Chapter 2

Network Models

2.1 Layer Architecture

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office.

Topics discussed in this section:

- Sender
- Receiver
- Carrier Hierarchy

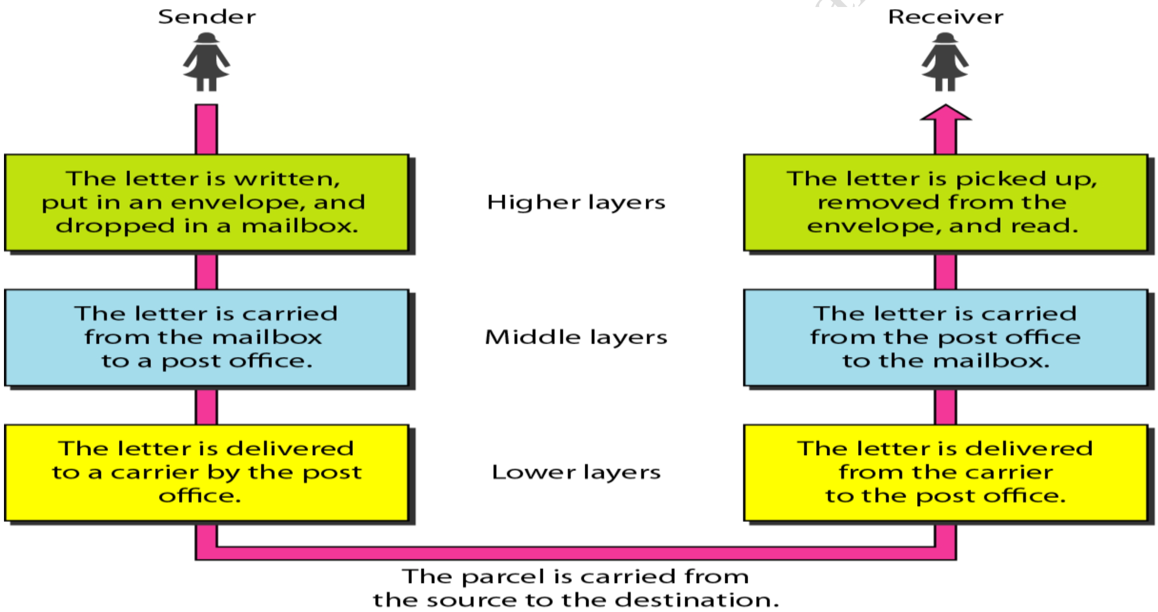

Figure 2.1 : Tasks involved in sending a letter

2.1 THE OSI MODEL

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

ISO is the organization
OSI is the model

ISO is the organization.
OSI is the model.

Topics discussed in this section:

- Layered Architecture
- Peer-to-Peer Processes
- Encapsulation

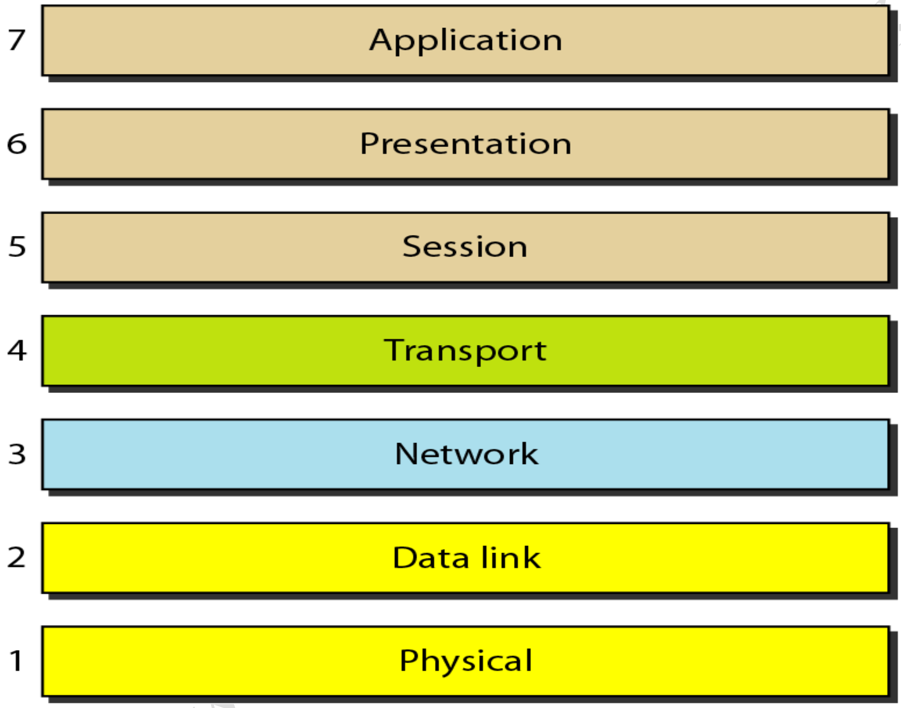

Figure 2.2 : *Seven layers of the OSI model*

Layer Architecture

- Layer architecture simplifies the network design.
- It is easy to debug network applications in a layered architecture network.
- The network management is easier due to the layered architecture.
- Network layers follow a set of rules ,called protocol.
- The protocol defines the format of the data being exchanged, and the control and timing for the hand shake between layers

Peer-to-Peer Processes

- Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it Figure 2.3.

Interfaces between Layers

- Each interface defines the information and services a layer must provide for the layer above it.
- As long as a layer provides the expected services to the layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding layers.

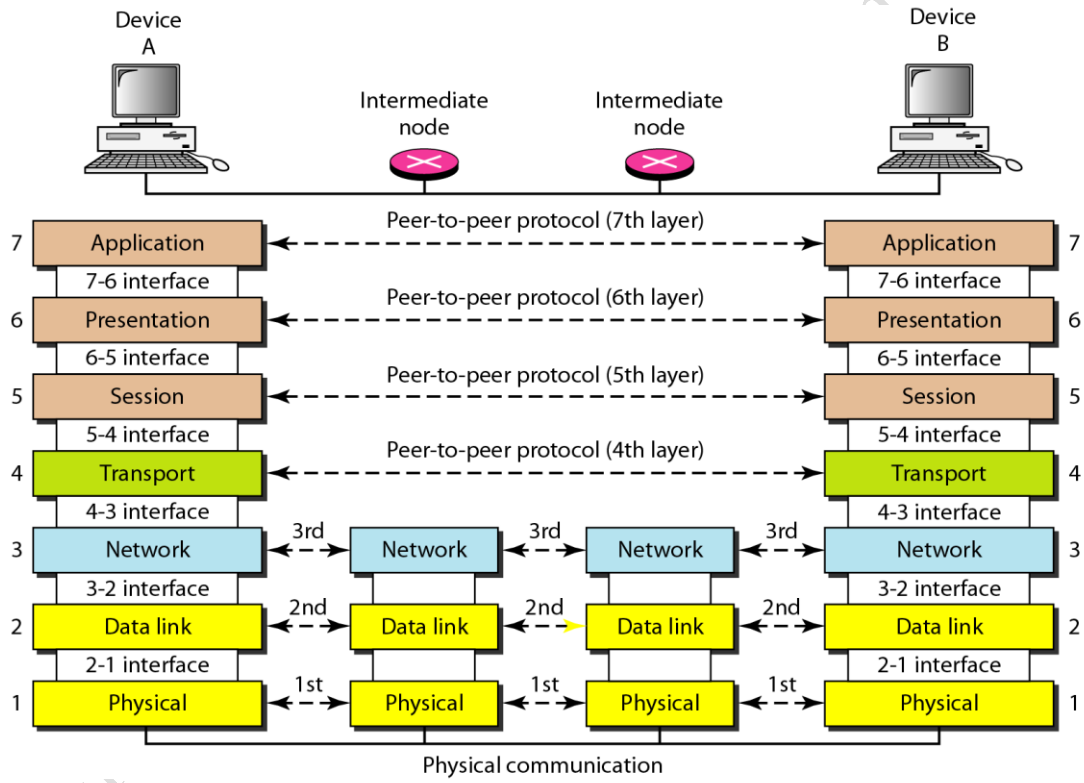

Figure 2.3 : The interaction between layers in the OSI model

Organization of the Layers

- The seven layers can be thought of as belonging to three subgroups:-
  - **Sub group _1** : Layers 1, 2, and 3-physical, data link, and network-are the network support layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability).

- **Sub group _2** : Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers; they allow interoperability among unrelated software systems.
- **Sub_group_3**: Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.

An exchange using the OSI model

- **D7** means the data unit at **layer 7**, **D6** means the data unit at **layer 6**, and so on.
- The process starts at layer 7 (the application layer), then moves from layer to layer in **descending**, **sequential order**.
- At each layer, **a header**, or possibly **a trailer**, can be added to the data unit.
- Commonly, the trailer is added only at layer 2.
- When the formatted data unit passes through the physical layer (layer 1), it is changed into an **electromagnetic signal** and **transported along a physical link.**
- Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers.
- As each block of data reaches the next higher layer, **the headers and trailers attached to it at the corresponding sending layer are removed**, and actions appropriate to that layer are taken.
- By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the **recipient**

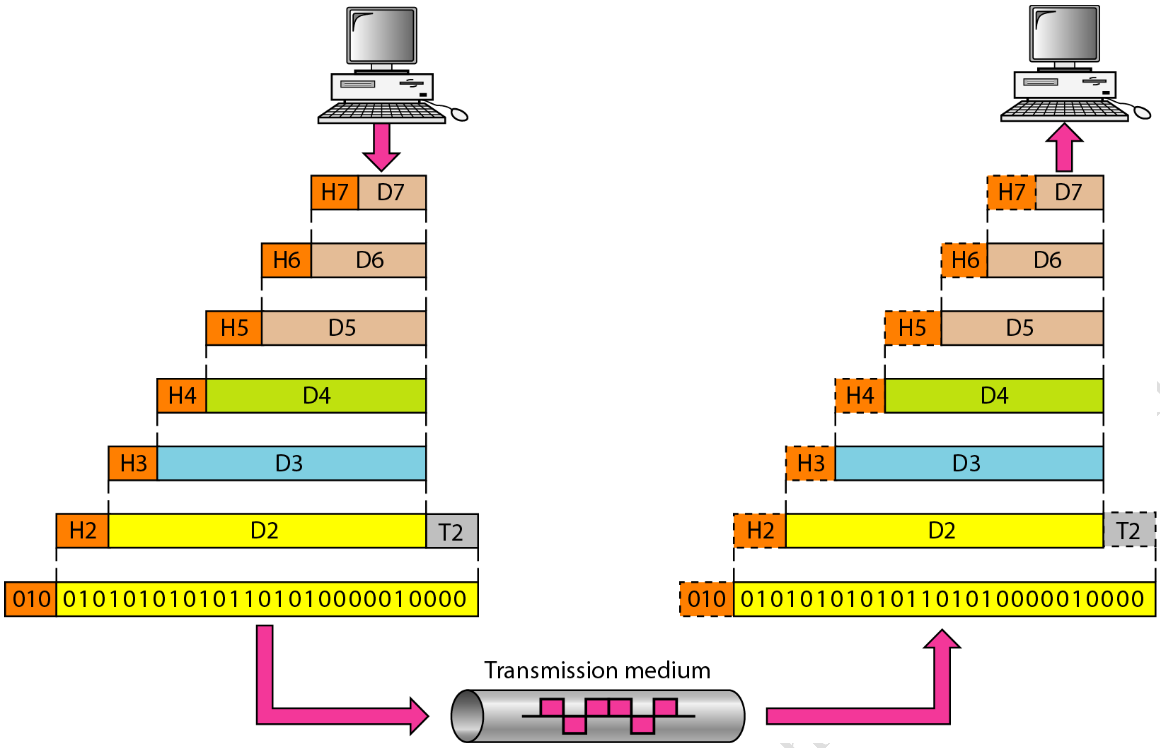

Figure 2.4 : An exchange using the OSI model

Encapsulation

- A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on.
- In other words, the data portion of a packet at level N - 1 carries the whole packet (data and header and maybe trailer) from level N.

2-3 LAYERS IN THE OSI MODEL

In this section we briefly describe the functions of each layer in the OSI model.

Topics discussed in this section:

1. **Physical Layer**
2. **Data Link Layer**
3. **Network Layer**
4. **Transport Layer**
5. **Session Layer**
6. **Presentation Layer**

7. **Application Layer**

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.
- The physical layer is also concerned with the following:
    - **Physical characteristics of interfaces and medium.**
    - **Representation of bits.**
    - **Data rate.**
    - **Synchronization of bits.**
    - **Line configuration.**
    - **Physical topology**
    - **Transmission mode.**
- **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 I s 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.

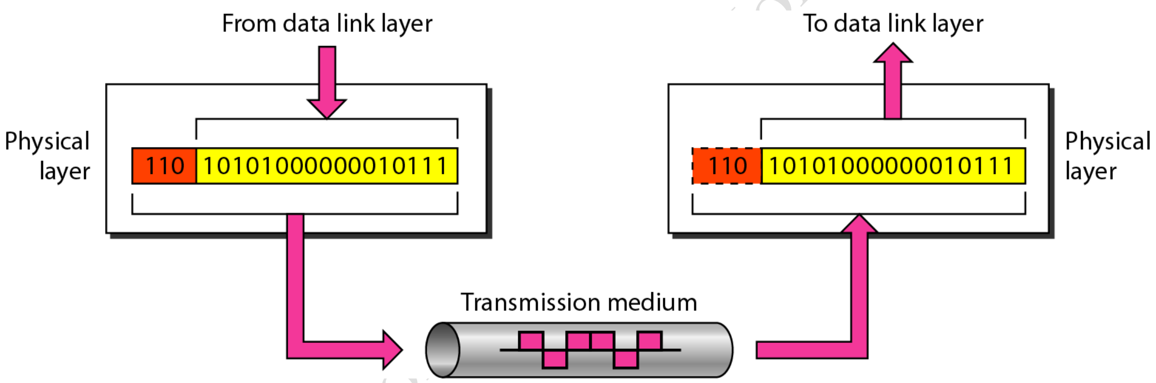

Figure 2.5 : ***Physical layer***

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

Data Link Layer

- The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).
- Figure 2.6 shows the relationship of the data link layer to the network and physical layers.

- Other responsibilities of the data link layer include the following:
    - **Framing.**
    - **Physical addressing.**
    - **Flow control.**
    - **Error control.**
    - **Access control**

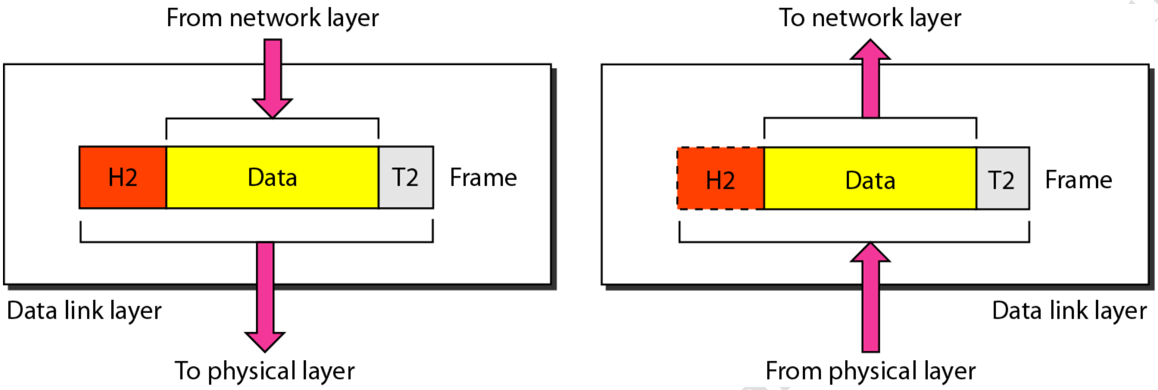

Figure 2.6: ***Data link layer***

The data link layer is responsible for moving frames from one hop (node) to the next.

- 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.

As the figure (2.7) shows, communication at the data link layer occurs between two adjacent nodes. To send data from A to F, three partial deliveries are made.

- **First,** the data link layer at A sends a frame to the data link layer at B (a router).
- **Second,** the data link layer at B sends a new frame to the data link layer at E.
- **Finally,** the data link layer at E sends a new frame to the data link layer at F.
- **Note that** the frames that are exchanged between the three nodes have different values in the headers.
- The frame from **A to B** has B as the destination address and A as the source address.
- The frame from **B to E** has E as the destination address and B as the source address.
- The frame from **E to F** has F as the destination address and E as the source address.
- The values of the trailers can also be different if error checking includes the header of the frame.

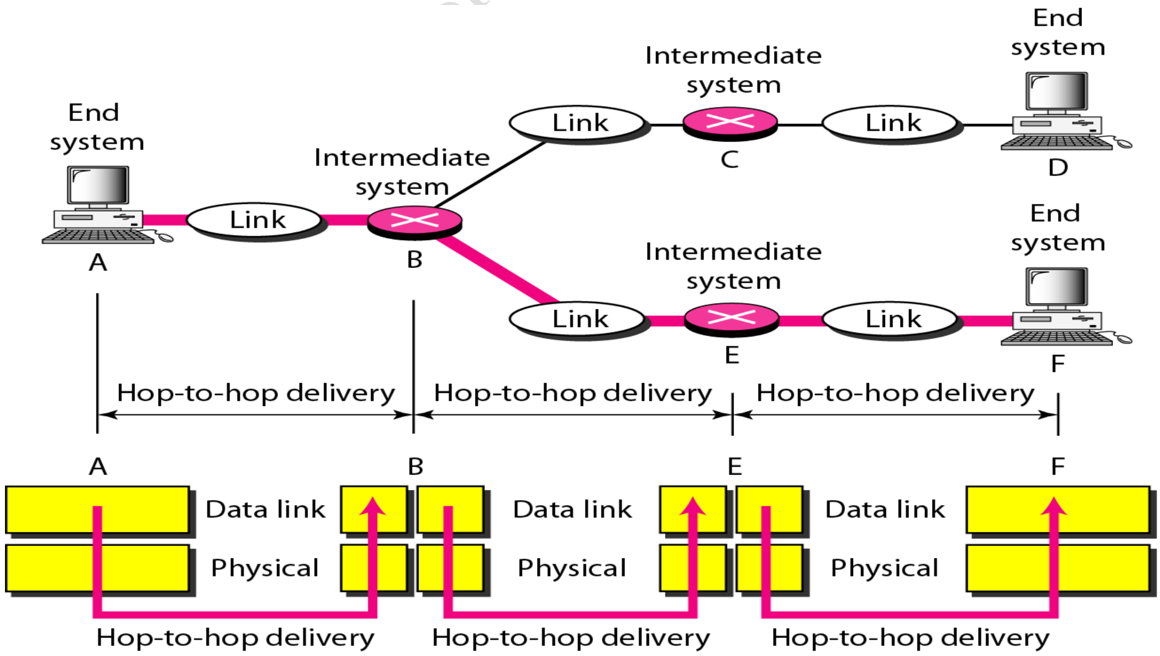

Figure 2.7 : ***Hop-to-hop delivery***

Network Layer

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

- If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. Figure 2.8 shows the relationship of the network layer to the data link and transport layers.

Logical addressing: IP addresses

1) **Data link layer address: MAC address**
2) **Routing.**

Responsibilities of the network layer include the following:

- **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
- **Routing**. When independent networks or links are connected to create internet works(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**.**

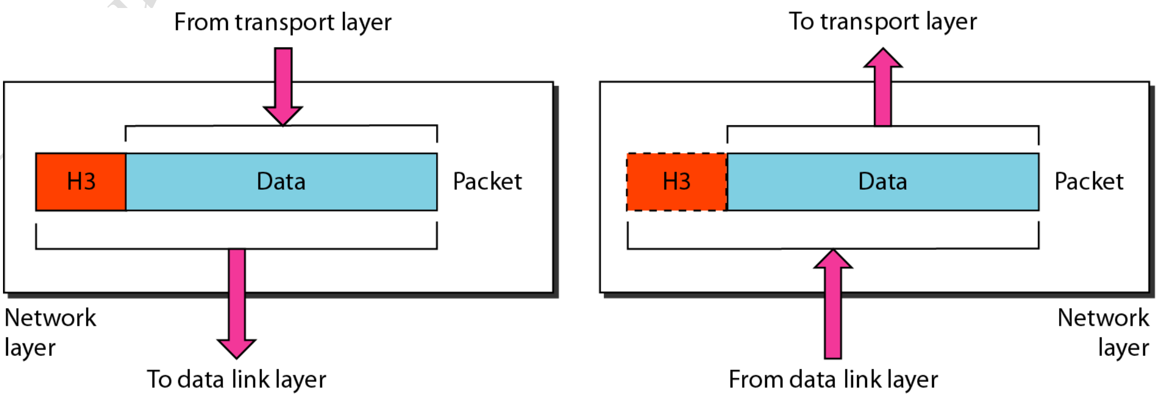

Figure 2.8 : ***Network layer***

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

As the figure (2.9) , now we need a source-to-destination delivery.

- The network layer at A sends the packet to the network layer at B. When the packet arrives at router B, the router makes a decision based on the final destination (F) of the packet.
- Router B uses its routing table to find that the next hop is router E.
- The network layer at B, therefore, sends the packet to the network layer at E.
- The network layer at E, in tum, sends the packet to the network layer at F.

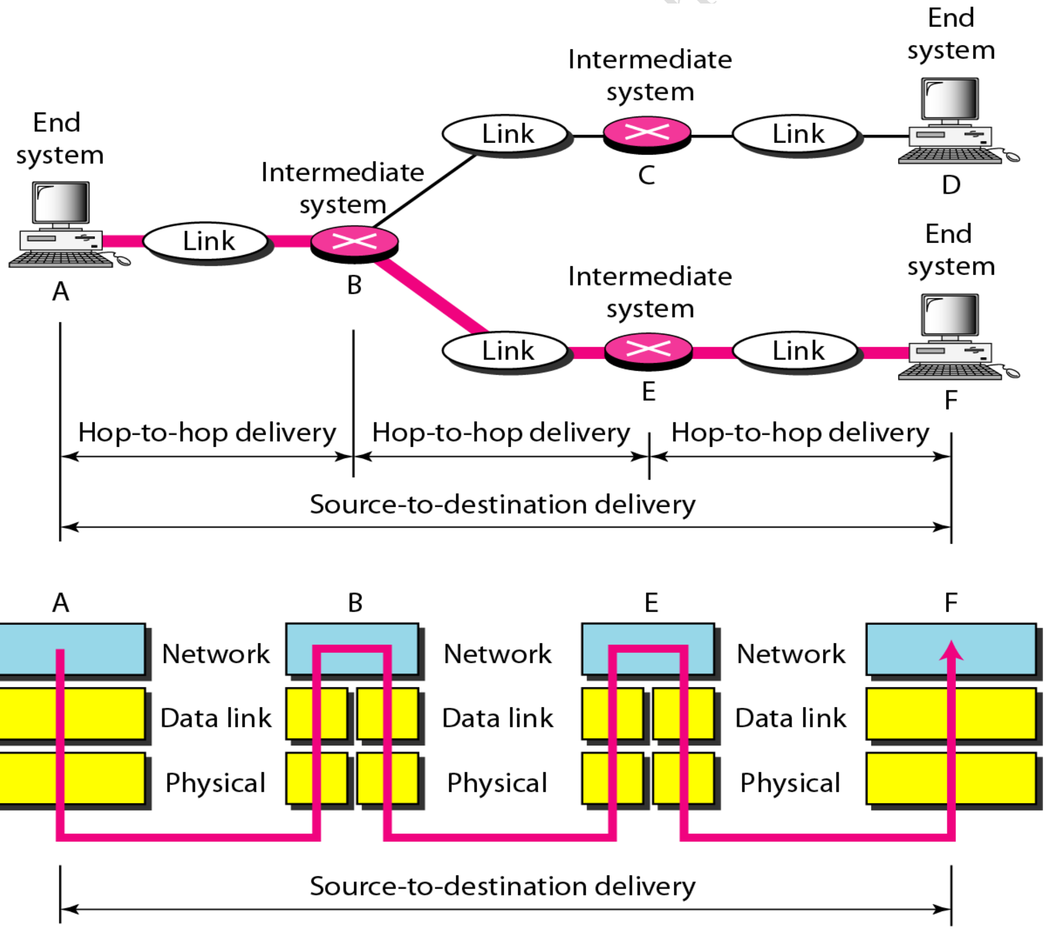

Figure 2.9 : *Source-to-destination delivery*

Transport Layer

- The transport layer is responsible for process-to-process delivery of the entire message.
- A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does.
- The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.
- Figure 2.10 shows the relationship of the transport layer to the network and session layers.
- Other responsibilities of the transport layer include the following:
    - **Service-point addressing.**
    - **Segmentation and reassembly.**
    - **Connection control.**
    - **Flow control.**
    - **Error control.**

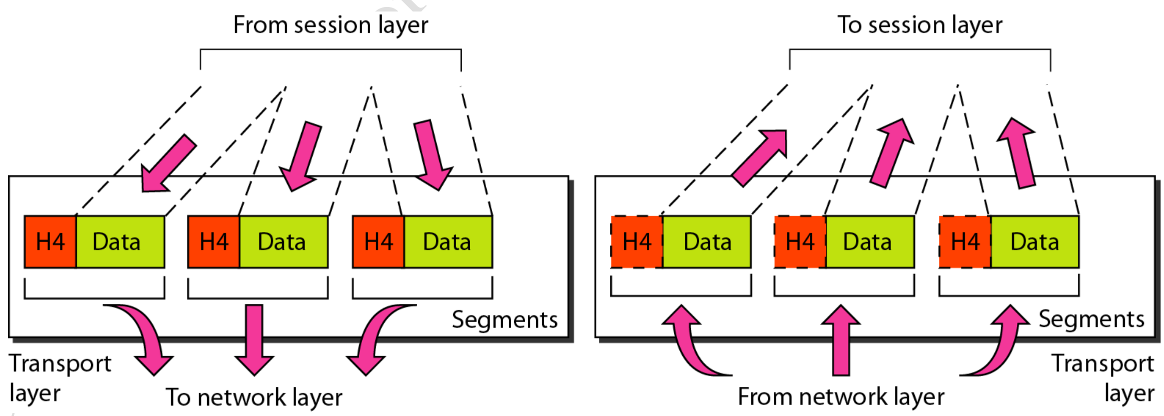

Figure 2.10 : Transport layer

The transport layer is responsible for the delivery of a message from one process to another.

Other responsibilities of the transport layer include the following:

- **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 illustrates process-to-process delivery by the transport layer

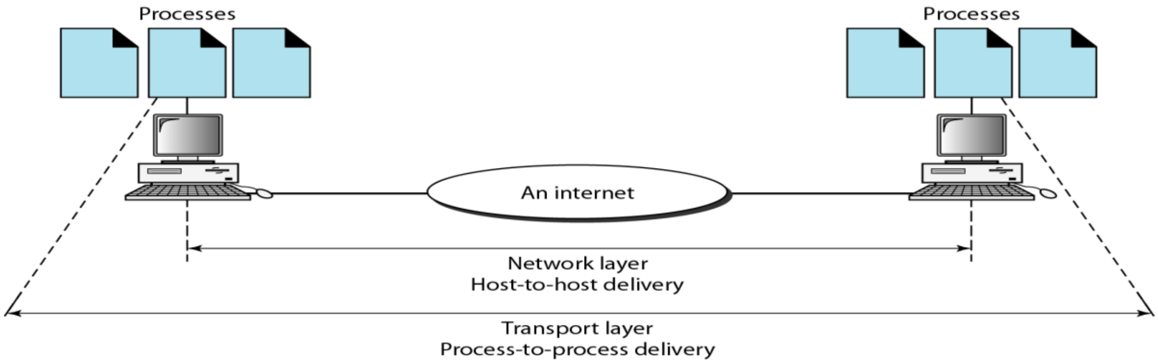

Figure 2.11 : ***Reliable process-to-process delivery of a message***

Session Layer

- The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes.
- The session layer is the network dialog controller.
- It establishes, maintains, and synchronizes the interaction among communicating systems.
- Figure 2.12 illustrates the relationship of the session layer to the transport and presentation layers.
- Specific responsibilities of the session layer include the following:
  - **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 syn-Chronization 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

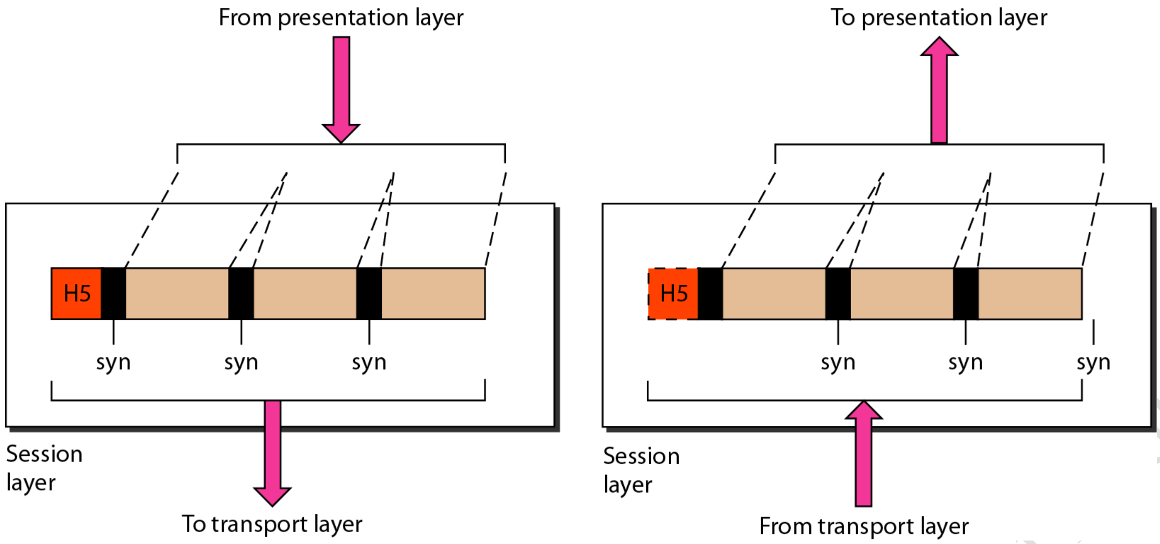

Figure 2.12 : *Session layer*

The session layer is responsible for dialog control and synchronization.

<u>Presentation Layer</u>

- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
- Figure 2.13 shows the relationship between the presentation layer and the application and session layers.
- Specific responsibilities of the presentation layer include the following:
- **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.

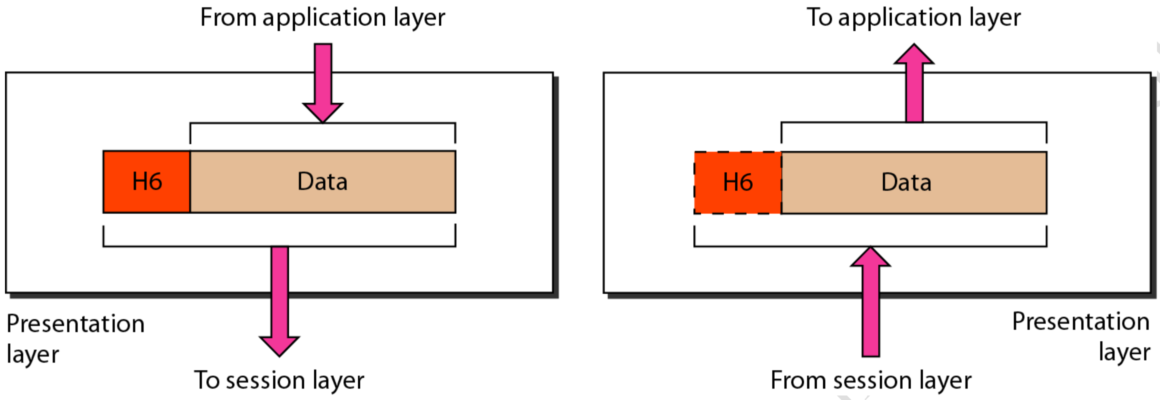

Figure 2.13 : ***Presentation layer***

The presentation layer is responsible for translation, compression, and encryption.

Application Layer

- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- Figure 2.14 shows the relationship of the application layer to the user and the presentation layer.
- Of the many application services available, the figure shows only three:
- **XAOO** (message-handling services), X.500 (directory services), and file transfer, access, and management **(FTAM).** The user in this example employs **XAOO** to send an e-mail message.
- Specific services provided by the application layer include the following:
    - **Network virtual terminal.**

- **File transfer, access, and management**
- **Mail services.**
- **Directory services.**

Specific services provided by the application layer include the following:

- **Network virtual terminal**. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
- **File transfer, access, and management**. This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services**. This application provides the basis for e-mail forwarding and storage.
- **Directory services**. This application provides distributed database sources and access for global information about various objects and services.

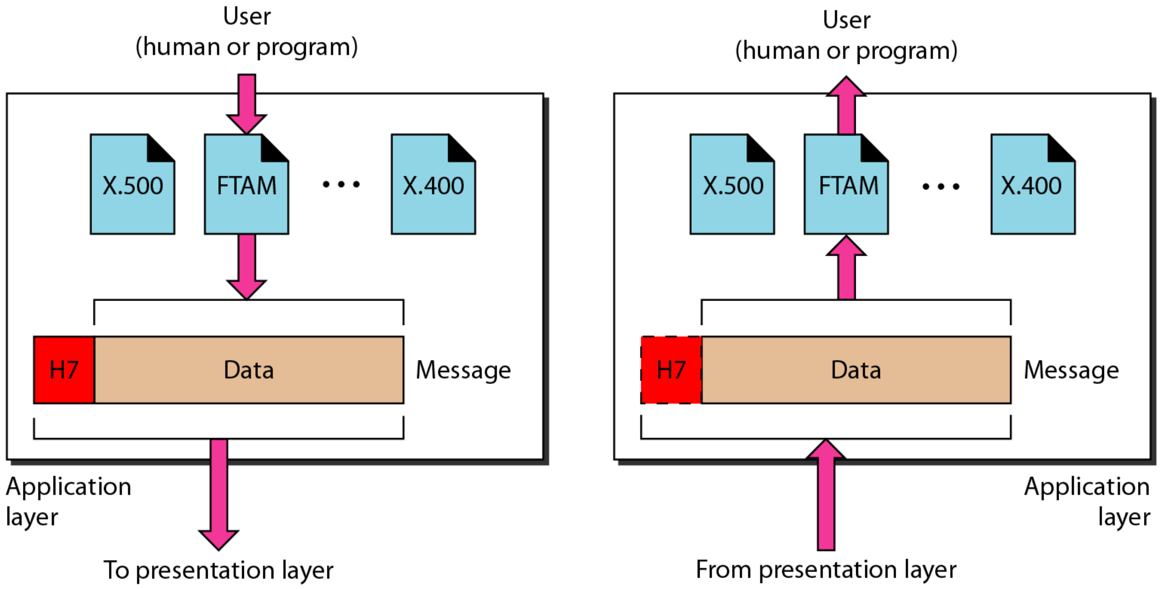

Figure 2.14 : ***Application layer***

The application layer is responsible for providing services to the user.

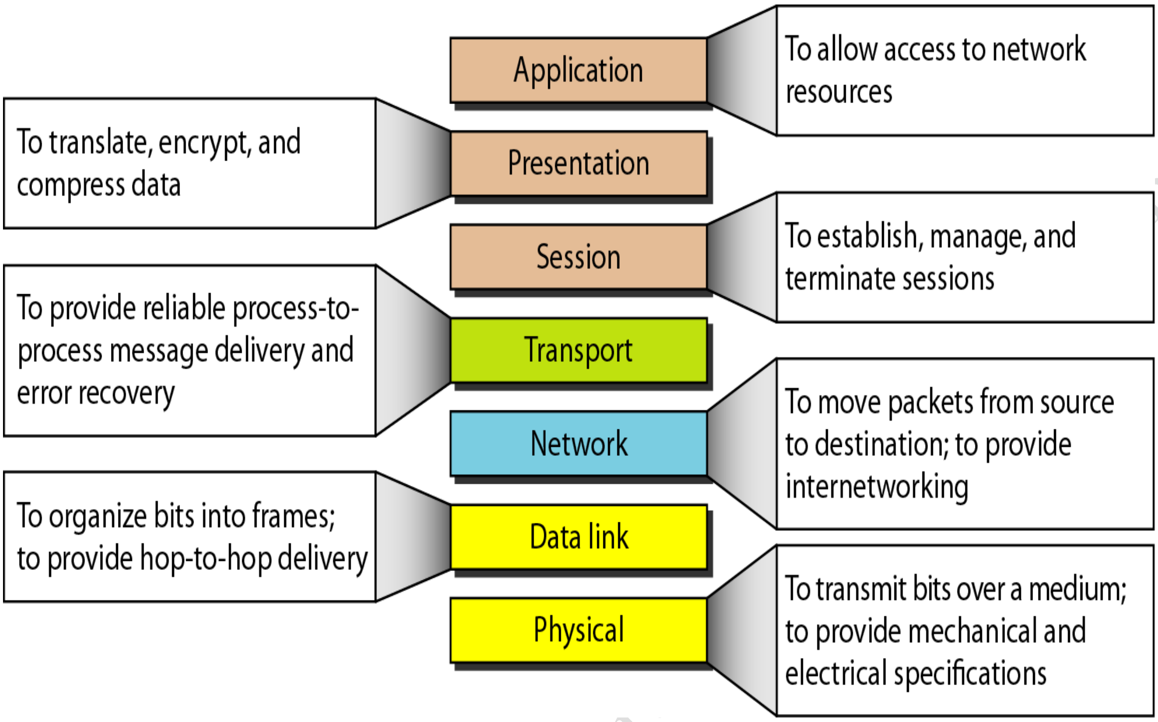

Figure 2.15 : *Summary of duties for each layer*

2. 4 TCP/IP PROTOCOL SUITE

The layers in the TCP/IP protocol suite (مجموعة)do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

Topics discussed in this section:

Physical and Data Link Layers
Network Layer
Transport Layer
Application Layer

- TCP/IP is a hierarchical protocol made up of **interactive modules**, each of which provides a specific functionality; however, the modules are not necessarily interdependent.
- Whereas the OSI model specifies which **functions belong to each of its layers,** the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system.
- At the transport layer, TCP/IP defines three protocols:
    - **Transmission Control Protocol (TCP)**
    - **User Datagram Protocol (UDP)**
    - **Stream Control Transmission Protocol (SCTP).**
- At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.
- At the physical and data link layers, TCPIIP does not define any specific protocol. It supports all the standard and proprietary protocols.
- A network in a TCPIIP internetwork can be a local-area network or a wide-area network.

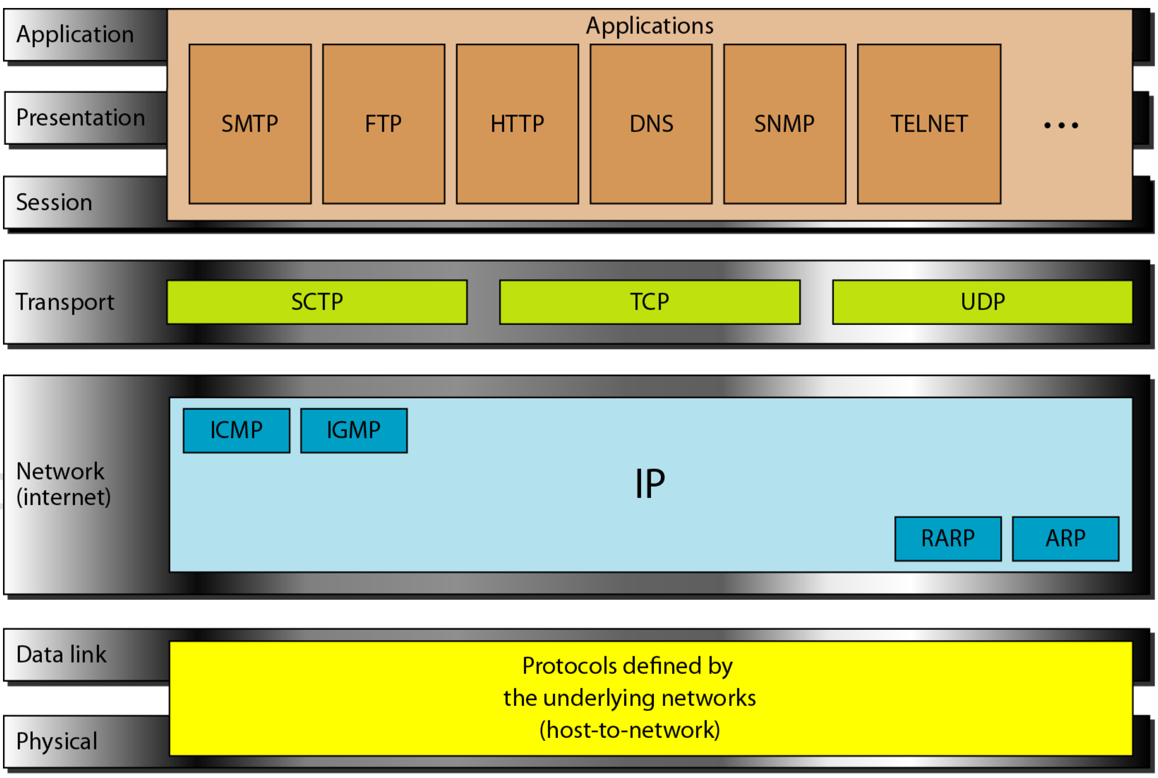

Figure 2.16 : ***TCP/IP and OSI model***

2.5 ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.

Topics discussed in this section:

Physical Addresses

Logical Addresses

Port Addresses

Specific Addresses

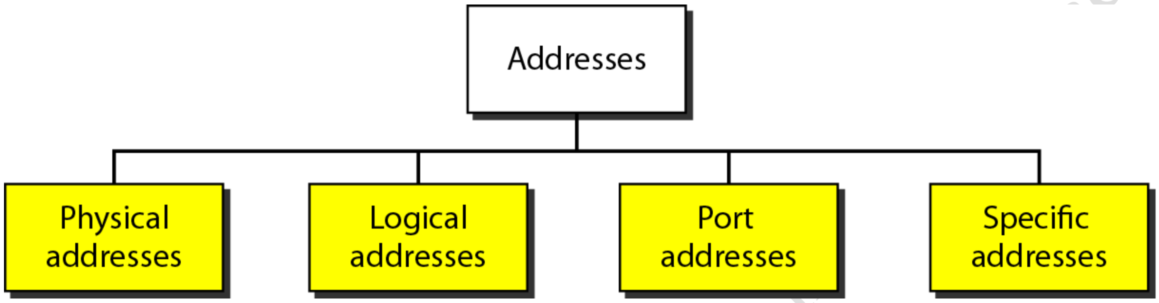

Figure 2.17 : ***Addresses in TCP/IP***

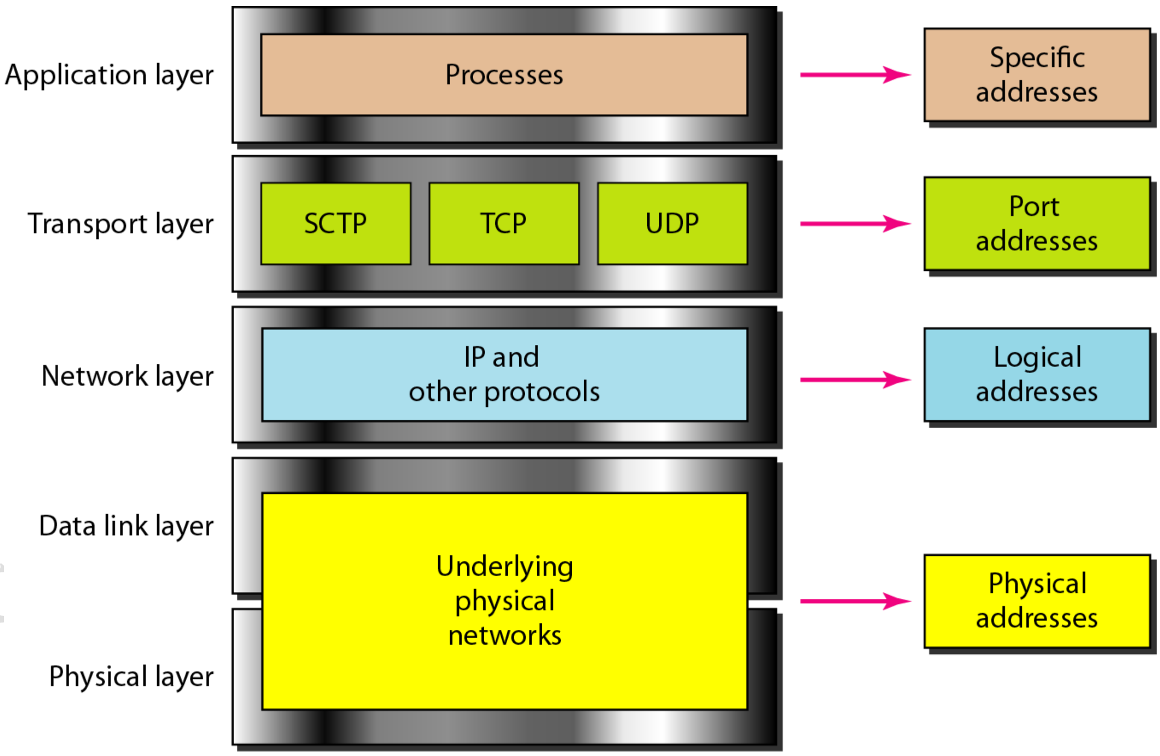

Figure 2.18 : ***Relationship of layers and addresses in TCP/IP***

Physical Address

- The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
- It is included in the frame used by the data link layer.
- It is the lowest-level address.
- The physical addresses have authority over the network (LAN or WAN).
- The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).

Example 2.1

In Figure 2.19 a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.

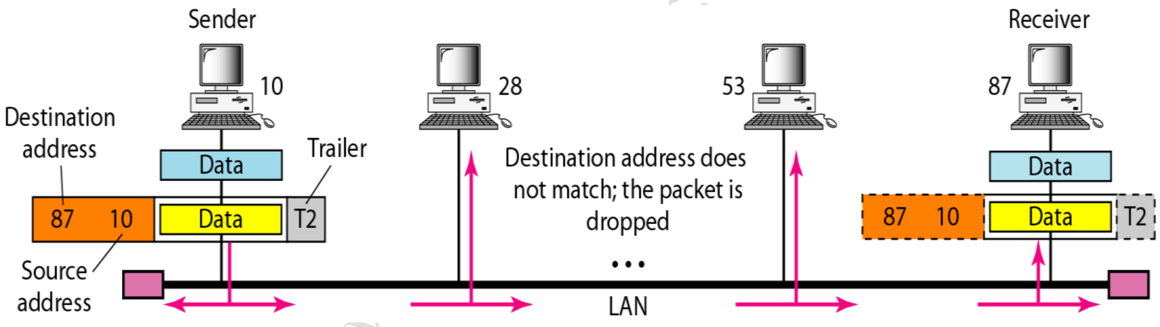

Figure 2.19: ***Physical addresses***

Example 2.2

Most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

07:01:02:01:2C:4B
A 6-byte (12 hexadecimal digits) physical address.

Logical Addresses

- Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats.
- A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.
- A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet.
- No two publicly addressed and visible hosts on the Internet can have the same IP address.

<u>Example 2.3</u>

Figure 2.20 shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection.

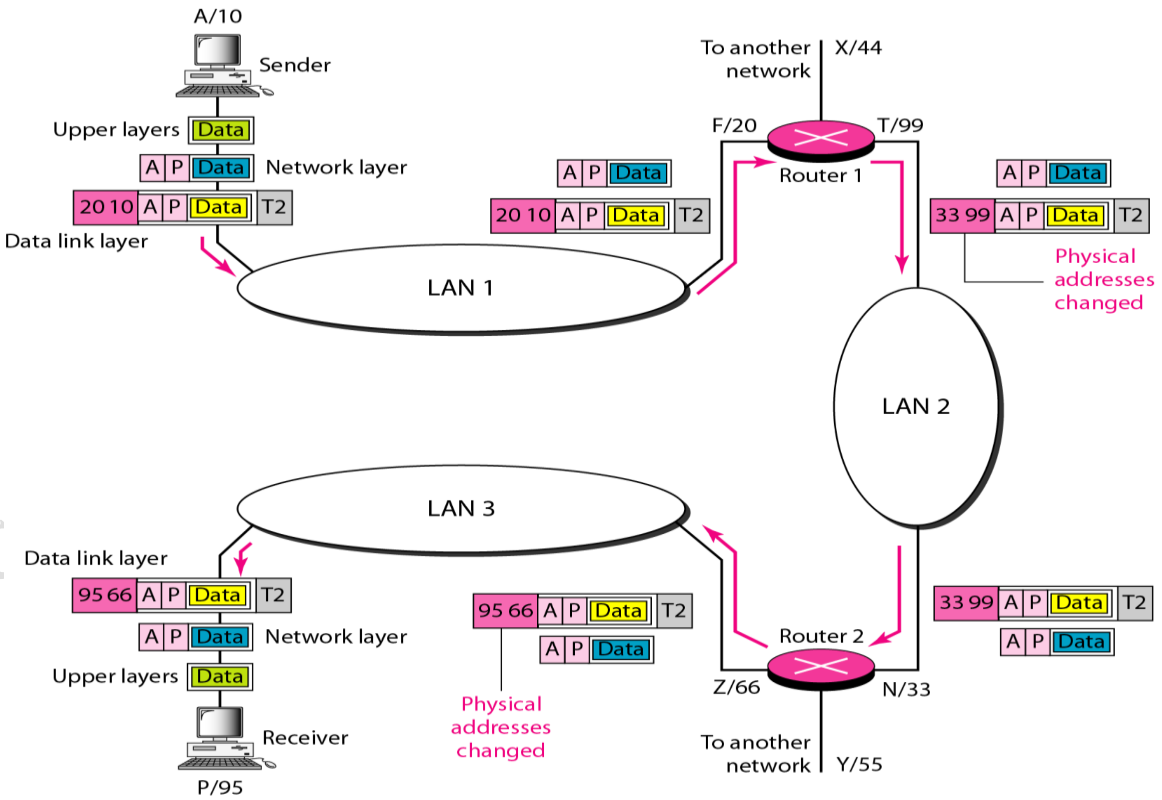

Figure 2.20 : ***IP addresses***

Port Addresses

- The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. **A system that sends nothing but data from one computer to another is not complete.**
- Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the **File Transfer Protocol (FTP).**
- For these processes to receive data simultaneously, **we need a method to label the different processes.**
- In other words, they need addresses. **In the TCPIIP architecture, the label assigned to a process is called a port address. A port address in TCPIIP is 16 bits in length.**

<u>Example 2.4</u>

Figure 2.21 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

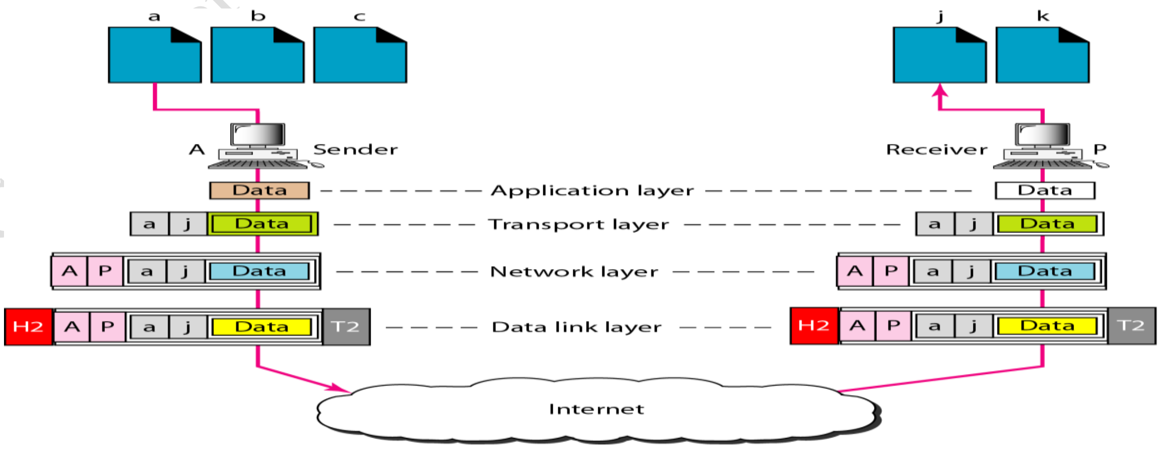

Figure 2.21: ***Port addresses***

Note

The physical addresses will change from hop to hop, but the logical addresses usually remain the same.

Example 2.5

A port address is a 16-bit address represented by one decimal number as shown.

753

A 16-bit port address represented as one single number.

Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific address.
- Examples include the e-mail address (for example, forouzan@fhda.edu) and the Universal Resource Locator (URL) (for example, ww.mhhe.com). The first defines the recipient of an e-mail ; the second is used to find a document on the World Wide Web .
- These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.