you should understand them. Chapter 4 describes binary notation in detail.

If you know a computer's MAC address, you can determine which company manufactured its NIC by looking up its block ID. IEEE maintains a database of block IDs and their manufacturers, which is accessible via the Web. At the time of this writing, the database search page could be found at *http://standards.ieee.org/regauth/oui/index.shtml*.

Because of their hardware addressing function, NICs can be said to perform in the Data Link layer of the OSI model. However, they also perform services in the Physical layer, which is described next.

Net+
4.1

Physical Layer

The **Physical layer** is the lowest, or first, layer of the OSI model. Protocols at the Physical layer accept frames from the Data Link layer and generate signals as changes in voltage at the NIC. (Signals are made of electrical impulses that, when issued in a certain pattern, represent information.) When the network uses copper as its transmission medium, these

Net+ 4.1

signals are also issued over the wire as voltage. In the case of fiber-optic cable, signals are issued as light pulses. When a network uses wireless transmission, the signals are sent from antennas as electromagnetic waves.

When receiving data, Physical layer protocols detect and accept signals, which they pass on to the Data Link layer. Physical layer protocols also set the data transmission rate and monitor data error rates. However, even if they recognize an error, they cannot perform error correction. When you install a NIC in your desktop PC and connect it to a cable, you are establishing the foundation that allows the computer to be networked. In other words, you are providing a Physical layer.

Simple connectivity devices such as hubs and repeaters operate at the Physical layer. NICs operate at both the Physical layer and at the Data Link layer. As you would expect, physical network problems, such as a severed wire or a broken connectivity device, affect the Physical layer. Similarly, if you insert a NIC but fail to seat it deeply enough in the computer's main circuit board, your computer will experience network problems at the Physical layer.

Most of the functions that network administrators are most concerned with happen in the first four layers of the OSI model: Physical, Data Link, Network, and Transport. Therefore, the bulk of material in this book and on the Network+ exam relates to these four layers. Software programmers, on the other hand, are more apt to be concerned with what happens at the Application, Presentation, and Session layers.

Applying the OSI Model

Net+ 4.1

Now that you have been introduced to the seven layers of the OSI model, you can take a closer look at exactly how the layers interact. For reference, Table 2-1 summarizes the functions of the seven OSI model layers.

Table 2-1 Functions of the OSI layers

OSI model layer	Function
Application (layer 7)	Provides interface between software applications and network for interpreting applications' requests and requirements
Presentation (layer 6)	Allows hosts and applications to use a common language; performs data formatting, encryption, and compression
Session (layer 5)	Establishes, maintains, and terminates user connections
Transport (layer 4)	Ensures accurate delivery of data through flow control, segmentation and reassembly, error correction, and acknowledgment
Network (layer 3)	Establishes network connections; translates network addresses into their physical counterparts and determines routing
Data Link (layer 2)	Packages data in frames appropriate to network transmission method
Physical (layer 1)	Manages signaling to and from physical network connections

Communication Between Two Systems

Net+ 4.1

Based on what you have learned about the OSI model, it should be clear to you that data issued from a software application is not in the same form as the data that your NIC sends to the network. At each layer of the OSI model, some information—for example, a format specification or a network address—is added to the original data. After it has followed the path from the Application layer to the Physical layer, data is significantly transformed, as shown in Figure 2-7. The following paragraphs describe this process in detail.

To understand how data changes, it is useful to trace the steps in a typical client/server exchange, such as retrieving a mail message from a mail server. Suppose that you connect to your company's network from your home computer via a broadband Internet connection, log on, start your e-mail application, and then click a button in the e-mail application to retrieve your mail from the server. At that point, Application layer services on your computer accept data from your mail application and formulate a request meant for the mail server software. They add an application header to the data that the program wants to send. The application header contains information about the e-mail application's requirements, so that the mail server can fulfill its request properly. The Application layer transfers the request to the Presentation layer, in the form of a protocol data unit (PDU).

The Presentation layer first determines whether and how it should format or encrypt the data request received from the Application layer. For example, if your mail client requires

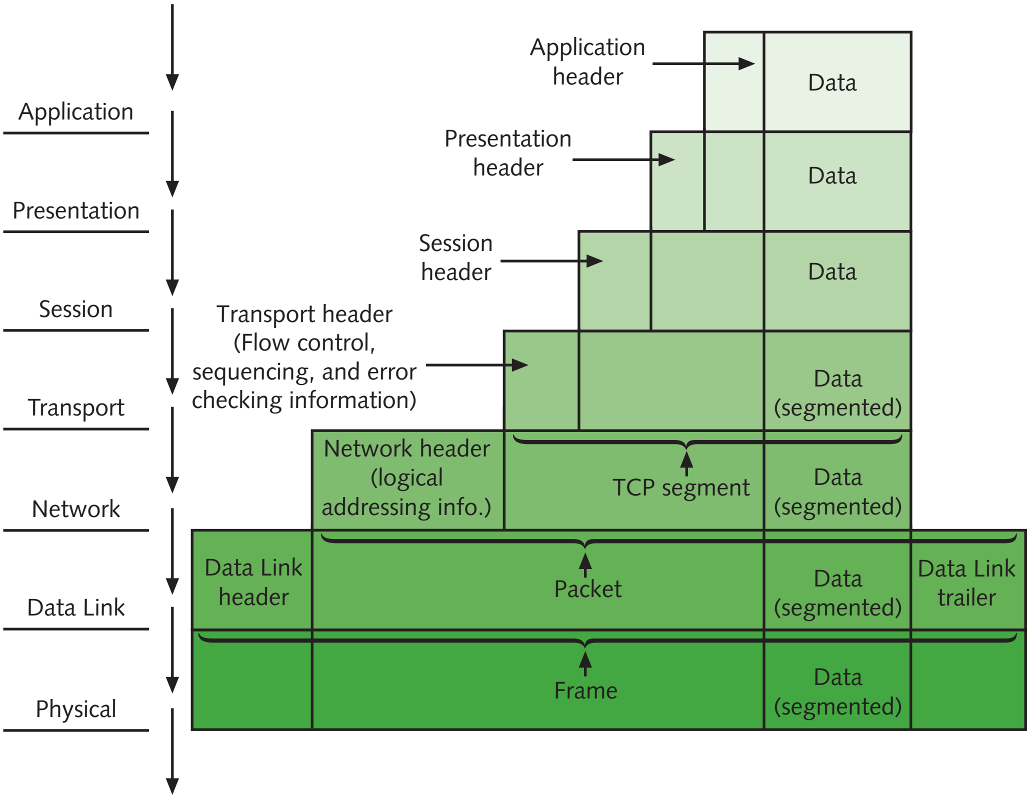


Figure 2-7 Data transformation through the OSI model

Net+ 4.1

encryption, the Presentation layer protocols will add that information to the PDU in a presentation header. If your e-mail message contains graphics or formatted text, that information will also be added.

Then, the Presentation layer sends its PDU to the Session layer, which adds a session header that contains information about how your home computer communicates with the network. For example, the session header might indicate that your Internet connection can only transmit and receive data at 512 Kbps. The Session layer then passes the PDU to the Transport layer.

At the Transport layer, the PDU—your request for mail and the headers added by previous layers—is broken down into smaller pieces of data, or segments. The segments' maximum size is dictated by the type of network transmission method in use (for example, Ethernet). Suppose your mail request PDU is too large to be a single segment. In that case, Transport layer protocols subdivide it into two or more smaller segments and assign sequence identifiers to all of the smaller segments. This information becomes part of the transport header. Protocols also add checksum, flow control, and acknowledgment data to the transport header. The Transport layer then passes these segments, one at a time, to the Network layer.

Next, Network layer protocols add logical addressing information to the segments, so that your request will be properly routed to the mail server and the mail server will respond to your computer. This information is contained in the network header. With the addition of network address information, the pieces of data are called packets. The Network layer then passes the packets to the Data Link layer.

At the Data Link layer, protocols add a header to the front of each packet and a trailer to the end of each packet to make frames. (The trailer indicates where a frame ends.) In other words, the Data Link layer protocols **encapsulate** the Network layer packets. Encapsulation is frequently compared to placing an envelope within a larger envelope. This analogy conveys the idea that the Data Link layer does not attempt to interpret any information added in the Network layer, but simply surrounds it.

Using frames reduces the possibility of lost data or errors on the network, because built into each frame is a way of checking for errors. After verifying that the data has not been damaged, the Data Link layer then passes the frames to the Physical layer.

Finally, your request for mail, in the form of many frames, hits the NIC at the Physical layer. The Physical layer does not interpret the frames or add information to the frames; it simply transmits them over the broadband connection to your LAN, across your office network, and to the mail server after the binary digits (bits), or ones and zeroes, have been converted to electrical pulses. As the frames arrive at the mail server, the server's Physical layer accepts the frames and transfers them to the Data Link layer. The mail server begins to unravel your request, reversing the process just described, until it responds to your request with its own transmission, beginning from its Application layer.

NOTE

The terms *frame*, *packet*, *datagram*, and *PDU* are often used interchangeably to refer to a small piece of data formatted for network transmission. Technically, however, a *packet* is a piece of information that contains network addressing information, and a *frame* is a piece of data enclosed by a Data Link layer header and trailer. *Datagram* is synonymous with packet. *PDU* generically refers to a unit of data at any layer of the OSI model. However, networking professionals often use the term *packet* to refer to *frames*, *PDU*s, and Transport layer segments alike.

Frame Specifications

You have learned that frames are composed of several smaller components, or fields. The characteristics of these components depend on the type of network on which the frames run and on the standards that they must follow. By far, the most popular type of networking technology in use today is Ethernet, which uses Ethernet frames. You'll learn much more about Ethernet in Chapter 5, but the following serves as an introduction, as well as a comparison between this favored network type and its historical rival, token ring.

Ethernet is a networking technology originally developed at Xerox in the early 1970s and improved by Digital Equipment Corporation, Intel, and Xerox. There are four different types of Ethernet frames. The most popular form of Ethernet is characterized by the unique way in which devices share a common transmission channel, described in the IEEE **802.3** standard.

A much less common networking technology, **token ring**, was developed by IBM in the 1980s. It relies upon direct links between nodes and a ring topology. Nodes pass around **tokens**, special control frames that indicate to the network when a particular node is about to transmit data. Although this networking technology is nearly obsolete, there is a remote chance that you might work on a token ring network. The IEEE has defined token ring technology in its **802.5** standard.

Ethernet frames are different from token ring frames, and the two will not interact with each other on a network. In fact, most LANs do not support more than one frame type, because devices cannot support more than one frame type per physical interface, or NIC. (NICs can, however, support multiple protocols.) Although you can conceivably transmit both token ring and Ethernet frames on a network, Ethernet interfaces cannot interpret token ring frames, and vice versa. Normally, LANs use *either* Ethernet or token ring, and almost all contemporary LANs use Ethernet.

It is important to know what frame type (or types) your network environment requires. You will use this information when installing network operating systems, configuring servers and client workstations, installing NICs, troubleshooting network problems, and purchasing network equipment.

IEEE Networking Specifications

In addition to frame types and addressing, IEEE networking specifications apply to connectivity, networking media, error-checking algorithms, encryption, emerging technologies, and more. All of these specifications fall under the IEEE's Project 802, an effort to standardize physical and logical elements of a network. IEEE developed these standards before the OSI model was standardized by ISO, but IEEE's 802 standards can be applied to the layers of the OSI model. Table 2-2 describes just some of the IEEE 802 specifications. The Network+ certification exam includes questions about IEEE 802 specifications, with an emphasis on the technologies described by 802.3 and 802.11.

Table 2-2 **IEEE 802 standards**

Standard	Name	Topic
802.1	Internetworking	Routing, bridging, and network-to-network communications
802.2	Logical Link Control	Error and flow control over data frames
802.3	Ethernet LAN	All forms of Ethernet media and interfaces
802.5	Token ring LAN	All forms of token ring media and interfaces
802.11	Wireless Networks	Standards for wireless networking for many different broadcast frequencies and usage techniques
802.15	Wireless personal area networks	The coexistence of wireless personal area networks with other wireless devices in unlicensed frequency bands
802.16	Broadband wireless metropolitan area networks	The atmospheric interface and related functions associated with broadband wireless connectivity; also known as WiMAX
802.17	Resilient packet rings	Access method, physical layer specifications, and management of shared packet-based transmission on resilient rings (such as SONET)
802.20	Mobile broadband wireless network	Packet handling and other specifications for multivendor, mobile high-speed wireless transmission, nicknamed "mobile WiMAX"
802.22	Wireless regional area networks (WRAN)	Wireless, broadcast-style network to operate in the UHF/VHF frequency bands formerly used for TV channels

Chapter Summary

- Standards are documented agreements containing precise criteria that are used as guidelines to ensure that materials, products, processes, and services suit their purpose. Standards also help to ensure interoperability between software and hardware from different manufacturers.
- Some of the significant standards organizations are ANSI, EIA/TIA, IEEE, ISO, ITU, ISOC, IANA, and ICANN.
- ISO's OSI (Open Systems Interconnection) model represents communication between two computers on a network. It divides networking architecture into seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Each layer has its own set of functions and interacts with the layers directly above and below it.
- Protocols in the Application layer, the seventh layer of the OSI model, enable software programs to negotiate their formatting, procedural, security, synchronization, and other requirements with the network.
- Protocols in the Presentation layer, the sixth OSI model layer, serve as translators between the application and the network, using a common language for different hosts and applications to exchange data.
- Protocols in the Session layer, the fifth OSI model layer, coordinate and maintain links between two devices for the duration of their communication. They also synchronize dialogue, determine whether communications have been cut off, and, if so, figure out where to restart transmission.

- The primary function of protocols in the Transport layer, the fourth OSI model layer, is to oversee end-to-end data delivery. In the case of connection-oriented protocols, this means data is delivered reliably. They verify that data is received in the same sequence in which it was sent. They are also responsible for flow control, segmentation, and reassembly of packets. Connectionless Transport layer protocols do not offer such guarantees.
- Protocols in the Network layer, the third OSI model layer, manage logical addressing and determine routes based on addressing, patterns of usage, and availability. Routers belong to the Network layer because they use this information to intelligently direct data from sender to receiver.
- Network layer addresses, also called logical or virtual addresses, are assigned to devices through operating system software. They are composed of hierarchical information, so they can be easily interpreted by routers and used to direct data to its destination.
- The primary function of protocols at the Data Link layer, the second layer of the OSI model, is to organize data they receive from the Network layer into frames that contain error-checking routines and can then be transmitted by the Physical layer.
- The Data Link layer is subdivided into the Logical Link Control and MAC sublayers. The LLC sublayer ensures a common interface for the Network layer protocols. The MAC sublayer is responsible for adding physical address data to frames. MAC addresses are hard coded into a device's NIC.
- Protocols at the Physical layer generate and detect signals so as to transmit and receive data over a network medium. These protocols also set the data transmission rate and monitor data error rates, but do not provide error correction.
- A data request from a software program is received by the Application layer protocols and is transferred down through the layers of the OSI model until it reaches the Physical layer (the network cable, for example). At that point, data is sent to its destination over the network medium, and the Physical layer protocols at the destination send it back up through the layers of the OSI model until it reaches the Application layer.
- Data frames are small blocks of data with control, addressing, and handling information attached to them. Frames are composed of several fields. The characteristics of these fields depend on the type of network on which the frames run and the standards that they must follow. Ethernet and token ring networks use different frame types, and one type of network cannot interpret the others' frames.
- In addition to frame types and addressing schemes, the IEEE networking specifications apply to connectivity, networking media, error-checking algorithms, encryption, emerging technologies, and more. All of these specifications fall under the IEEE's Project 802, an effort to standardize the elements of networking.
- Significant IEEE 802 standards are 802.3, which describes Ethernet; 802.11, which describes wireless networking, and 802.16, which describes broadband wireless metropolitan area networks.

Key Terms

802.2 The IEEE standard for error and flow control in data frames.

802.3 The IEEE standard for Ethernet networking devices and data handling (using the CSMA/CD access method).

802.5 The IEEE standard for token ring networking devices and data handling.

802.11 The IEEE standard for wireless networking.

802.16 The IEEE standard for broadband wireless metropolitan area networking (also known as WiMAX).

ACK (acknowledgment) A response generated at the Transport layer of the OSI model that confirms to a sender that its frame was received. The ACK packet is the third of three in the three-step process of establishing a connection.

acknowledgment *See* ACK.

American National Standards Institute *See* ANSI.

ANSI (American National Standards Institute) An organization composed of more than 1000 representatives from industry and government who together determine standards for the electronics industry in addition to other fields, such as chemical and nuclear engineering, health and safety, and construction.

API (application program interface) A set of routines that make up part of a software application.

Application layer The seventh layer of the OSI model. Application layer protocols enable software programs to negotiate formatting, procedural, security, synchronization, and other requirements with the network.

application program interface *See* API.

block ID The first set of six characters that make up the MAC address and that are unique to a particular manufacturer.

checksum A method of error checking that determines if the contents of an arriving data unit match the contents of the data unit sent by the source.

connection oriented A type of Transport layer protocol that requires the establishment of a connection between communicating nodes before it will transmit data.

connectionless A type of Transport layer protocol that services a request without requiring a verified session and without guaranteeing delivery of data.

CRC (cyclic redundancy check) An algorithm (or mathematical routine) used to verify the accuracy of data contained in a data frame.

cyclic redundancy check *See* CRC.

Data Link layer The second layer in the OSI model. The Data Link layer bridges the networking media with the Network layer. Its primary function is to divide the data it receives from the Network layer into frames that can then be transmitted by the Physical layer.

Data Link layer address *See* MAC address.

device ID The second set of six characters that make up a network device's MAC address. The device ID, which is added at the factory, is based on the device's model and manufacture date.

EIA (Electronic Industries Alliance) A trade organization composed of representatives from electronics manufacturing firms across the United States that sets standards for electronic equipment and lobbies for legislation favorable to the growth of the computer and electronics industries.

Electronic Industries Alliance *See* EIA.

encapsulate The process of wrapping one layer's PDU with protocol information so that it can be interpreted by a lower layer. For example, Data Link layer protocols encapsulate Network layer packets in frames.

Ethernet A networking technology originally developed at Xerox in the 1970s and improved by Digital Equipment Corporation, Intel, and Xerox. Ethernet, which is the most common form of network transmission technology, follows the IEEE 802.3 standard.

FCS (frame check sequence) The field in a frame responsible for ensuring that data carried by the frame arrives intact. It uses an algorithm, such as CRC, to accomplish this verification.

flow control A method of gauging the appropriate rate of data transmission based on how fast the recipient can accept data.

fragmentation A Network layer service that subdivides segments it receives from the Transport layer into smaller packets.

frame A package for data that includes not only the raw data, or "payload," but also the sender's and recipient's addressing and control information. Frames are generated at the Data Link layer of the OSI model and are issued to the network at the Physical layer.

frame check sequence *See* FCS.

hardware address *See* MAC address.

HTTP (Hypertext Transfer Protocol) An Application layer protocol that formulates and interprets requests between Web clients and servers.

Hypertext Transfer Protocol *See* HTTP.

IAB (Internet Architecture Board) A technical advisory group of researchers and technical professionals responsible for Internet growth and management strategy, resolution of technical disputes, and standards oversight.

IANA (Internet Assigned Numbers Authority) A nonprofit, United States government-funded group that was established at the University of Southern California and charged with managing IP address allocation and the domain name system. The oversight for many of IANA's functions was given to ICANN in 1998; however, IANA continues to perform Internet addressing and domain name system administration.

ICANN (Internet Corporation for Assigned Names and Numbers) The nonprofit corporation currently designated by the United States government to maintain and assign IP addresses.

IEEE (Institute of Electrical and Electronics Engineers) An international society composed of engineering professionals. Its goals are to promote development and education in the electrical engineering and computer science fields.

IETF (Internet Engineering Task Force) An organization that sets standards for how systems communicate over the Internet (for example, how protocols operate and interact).

Institute of Electrical and Electronics Engineers *See* IEEE.

International Organization for Standardization *See* ISO.

International Telecommunication Union *See* ITU.

Internet Architecture Board *See* IAB.

Internet Assigned Numbers Authority *See* IANA.

Internet Corporation for Assigned Names and Numbers *See* ICANN.

Internet Engineering Task Force *See* IETF.

Internet Protocol *See* IP.

Internet Protocol address *See* IP address.

Internet service provider *See* ISP.

Internet Society *See* ISOC.

IP (Internet Protocol) A core protocol in the TCP/IP suite that operates in the Network layer of the OSI model and provides information about how and where data should be delivered. IP is the subprotocol that enables TCP/IP to internetwork.

IP address (Internet Protocol address) The Network layer address assigned to nodes to uniquely identify them on a TCP/IP network. IP addresses consist of 32 bits divided into four octets, or bytes.

ISO (International Organization for Standardization) A collection of standards organizations representing 157 countries with headquarters located in Geneva, Switzerland. Its goal is to establish international technological standards to facilitate the global exchange of information and barrier-free trade.

ISOC (Internet Society) A professional organization with members from 90 chapters around the world that helps to establish technical standards for the Internet.

ISP (Internet service provider) A business that provides organizations and individuals with Internet access and often, other services, such as e-mail and Web hosting.

ITU (International Telecommunication Union) A United Nations agency that regulates international telecommunications and provides developing countries with technical expertise and equipment to advance their technological bases.

LLC (Logical Link Control) sublayer The upper sublayer in the Data Link layer. The LLC provides a common interface and supplies reliability and flow control services.

logical address *See* network address.

Logical Link Control sublayer *See* LLC (Logical Link Control) sublayer.

MAC address A 12-character string that uniquely identifies a network node. The manufacturer hard codes the MAC address into the NIC. This address is composed of the block ID and device ID.

MAC (Media Access Control) sublayer The lower sublayer of the Data Link layer. The MAC appends the physical address of the destination computer onto the frame.

maximum transmission unit *See* MTU.

Media Access Control sublayer *See* MAC (Media Access Control) sublayer.

MTU (maximum transmission unit) The largest data unit a network (for example, Ethernet or token ring) will accept for transmission.

network address A unique identifying number for a network node that follows a hierarchical addressing scheme and can be assigned through operating system software. Network addresses are added to data packets and interpreted by protocols at the Network layer of the OSI model.

Network layer The third layer in the OSI model. Protocols in the Network layer translate network addresses into their physical counterparts and decide how to route data from the sender to the receiver.

Network layer address *See* network address.

Open Systems Interconnection model *See* OSI (Open Systems Interconnection) Model.

OSI (Open Systems Interconnection) model A model for understanding and developing computer-to-computer communication developed in the 1980s by ISO. It divides networking functions among seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

PDU (protocol data unit) A unit of data at any layer of the OSI model.

physical address *See* MAC address.

Physical layer The lowest, or first, layer of the OSI model. Protocols in the Physical layer generate and detect signals so as to transmit and receive data over a network medium. These protocols also set the data transmission rate and monitor data error rates, but do not provide error correction.

Presentation layer The sixth layer of the OSI model. Protocols in the Presentation layer translate between the application and the network. Here, data are formatted in a schema that the network can understand, with the format varying according to the type of network used. The Presentation layer also manages data encryption and decryption, such as the scrambling of system passwords.

protocol data unit *See* PDU.

reassembly The process of reconstructing data units that have been segmented.

Regional Internet Registry *See* RIR.

RIR (Regional Internet Registry) A not-for-profit agency that manages the distribution of IP addresses to private and public entities. ARIN is the RIR for North, Central, and South America and sub-Saharan Africa. APNIC is the RIR for Asia and the Pacific region. RIPE is the RIR for Europe and North Africa.

route To intelligently direct data between networks based on addressing, patterns of usage, and availability of network segments.

router A device that connects network segments and directs data based on information contained in the data packet.

segment A unit of data that results from subdividing a larger protocol data unit.

segmentation The process of decreasing the size of data units when moving data from a network that can handle larger data units to a network that can handle only smaller data units.

sequencing The process of assigning a placeholder to each piece of a data block to allow the receiving node's Transport layer to reassemble the data in the correct order.

session A connection for data exchange between two parties. The term *session* may be used in the context of Web, remote access, or terminal and mainframe communications, for example.

Session layer The fifth layer in the OSI model. The Session layer establishes and maintains communication between two nodes on the network. It can be considered the "traffic cop" for network communications.

standard A documented agreement containing technical specifications or other precise criteria that are used as guidelines to ensure that materials, products, processes, and services suit their intended purpose.

SYN (synchronization) The packet one node sends to request a connection with another node on the network. The SYN packet is the first of three in the three-step process of establishing a connection.

SYN-ACK (synchronization-acknowledgment) The packet a node sends to acknowledge to another node that it has received a SYN request for connection. The SYN-ACK packet is the second of three in the three-step process of establishing a connection.

synchronization *See* SYN.

synchronization-acknowledgment *See* SYN-ACK.

Telecommunications Industry Association *See* TIA.

terminal A device with little (if any) of its own processing or disk capacity that depends on a host to supply it with applications and data-processing services.

TIA (Telecommunications Industry Association) A subgroup of the EIA that focuses on standards for information technology, wireless, satellite, fiber optics, and telephone equipment. Probably the best known standards to come from the TIA/EIA alliance are its guidelines for how network cable should be installed in commercial buildings, known as the "TIA/EIA 568-B Series."

token A special control frame that indicates to the rest of the network that a particular node has the right to transmit data.

token ring A networking technology developed by IBM in the 1980s. It relies upon direct links between nodes and a ring topology, using tokens to allow nodes to transmit data.

Transport layer The fourth layer of the OSI model. In the Transport layer protocols ensure that data are transferred from point A to point B reliably and without errors. Transport layer services include flow control, acknowledgment, error correction, segmentation, reassembly, and sequencing.

virtual address *See* network address.

Review Questions

1. Which of the following standards organizations has established guidelines for installing network cables in commercial buildings?
   a. TIA/EIA
   b. ITU
   c. ANSI
   d. IEEE

2. Which technology does the IEEE 802.3 specification describe?
   a. Network security
   b. Ethernet LANs
   c. Logical Link Control
   d. Token ring LANs

3. Which of the following IEEE specifications pertains to wireless networking?
   a. 802.1
   b. 802.3
   c. 802.7
   d. 802.11

4. Which layer of the OSI model is responsible for issuing acknowledgments (ACKs)?
   a. Application layer
   b. Data Link layer
   c. Network layer
   d. Transport layer

5. Which OSI model layer is responsible for keeping open a communications path between your computer and the server when you dial in to a remote access server?
   a. Physical layer
   b. Data Link layer
   c. Presentation layer
   d. Session layer

6. Suppose your network is connected to another network via a router. Which OSI model layer provides the information necessary to direct data between the two networks?
   a. Network layer
   b. Physical layer
   c. Data Link layer
   d. Session layer

7. In which two layers of the OSI model do NICs belong?
   a. Presentation and Application layers
   b. Transport and Network layers
   c. Network and Data Link layers
   d. Physical and Data Link layers

8. Which standards organization developed the OSI model?
   a. ISO
   b. ITU
   c. ISOC
   d. OSI

9. Under what circumstances would the Transport layer use segmentation?
   a. When too many data frames are flooding into a receiving node's NIC
   b. When more than 10 percent of transmitted frames are damaged
   c. When the destination node cannot accept the size of the data blocks transmitted by the source node
   d. When the source node requests that data blocks be segmented for faster processing

10. Which OSI model layer generates and detects voltage so as to transmit and receive signals carrying data?

    a. Physical layer

    b. Data Link layer

    c. Network layer

    d. Transport layer

11. What type of address follows a hierarchical format?

    a. Physical addresses

    b. MAC addresses

    c. Network addresses

    d. Data Link layer addresses

12. If the TCP protocol did not receive an acknowledgment for data it transmitted, what would it do?

    a. Issue its own acknowledgment, indicating to the recipient that it did not receive the acknowledgment it expected

    b. Issue a warning frame to tell the recipient it would retransmit the data if it did not receive the acknowledgment within a certain time frame

    c. Retransmit the data to the recipient

    d. Reestablish the connection with the recipient

13. You have just installed a new NIC in your computer and see the following stamped on it: 000A5E1A8DA2. This unique identifier is an example of what kind of address?

    a. Virtual address

    b. MAC address

    c. Network address

    d. IP address

14. Which part of a MAC address is unique to each manufacturer?

    a. The destination ID

    b. The block ID

    c. The physical node ID

    d. The segment ID

15. What is the purpose of the trailer field added to a frame in the Data Link layer?

    a. To mark the end of a frame

    b. To indicate the rate at which a node can receive the data

    c. To encode the sum of the error-checking algorithm

    d. To represent the frame's sequence number

16. What are the sublayers of the Data Link layer as defined in the IEEE 802 standards?

    a. Logical Link Control sublayer and Media Access Control sublayer

    b. Transport Control sublayer and Media Access Control sublayer

    c. Logical Link Control sublayer and Physical Addressing sublayer

    d. Transport Control sublayer and Data Link Control sublayer

17. Which layer of the OSI model encapsulates Network layer packets?

    a. Physical layer

    b. Session layer

    c. Data Link layer

    d. Transport layer

18. Suppose that, at the receiving node, a frame's FCS doesn't match the FCS it was issued at the transmitting node. What happens as a result?

    a. The receiving node's Transport layer assesses the error and corrects it.

    b. The receiving node's Data Link layer requests a retransmission.

    c. The transmitting node's Transport layer immediately issues a replacement frame.

    d. The transmitting node's Data Link layer assesses the error and corrects it.

19. In which of the following situations would it be most desirable to use a connectionless Transport layer protocol?

    a. When retrieving a spreadsheet from a busy file server

    b. When connecting to a graphics-intensive Web site

    c. When viewing a movie clip on the Web

    d. When sending an e-mail message to a long list of recipients

20. Which of the following would be found in a Data Link layer header?

    a. The packet's fragmentation offset

    b. The packet's sequence number

    c. The source's logical address

    d. The source's physical address

Hands-On Projects

Project 2-1

To better understand the impact IEEE has on networking standards, it is helpful to read the actual standards and consider how they are used. This project will guide you through the process of searching for IEEE specifications on the Web. You will also take a look at the IEEE 802.3 standard for the most popular form of LAN technology, Ethernet. To complete this project, you need a computer with access to the Internet (through a high-speed connection), a Web browser, and version 6.0 or higher of the Adobe Acrobat reader (available free at Adobe's Web site, *www.adobe.com*). This exercise further assumes that your Web browser is configured to recognize and open Adobe Acrobat documents automatically when one is selected.

Steps in this project matched the Web sites mentioned at the time this book was published. If you notice discrepancies, look for similar links and follow the same general steps.

1. Access the Internet and navigate to **standards.ieee.org**. The IEEE Standards Association Home page appears.
2. On the navigation bar near the upper-right side of the screen, click the **PROJECT SEARCH** link. The Information Database – IEEE Standards Status Web page appears.
3. In the text box below the Search for: prompt, type **Ethernet**, then click the **Search!** button.
4. Scroll down the results page and note the number of abstracts your search returned. For those abstracts that give designation numbers (for example, 802.3av), note the numbers as well.
5. What was the revision date of the most recent standard beginning with 802.3? Why do you suppose this standard would be updated frequently?
6. If you were to click on the standards returned by this search, you would need to enter a logon ID and password to read that standard. However, IEEE's 802 (LAN/MAN) committee has made available archived versions of its popular standards at no cost. To access the free online standards, point your browser to the following Web page: **http://standards.ieee.org/getieee802/portfolio.html**. The Get IEEE 802 Portfolio of IEEE Standards Web page appears.
7. The list of IEEE 802 committee standards should look familiar to you. Click the link for 802.3 called **CSMA/CD Access Method** (this is the method of sharing a single channel that devices use on an Ethernet network, which you'll learn more about in Chapter 5). The IEEE-SA Get IEEE 802.3 LAN/MAN CSMA/CD Access Method Web page appears.
8. Notice that the 802.3 standard is downloadable in five parts. (Below those five documents are recent amendments to the standard, which can also be downloaded.) For this exercise, you'll take a look at one part of the standard. Under the For download prompt, click **IEEE 802.3-2005 – Section One** to open the first section of this standard. The Get IEEE 802 Download Web page appears.
9. Note that this document is protected by copyright laws, and that IEEE makes no warranties about its content. Scroll to the bottom of this page and click **Academic/Student** in the USER TYPE drop-down list box.
10. Click **ACCEPT/BEGIN DOWNLOAD** to open the document.
11. Because this is a rather long standard, it may take several minutes to retrieve the document. After it loads, scroll through the document's table of contents on the left side of the screen.
12. Suppose you want to know the maximum frame size for an Ethernet 802.3 frame. To find this information in the standard, click the small **Search** icon (it looks like a pair of binoculars) in the Adobe Acrobat Reader task bar. The Search dialog box appears.
13. In the "What word or phrase would you like to search for?" text box, type **minFrameSize**. Click **Search** to search for the first instance of this term, which is the parameter

that indicates the minimum length of an Ethernet frame. In fact, the 802.3 standard specifies several parameters for Ethernet frames, depending on the rate at which the network is expected to send and receive data. However, the minimum and maximum frame sizes for all types are the same. What is the minimum frame size for 802.3 Ethernet? (For reference, an octet equals 1 byte.) In the same table that lists this parameter (on page 81 of the 802.3 standard published in 2002), the maximum frame size is listed one line above, and is called "maxUntaggedFrameSize." Note both the minimum and maximum Ethernet frame sizes. This information will be used in the following project.

14. If you have time, read more selections from the 802.3 Ethernet standard. When you have finished, close your browser.

Net+ 4.1

Project 2-2

In this project, you will deepen your understanding of how data is divided into protocol data units and how those units are modified through every layer of the OSI model. In effect, you will be acting as a computer on a network, splitting up one large message into smaller pieces and adding control information so that the message can be reconstructed at its destination. (Though, of course, your reenactment is a simplified and much slower version of what a computer would do.) For this project you need only a pencil and paper. You may want to refer to Figures 2-1 and 2-7 and Table 2-1 for reference.

1. To begin, draw the OSI model on the left side of your paper, being certain to label each layer.

2. Above the top layer of the OSI model, write *Software*. Then, below the bottom layer, write *Network*.

3. Suppose the software issues a message to the network that is 3400 bytes in size. Next to the Application layer, Presentation layer, and Session layer, draw the PDU for this message as it appears at each of these layers (adding the appropriate header at each layer). Label the fields of the PDU, including the original message data. At the Session layer, how many fields does the PDU contain?

4. At the Transport layer, add a Transport layer header to the PDU. Recall that the Transport layer is responsible for breaking PDUs into the smaller units—or segments—that a network can handle. Suppose the network carrying this request uses Ethernet 802.3 technology, which, as you learned in Project 2-1, specifies that frames can be no smaller than 64 bytes and no greater than 1518 bytes in size. However, PDUs are not frames (until they reach the Data Link layer), and those limits include an added minimum of 18 bytes of control information. Thus, at the Transport layer, segments can be between 46 (or 64 minus 18) and 1500 (or 1518 minus 18) bytes in size. Given this information, what is the minimum number of segments the Transport layer will divide this message into?

5. Next to the Network layer, draw a segment after it has been broken down by the Transport layer, and add a field that represents this segment's sequence number and length.

6. To make the segment into a packet, next add the Network layer address fields required for the data to be routed over a network.

7. Next to the Data Link layer, add a header, frame check sequence field, and trailer to transform the packet into a frame. The frame is now ready for transmission, via the Physical layer, to the network.

Net+
1.3
5.1

Project 2-3

You will need to know how to find and interpret MAC addresses when supporting networks. In this project, you will discover two ways of finding your computer's MAC address, also known as its physical address, or sometimes, its hardware address. For this project you will need a desktop computer running the Windows XP, Windows Vista, or Linux operating system. The workstation's TCP/IP protocols should be property installed, configured, and connected to a server that is also running the TCP/IP protocols. (The project assumes the workstation has only one NIC.) You will also need a screwdriver that fits the workstation's cover screws, if the computer's cover is attached with screws.

If your workstation is running the Windows XP or Windows Vista operating system, perform the following steps:

1. Click the **Start** button, point to **All Programs**, select **Accessories**, and then select **Command Prompt**. The Command Prompt window opens with a cursor blinking at the C:\> prompt.
2. Type **`ipconfig /all`** then press **Enter**. A list of your Windows XP or Windows Vista configuration and Ethernet adapter parameters appears. This includes your workstation's TCP/IP properties, as well as its MAC address.
3. Search the output for the 12-digit hexadecimal MAC address currently assigned to your NIC. (*Hint*: Look for the Physical Address line.) On a separate piece of paper, write down the MAC address.
4. Type **exit** and then press **Enter** to close the Command Prompt window.

If your workstation is running a version of the Linux operating system, be certain that you have sufficient privileges (such as root access) to view addressing information. Then perform the following steps:

1. If you are not already at the command line—that is, if you're using a graphical interface, or desktop—start by opening a command shell. Methods of opening a command shell differ according to your graphical environment. If you are not sure how to get to the command line from your Linux desktop, look in your program menu for an option such as Shell, Terminal Prompt, or Command Prompt.
2. Type **`ifconfig`** and press **Enter**. Information about your network interface appears.
3. Your NIC's MAC address is shown at the end of the first line of the information returned in the previous step. It follows the HWaddr prompt. On a separate piece of paper, write down the MAC address.
4. Type **exit** and then press **Enter** to close the command shell.

Perform the following steps no matter which operating system your workstation uses:

1. Log off the network and shut down your workstation.
2. If a cable is connected to your NIC, remove the cable.
3. If necessary, use the screwdriver to remove the screws that secure the workstation's housing. Ask your instructor for help if you can't find the correct screws. Usually, there are three to five screws. In some cases, a computer housing may use no screws.
4. Remove the cover from the rest of the computer.

Net+ 1.3 5.1

5. With the computer open, remove the screw that holds the NIC in place. Gently remove the NIC from its place in the computer's motherboard.
6. In most cases, a NIC's MAC address is printed on a small white sticker attached to the NIC; alternatively, it may be stamped directly on the NIC itself. Find the MAC address and compare it to the one you discovered in the first part of this exercise.
7. Reinsert the NIC into its slot so that it is secure and replace the screw that holds it in.
8. Replace the computer's housing and the screws that fasten it to the rest of the computer.
9. Reattach the cable that you removed from the NIC previously.

Case Projects

Case Project 2-1

You are a networking professional who works in a college computer lab. The computers run only the TCP/IP protocol on an Ethernet network, and all computers use 3Com NICs. Many beginning computer science students use this lab for homework; you help them access the network and troubleshoot problems with their connections on a daily basis. One day, a student begins tampering with his computer; when he restarts the computer, it alerts him that it can't find the network. He calls you over to help. You ensure all the physical connections are sound. Then, you check the workstation's network properties and find that he has changed the frame type that his NIC uses to transmit data from Ethernet to token ring. Explain why this has prevented the workstation from connecting to the network.

Net+ 4.1

Case Project 2-2

The same student is curious about how a Web site appears on his computer screen. On a separate piece of paper, draw and explain the process that occurs between a client and a server when requesting a Web page, using the OSI model as a reference. For example, what Application layer protocol is required? How will the process differ if the student is sending or retrieving information to or from a secure Web site? Explain to the student how each OSI model layer contributes to data arriving in the correct place without errors.

Net+ 4.1

Case Project 2-3

The student appreciates the time you spent explaining what happens to the data as it moves through the OSI model layers, but he wonders why he should ever care about the OSI model or data frames. He says he wants to become a network architect and concern himself with routers, switches, and cabling. The student indicates that he doesn't care about the little details like packets. In response, describe how OSI model layers can affect a network's design and networking in general. For example, if the student wants to concentrate on designing a network that makes use of routers, what layer of the OSI model might he take the greatest interest in? How can the OSI model be a useful reference when troubleshooting network problems? For instance, if one node can send and receive data, yet the data is not encoded properly, at what layer of the OSI model might problems be occurring?