

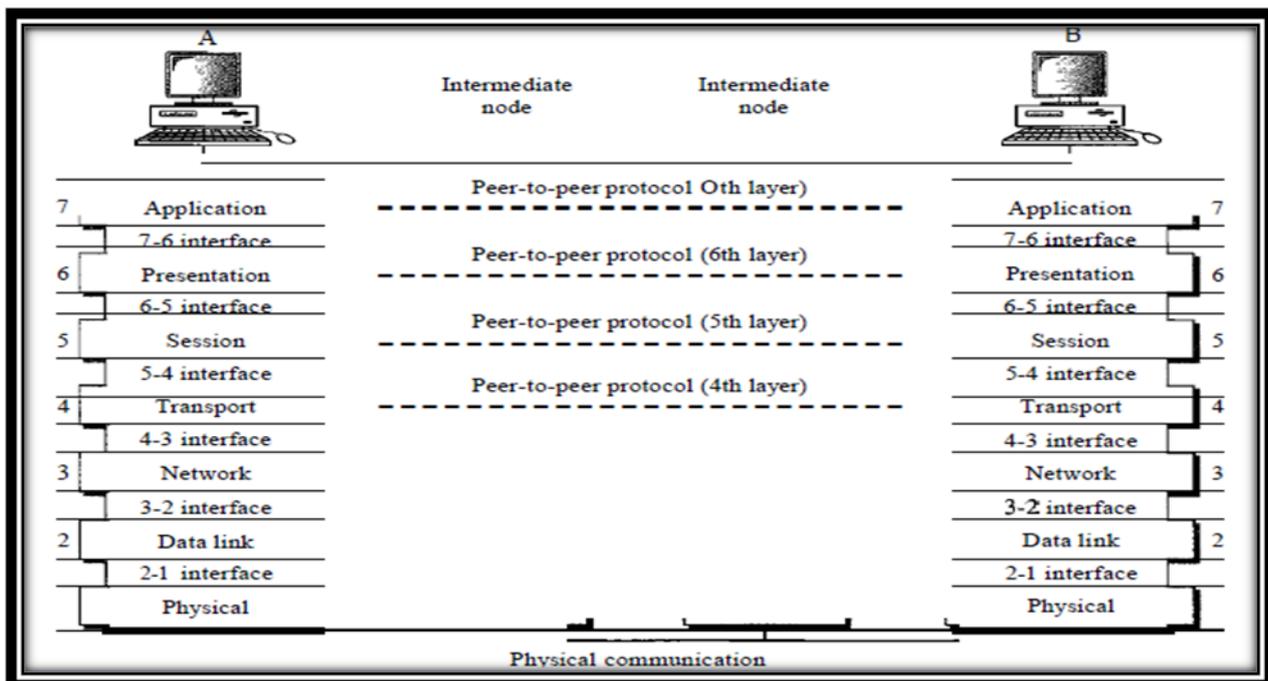
## **Layered Architecture**

The OSI model is composed of seven ordered layers: ***physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7)***. Figure (3) shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model. In *developing* the model, the designers distilled the process of transmitting data to its most fundamental elements. They identified which networking functions had related uses and collected those functions into discrete groups that became the layers. Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible. Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems. Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer  $x$  on one machine communicates with layer  $x$  on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

## **Peer-to-Peer Processes**

At the physical layer, communication is direct: In Figure (3), device A sends a stream of bits to device B (through intermediate nodes). At the higher layers, however, communication must move down through the layers on device A, over to device B, and then back up through the layers. 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. At layer 1 the entire package is converted to a form that can be transmitted to the receiving device. At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it. For example, layer 2 removes the data meant for it, then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.



*Figure (3) the layers involved when a message is sent from device A to device B.*

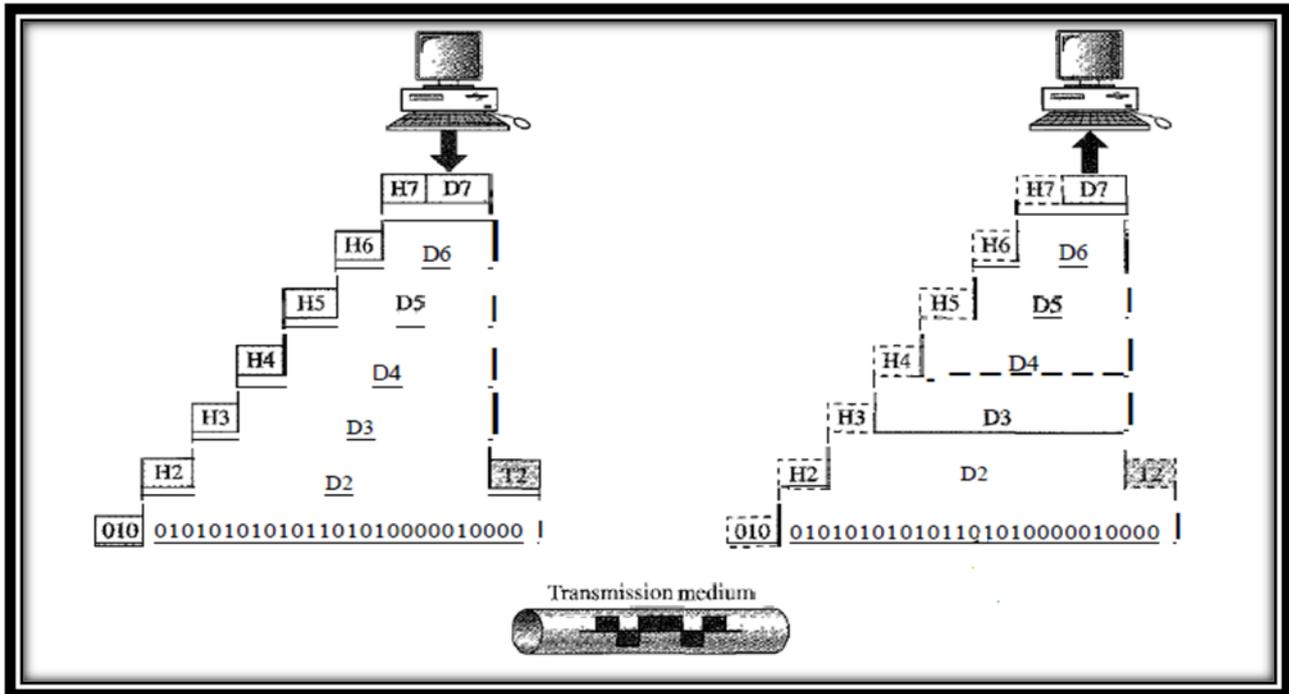
### Interfaces Between Layers

The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers. Each interface defines the information and services a layer must provide for the layer above it. Well-defined interfaces and layer functions provide modularity to a network. 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.

### **Organization of the Layers**

The seven layers can be thought of as belonging to **three subgroups**. **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*). **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. **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**. The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware. In Figure (4), which gives an overall view of the OSI layers, 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.



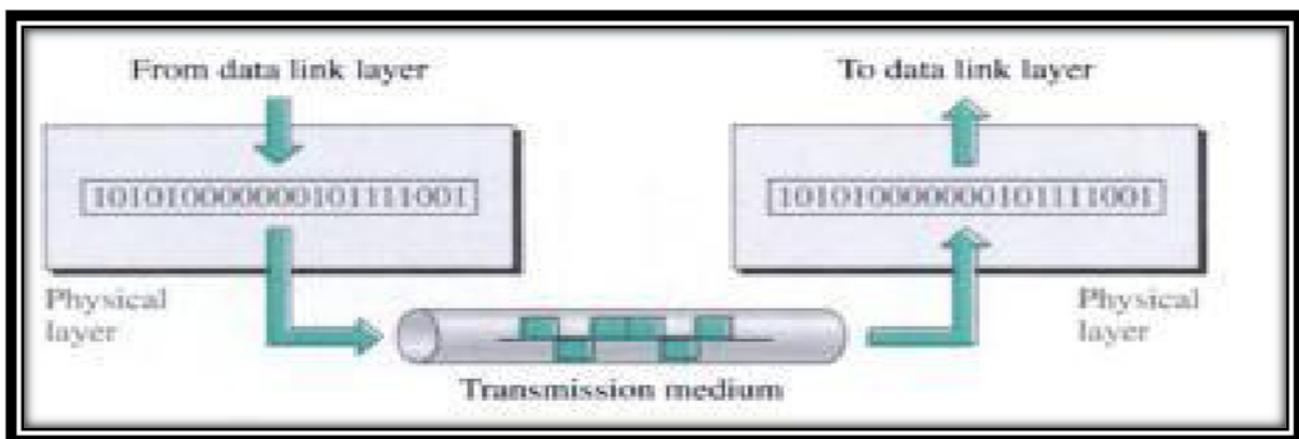
*Figure (4) which gives an overall view of the OSI layers*

## **FUNCTIONS OF LAYERS**

In this section we briefly describe the functions of each layer in 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 (*The physical layer is responsible for movements of individual bits from one hop (node) to the next.*) It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur. Figure (5) shows the position of the physical layer with respect to the transmission medium and the data link layer.



**Figure (5) position of the physical layer**

The physical layer is also concerned with the following:

**1- 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.

**2- Representation of bits :** The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded

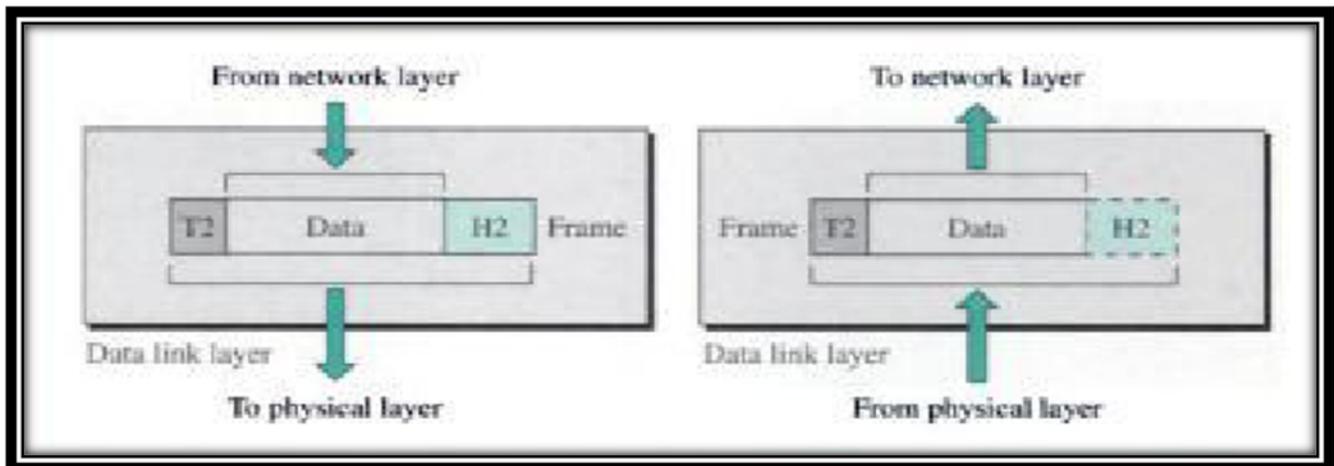
into signals--electrical or optical. The physical layer defines the type of encoding (how 0s and 1s are changed to signals).

**3- 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.

**4- Synchronization of bit :** 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.

### **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 (6) shows the relationship of the data link layer to the network and physical layers



*Figure (6) shows the relationship of the data link layer to the network and physical layers*

*(The data link layer is responsible for moving frames from one hop (node) to the next).* Other responsibilities of the data link layer include the following:

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

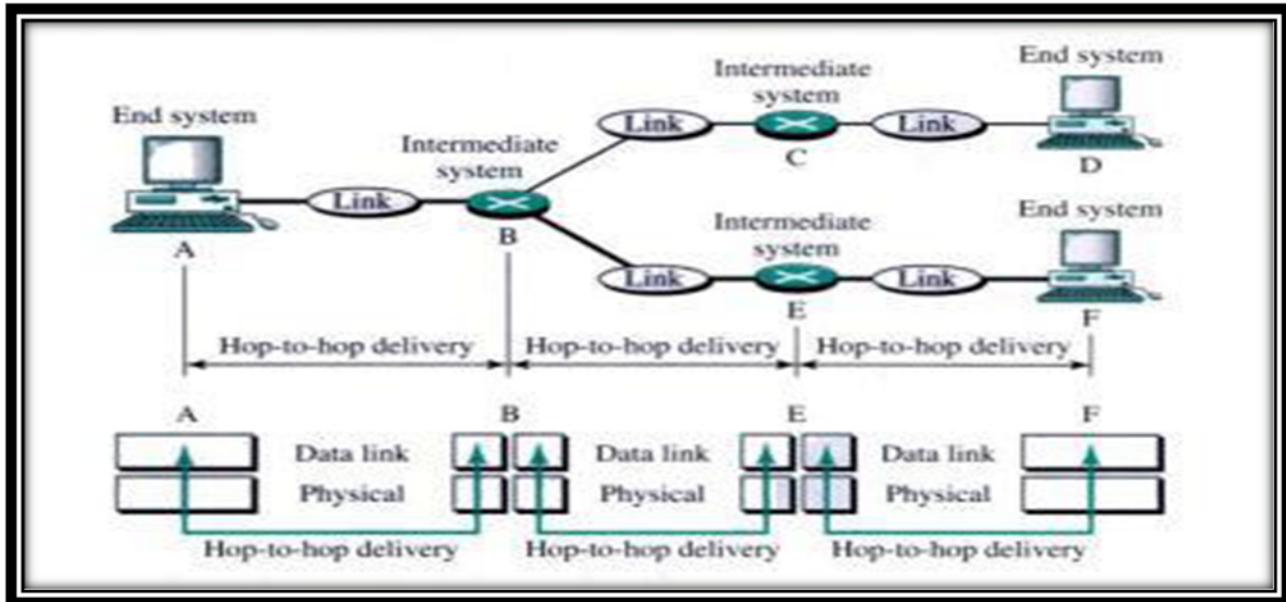
**2- Physical addressing:** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of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

**3- 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.

**4- 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.

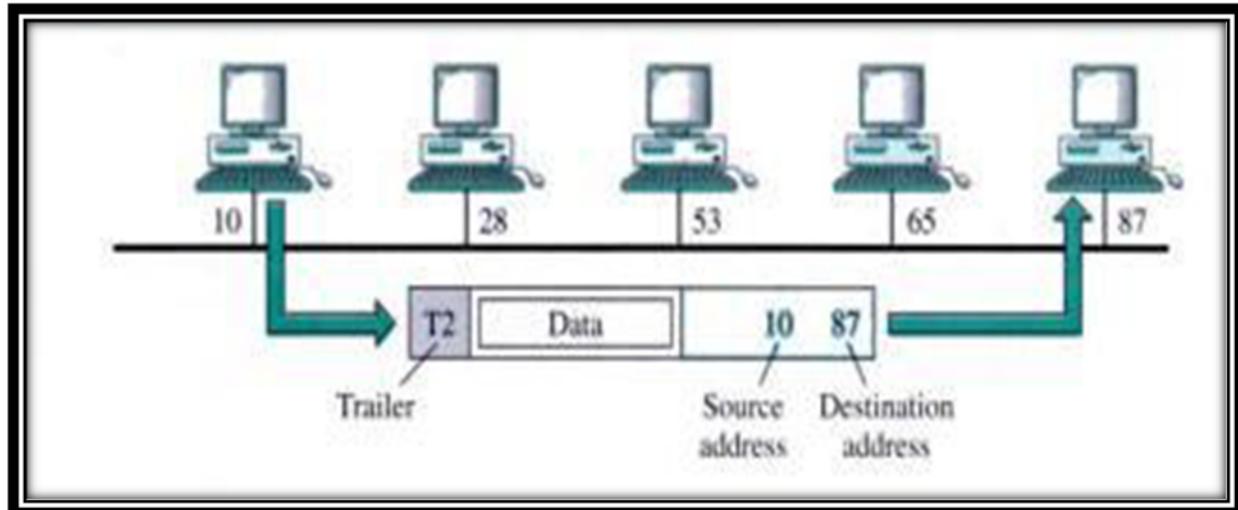
**5- Access control:** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Figure (7) illustrates hop-to-hop (node-to-node) delivery by the data link layer. As the figure 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 (7) illustrates hop-to-hop (node-to-node) delivery by the data link layer*

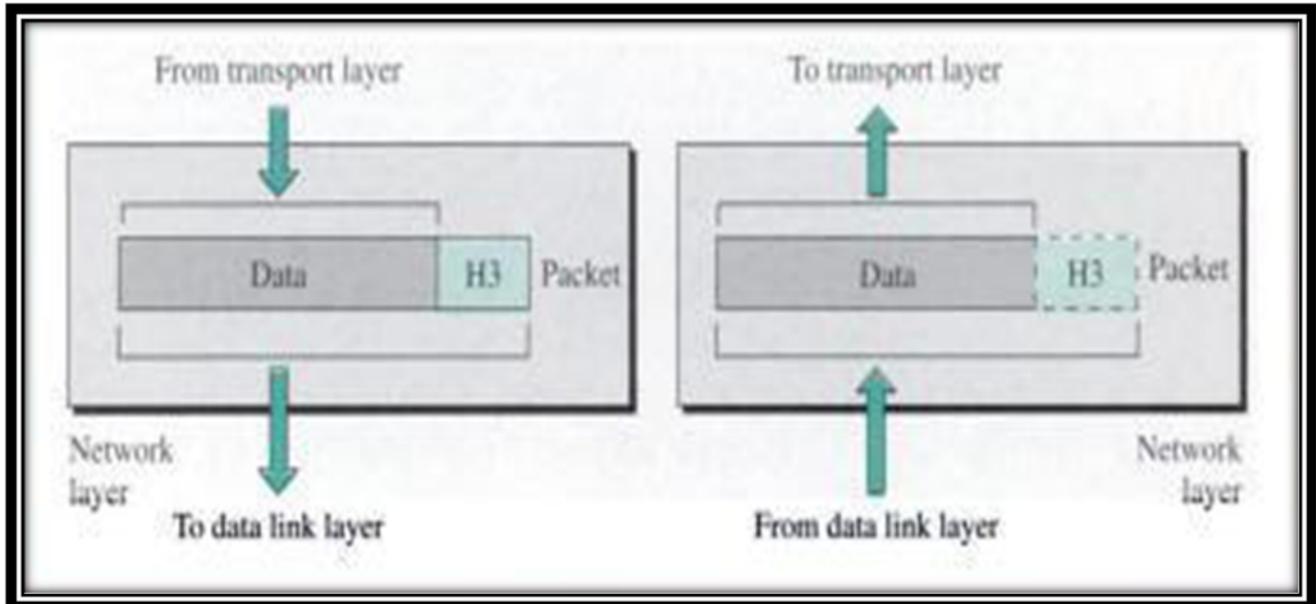
**Example(1) :** In figure (8) a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link. At the data link level this frame contains physical addresses in the header. These are only addresses needed. The trailer usually contains extra bits needed for detection.



*Figure (8) Example(1)*

### 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 (9) shows the relationship of the network layer to the data link and transport layers.



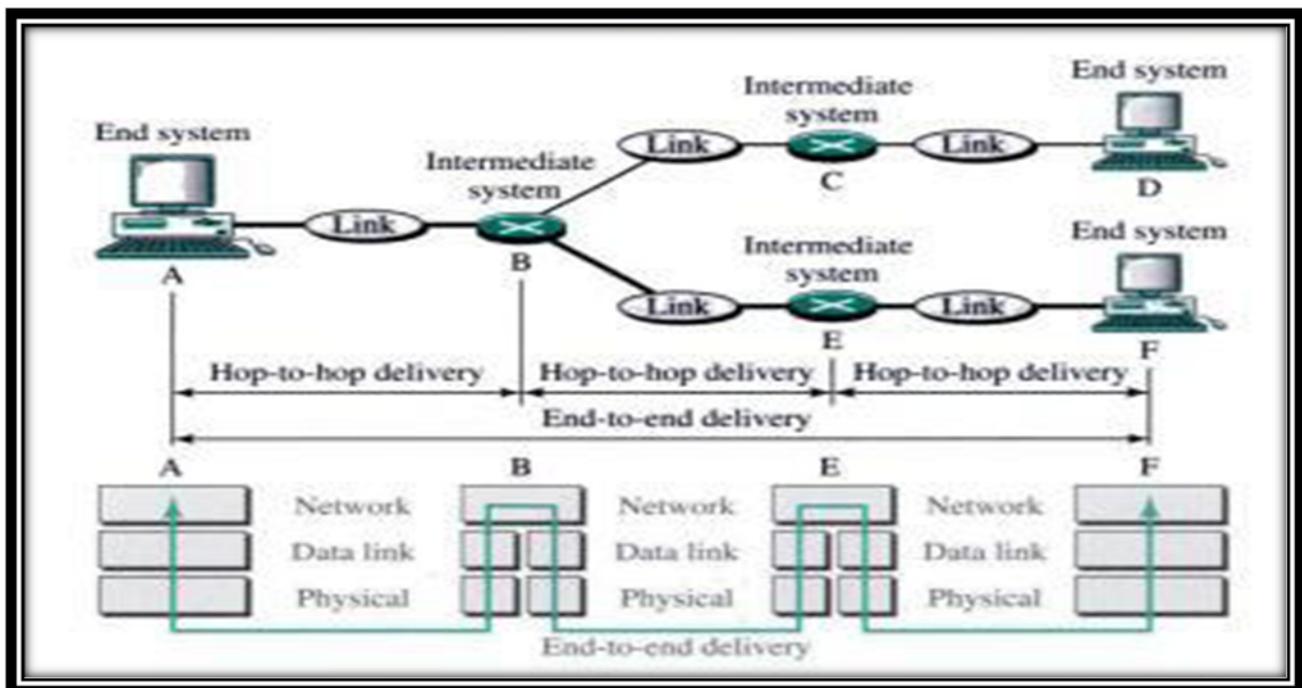
**Figure (9) The relationship of the network layer to the data link and transport layers**

*The network layer is responsible for the delivery of individual packets from the source host to the destination host.* Other responsibilities of the network layer include the following:

**1- 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.

**2- Routing:** When independent networks or links are connected to create *internetworks* (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 (10) illustrates end-to-end delivery by the network layer. As the figure shows, 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 turn, sends the packet to the network layer at F.



**Figure (10) end-to-end delivery by the network layer**

**Example 2:** In figure (11) we want to send data from anode with network address 10 ,located on one LAN, to anode with network address P and physical address 95, located on another LAN .because the two devices are located on different networks, we cannot use physical addresses only :the physical addresses local jurisdiction. What we need here are universal addresses that can pass through the LAN boundaries. The network (logical) addresses have this characteristic. The packet at the network layer

contains the logical addresses . Which remain the same from the original source to the final destination (A&P. respectively in the figure ). They will not change when we go from network to network. However, the physical addresses will change as the packet moves from one network to another.

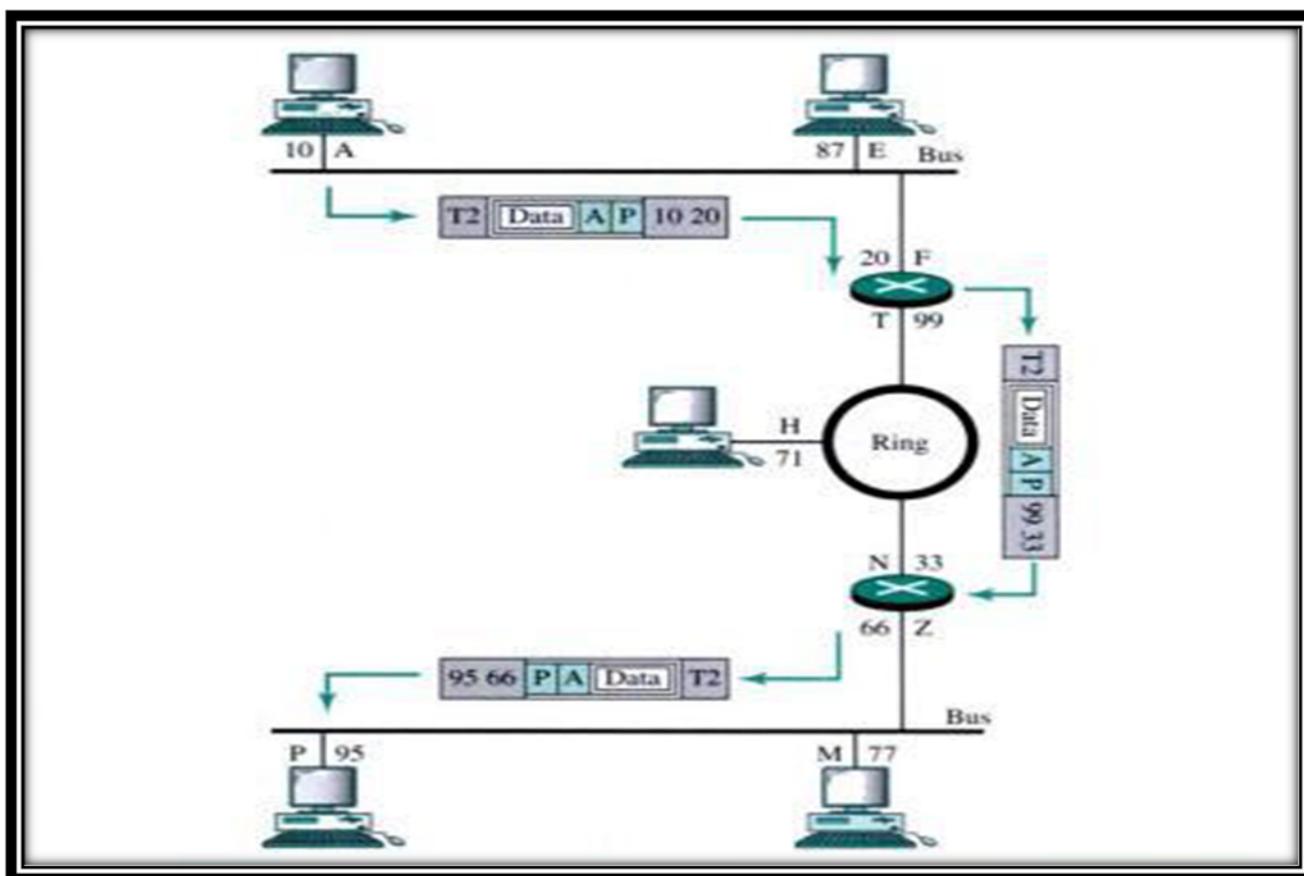
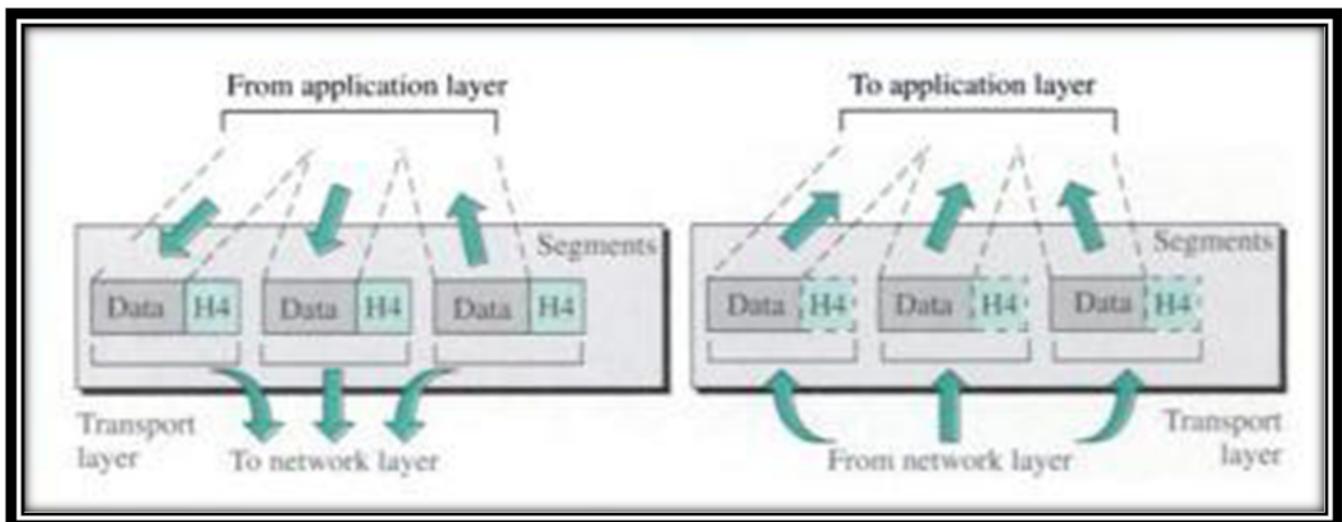


Figure (11) Example 2

### 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 (12) shows the relationship of the transport layer to the network and session layers.



(12) The relationship of the transport layer to the network and session layers.

**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:

**1- 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

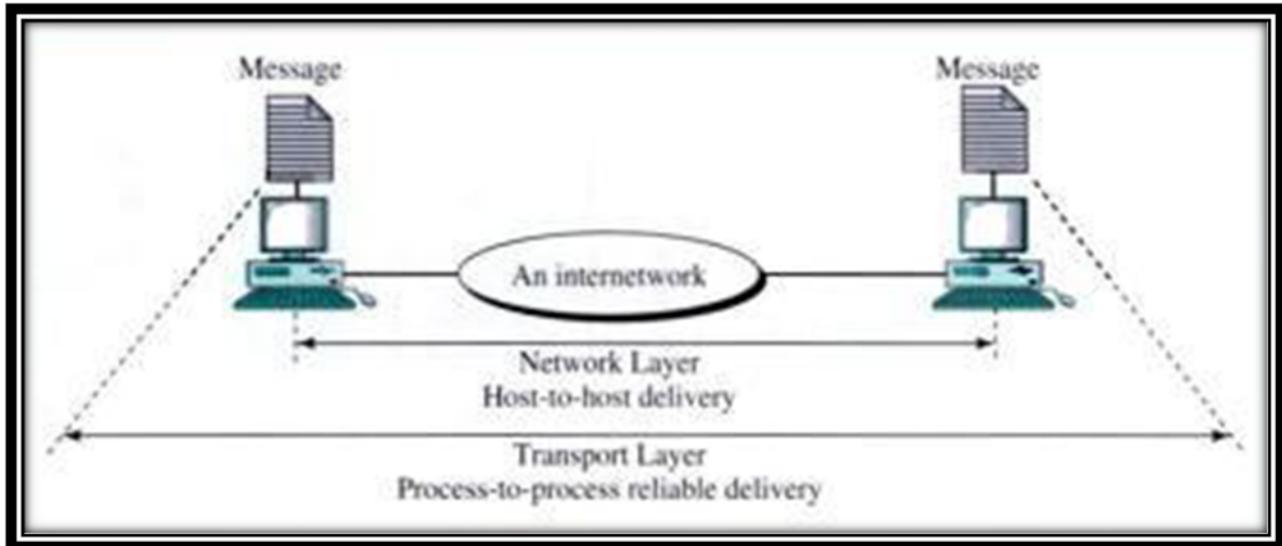
address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

**2-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.

**3-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.

**4-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.

**5- 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 (13) illustrates process-to-process delivery by the transport layer.



*Figure (13) process-to-process delivery by the transport layer.*

### 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.

***The session layer is responsible for dialog control and synchronization.*** Specific responsibilities of the session layer include the following:

***1- 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.

**2- 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.

### **Presentation Layer**

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. ***The presentation layer is responsible for translation, compression, and encryption.*** Specific responsibilities of the presentation layer include the following:

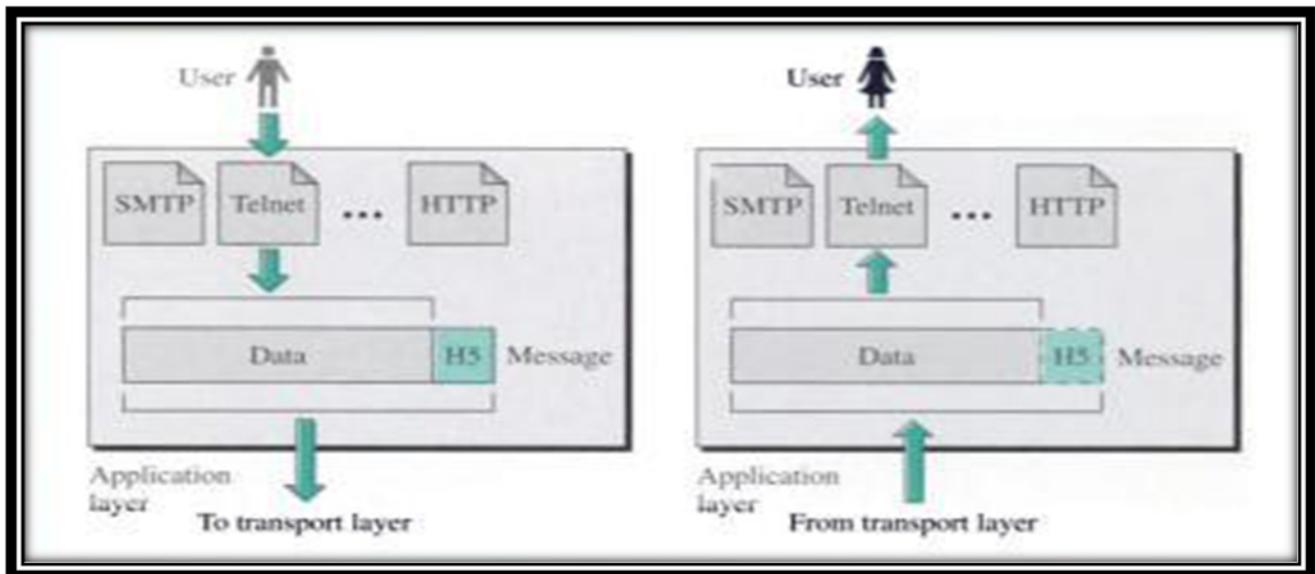
**1- Translation:** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation 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.

**2- 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.

**3- 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.

### **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 (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.



**Figure (14) The relationship of the application layer to the user and the presentation layer**

**The application layer is responsible for providing services to the user.** Specific services provided by the application layer include the following:

**1-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.

**2- 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

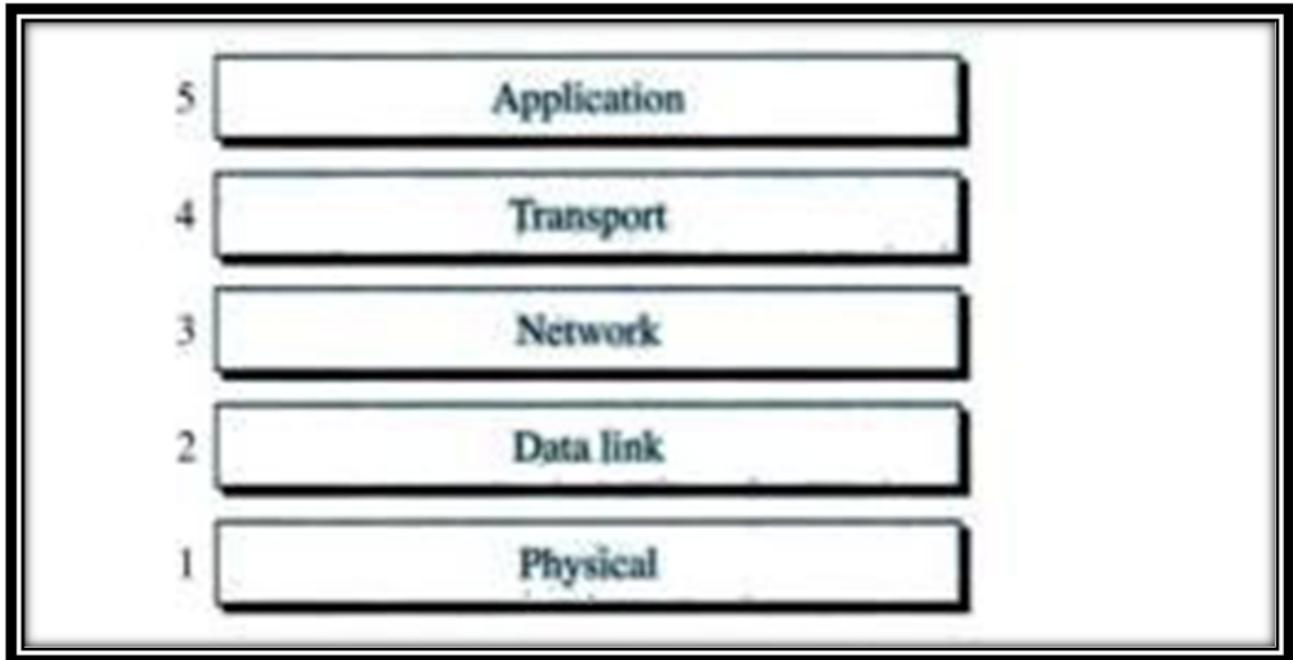
computer for use in the local computer, and to manage or control files in a remote computer locally.

**3- Mail services:** This application provides the basis for e-mail forwarding and storage.

**4- Directory services:** This application provides distributed database sources and access for global information about various objects and services.

### **Internet Model**

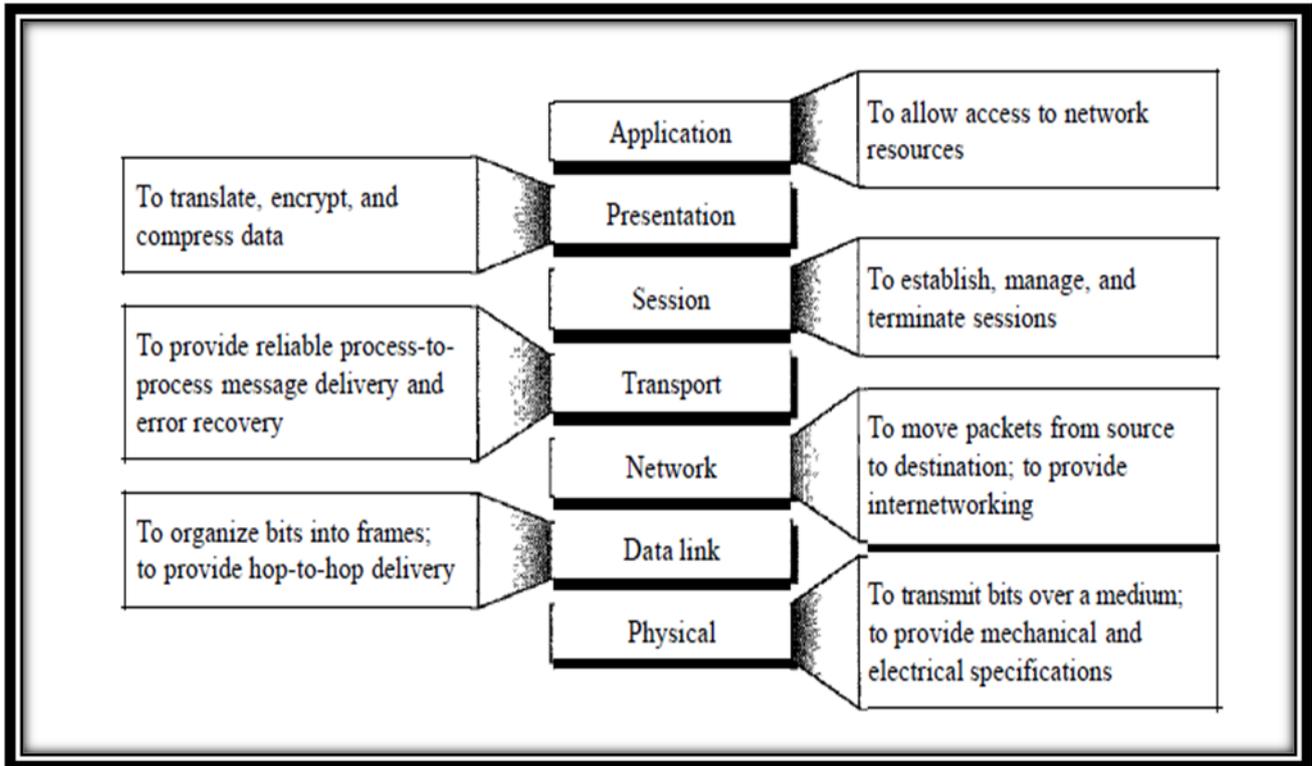
The layered protocol stack that dominates data communications and networking today is the **five \_layer Internet model**, sometimes called the **TCP\IP protocol suit** (see figure 15). The model is composed of five ordered layers :physical layer, data link layer, network layer, transport layer and application layer. Figure (15) shows the layers involved when a message is sent from device A to device B.



*Figure (15) Internet Model layers*

**Summary of Layers**

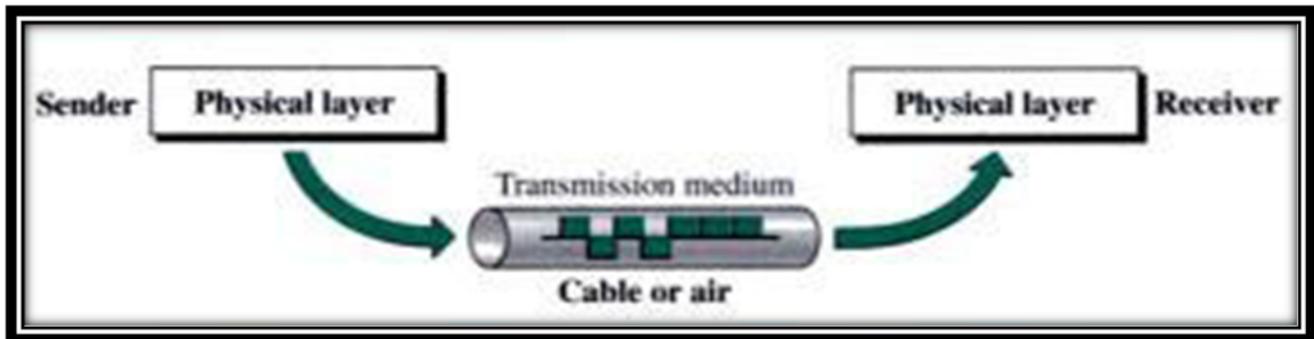
Figure (16) shows a summary of duties for each layer.



*Figure (16) Summary of layers*

## Transmission Media

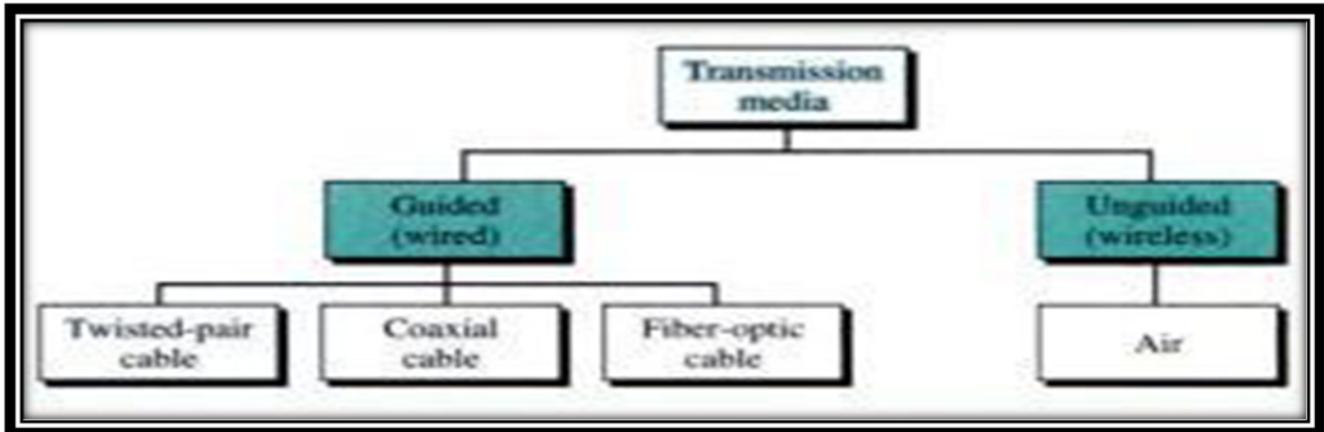
Transmission media are actually located below the physical layer and are directly controlled by the physical layer. You could say that transmission media belong to layer zero. Figure (1) shows the position of transmission media in relation to the physical layer.



*Figure (1) The position of transmission media in relation to the physical layer.*

A transmission **medium** can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air. The air can also be used to convey the message in a smoke signal or semaphore. 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. The use of long-distance communication using electric signals started with the invention of the telegraph by Morse in the 19th century. Communication by telegraph was slow and dependent on a metallic medium. Extending the range of the human voice became possible when the telephone was invented in 1869. Telephone communication at that time also needed a metallic medium to carry the electric signals

that were the result of a conversion from the human voice. The communication was, however, unreliable due to the poor quality of the wires. The lines were often noisy and the technology was unsophisticated. Wireless communication started in 1895 when Hertz was able to send high frequency signals. Later, Marconi devised a method to send telegraph-type messages over the Atlantic Ocean. We have come a long way. Better metallic media have been invented (twisted pair and coaxial cables, for example). The use of optical fibers has increased the data rate incredibly. Free space (air, vacuum, and water) is used more efficiently, in part due to the technologies (such as modulation and multiplexing). computers and other telecommunication devices use signals to represent data. These signals are transmitted from one device to another in the form of electromagnetic energy, which is propagated through transmission media. Electromagnetic energy, a combination of electric and magnetic fields vibrating in relation to each other, includes power, radio waves, infrared light, visible light, ultraviolet light, and X, gamma, and cosmic rays. Each of these constitutes a portion of the electromagnetic spectrum. Not all portions of the spectrum are currently usable for telecommunications, however. The media to harness those that are usable are also limited to a few types. 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. Figure (2) shows this taxonomy.



*Figure (2) Classes of transmission media*

### **GUIDED MEDIA**

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

#### **Twisted-Pair Cable**

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure (3)



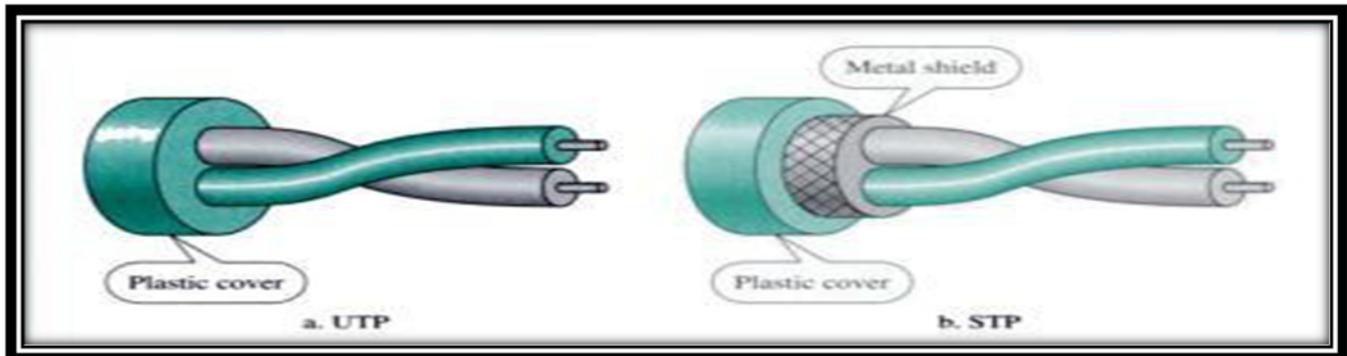
***Figure (3) Twisted-pair cable***

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 sent by the sender on one of the wires, 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 (e.g., one is closer and the other is farther). This results in a difference at the receiver. By twisting the pairs, a balance is maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true. Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly canceled out. From the above discussion, it is clear that the number of twists per unit of length (e.g., inch) has some effect on the quality of the cable.

### **Unshielded Versus Shielded Twisted-Pair Cable**

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(4) shows the difference between UTP and STP. Our discussion focuses primarily on UTP because STP is seldom used outside of IBM.



***Figure(4) shows the difference between UTP and STP Categories***

### **Categories**

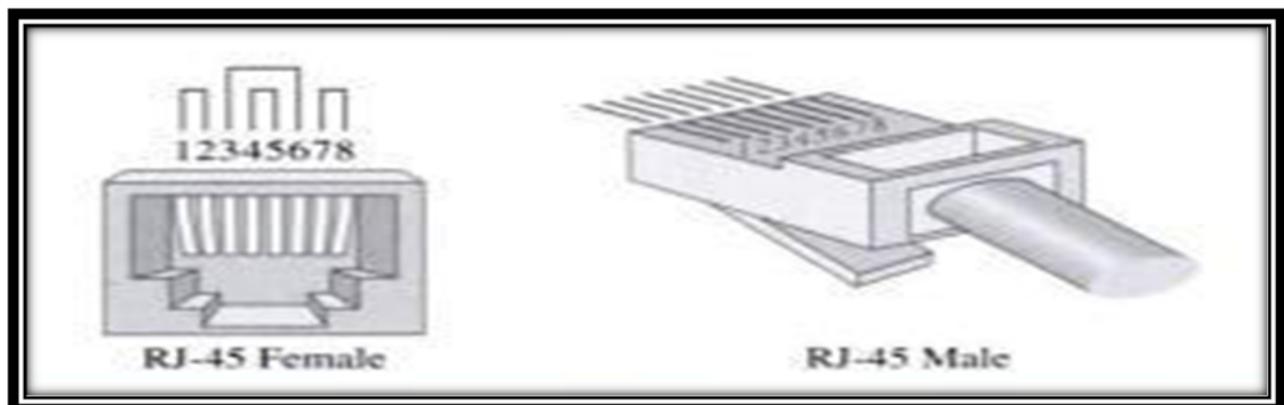
The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories. Categories are determined by cable quality, with 1 as the lowest and 7 as the highest. Each EIA category is suitable for specific uses. Table (!) shows these categories.

**Table (1) *Categories of unshielded twisted-pair cables***

Category	Bandwidth	Data Rate	Digital/Analog	Use
1	Very low	<100 Kbps	Analog	Telephone
2	<2 MHz	2 Mbps	Analog/digital	T-1 lines
3	16 MHz	10 Mbps	Digital	LANs
4	20 MHz	20 Mbps	Digital	LANs
5	100 MHz	100 Mbps	Digital	LANs
6 (draft)	200 MHz	200 Mbps	Digital	LANs
7 (draft)	600 MHz	600 Mbps	Digital	LANs

### Connectors

The most common UTP connector is RJ45 (RJ stands for registered jack), as shown in Figure (5). The RJ45 is a keyed connector, meaning the connector can be inserted in only one way.



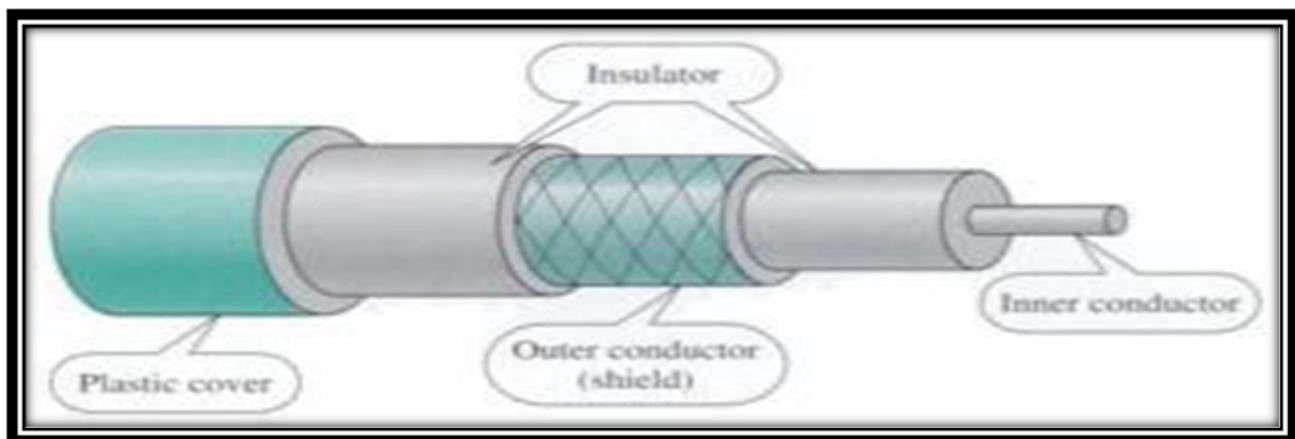
*Figure (5) UTP connector*

## Applications

Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop—the line that connects subscribers to the central telephone office—commonly consists of unshielded twisted-pair cables.

## Coaxial 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 6).



*Figure (6) Coaxial cable*

## Coaxial Cable Standards

Coaxial cables are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function, as shown in Table 2.

***Table (2) Categories of coaxial cables***

<i>Category</i>	<i>Impedance</i>	<i>use</i>
RG-59	75 $\Omega$	Cable TV
RG-58	50 $\Omega$	Thin Ethernet
RG-11	50 $\Omega$	Thick Ethernet

### **Coaxial Cable Connectors**

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNC), connector. Figure (7) shows three popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator. The BNC connector is used to connect the end of the cable to a device, such as a TV set. The BNC T connector is used in Ethernet networks (to branch out to a connection to a computer or other device). The BNC terminator is used at the end of the cable to prevent the reflection of the signal.