Reference Models:-

There are two important network architecture, the **OSI** reference model and the **TCP/IP** reference model.

- The OSI Model :-

This model is based on a proposed developed by the international standard organization (ISO). The model is called OSI (Open System Interconnecting) because it deals with connecting open system [Systems that are open for communication with other systems]. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

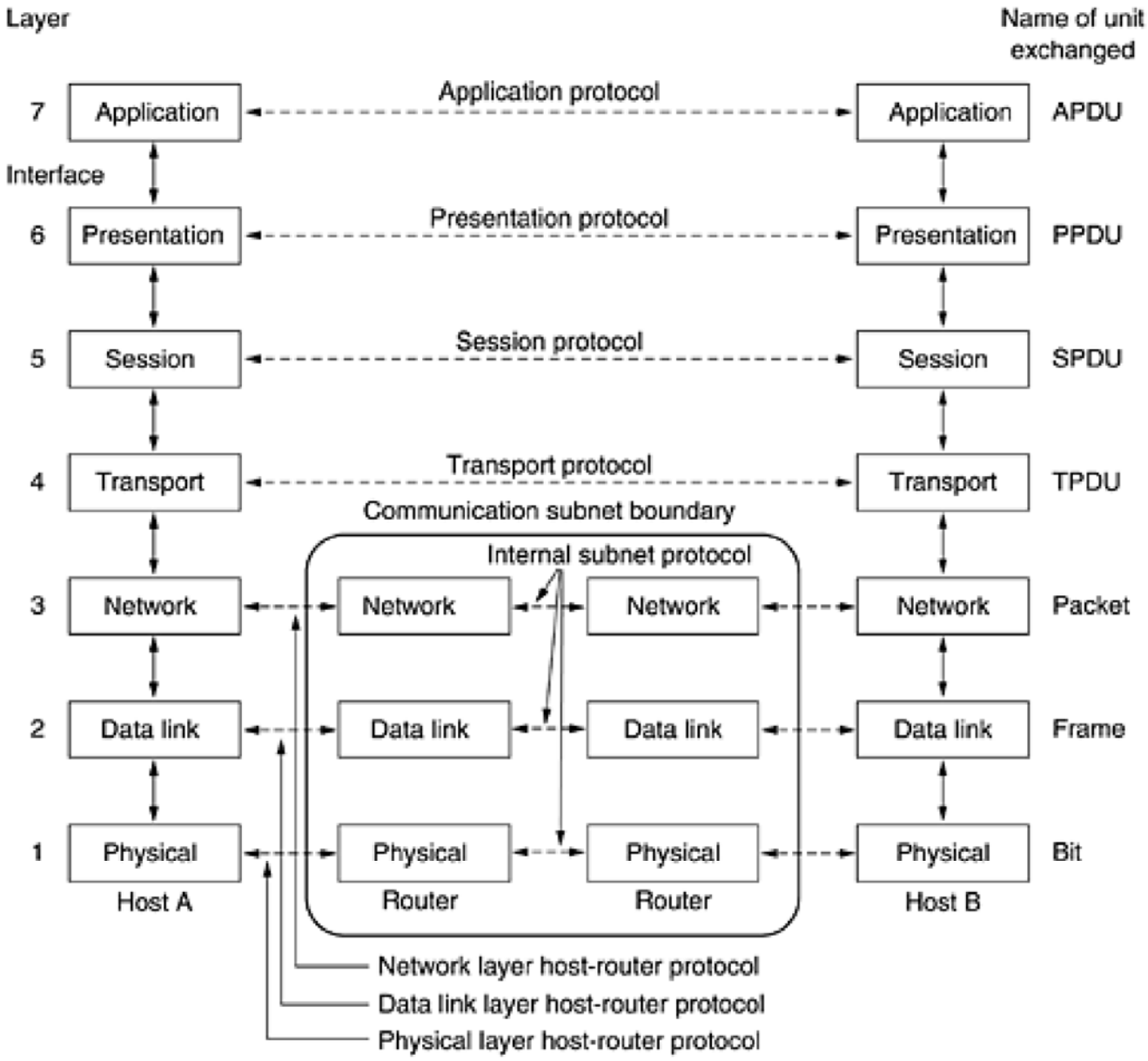
The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

The OSI model is built of seven ordered layers. As shown in figure (OSI reference model) , as the message travels from device A to device B it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

The seven layers can be thought of as belonging to three subgroups. Layers (1, 2, and 3) are the network support layers, they deals 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) can be thought of as the user support layers, the allow interpretability among unrelated software systems. Layers 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.



OSI reference model

Function of The Layers :-

1- Physical layer :-

The physical layer coordinates the functions required to transmit a bit stream over physical medium. It deals with the mechanical and electrical specifications of the primary connections, such as cables, connectors, and signaling options that physically ink two nodes on a network.

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 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 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.

- ❖ Transmission mode. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

2- Data link layer :-

The main task of Data link layer is to transmission facility into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break up the data into data frames, and transmit the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgment frame.

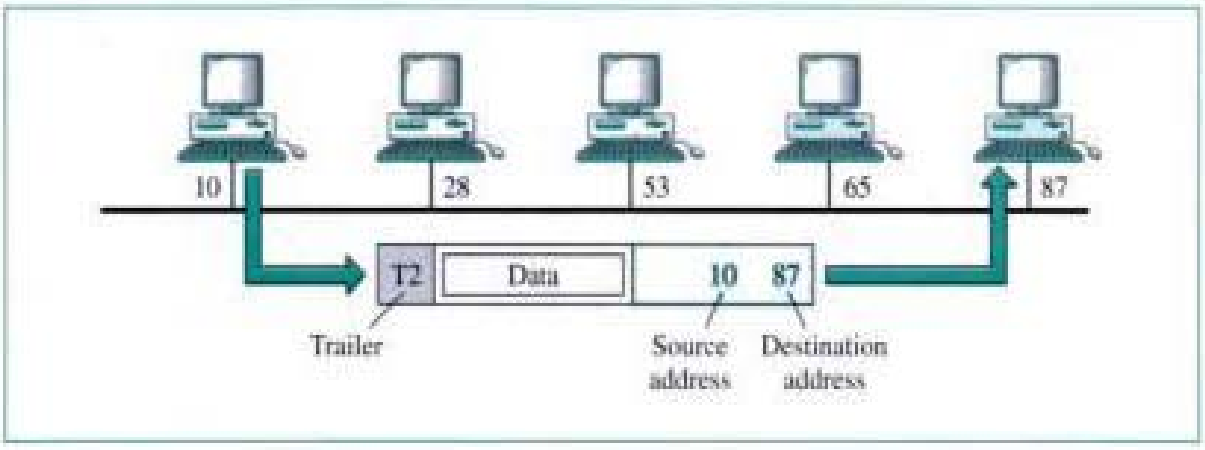
Specific responsibilities of the data link layer include the following :-

- o Node – to – Node delivery.
- o Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- o 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.
- o Access control :- When two or more devices are connected to the same link, it necessary to determine which device has control over the line at any given time.
- o Flow control :- To avoid overwhelming the receiver, the data link layer regulates the amount of data that can be transmitted at one time. It adds identifying numbers to enable the receiving node to control the ordering of the frames.
- o Error handling : Data link layer provide for data recovery, usually by having the entire frame retransmitted.
- o Synchronization :- Headers contain bits to alert the receiving station that a frame is arriving. These bits allow the receiver to synchronize its timing to that of the

transmission (Know duration of each bit). Trailers contain bits for error control and also bits that indicate the frame has ended, and that anything to follow is either a new frame or an idle channel.

The Data link layer is subdivided into two sub layers : **Logical Link Control (LLC)**, and **Media Access Control (MAC)**.

Example:- in figure below, 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 the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection.



3- Network Layers :-

The network layer is responsible for the source – to – destination delivery of a packet across multiple network links.

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.

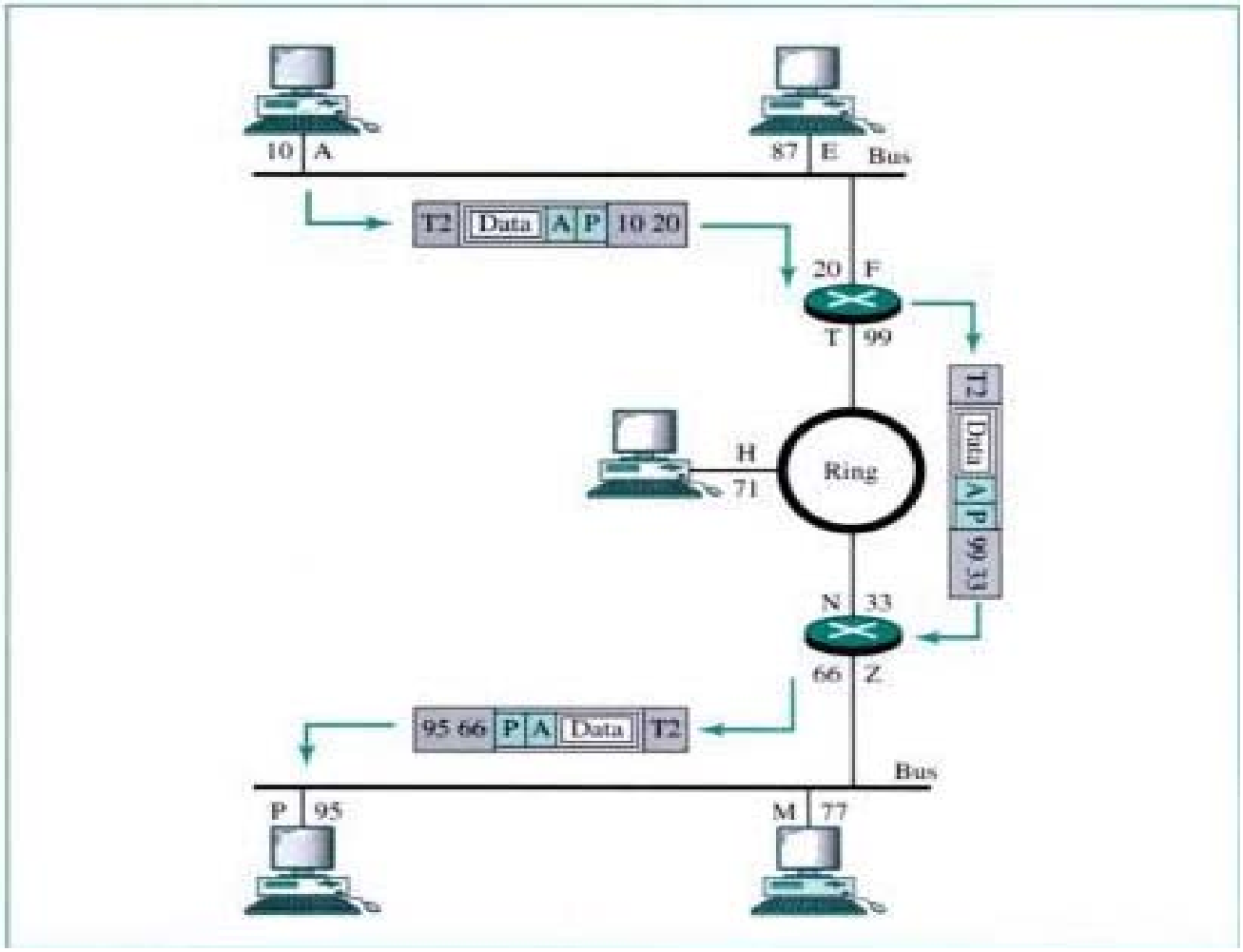
The network layer provider two related services : **Switching** and **Routing**.

Switching refers to temporary connections between physical links, resulting in longer links for network transmission [e.g. telephone conversation].

Routing means selecting the best path for sending a packet from one point to another when more than one path is available.

Routing and switching require the addition of a header that includes, the source and destination addresses of the packet. Data link addresses (physical Addresses) changes as a frame moves from one node to the next. While Network layer addresses [Logical Addresses] don't change during transmission.

Example: in the figure below, we want to send data from a node with network address **A** and physical address **10** located on one LAN, to a node with network address **P** and physical address **95** located on another LAN.



4- 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.

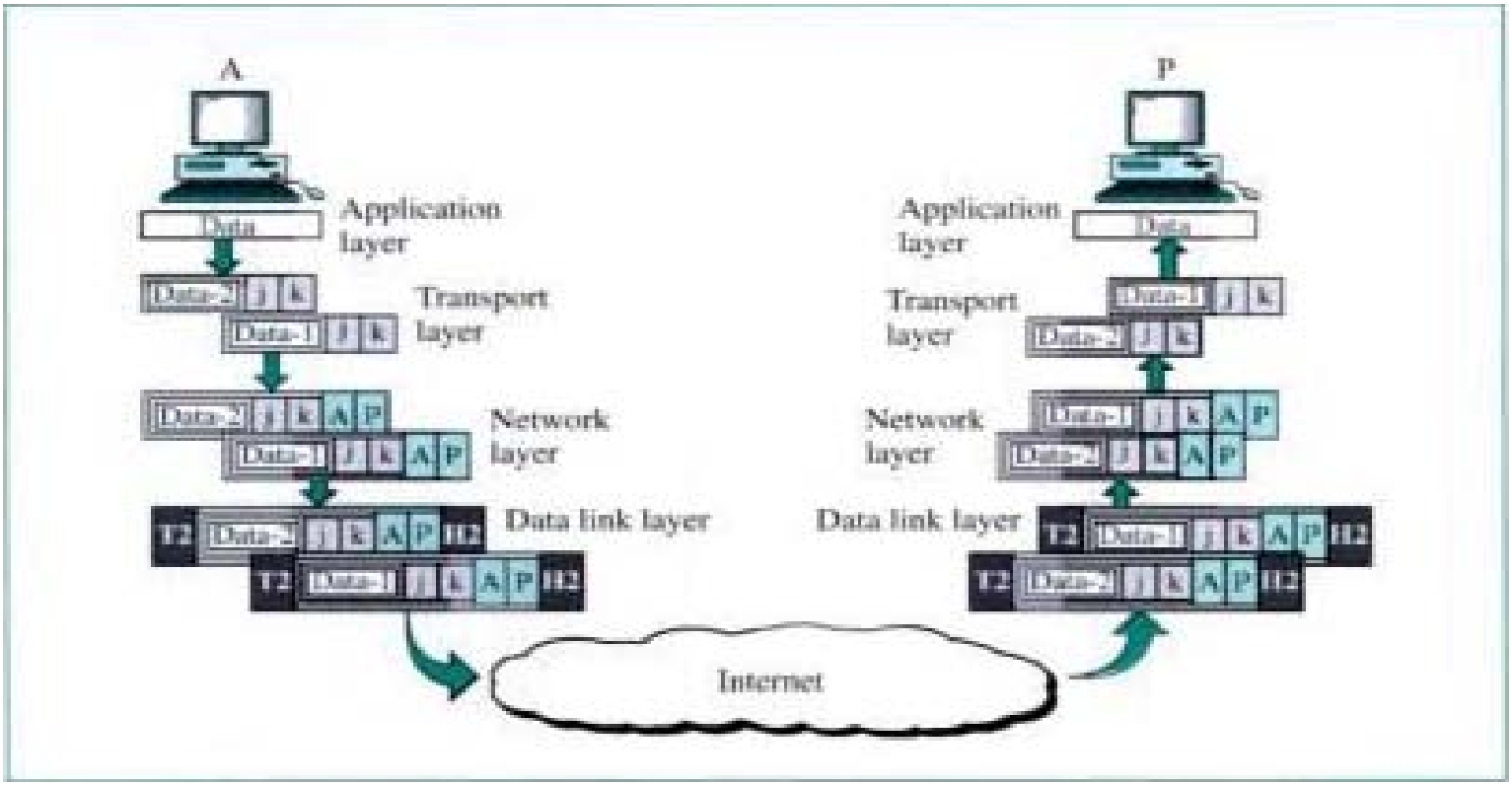
Specific responsibilities of the transport layer include the following :-

- End – to – End message delivery. Overseeing the transmission and arrival of all packets of a message at the destination point.
- 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.

Example:- figure below shows example of transport layer communication, data coming from an upper layers have port addresses **j** and **k** , (**j** as address for sending process, and **k** is the address of receiving process). Since the data are larger than the network layer can handle, the data are split into two packets, each packet retaining the port addresses (**j** and **k**), then in the network layer, network addresses **A** and **P** are added to each packet. The packets can travel on different path and arrive on the destination either on order or out of order.



5- Session Layer :-

The session layer allows users on different machines to establish sessions between them.

Sessions offer various services, including:-

- dialog control (keeping track of whose turn it is to transmit).
- token management (preventing two parties from attempting the same critical operation at the same time).
- 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.
- Graceful Close: - Ensuring that the exchange has been completed appropriately before the session closes.

6- Presentation layer :-

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

Specific responsibilities of this layer include:-

- Translation: - changing the format of a message from that used by sender into one mutually acceptable for transmission. Then at the destination changing the format into the one understood by the receiver.
- Encryption: - encryption and decryption of data for security purposes.

- Compression :- Compression and decompressing data to make transmission more efficient.
- Security :- Validating passwords and log – in codes.

7- Application layer:

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for some services.

The application layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (HyperText Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back. Other application protocols are used for file transfer, electronic mail, and network news.