Course Title: Computer Networks

<table>
<tr><td rowspan="2">Semester</td><td rowspan="2">VII</td><td colspan="4" rowspan="2">Teaching Scheme</td><td colspan="5">Evaluation Scheme</td></tr>
<tr><td colspan="3">Theory</td><td colspan="2">Practical</td></tr>
<tr><td>Term</td><td>ODD</td><td>TH</td><td>TU</td><td>PR</td><td>Credits</td><td>TAE</td><td>CAE</td><td>ESE</td><td>INT</td><td>EXT</td></tr>
<tr><td>Course Category</td><td>EL</td><td rowspan="2">3 Hrs.</td><td rowspan="2">-- Hr.</td><td rowspan="2">2 Hrs.</td><td rowspan="2">4</td><td rowspan="2">10</td><td rowspan="2">15</td><td rowspan="2">50</td><td rowspan="2">25</td><td rowspan="2"></td></tr>
<tr><td>Course Code</td><td>UITL202
UITP202</td></tr>
<tr><td>Teaching Mode</td><td>Offline</td><td colspan="3" rowspan="2">5 Hrs.</td><td rowspan="2">TOTAL Marks→</td><td colspan="3">75</td><td colspan="2">25</td></tr>
<tr><td>Duration of ESE</td><td>2 Hrs.</td><td colspan="5">100</td></tr>
</table>

Course Objectives	**1. To develop an understanding of computer networking basics.**
	2. To develop an understanding of different components of computer networks, various protocols, modern technologies and their applications.
Course Outcomes	Upon successful completion of this course, student will be able to:
	CO-1: Recognize the technological trends of Computer Networking.
	CO-2: Discuss the key technological components of the Network.
	CO-3: Evaluate the challenges in building networks and solutions to those.
	CO-4: Solve and apply various Routing Algorithm & Protocols
	CO-5: Use Technique involved in developing transport & application layer of computer network

Unit	Contents	Hours
I	INTRODUCTION: Network applications, hardware and software networks, reference models: OSI, TCP/IP, Internet, Connection-oriented network - X.25, frame relay. PHYSICAL LAYER: Theoretical basis for communication, guided transmission media, wireless transmission, the public switched telephone networks and mobile telephone system.	8
II	THE DATA LINK LAYER: Design issues, detection and correction of error, elementary data link and sliding window protocols, example data link protocols - HDLC. THE MEDIUM ACCESS SUBLAYER: Channel allocations problem, multiple access protocols, Ethernet, Data Link Layer switching, Broadband Wireless, and Bluetooth.	8
III	THE NETWORK LAYER: Network layer design issues, routing, and congestion control algorithms, Quality of Service. Internet working, the network layer on the internet.	8
IV	THE TRANSPORT LAYER: Transport service, elements of transport protocol, Simple Transport Protocol, Internet transport layer protocols: UDP and TCP.	8
V	THE APPLICATION LAYER: Domain name system, electronic mail, World Wide Web: architectural overview, dynamic web document and http. APPLICATION LAYER PROTOCOLS: Simple Network Management Protocol and File Transfer Protocol, Telnet.	8

References

Text Books		**A. S. Tanenbaum (2003), Computer Networks, 4th edition, Pearson Education/ PHI, New Delhi, India.**
Reference Books	1.	Behrouz A. Forouzan (2006), Data communication and Networking, 4th Edition, Mc Graw-Hill, India.
	2.	Kurose, Ross (2010), Computer Networking: A top down approach, Pearson Education, India.

our goal:

- get "feel" and terminology
- more depth, detail *later*
- approach:
  - use Internet as example

overview:

- what's the Internet?
- what's a protocol?
- network edge; hosts, access net, physical media
- network core: packet/circuit switching, Internet structure
- performance: loss, delay, throughput
- security
- protocol layers, service models
- history

‘‘computer network’’ is a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used.

Networks come in many sizes, shapes and forms.

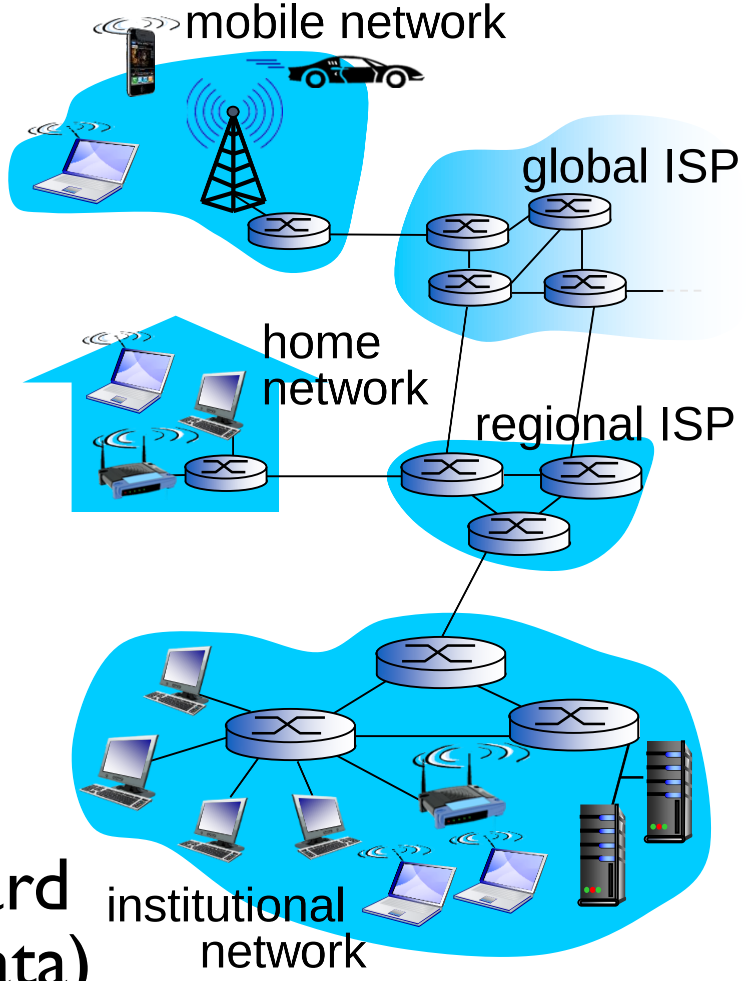
They are usually connected together to make larger networks, with the **Internet** being the most well-known example of a network of networks

What's the Internet: "nuts and bolts" view

- millions of connected computing devices:
  - *hosts = end systems*
  - running *network apps*

❖ *communication links*
  - fiber, copper, radio, satellite
  - transmission rate: *bandwidth*

❖ *Packet switches:* forward packets (chunks of data)
  - *routers* and *switches*



- The Internet connects a huge number of computing devices like:
- PCs
- Servers
- Wireless laptops
- Smartphones
- These are called hosts or end systems because they sit at the end of the network and interact with users.
- These devices run network applications (like web browsers, messaging apps, video streaming services, etc.)
- **Communication links:**
- These links physically connect devices and transfer data.
- Types of communication links:
- Fiber-optic cables
- Radio signals (like WiFi, mobile networks)
- Satellite connections
- Copper wires
- Data moves over these links at a certain transmission rate, also known as bandwidth, which indicates how much data can be sent per second.

•The internet sends data in small pieces called **packets**.
•**Packet switches** are network devices that direct these packets to their destination.
•Two types:
•**Routers**: Connect different networks (like your home network to your Internet Service Provider)
•**Switches**: Connect multiple devices within a single network (like inside your college or office)

Application of Computer Network

Business & Commerce:

A computer network can provide a powerful communication medium among employees. Virtually every company that has two or more computers now has **email (electronic mail)**

Telephone calls between employees may be carried by the computer network instead of by the phone company. This technology is called IP telephony or **Voice over IP (VoIP**) when Internet technology is used.

Healthcare: Electronic health records, Remote patient monitoring

Education: E-learning platforms, virtual classrooms

Entertainment: Social Media platform, Online gaming

Home Applications

Networks are commonly used at home for:

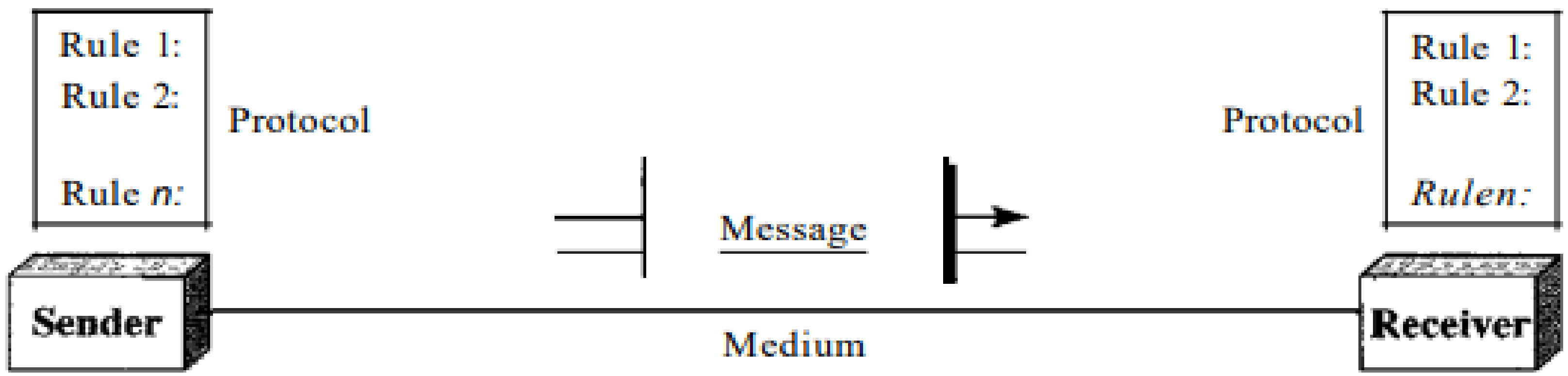
- Internet browsing
- Email and video calls
- Streaming services (Netflix, YouTube)
- Online gaming
- Home automation (smart lights, appliances, security systems)

Electronic Commerce (E-Commerce)

Use of networks in business transactions like:

- Online shopping (Amazon, Flipkart)
- Online banking and fund transfers
- Digital marketing and advertisements

Figure 1.1 *Five components ofdata communication*



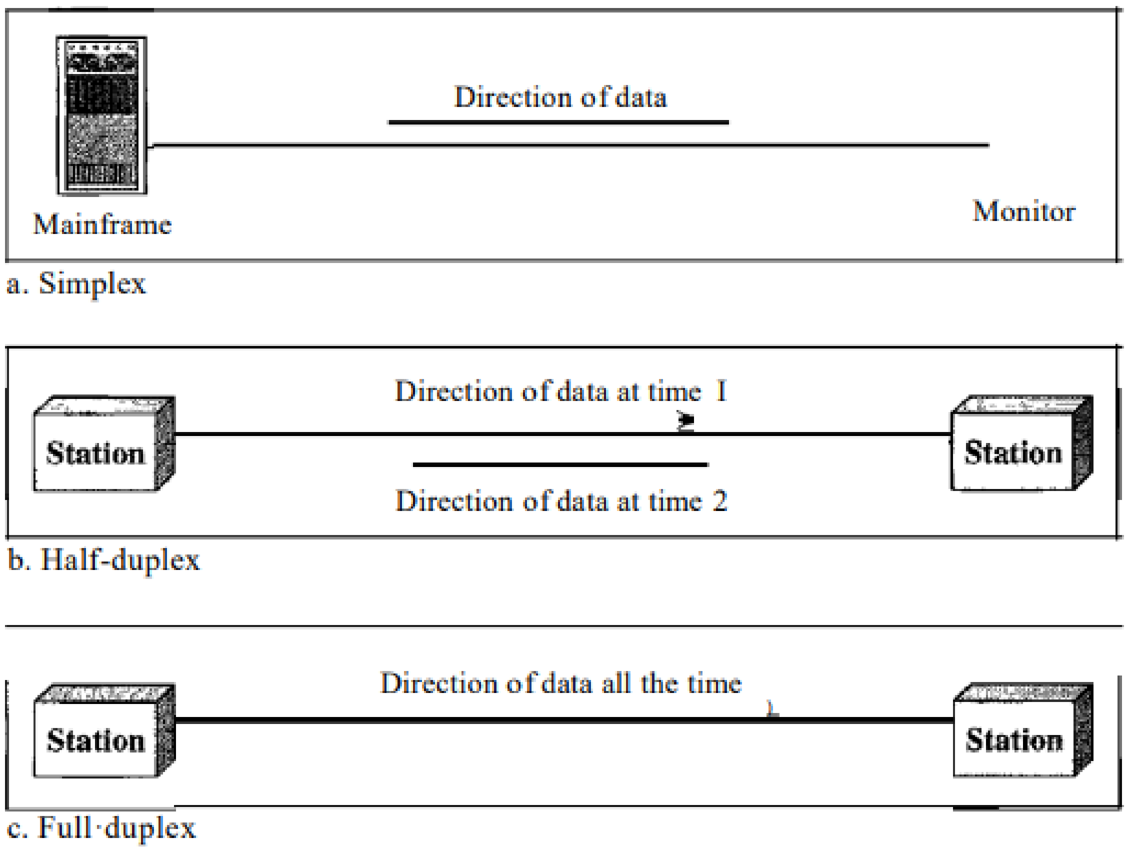
I. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
II. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
III. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
IV. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
V. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Representation Information today comes in different forms such as text, numbers, images, audio, and video.

Data Flow:

Data Flow Communication between two devices can be simplex, half-duplex, or full-duplex

Figure 1.2 *Data flow (simplex, half-duplex, and full-duplex)*



Simplex In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure 1.2a). Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

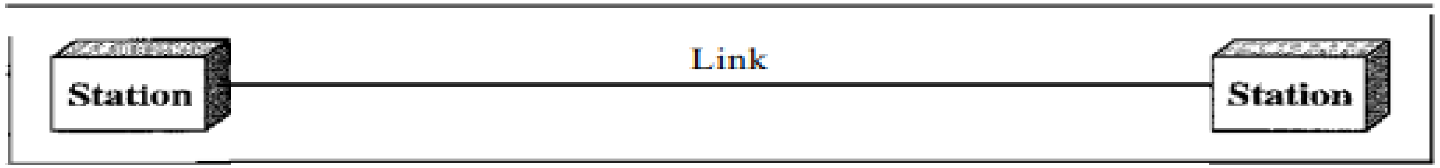
Half-Duplex In half-duplex mode, each station can both transmit and receive, but not at the same time. : When one device is sending, the other can only receive, and vice versa (see Figure 1.2b).
The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

Full-Duplex In full-duplex mode, both stations can transmit and receive simultaneously (see Figure 1.2c). The full-duplex mode is like a two way traffic at the same time in both the directions.
One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

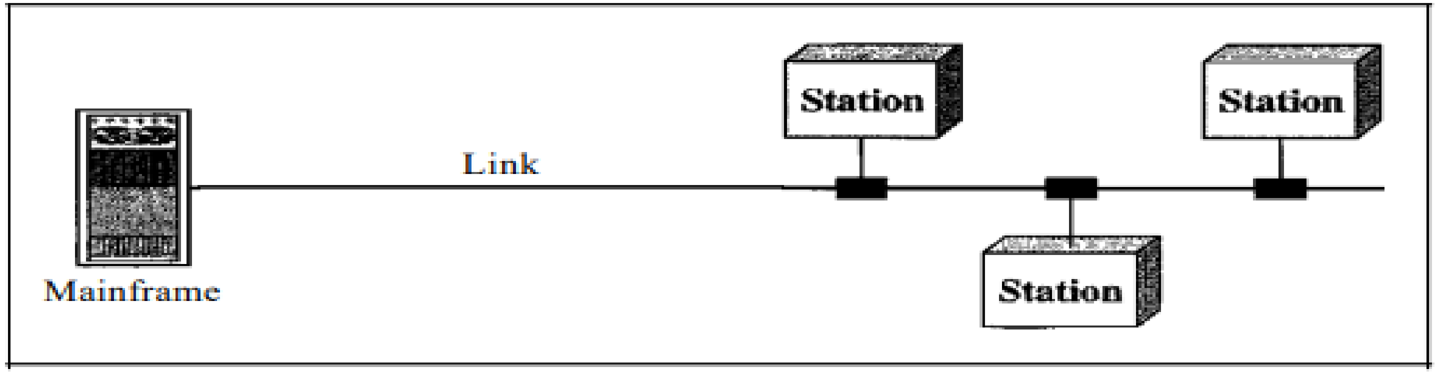
NETWORKS A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Type Of Connections:

Figure 1.3 *Types ofconnections: point-to-point and multipoint*



a. Point-to-point



b. Multipoint

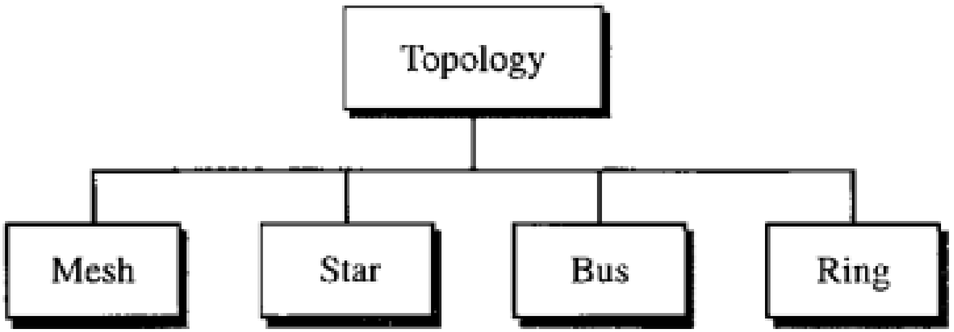
Point-to-Point: A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible (see Figure 1.3a). When user changes television channels by infrared remote control, user establishing a point-to-point connection between the remote control and the television's control system, **Computer to Printer via USB Cable:** A single USB cable directly connects one computer to one printer

Multipoint: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 1.3b). In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection. E.g. One cable connects multiple subscribers' TVs, Conference call

Physical Topology

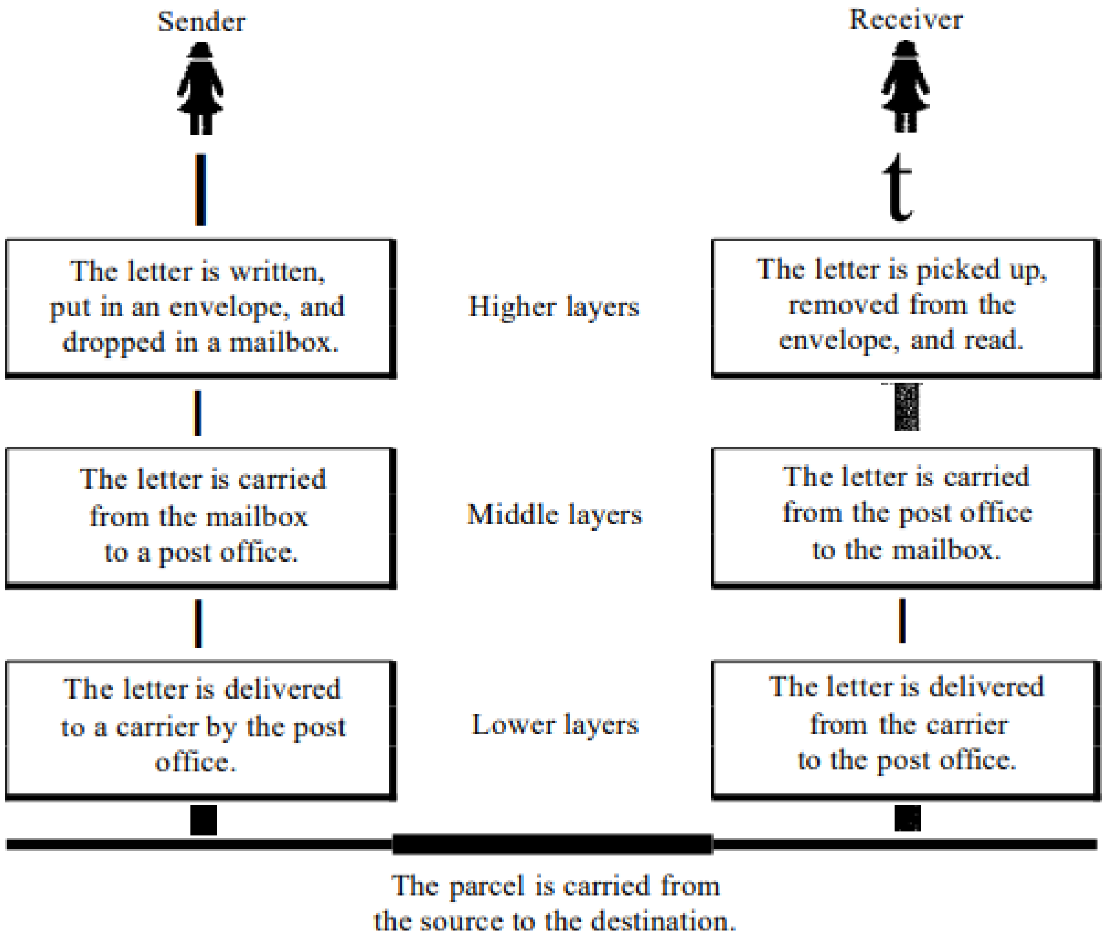
Two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring (see Figure 1.4)

Figure 1.4 *Categories oftopology*



LAYERED TASKS

Figure 2.1 *Tasks involved in sending a letter*



Hierarchy According to the analysis, there are three different activities at the sender site and another three activities at the receiver site. The task of transporting the letter between the sender and the receiver is done by the carrier. Something that is not obvious immediately is that the tasks must be done in the order given in the hierarchy. At the sender site, the letter must be written and dropped in the mailbox before being picked up by the letter carrier and delivered to the post office. At the receiver site, the letter must be dropped in the recipient mailbox before being picked up and read by the recipient

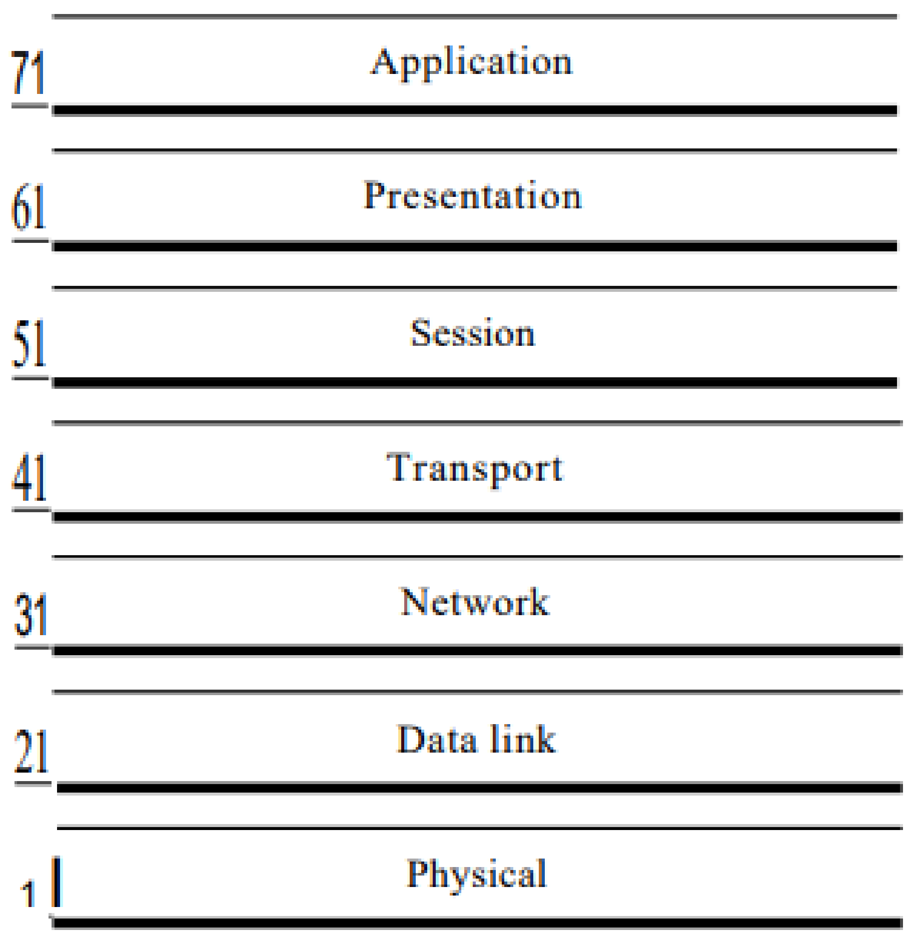
Services Each layer at the sending site uses the services of the layer immediately below it. The sender at the higher layer uses the services of the middle layer. The middle layer uses the services of the lower layer. The lower layer uses the services of the carrier.

THE OSI MODEL

An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture.

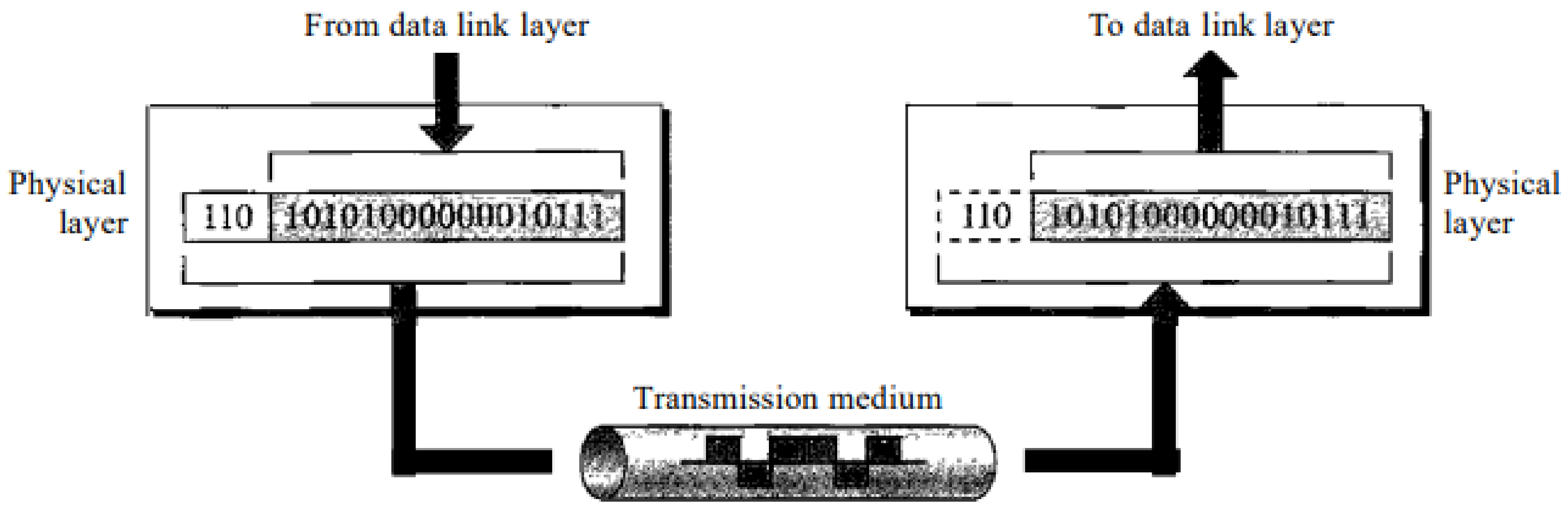
The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network. An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.

Seven layers of the OSI model



Physical Layer The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur. Figure 2.5 shows the position of the physical layer with respect to the transmission medium and the data link layer.

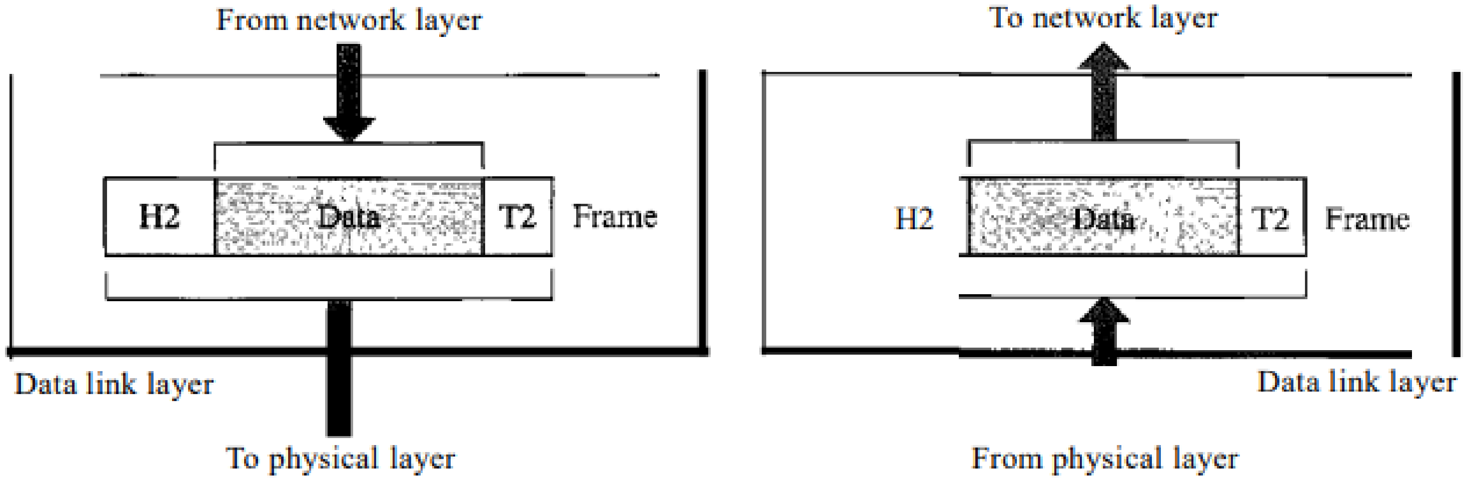
Figure 2.5 *Physical layer*



The physical layer is responsible for movements of individual bits from one hop (node) to the next.

The physical layer is also concerned with the following:
Physical characteristics: of interfaces and medium. The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
Representation of bits: The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and Is are changed to signals).
Data rate: The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
Synchronization of bits: The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.
Line configuration: The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
Physical topology: The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).
Transmission mode: The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

Figure 2.6 *Data link layer*



Other responsibilities of the data link layer include the following:

Framing: The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

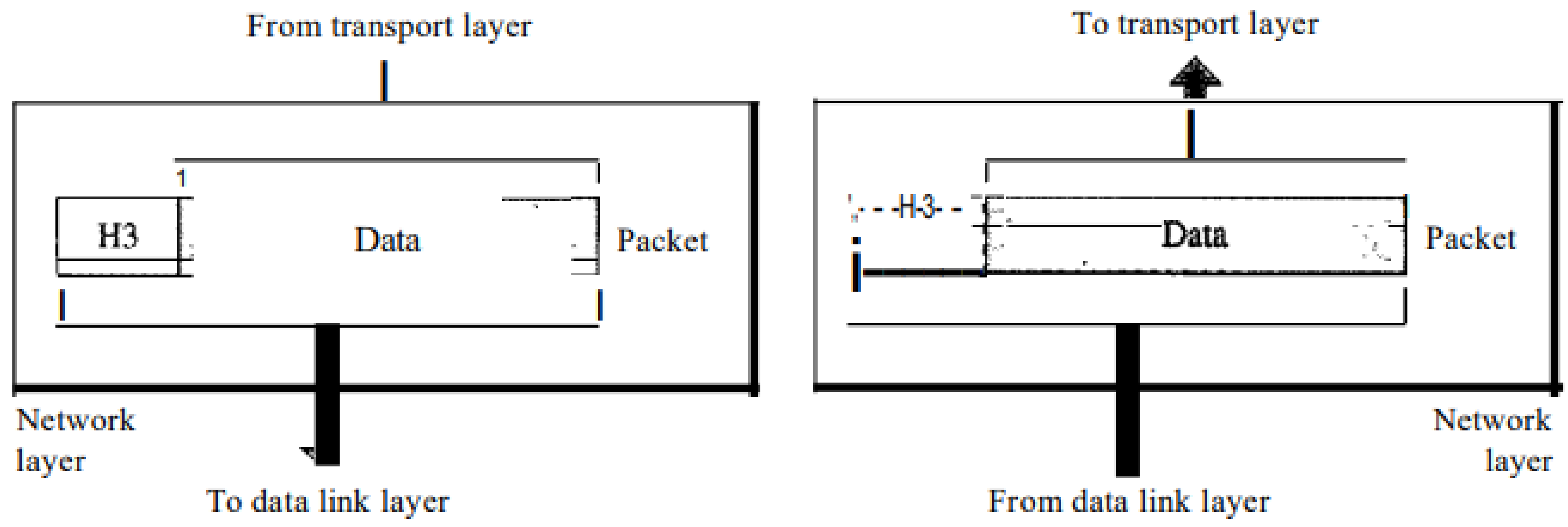
Physical addressing: If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

Flow control: If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Error control: The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

Access control: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Figure 2.8 *Network layer*



The network layer is responsible for the delivery of individual packets from the source host to the destination host.

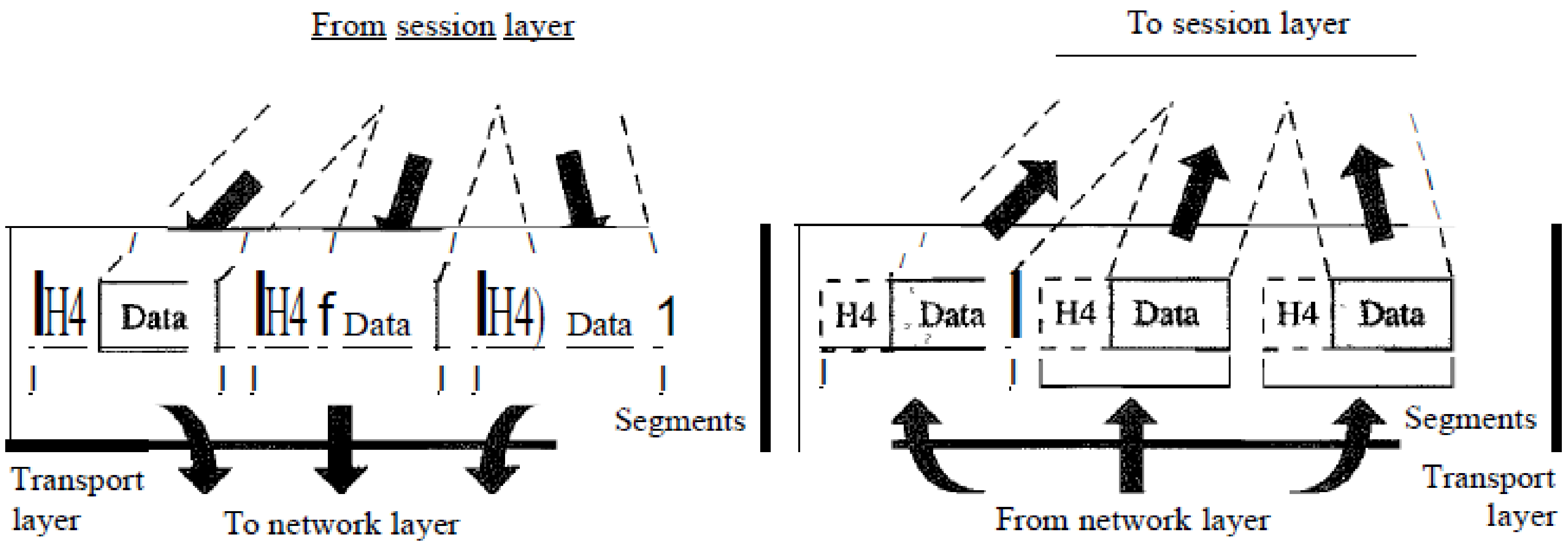
Logical addressing: The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver. We discuss logical addresses later in this chapter. o

Routing: When independent networks or links are connected to create intenetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

Logical addressing: The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver. We discuss logical addresses later in this chapter.

Routing: When independent networks or links are connected to create intenetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

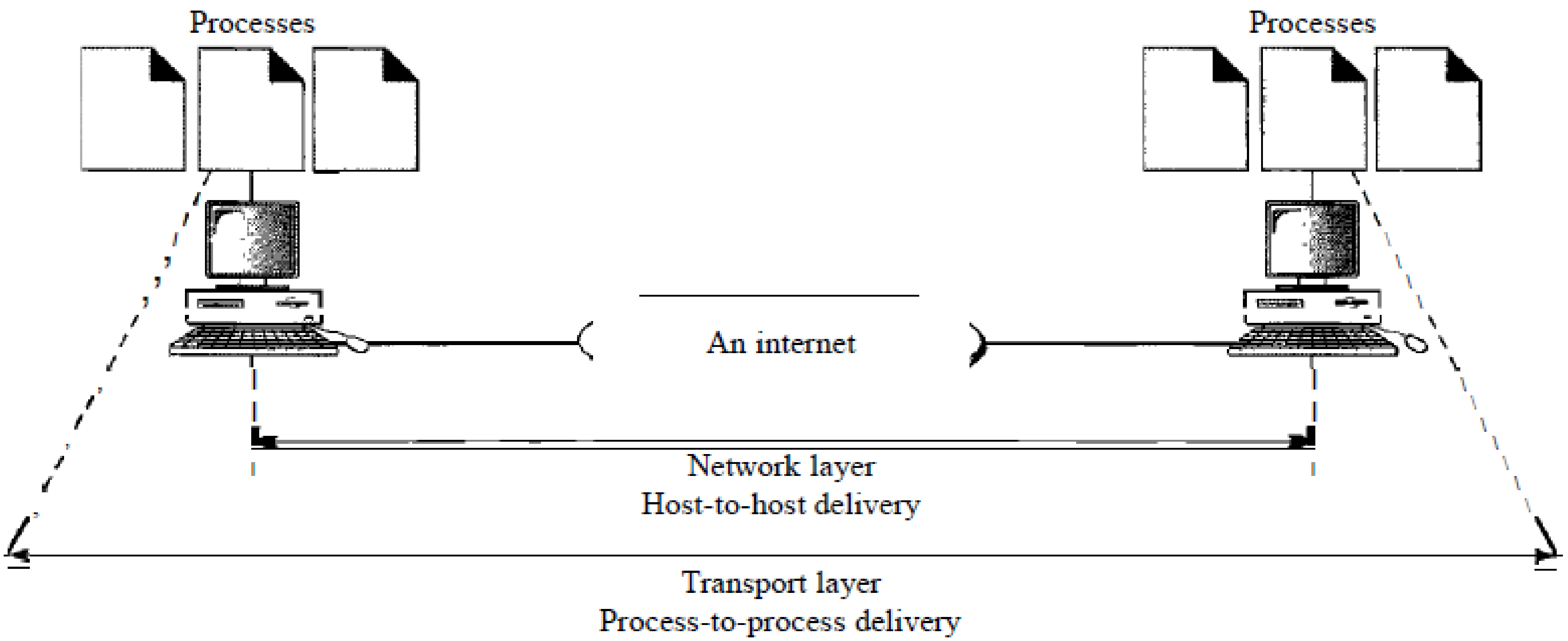
Figure 2.10 *Transport layer*



Service-point addressing: Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a *service-point address* (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

- Segmentation and reassembly: A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
- Connection control: The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
- Flow control: Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- Error control: Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

Figure 2.11 *Reliable process-to-process delivery ofa message*



Session Layer

- Dialog control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
- Synchronization: The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent. Figure 2.12 illustrates the relationship of the session layer to the transport and presentation layers.

Figure 2.12 *Session layer*

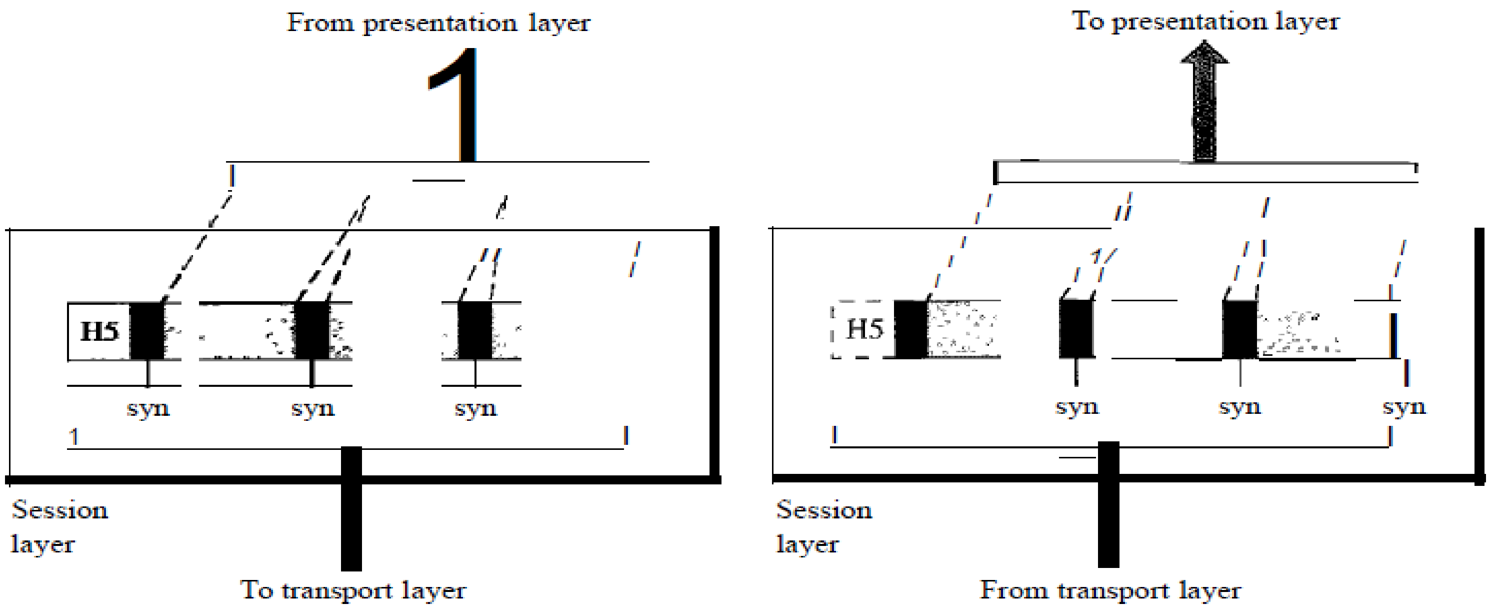
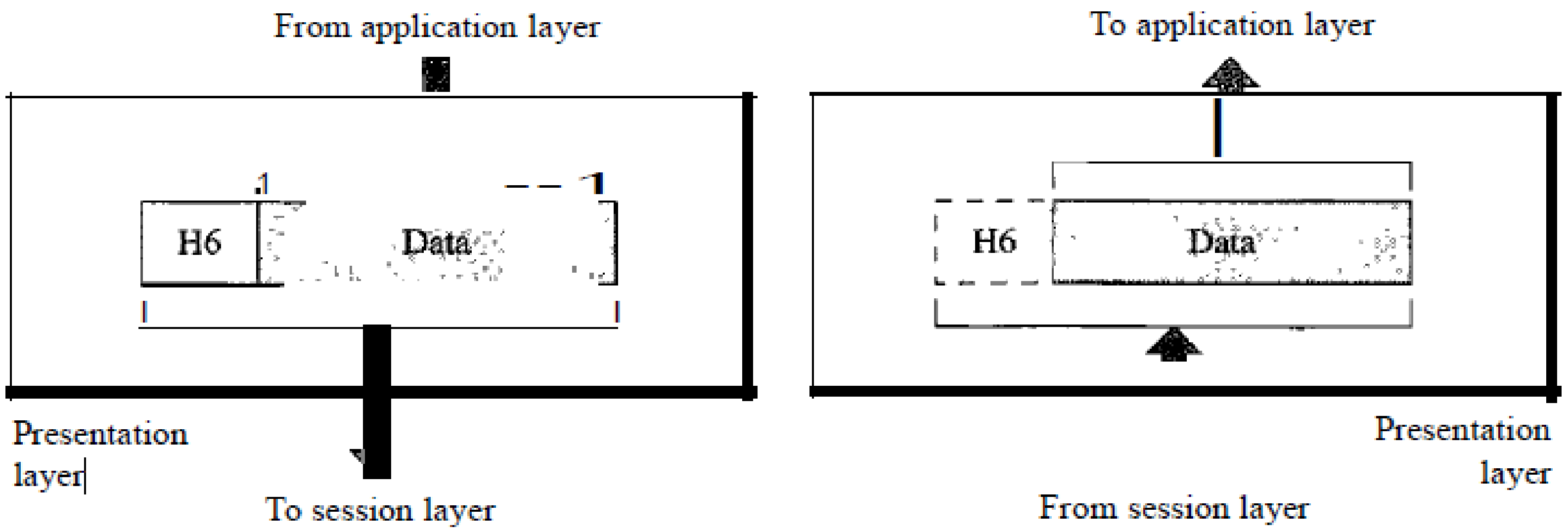
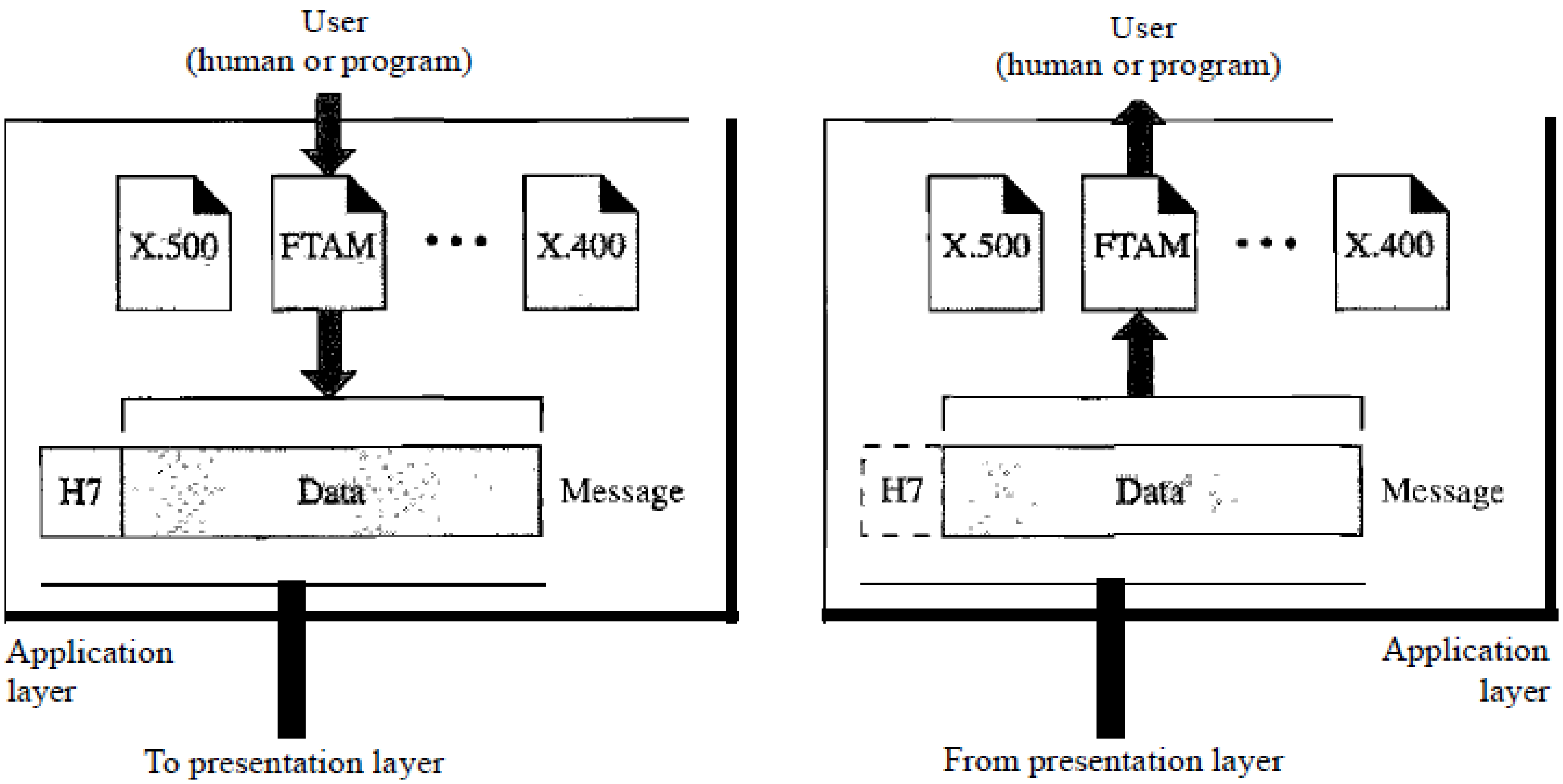


Figure 2.13 *Presentation layer*



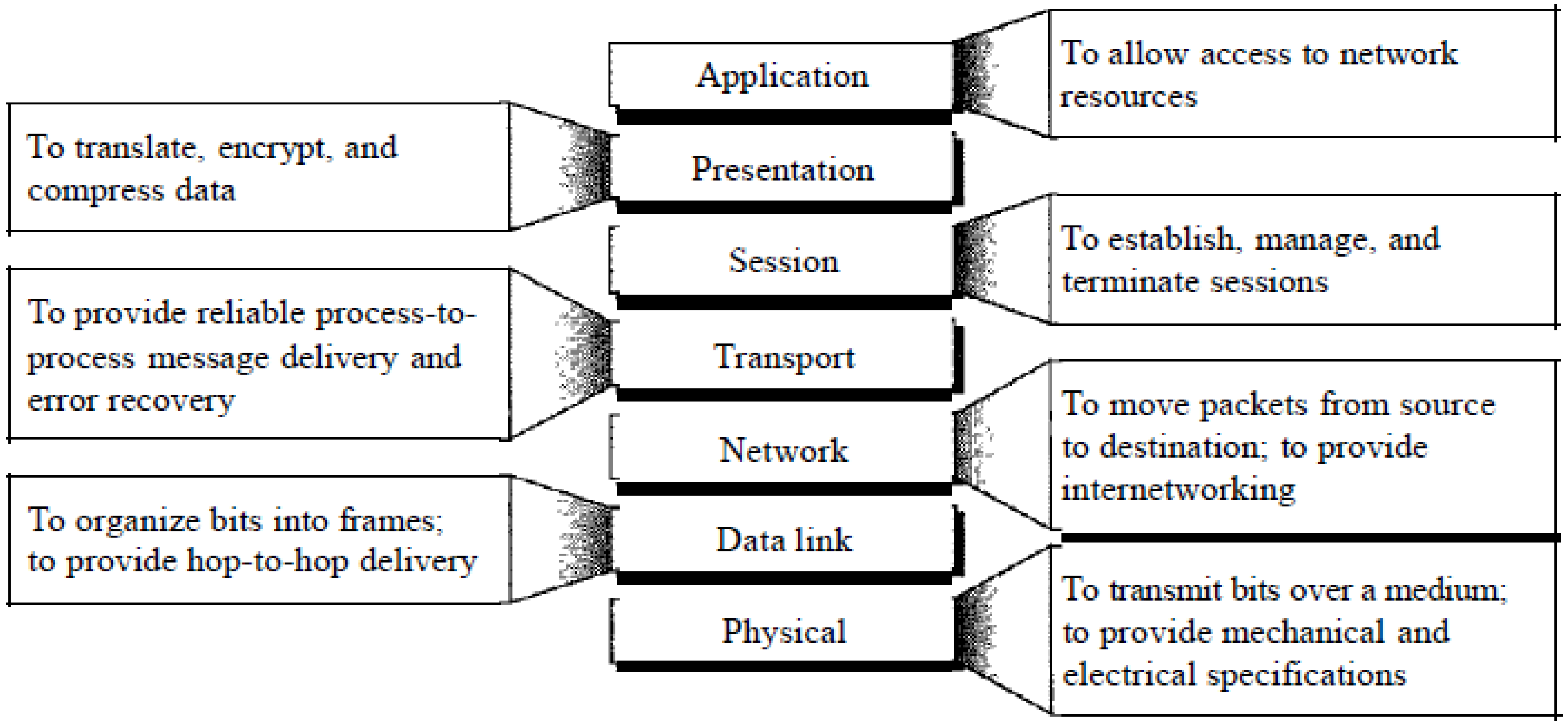
- Translation. The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
- Encryption. To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- Compression. Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Figure 2.14 *Application layer*



Summary of Layers

Figure 2.15 *Summary of layers*



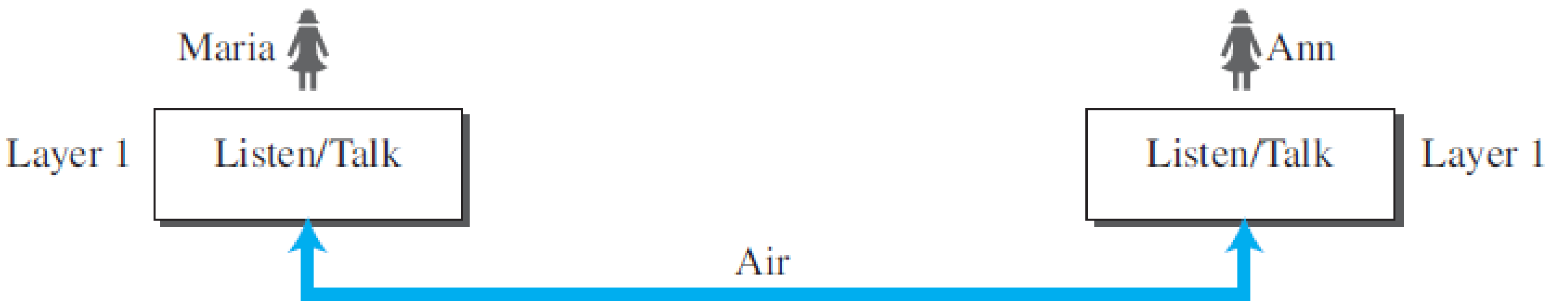
PROTOCOL LAYERING

A protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively. When communication is simple, we may need only one simple protocol; when the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or protocol layering.

First Scenario

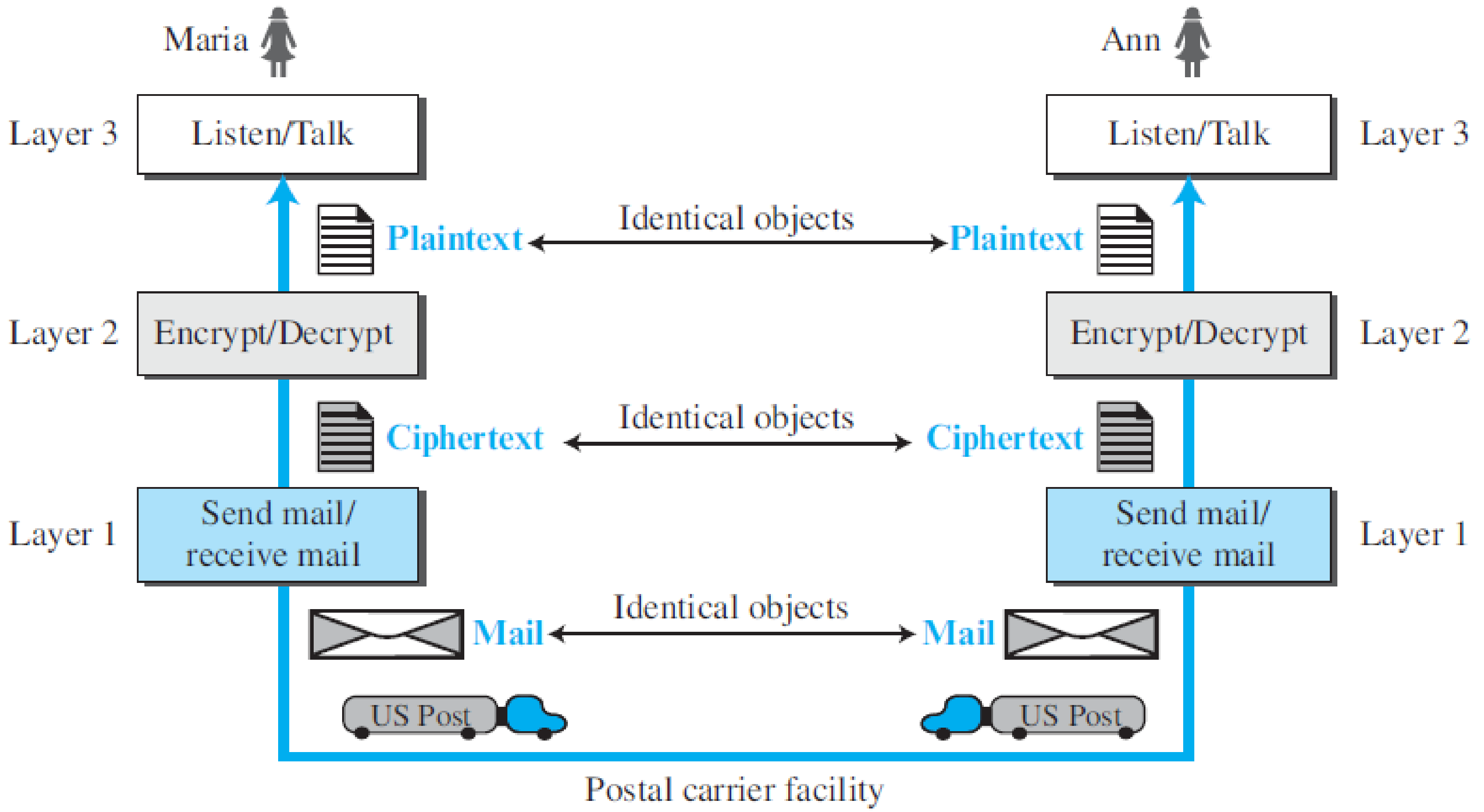
In the first scenario, communication is so simple that it can occur in only one layer. Assume Maria and Ann are neighbors with a lot of common ideas. Communication between Maria and Ann takes place in one layer, face to face, in the same language, as shown in Figure 1.9.

Figure 1.9 *A single-layer protocol*



Second Scenario

Figure 1.10 *A three-layer protocol*



Principles of Protocol Layering

Let us discuss some principles of protocol layering.

The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction. For example, the third layer task is to

listen (in one direction) and talk (in the other direction). The second layer needs to be able to encrypt and decrypt. The first layer needs to send and receive mail.

The second important principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical. For example, the object under layer 3 at both sites should be a plaintext letter. The object under layer 2 at both sites should be a cipher text letter. The object under layer 1 at both sites should be a piece of mail.

Logical Connections

After following the above two principles, we can think about logical connection between each layer as shown in Figure 1.11. This means that we have layer-to-layer communication. Maria and Ann can think that there is a logical (imaginary) connection at each layer through which they can send the object created from that layer. We will see that the concept of logical connection will help us better understand the task of layering we encounter in data communication and networking.

Figure 1.11 *Logical connection between peer layers*

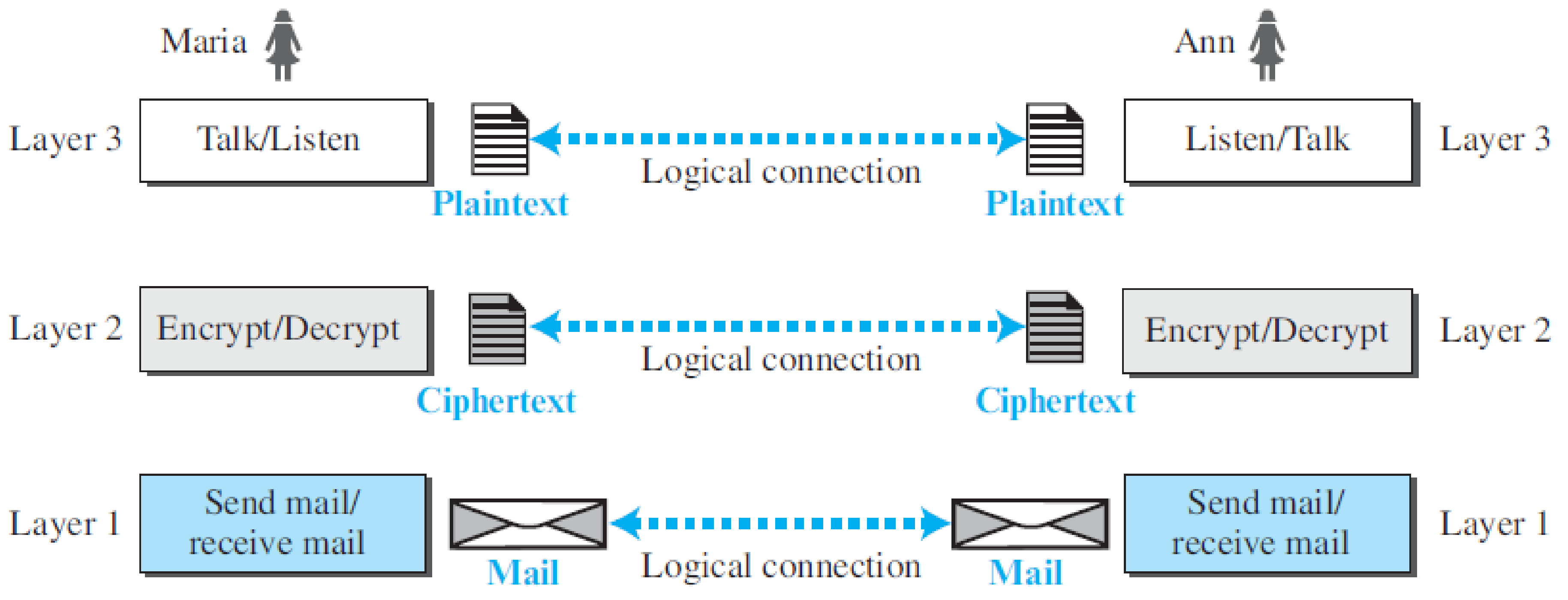
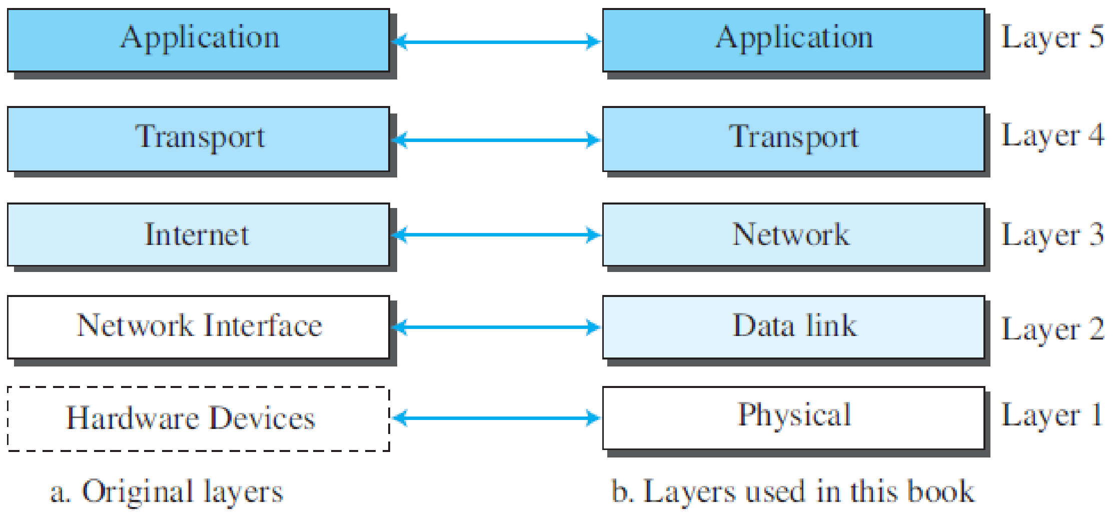


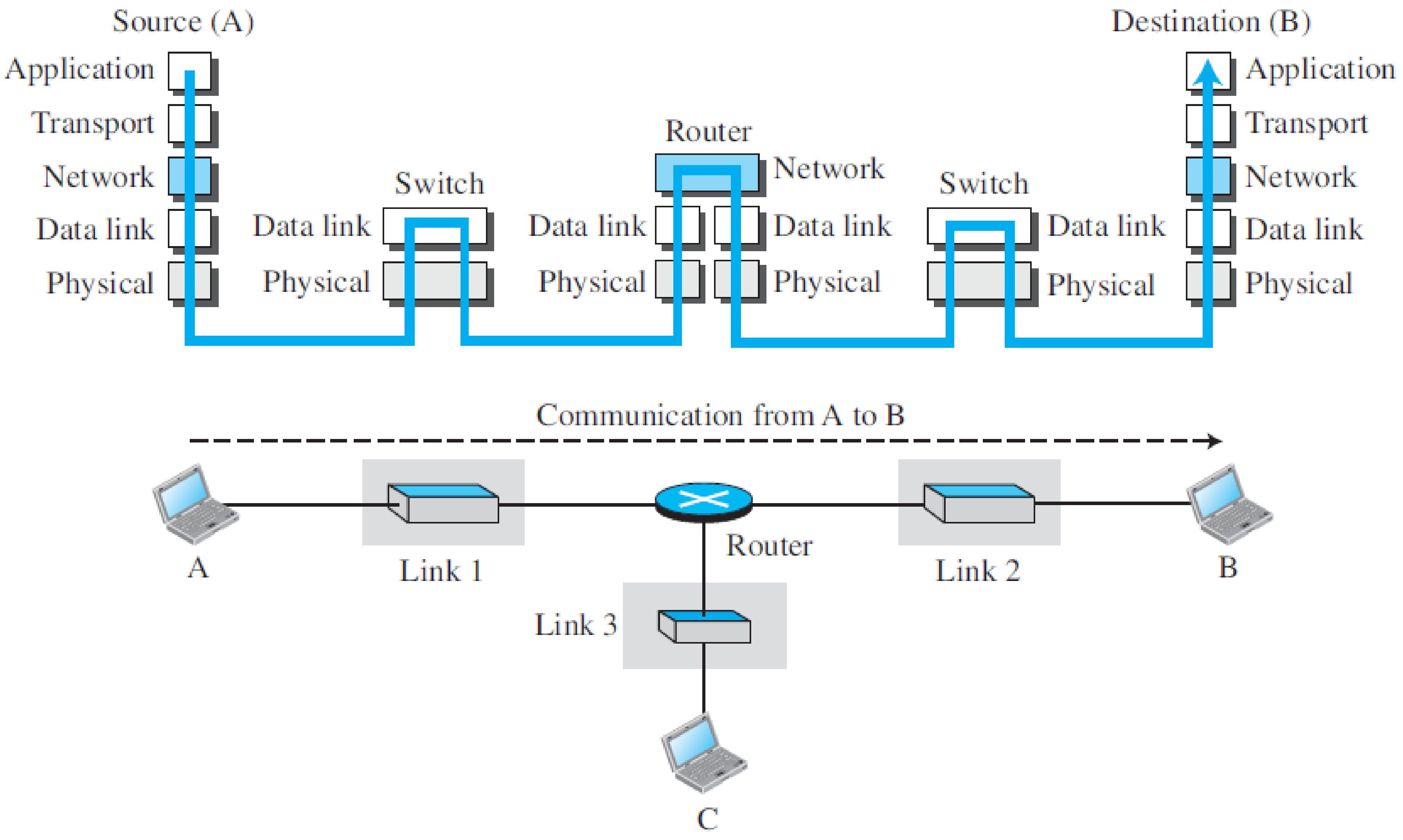
Figure 1.12 *Layers in the TCP/IP protocol suite*



TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols. The original TCP/IP protocol suite was defined as four software layers built upon the hardware.

Layered Architecture

Figure 1.13 *Communication through an internet*



Layers in the TCP/IP Protocol Suite

Figure 1.14 *Logical connections between layers of the TCP/IP protocol suite*

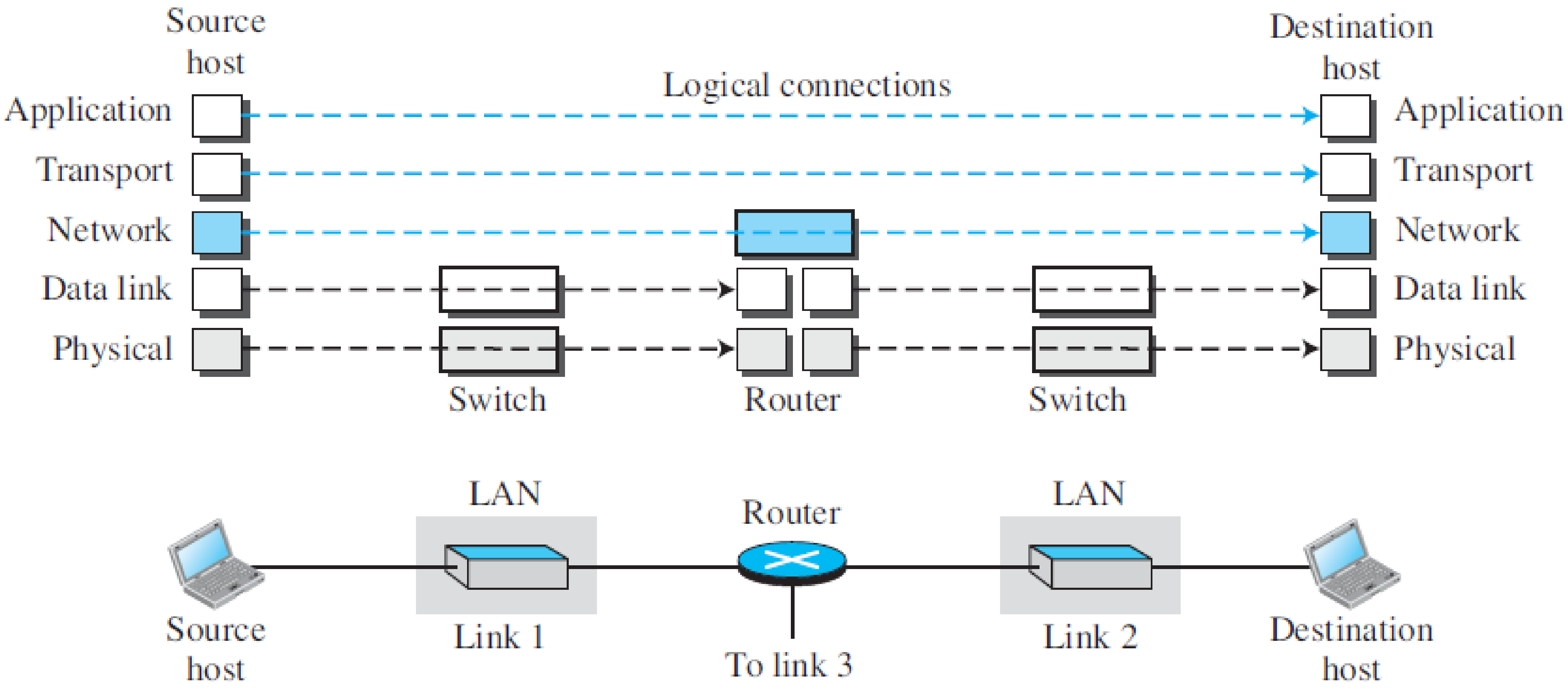
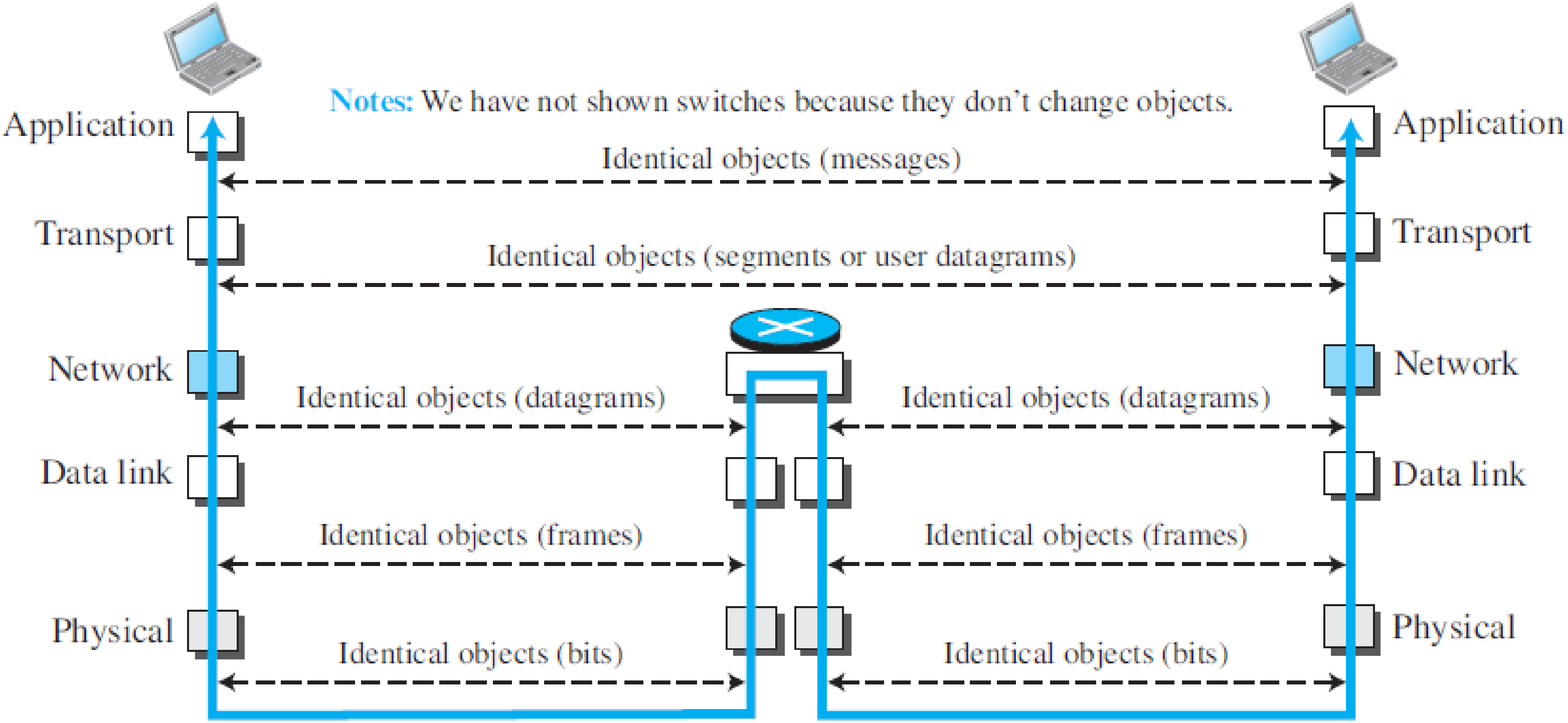
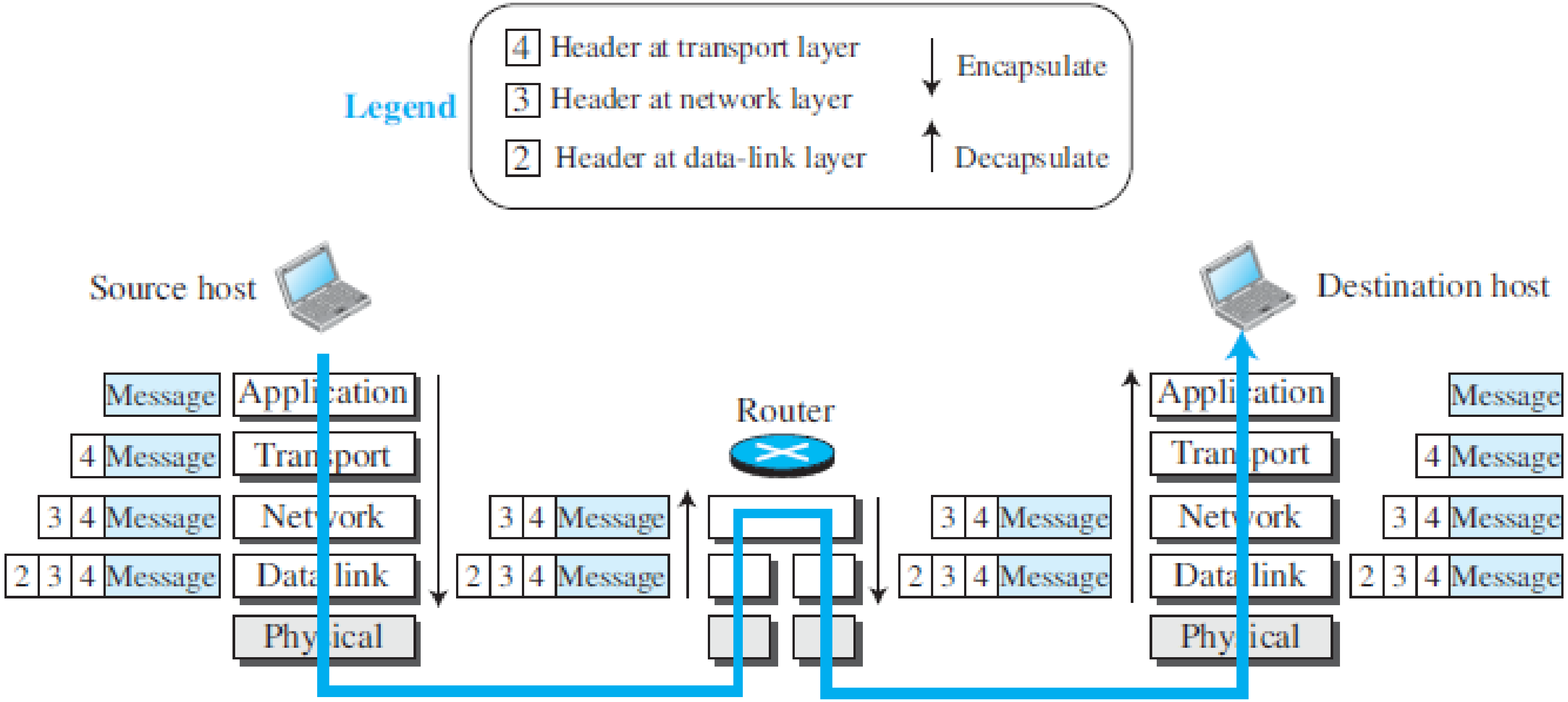


Figure 1.15 *Identical objects in the TCP/IP protocol suite*



Encapsulation and Decapsulation

Figure 1.16 *Encapsulation/Decapsulation*



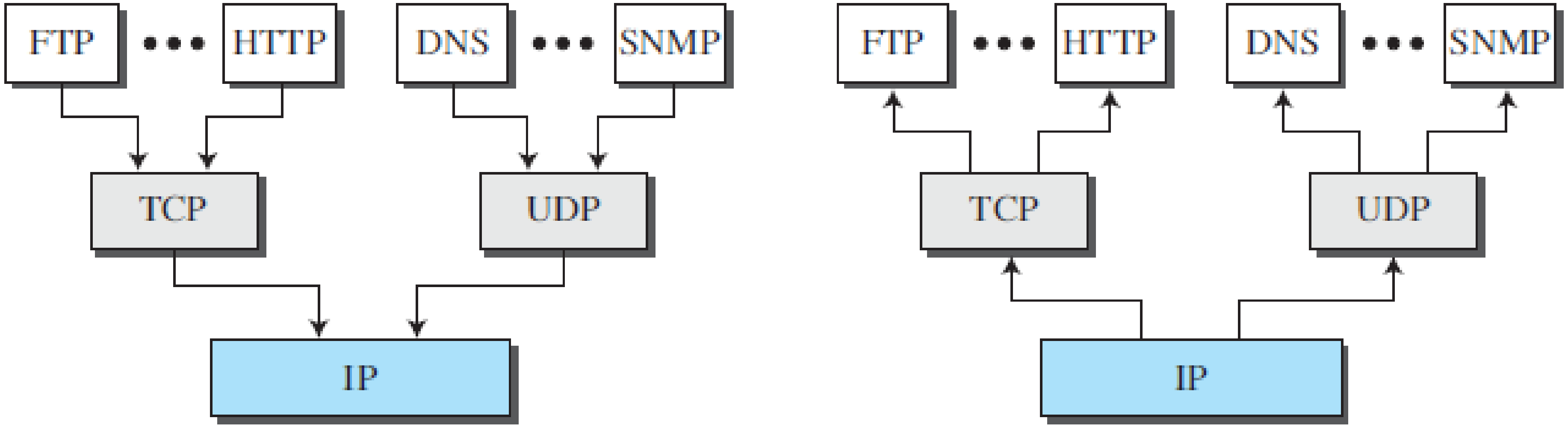
Addressing

Figure 1.17 *Addressing in the TCP/IP protocol suite*

Packet names	Layers	Addresses
Message	Application layer	**Names**
Segment / User datagram	Transport layer	**Port numbers**
Datagram	Network layer	**Logical addresses**
Frame	Data-link layer	**Link-layer addresses**
Bits	Physical layer	

Multiplexing and Demultiplexing

Figure 1.18 *Multiplexing and demultiplexing*

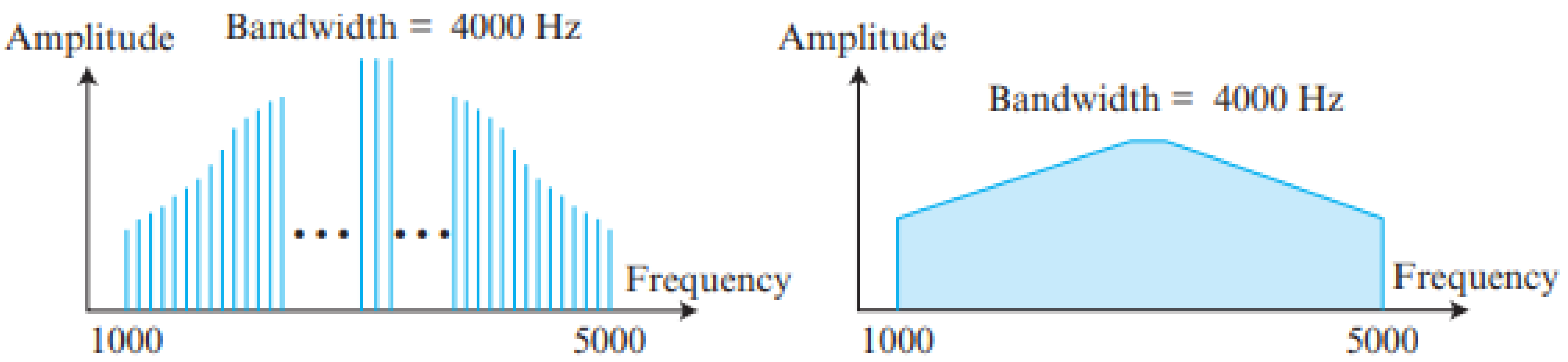


a. Multiplexing at source

b. Demultiplexing at destination

Bandwidth The range of frequencies contained in a composite signal is its bandwidth. The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 – 1000, or 4000. Figure 7.7 shows the concept of bandwidth. The figure depicts two composite signals, one periodic and the other non periodic. The bandwidth of the periodic signal contains many discrete frequencies that are integral multiples of the fundamental frequency. The bandwidth of the non periodic signal has the same range, but the frequencies are continuous.

Figure 7.7 *The bandwidth of periodic and nonperiodic composite signals*

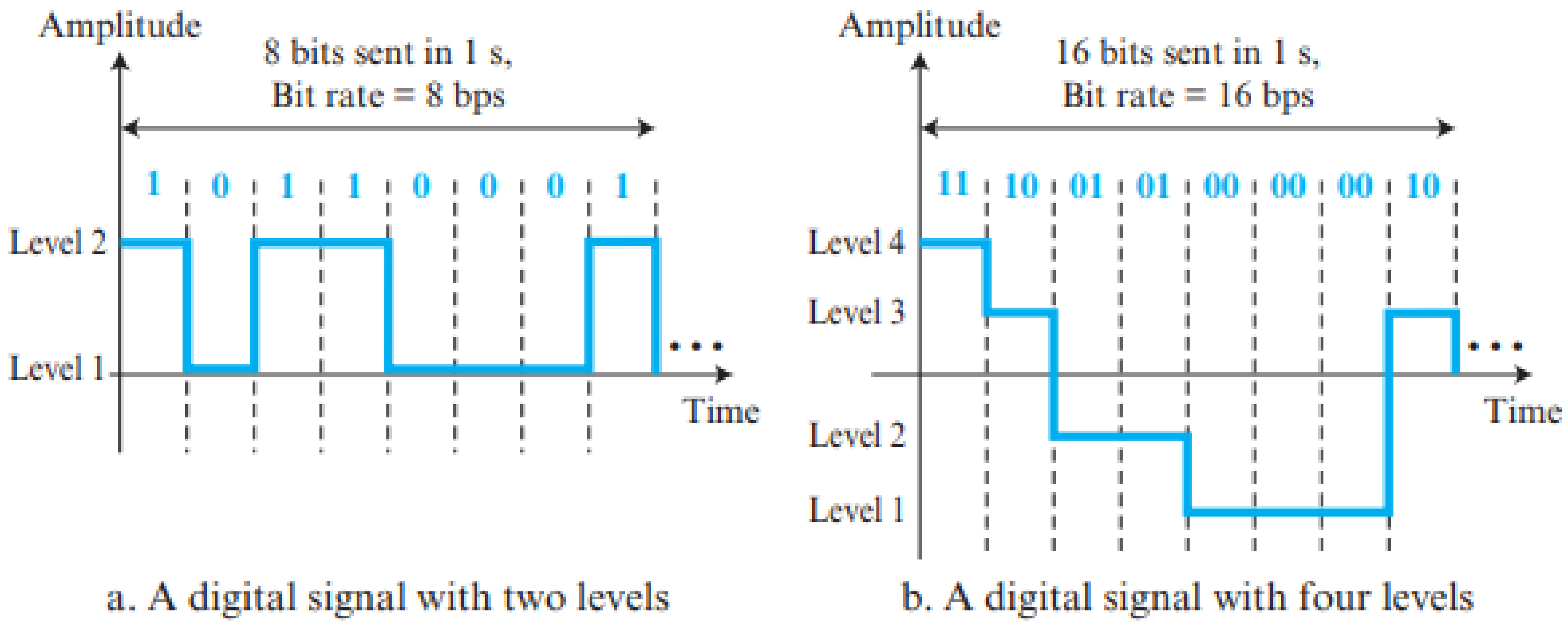


a. Bandwidth of a periodic signal

b. Bandwidth of a nonperiodic signal

Digital Signals In addition to being represented by an analog signal, information can also be represented by a digital signal. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage. A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level. Figure 7.8 shows two signals, one with two levels and the other with four. We send 1 bit per level in part a of the figure and 2 bits per level in part b of the figure. In general, if a signal has L levels, each level needs log2L bits. **The bit rate** is the number of bits sent in 1 second, expressed in bits per second (bps).

Figure 7.8 *Two digital signals: one with two signal levels and the other with four signal levels*



Assume we need to download text documents at the rate of 100 pages per minute. What is the required bit rate of the channel? A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires 8 bits, the bit rate is

The **bit length** is the distance one bit occupies on the transmission medium

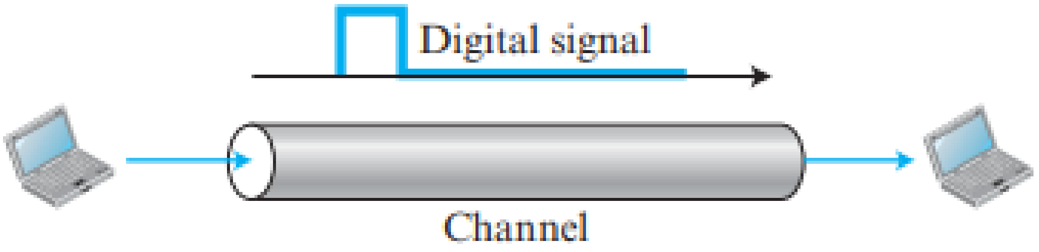
$$\text{Bit length} = \text{propagation speed} \times \text{bit duration}$$

Transmission of Digital Signals

Baseband Transmission

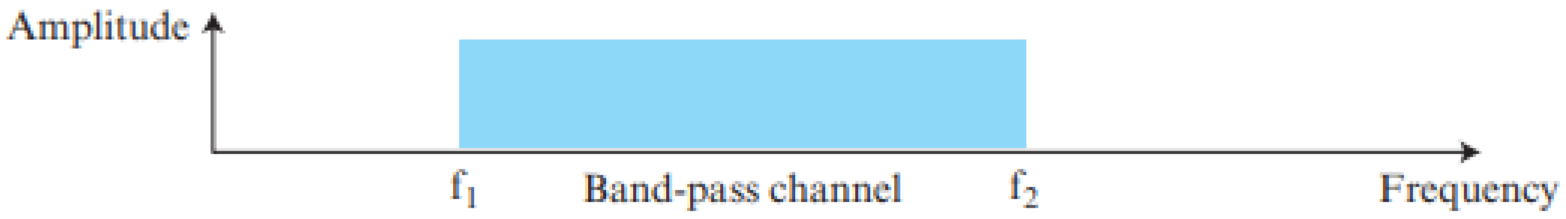
Baseband transmission means sending a digital signal over a channel without changing the digital signal to an analog signal. Figure 7.10 shows baseband transmission. Baseband transmission requires that we have a low-pass channel, a channel with a bandwidth that starts from zero. This is the case if we have a dedicated medium with a bandwidth constituting only one channel. For example, the entire bandwidth of a cable connecting two computers is one single channel. As another example, we may connect several computers to a medium, but not allow more than two stations to communicate at a time. Again we have a low-pass channel, and we can use it for baseband communication.

Figure 7.10 *Baseband transmission*



Broadband transmission or modulation means changing the digital signal to an analog signal for transmission. Modulation allows us to use a band-pass channel—a channel with a bandwidth that does not start from zero. This type of channel is more available than a low pass channel. Figure 7.11 shows a band pass channel.

Figure 7.11 *Bandwidth of a band-pass channel*



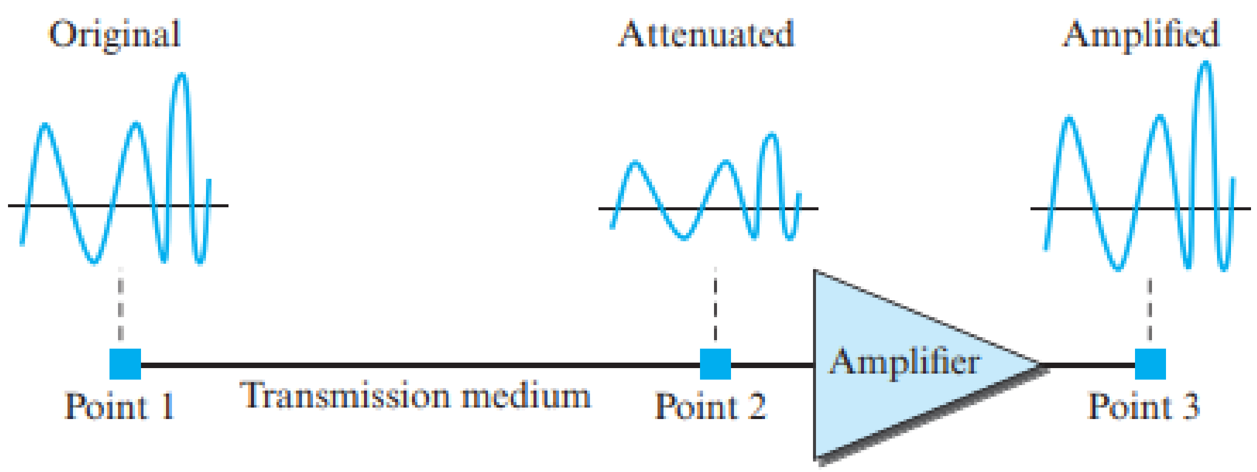
Transmission Impairment

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise.

Attenuation:

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal. Figure 7.13 shows the effect of attenuation and amplification.

Figure 7.13 *Attenuation and amplification*



To show that a signal has lost or gained strength, engineers use the unit of the decibel. The decibel (dB) measures the relative strengths of two signals or one signal at two different points. Note that the decibel is negative if a signal is attenuated and positive if a signal is amplified.

Variables P1 and P2 are the powers of a signal at points 1 and 2, respectively.

Figure 7.13 Attenuation and amplification

$dB = 10 \log_{10} (P2/P1)$

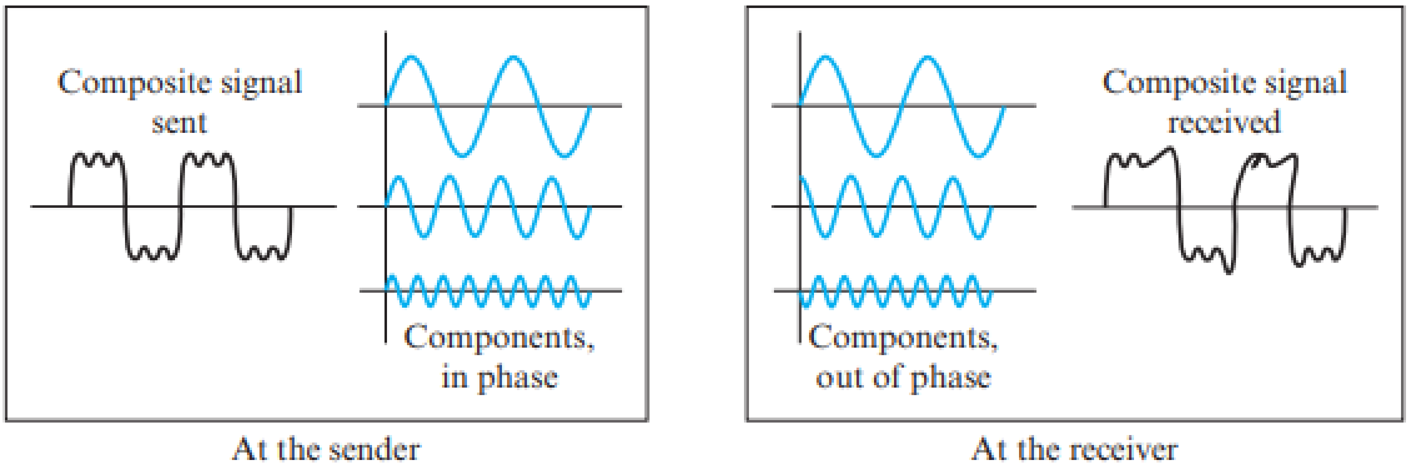
Suppose a signal travels through a transmission medium and its power is reduced to one half. This means that P2 = 0.5 P1. In this case, the attenuation (loss of power) can be calculated as

$10 \log_{10} P2/P1 = 10 \log_{10} (0.5\ P1) / P1 = 10 \log_{10} 0.5 = 10 \times (-0.3) = -3$ dB.

A loss of 3 dB (−3 dB) is equivalent to losing one-half the power

Distortion: Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made up of different frequencies. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration. In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same. Figure 7.14 shows the effect of distortion on a composite signal.

Figure 7.14 *Distortion*



Noise

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. Thermal noise is the random motion of electrons in a wire, which creates an extra signal not originally sent by the transmitter. Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna. Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna. Impulse noise is a spike (a signal with high energy and very short duration) that comes from power lines, lightning, and so on.

Data Rate Limits

A very important consideration in data communications is how fast we can send data, in bits per second, over a channel. Data rate depends on three factors:

1. The bandwidth available
2. The level of the signals we use
3. The quality of the channel (the level of noise) Two theoretical formulas were developed to calculate the data rate: one by Nyquist for a noiseless channel, another by Shannon for a noisy channel.

Noiseless Channel: Nyquist Bit Rate For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

$$\text{Bit Rate} = 2 \times B \times \log 2\ L$$

In this formula, B is the bandwidth of the channel, L is the number of signal levels used to represent data, and BitRate is the number of bits per second.

According to the formula, we might think that, given a specific bandwidth, we can have any bit rate we want by increasing the number of signal levels. Although the idea is theoretically correct, practically there is a limit. When we increase the number of signal levels, we impose a burden on the receiver. If the number of levels in a signal is just 2, the receiver can easily distinguish between a 0 and a 1. If the level of a signal is 64, the receiver must be very sophisticated to distinguish between 64 different levels. In other words, increasing the levels of a signal reduces the reliability of the system.

We need to send 265 kbps over a noiseless (ideal) channel with a bandwidth of 20 kHz. How many signal levels do we need? We can use the Nyquist formula as shown:

Noisy Channel: Shannon Capacity In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel below.

$$C = B \times \log2\ (1 + SNR)$$

In this formula, B is the bandwidth of the channel, SNR is the signal-to-noise ratio, and C is the capacity of the channel in bits per second. Note that in the Shannon formula there is no indication of the signal level, which means that no matter how many levels we have, we cannot achieve a data rate higher than the capacity of the channel. In other words, the formula defines a characteristic of the channel, not the method of transmission. The capacity defines the upper boundary of the channel bit rate.

Performance

Up to now, we have discussed the tools of transmitting data (signals) over a network and how the data behave. One important issue in networking is the performance of the network—how good is it? We discuss quality of service, an overall measurement of network performance, in detail in Chapter 8.

Bandwidth One characteristic that measures network performance is bandwidth. However, the term can be used in two different contexts with two different measuring values: bandwidth in hertz and bandwidth in bits per second.

Bandwidth in Hertz

We have discussed this concept. Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass. For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

Bandwidth in Bits per Seconds

The term bandwidth can also refer to the number of bits per second that a channel, a link, or even a network can transmit. For example, one can say the bandwidth of a Fast Ethernet network (or the links in this network) is 100 Mbps. This means that this network can send 100 Mbps.

Throughput

The throughput is a measure of how fast we can actually send data through a network. Although, at first glance, bandwidth in bits per second and throughput seem the same, they are different. A link may have a bandwidth of B bps, but we can send only T bps through this link, with T always less than B. In other words, the bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data.

For example, we may have a link with a bandwidth of 1 Mbps, but the
devices connected to the end of the link may handle only 200 kbps. This means that we
cannot send more than 200 kbps through this link.

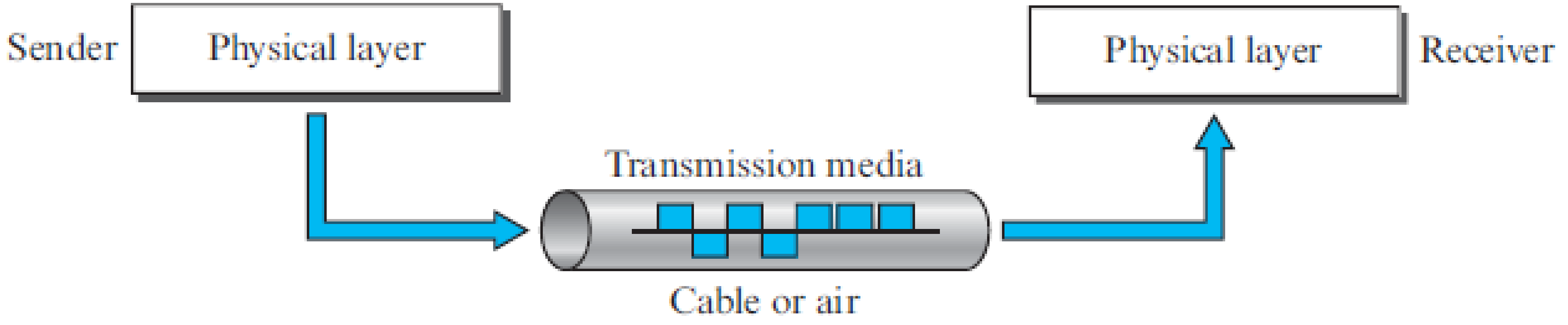
Latency (Delay)
The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.
There are four types of delay:
propagation delay, transmission delay, queuing delay, and processing delay. The latency or total delay is

Latency = propagation delay + transmission delay + queuing delay + processing delay.

Jitter Another performance issue that is related to delay is jitter. We can roughly say that jitter is a problem if different packets of data encounter different delays and the application using the data at the receiver site is time-sensitive (audio and video data, for example). If the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets endures jitter.

TRANSMISSION MEDIA

Figure 7.58 *Transmission media and physical layer*



A transmission medium can be broadly defined as anything that can carry information from a source to a destination. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane. In data communications the definition of the information and the transmission medium is more specific. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form.

In telecommunications, transmission media can be divided into two broad categories:

guided and unguided. **Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable.**

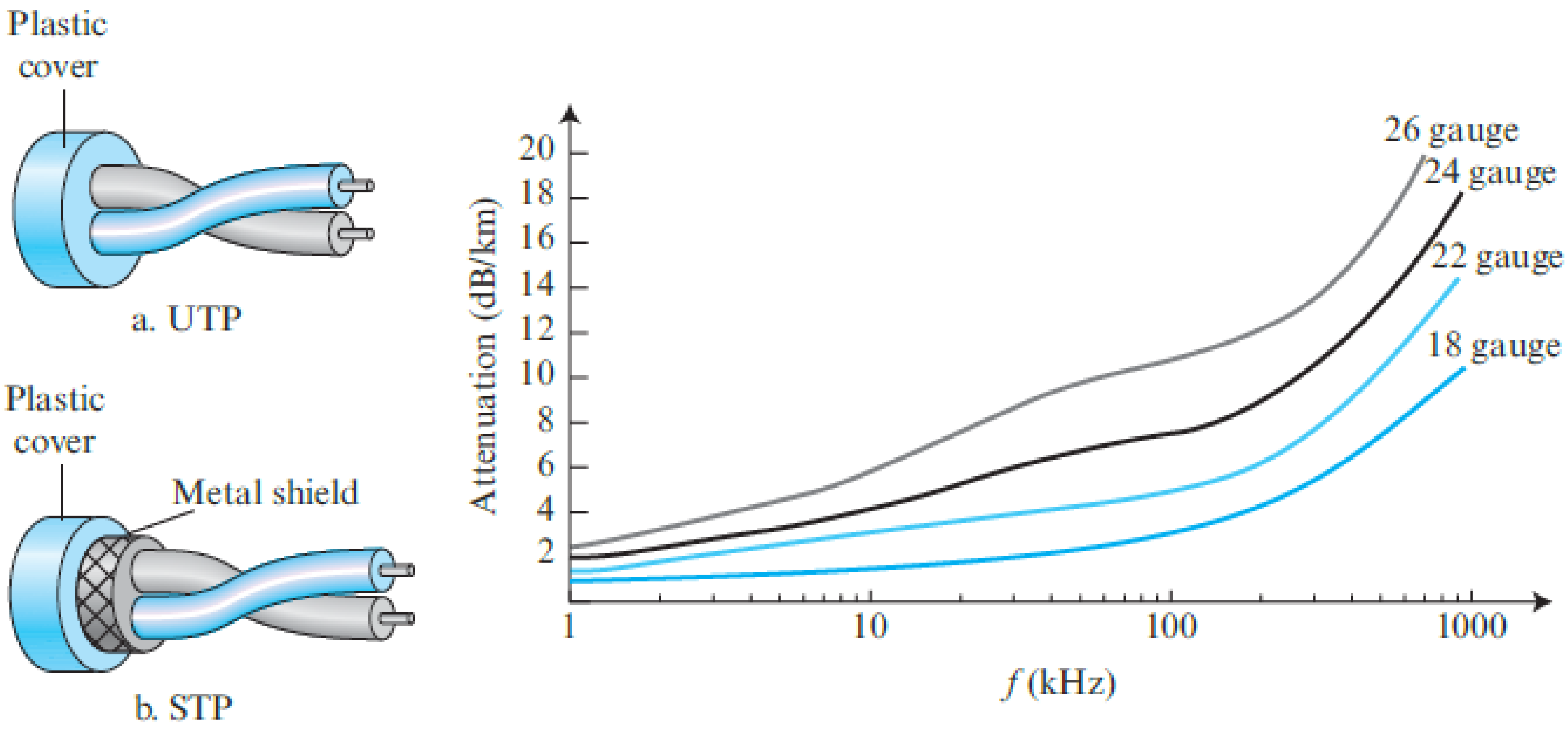
Unguided medium is free space.

Twisted-Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure 7.59.

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal from the sender, interference (noise) and crosstalk may affect both wires and create unwanted signals. If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources. This results in a difference at the receiver. By twisting the pairs, a balance is maintained. The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP). STP cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.

Figure 7.59 *Twisted-pair cable*



Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover (see Figure 7.60).

Figure 7.60 *Coaxial cable*