

Unit – II

The Reference Model for Network Communication

Topic Covered in this Unit

- ▶ 2.1 OSI model & function of each Layer
- ▶ 2.2 TCP/ IP model
- ▶ 2.3 Comparison of OSI & TCP/IP Models

The OSI Model

- ▶ OSI stands for **Open Systems Interconnection**. It was developed by ISO – ‘**International Organization for Standardization**’, in the year **1984**. It is a **7-layer architecture** with each layer having specific functionality to perform.
- ▶ All these 7 layers work collaboratively to transmit the data from one person to another across the globe.
- ▶ 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**.

The OSI Model

- ▶ 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 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.

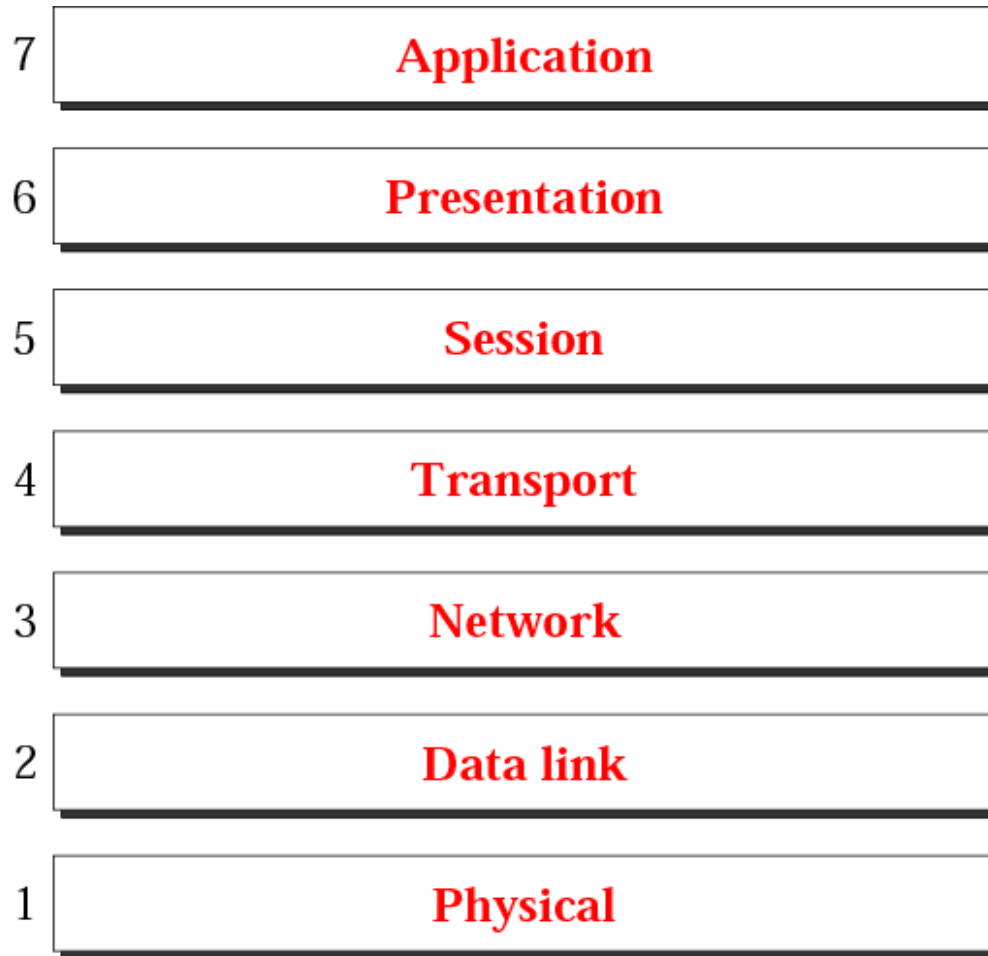
■

Purpose of OSI model

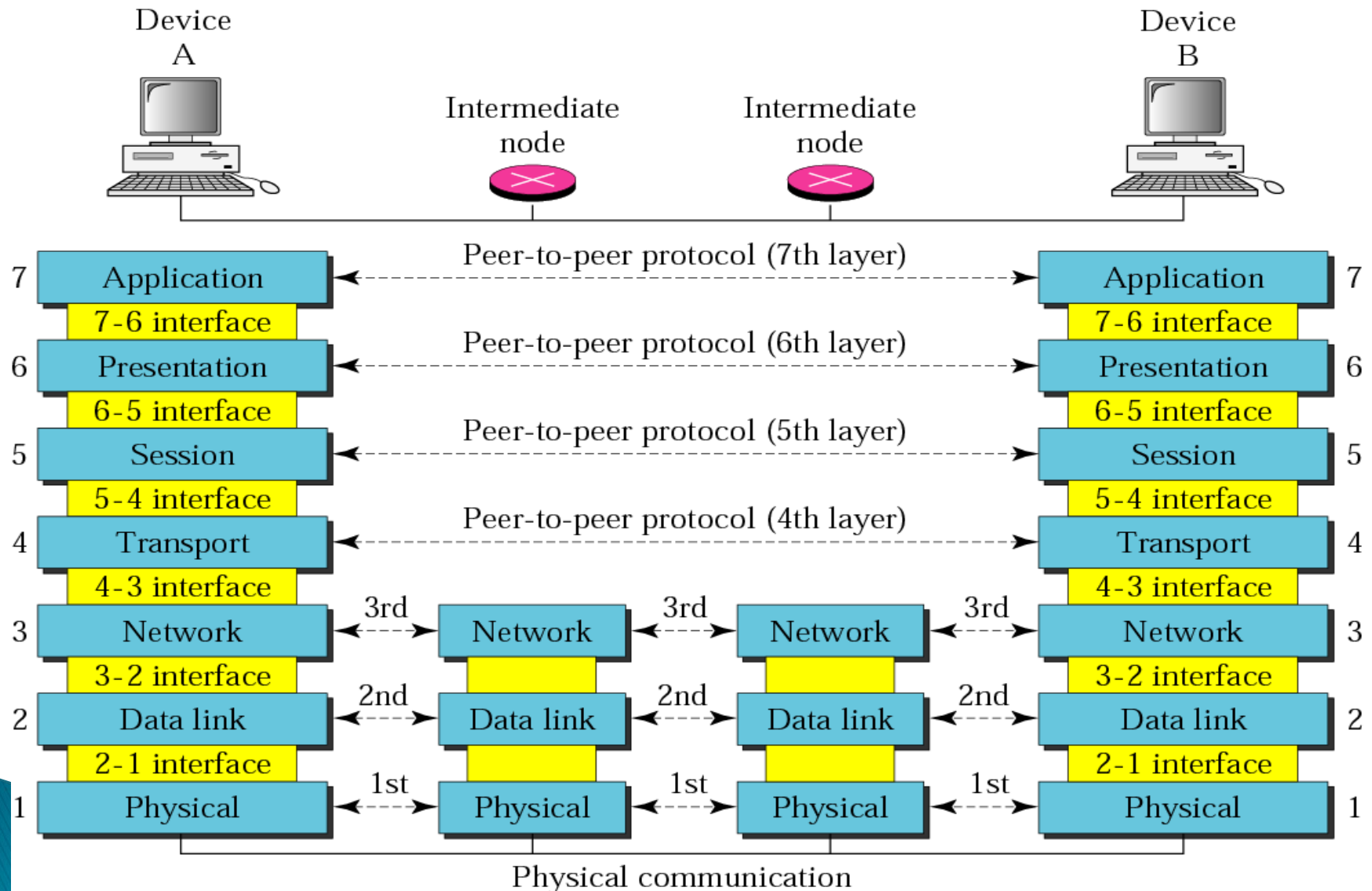
- ▶ OSI model is key to troubleshooting network devices. When a networking unit fails, or an application goes down and cannot communicate with the rest of the network.
- ▶ OSI provides a standard for different computer systems to be able to communicate with each other.
- ▶ The OSI model allows equipment manufacturers to define their standards and protocols while maintaining interconnectivity with other manufacturers.
- ▶ OSI framework is used for designing, manufacturing, and troubleshooting network technology.




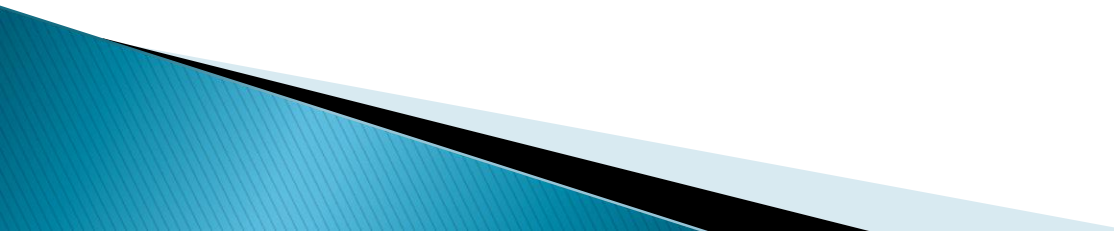
The OSI model



OSI layers Peer-to-Peer layer communication Processes



- ▶ At the physical layer, communication is direct. Device A sends a stream of bits to device B
 - ▶ At the higher layers, communication moves 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 I 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.
- 

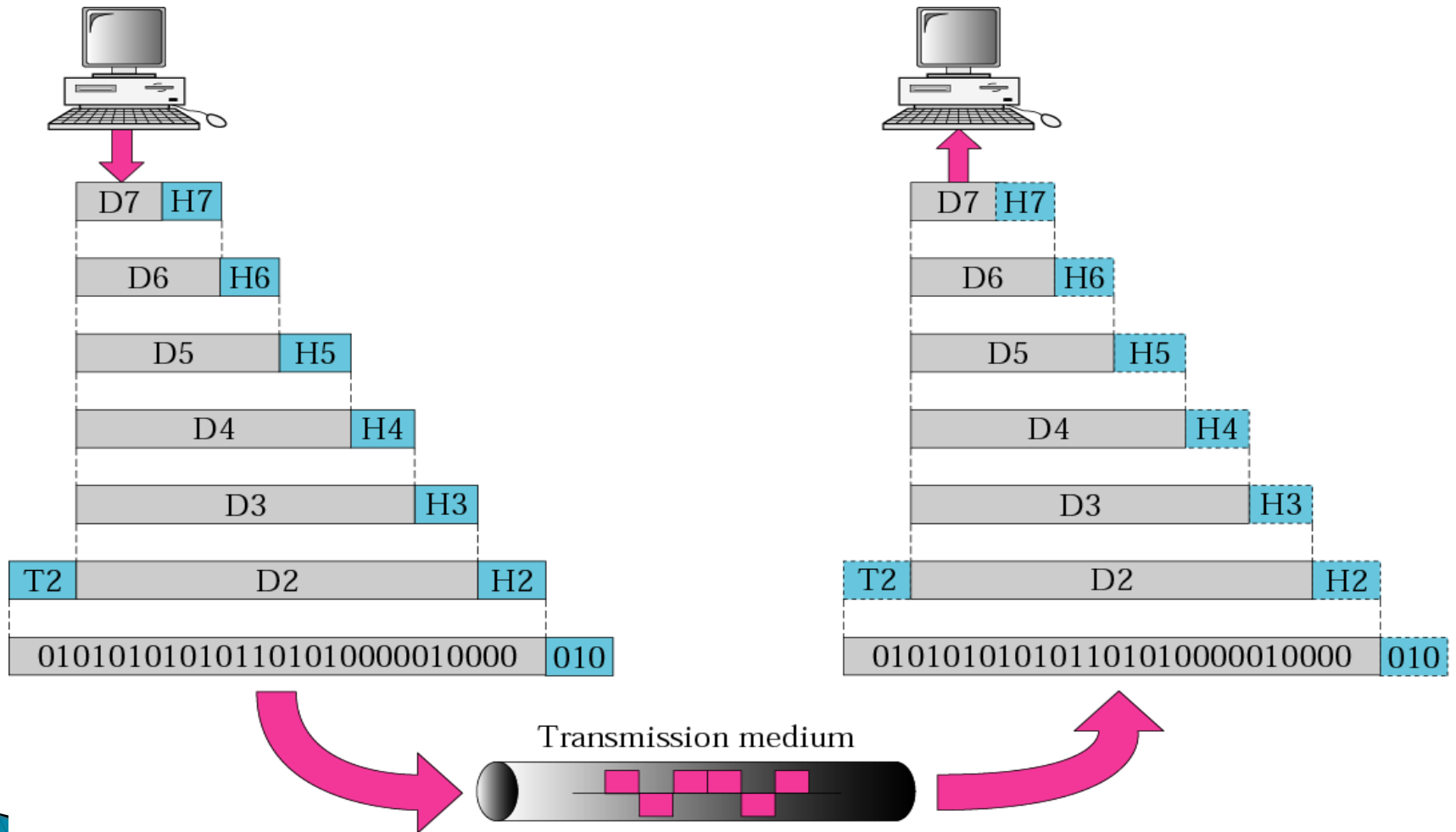
- ▶ The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers.
 - ▶ Each interface defines the information and services a layer must provide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

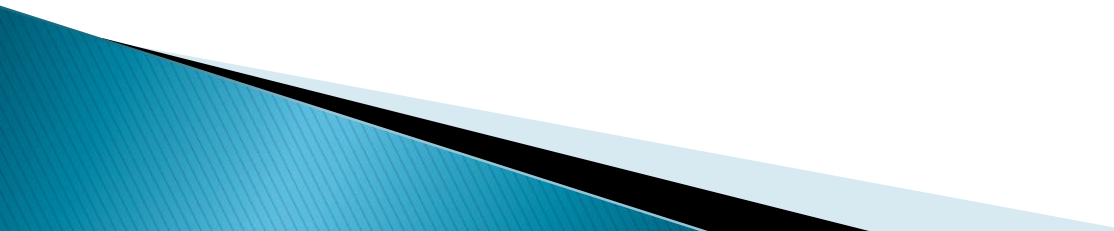
- ▶ The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.
- ▶ At the physical layer, communication is direct as shown in the following Figure. 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.

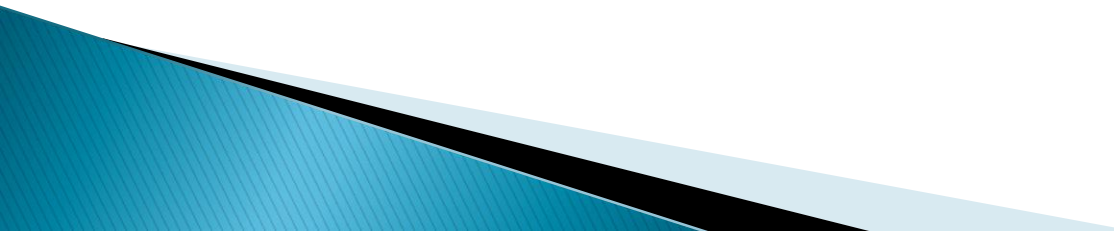
- ▶ At layer 1 the entire package is converted to a form that can be transmitted to the receiving device.
- ▶ At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it. For example, layer 2 removes the data meant for it, and then 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.



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.
 - ▶ 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.
- 

Protocol data unit

- ▶ A protocol data unit, or a PDU, is a unit of information that is sent by a protocol at a particular OSI layer.

GeeksforGeeks	
PDU Name	OSI Model Layers
Data	Application Layer
Data	Presentation Layer
Data	Session Layer
Segments	Transport Layer
Packets	Network Layer
Frames	Data Link Layer
Bits	Physical Layer

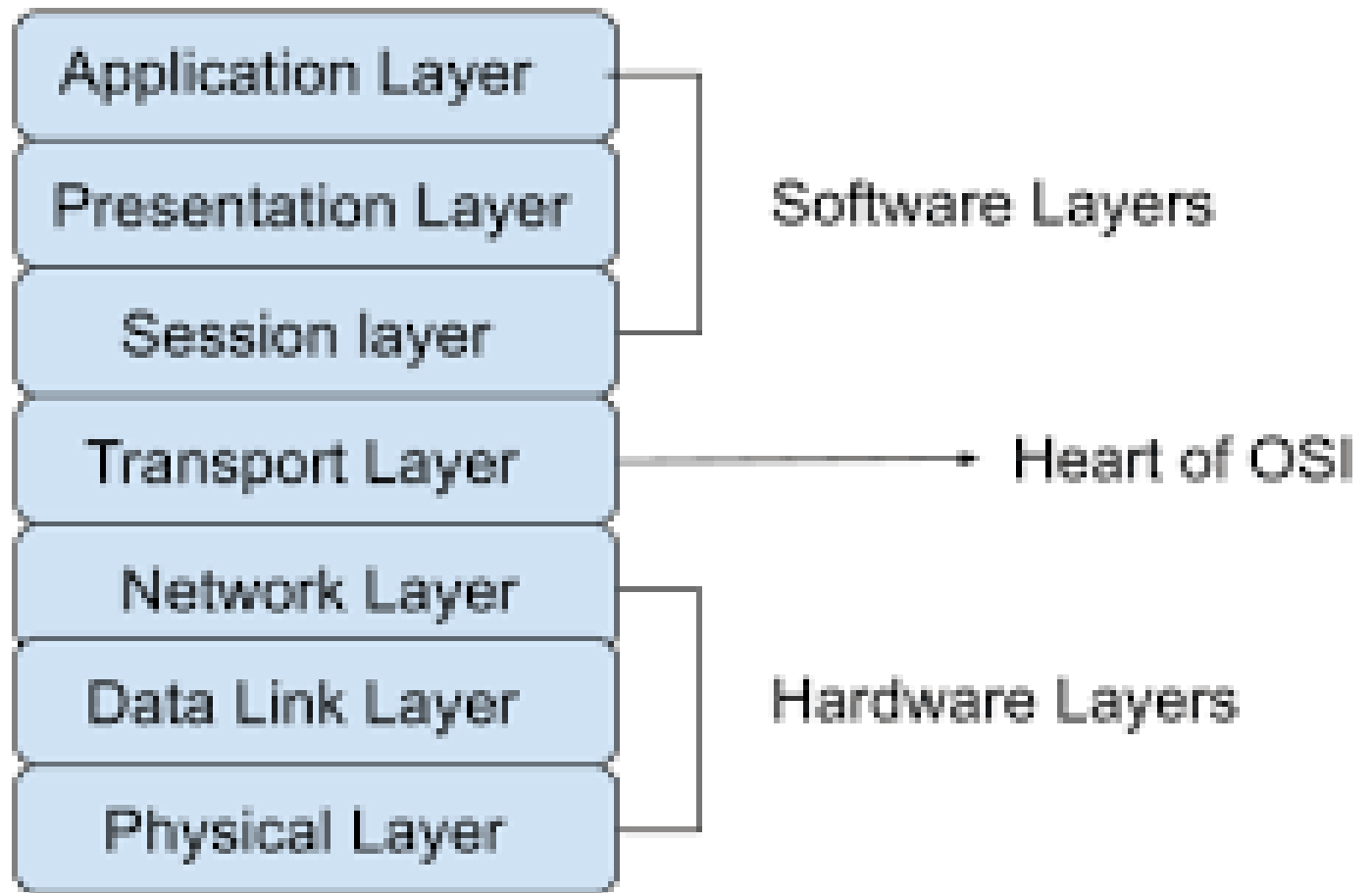
- ▶ the Application, Presentation and Session layer take user input and converts it into data.
- ▶ the Transport layer adds a segment header converting the data into segments.
- ▶ the Network layer adds a network header and converts the segments into packets / datagrams.
- ▶ the Data Link layer adds a frame header converting the packets/datagrams into frames.
- ▶ the MAC sub layer converts the frames into a bits, which the Physical layer can put on the wire.

OSI: A Layered Network Model

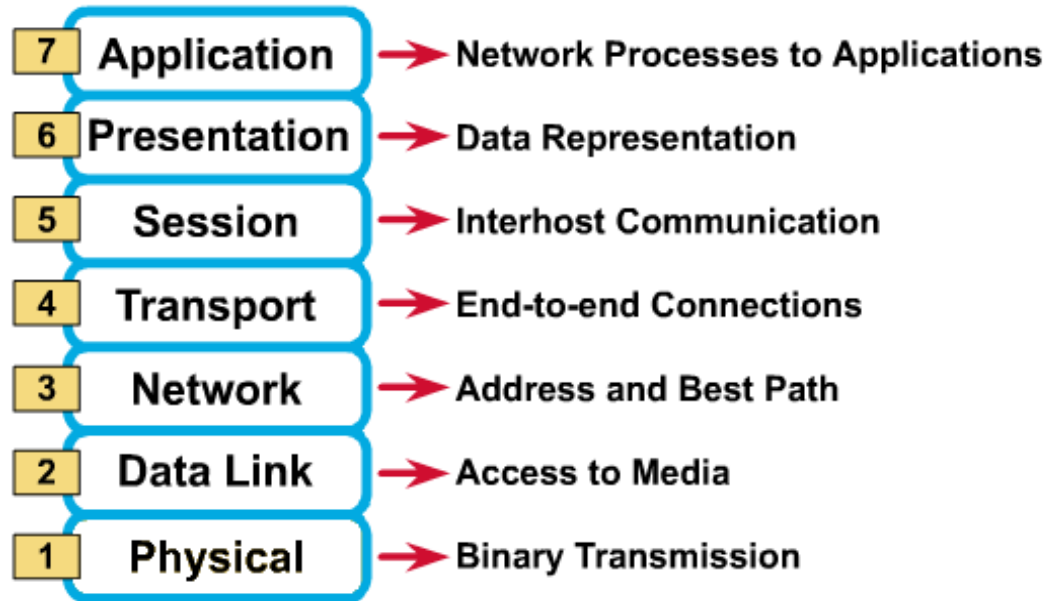
- ▶ The process of breaking up the functions or tasks of networking into layers reduces complexity.
- ▶ Each layer provides a service to the layer above it in the protocol specification.
- ▶ Each layer communicates with the same layer's software or hardware on other computers.

OSI: A Layered Network Model

- Layer 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 physical connections, physical addressing and transport timing and reliability)
- Layer 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.



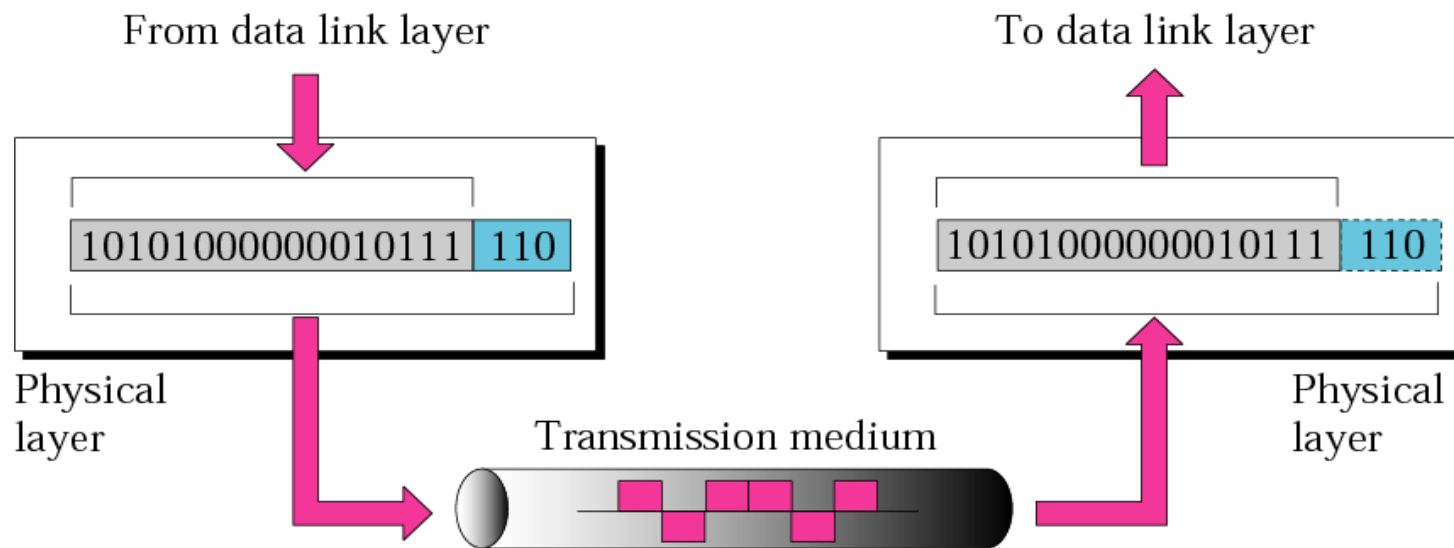
OSI Reference Model: 7 Layers



- ▶ The Application, Presentation and Session layers are known as the *Upper Layers* and are implemented in software.
- ▶ The Transport and Network layer are mainly concerned with protocols for delivery and routing of packets and are implemented in software as well.
- ▶ The Data Link is implemented in hard- and software and the Physical layer is implemented in hardware only.

- ▶ These lower two layers define LAN and WAN specifications.
- ▶ A more detailed description of each layer follows below, but here's what basically happens when data passes from device A to device B:

Physical layer



Physical layer

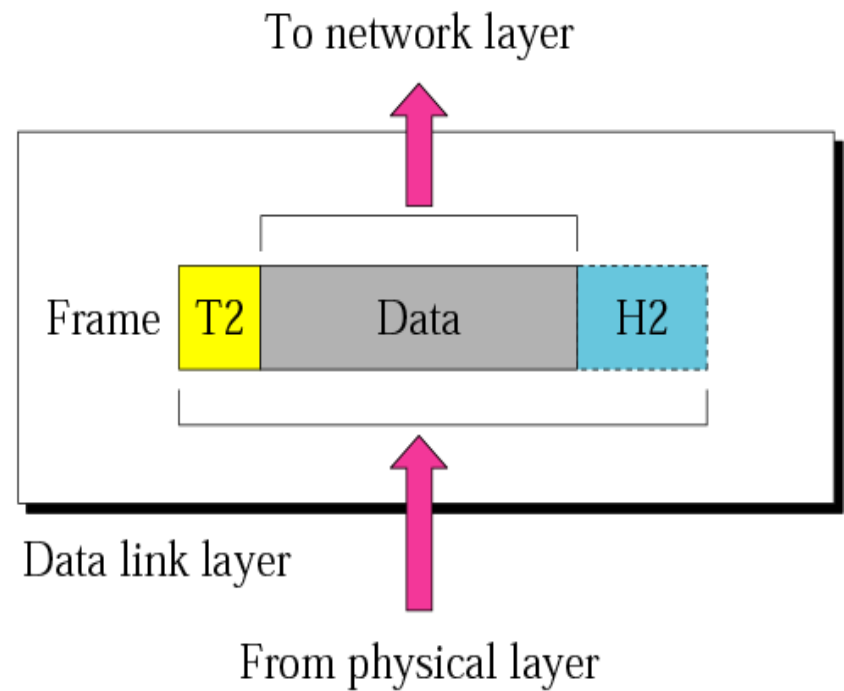
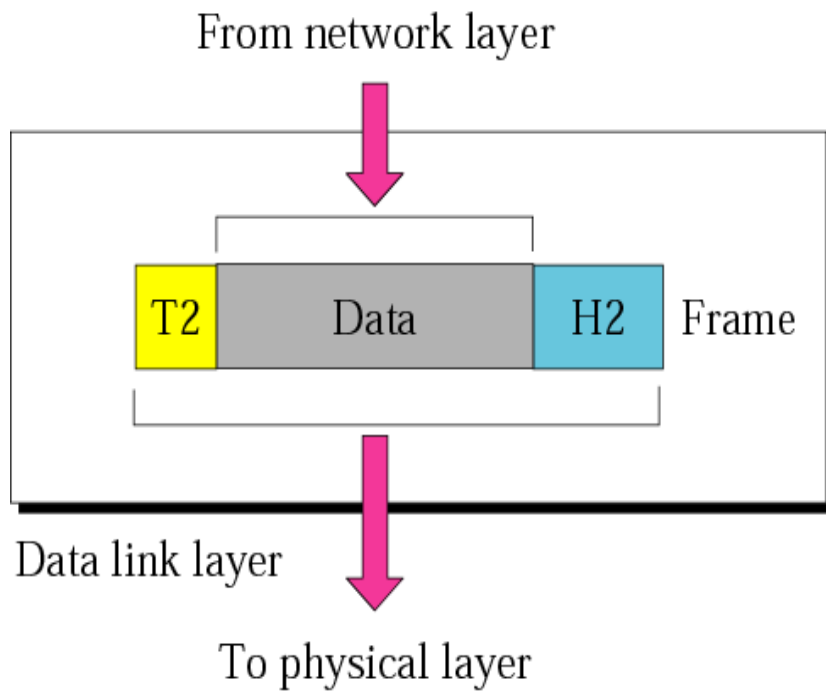
- ▶ Provides physical interface for transmission of information.
- ▶ Defines rules by which bits are passed from one system to another on a physical communication medium.
- ▶ The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- ▶ It is the lowest layer of the OSI model.
- ▶ It establishes, maintains and deactivates the physical connection.
- ▶ It specifies the mechanical, electrical and procedural network interface specifications.

Function

- ▶ Physical characteristics of interfaces and medium.
- ▶ Representation of bits: The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. Bits to be transmitted are encoded into signals--electrical or optical. It also defines encoding (how 0s and 1 s are changed to signals).
- ▶ **Signals:** It determines the type of the signal used for transmitting the information.
- ▶ **Data rate:** the number of bits sent per second.
- ▶ **Synchronization of bits:** The sender and receiver must use the same bit rate.

- ▶ **Line configuration:** It defines the way how two or more devices can be connected physically.
- ▶ **Physical topology:** It defines the way how network devices are arranged.
- ▶ **Transmission mode:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.

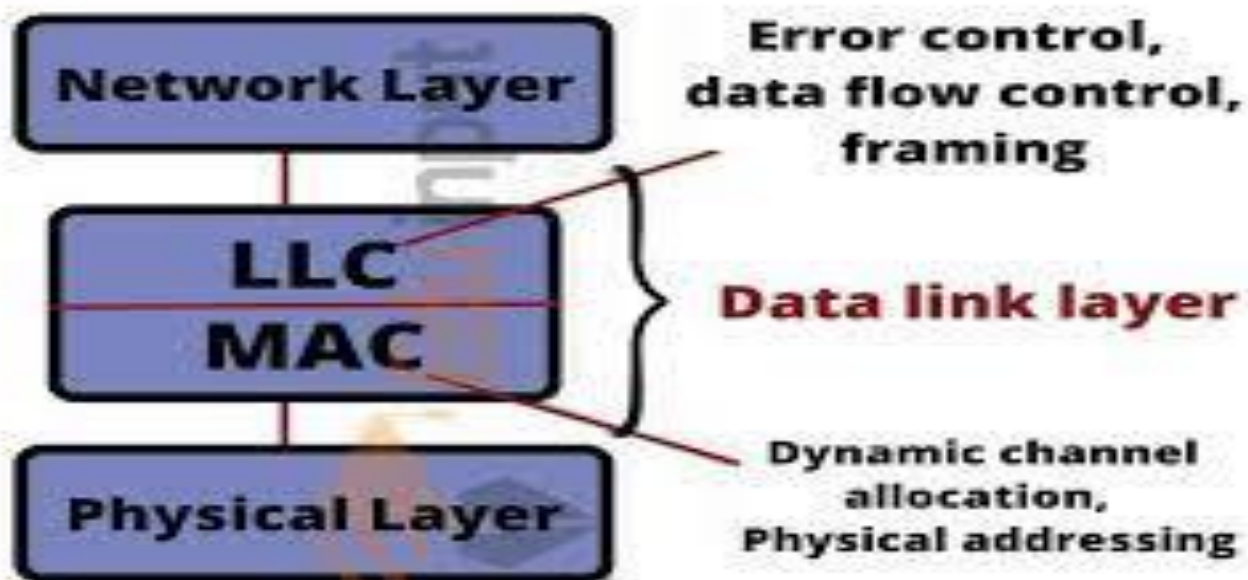
Data link layer



Data Link Layer

- ▶ Data link layer attempts to provide reliable communication over the physical layer interface.
- ▶ Breaks the outgoing data into frames and reassemble the received frames.
- ▶ Create and detect frame boundaries.
- ▶ Handle errors by implementing an acknowledgement and retransmission scheme.
- ▶ This layer is responsible for the error-free transfer of data frames.
- ▶ It defines the format of the data on the network.
- ▶ The primary role of the data link layer is to check whether the data transmitted from one point to another node point on the physical layer is error-free or not.

- ▶ It provides a reliable and efficient communication between two or more devices.
- ▶ It is mainly responsible for the unique identification of each device that resides on a local network.
- ▶ It contains two sub-layers:



- ▶ The data link layer is divided into **two** sub layers:

- 1) Logical Link Control (LLC) layer
- 2) Media Access Control (MAC) layer

1) Logical Link Control (LLC) layer :-

- LLC or DLC is the topmost layer of the data link layer.
- The top sublayer is called Logical Link Control and it is communicating only with Network layer providing reliability and flow control functions.
- It is responsible for assigning the frame sequence number
- ▶ The LLC layer controls **frame synchronization, flow control and error checking and control.**

2) Media Access Control (MAC) layer:-

- ▶ The bottom sublayer called Media Access Control is responsible only for **adding physical address to the frame** and does the communication with the Physical layer.
- ▶ Physical address is the unique ID assigned to every network interface in the node.
- ▶ In some cases it might be called MAC address, hardware address, or Data Link layer address.
- ▶ The MAC controls how a computer on the network gains access to the data and permission to transmit it so responsible for **access control**.

Data Link Layer

Functions

- ▶ **Framing:**–The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- ▶ The Data link layer adds the header and trailer to the frame.
- ▶ The header which is added to the frame contains the hardware destination and source address.



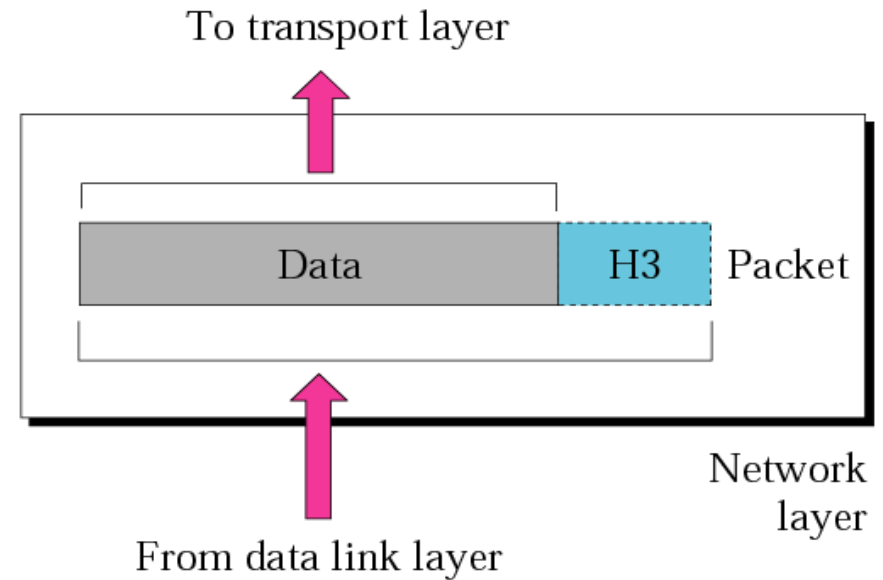
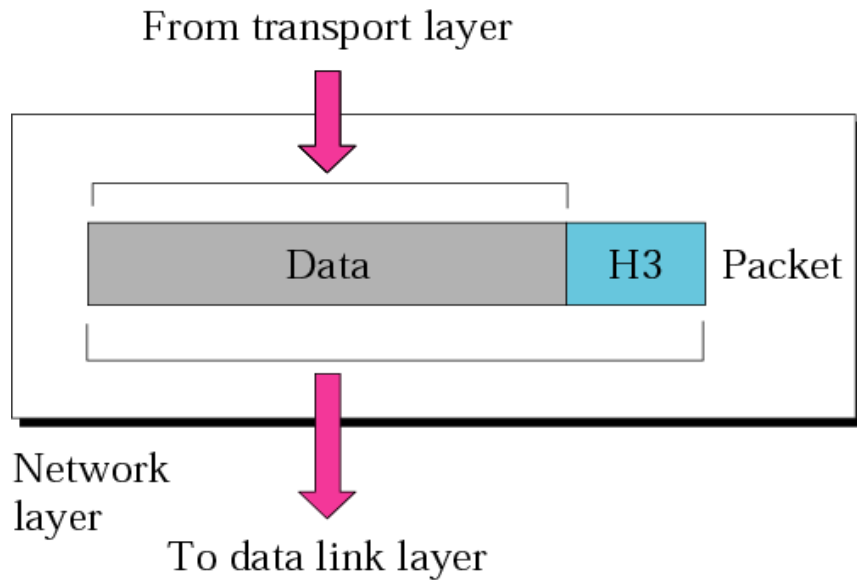
- ▶ **Physical addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- ▶ **flow control :-** is the main functionality of the Data-link layer.
- ▶ It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted.
- ▶ It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- ▶ The data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Data Link Layer

- ▶ **Error control.** The data link layer provides mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames.
- ▶ The error can be controlled in the data link layer in **three** phases of error control as follows:
 - 1) **Error detection:** The error in the data frame is detected with the help of error detection bits present in the frame trailer.
 - 2)**Acknowledgment:** After receiving the data frame, the receiver responds to inform the sender about the successful delivery of the data frame.

- ▶ This acknowledgment can be positive or negative. If the data frame is received successfully, it sends positive feedback to the sender; otherwise, it sends negative feedback to the sender.
- ▶ **3) Retransmission:** If the receiver successfully receives the data frame, the sender sends the next set of data frames, but if the data frame does not reach the receiver successfully, the sender must resend the data frames.
- ▶ **Access control:** When two or more devices are connected to the same link, protocols are necessary to determine which device has control over the link at any given time

Network layer



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.
- ▶ 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 with connecting devices between the networks, there is often a need for the network layer to accomplish source-to-destination delivery.

Network Layer

- ▶ Implements routing of frames (packets) through the network.
- ▶ Defines the most optimum path the packet should take from the source to the destination
- ▶ Defines logical addressing so that any endpoint can be identified.
- ▶ Handles congestion in the network.
- ▶ Facilitates interconnection between heterogeneous networks (Internetworking).

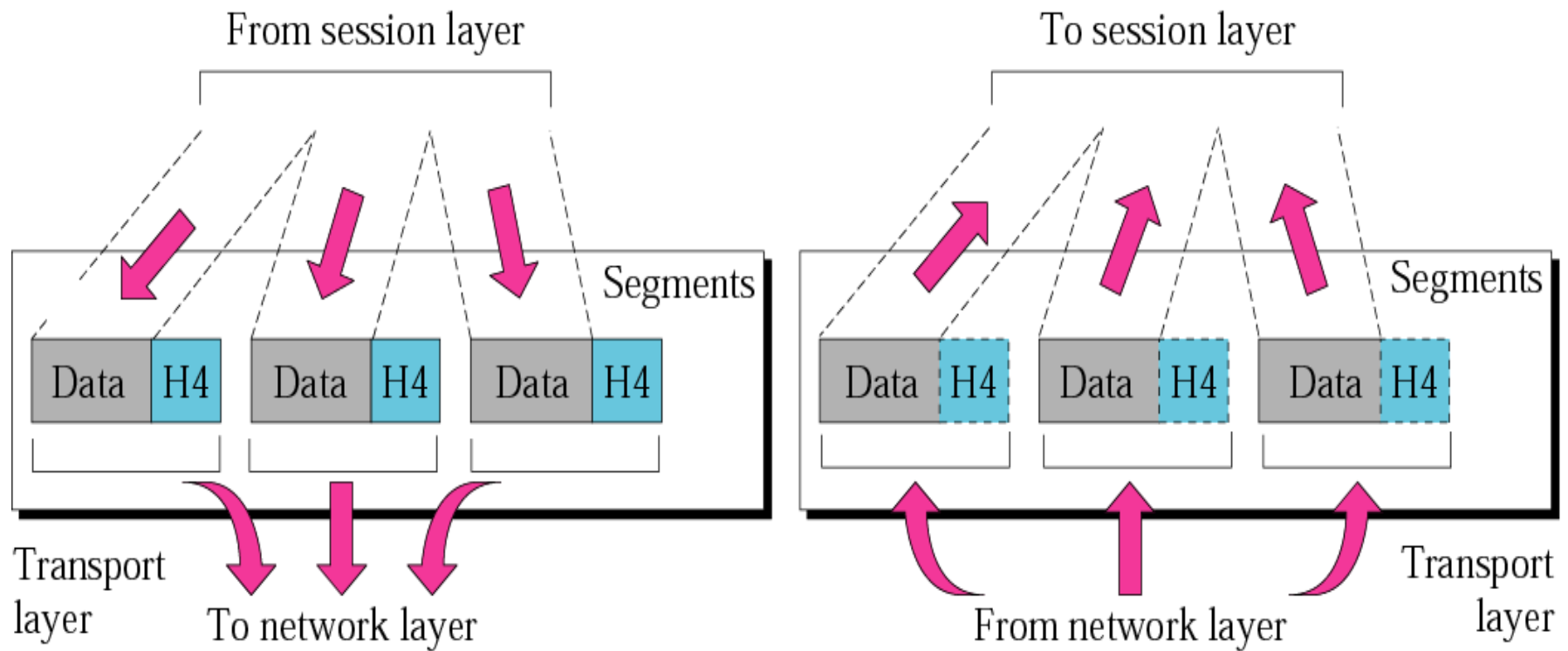
Network Layer

Functions:

- ▶ **Internet working:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- ▶ **Logical Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- ▶ **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- ▶ When independent networks or links are connected to create internetworks or a large network, the connecting devices route or switch the packets to their final destination.

- ▶ **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).
- ▶ Network layer routing protocol
 - IP, IPX, ICMP,IGMP

Transport layer

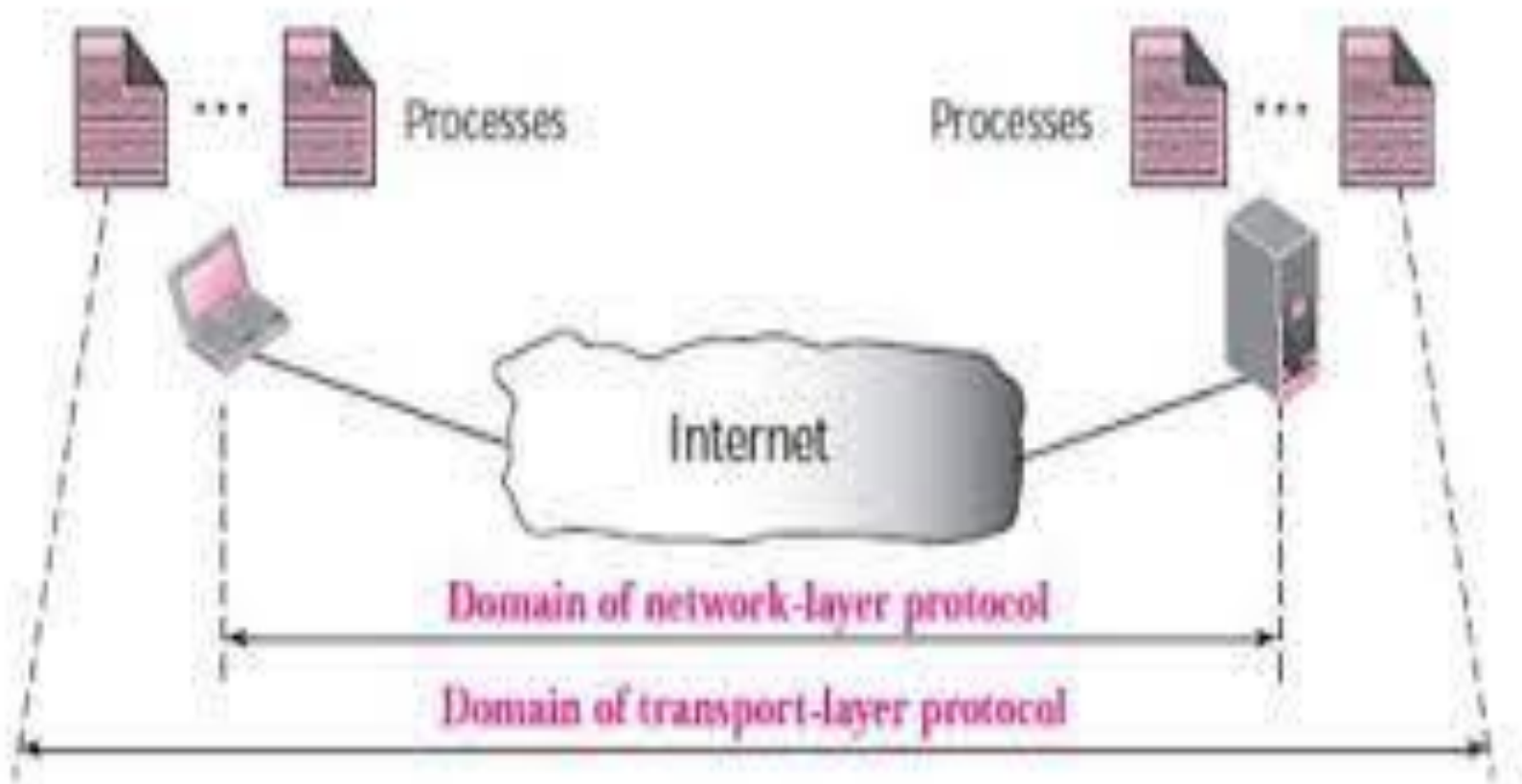


Transport layer

- ▶ The transport layer is responsible for **process-to-process** delivery of the entire message.
- ▶ A process is an application program running on a host.
- ▶ The data in the transport layer is referred to as **Segments**. It is responsible for the **End to End Delivery of the complete message**.
- ▶ 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 **whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level**, ensures that the.

- ▶ The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- ▶ The main responsibility of the transport layer is **to transfer the data completely**.
- ▶ It receives the data from the upper layer and converts them into smaller units known as segments.
- ▶ This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

Transport layer



Transport Layer

Functions

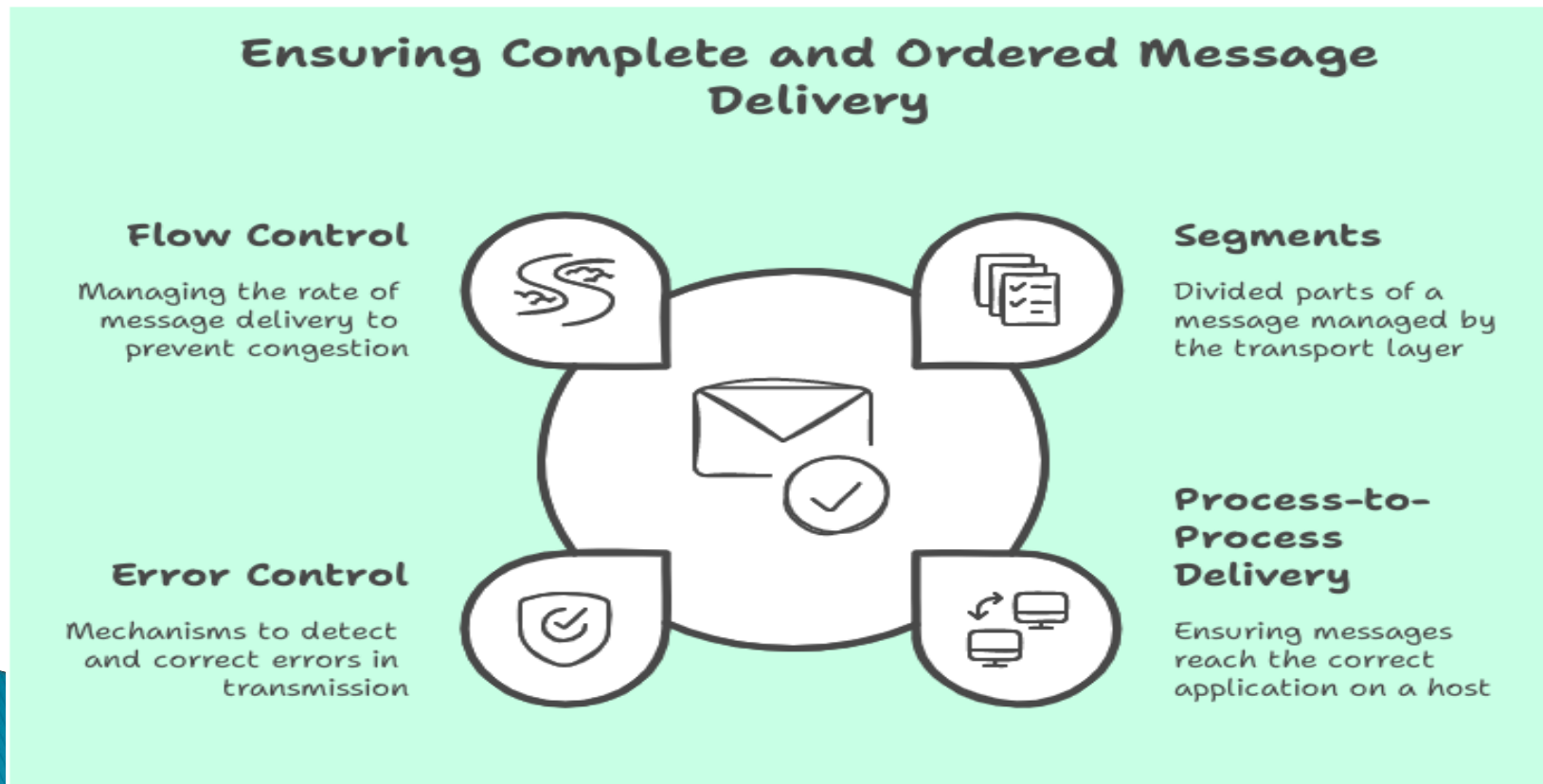
- ▶ **Service Point Addressing:-** . Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) 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 network; the transport layer gets the entire message to the correct process on that computer.

- ▶ **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple **segments**, and each segment is **assigned with a sequence number** that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

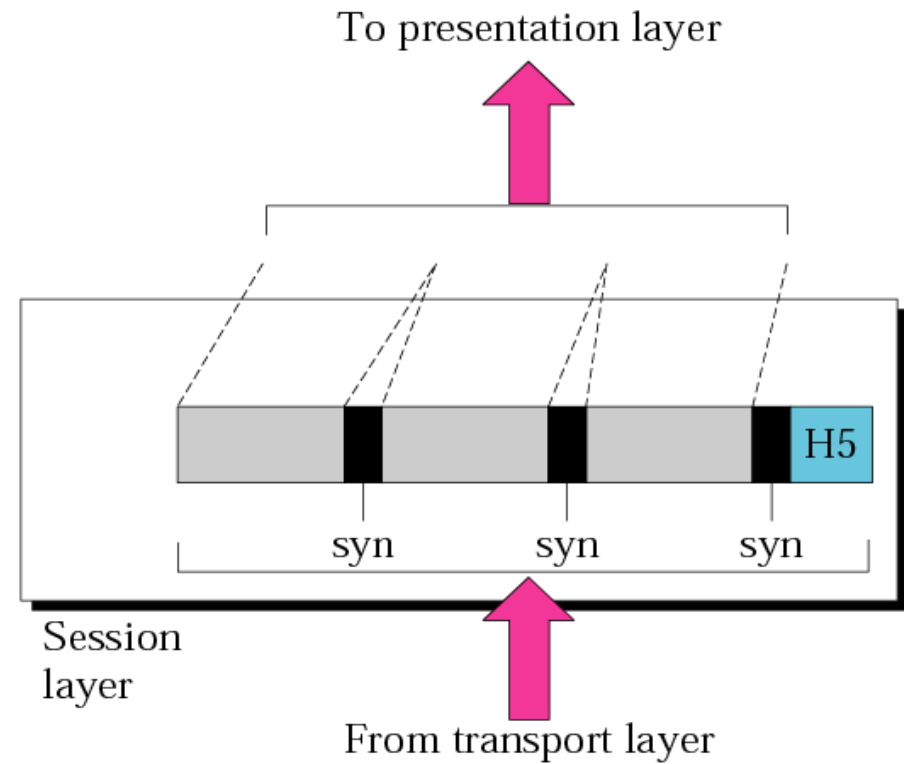
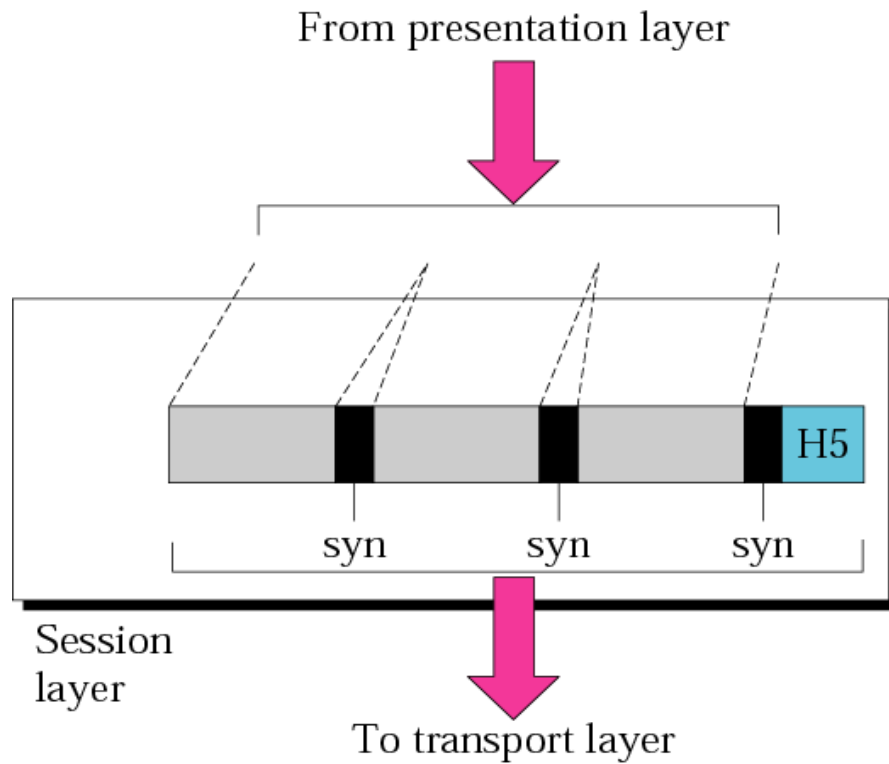
- ▶ **Connection control:-** Transport layer provides two services Connection-oriented service and connectionless service.
- ▶ A **connectionless** service treats each segment as an individual packet, and they all travel in different routes to reach the destination. Example: UDP
- ▶ A **connection-oriented** service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- ▶ Example :- TCP

- ▶ **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.
- ▶ **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.

it controls the traffic that happens in the network. If the sender is sending the data faster or the receiver is receiving the data in a slower mode, then it controls the data loss occurring in it.



Session layer



Session layer

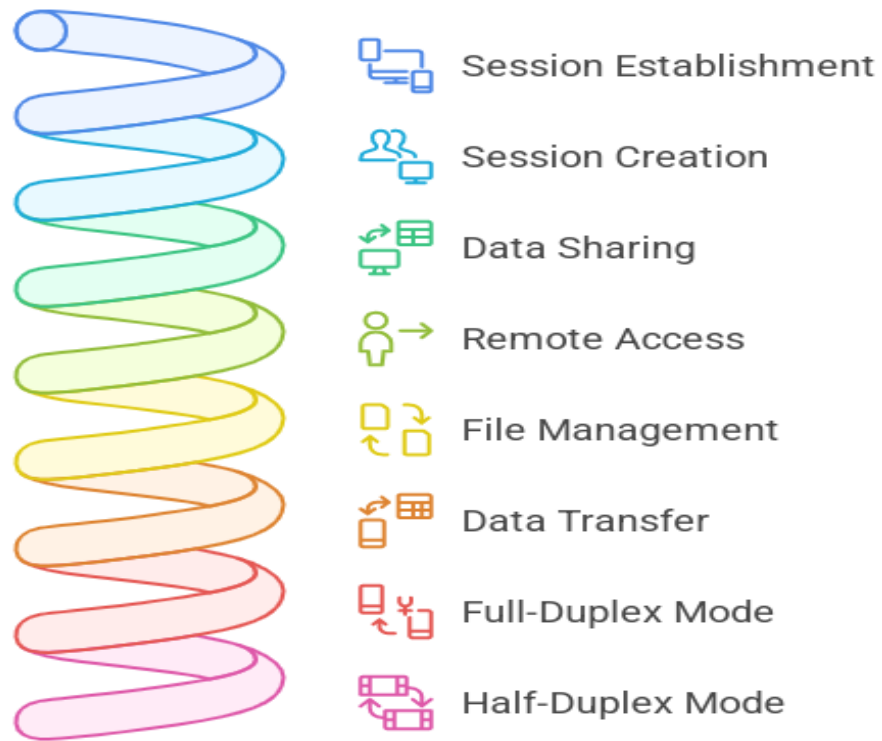
- ▶ It is a layer 5 in the OSI model.
- ▶ The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.
- ▶ This layer is responsible for setting up, coordinating, and terminating conversations, exchanges, and dialogues between the applications at each end

Session Layer Process in OSI Model



- ▶ **Session Establishment:** The session layer establishes connections between devices which is known as sessions. The session which is created allows users to share data, remote access, and file management.
- ▶ **Data Transfer:** It is the very basic function of the session layer, which handles the exchange of data between systems in a full-duplex or half-duplex mode of transmission.

Session Layer Functions in Networking



Session Layer

Function

- ❑ **Dialog control:** Session layer provides mechanism for controlling the dialogue between the two end systems.
- ❑ It defines how to start, control and end conversations (called sessions) between applications.
- ❑ This layer requests for a logical connection to be established on an end-user's request.
- ❑ Any necessary log-on or password validation is also handled by this layer.
- ❑ It is accountable for establishing, synchronizing, preserving, and ending the conversation between the sender and the receiver.

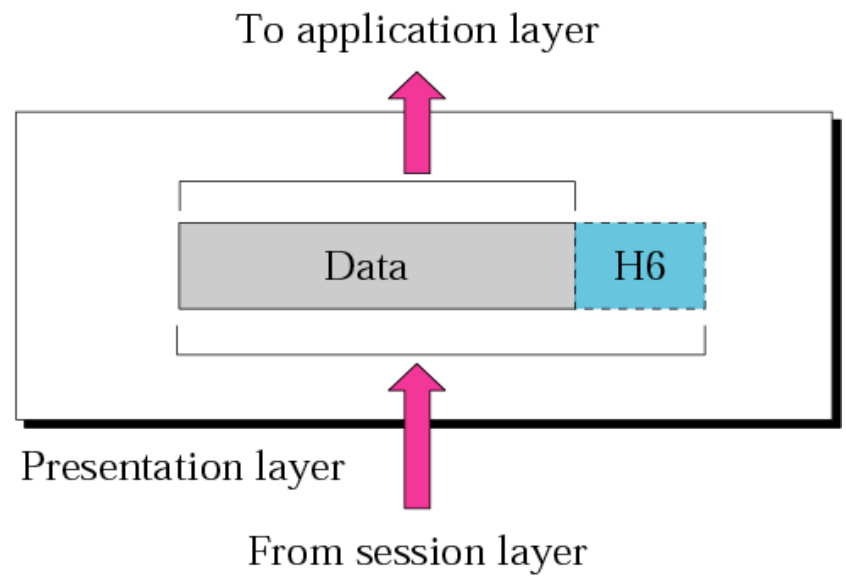
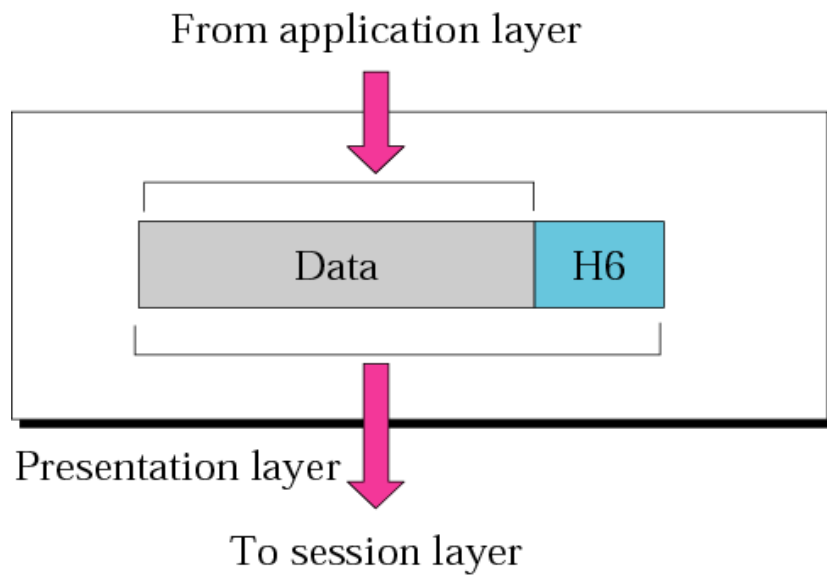
Session Layer

- ❑ Session layer is also responsible for terminating the connection.
- ❑ **Token management** : It uses a token mechanism in which the user sharing the data is given a token in case of half duplex mode and, after the exchange, transfers it to another device. The token method maintains the efficiency of the connection.

- **Synchronization** : Session layer adds some checkpoints when transmitting the data in a sequence. The session layer adds synchronization bits to the message to use the known state in the event of an error. These bits can be used as checkpoints. It adds synchronization points or checkpoints to the data stream for longer communication.
- If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint.
- This process is known as Synchronization and recovery.

■ Example Protocols:- NFS, RPCP, PAP

Presentation layer



Presentation layer

- Presentation Layer is the 6th layer in the Open System Interconnection (OSI) model.
- This layer is also known as **Translation layer**, as this layer serves as a data translator for the network.
- The data which this layer receives from the **Application Layer** is extracted and manipulated here as per the required format to transmit over the network. The main responsibility of this layer is to provide or define the **data format and encryption**.
- The presentation layer is also called as **Syntax layer** since it is responsible for maintaining the proper syntax of the data which it either receives or transmits to other layer(s).

Functions

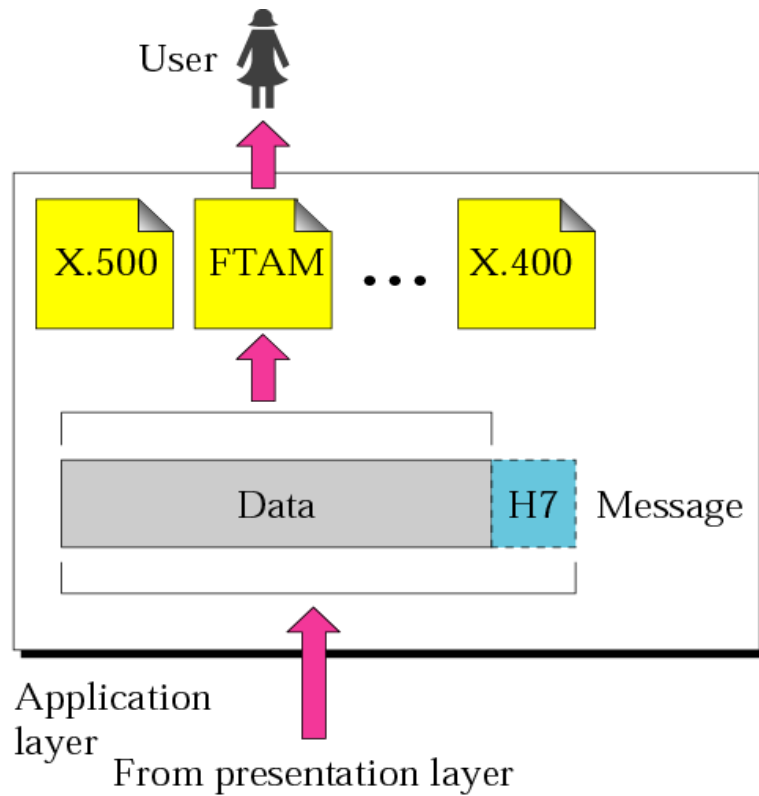
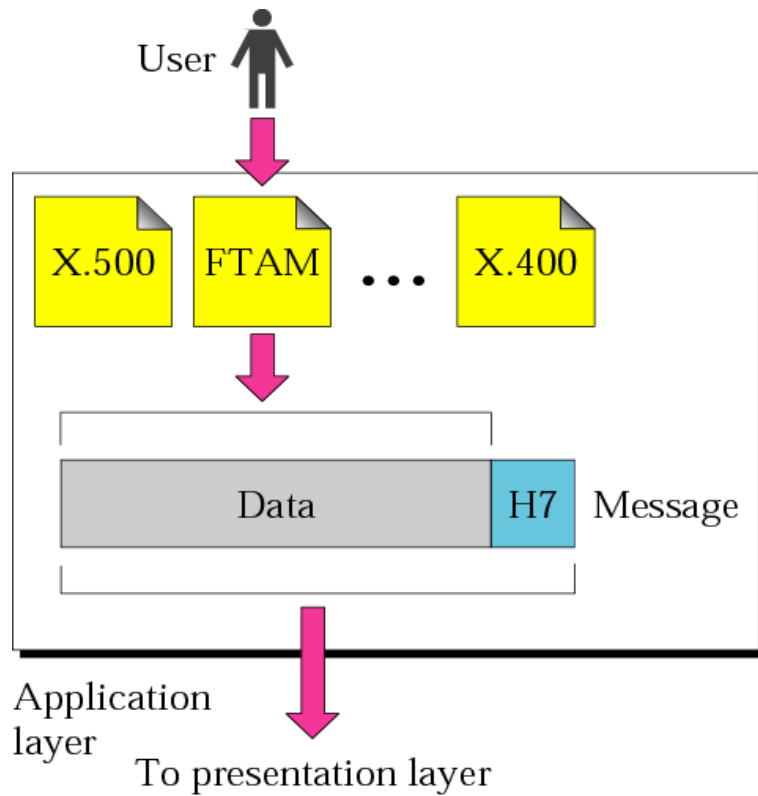
- ▶ Presentation layer format and encrypts data to be sent across the network.
- ▶ This layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the **data efficiently and effectively**.
- ▶ This layer manages the abstract **data structures**.
- ▶ This layer carries out the **encryption** at the transmitter and **decryption** at the receiver.
- ▶ This layer carries out **data compression** to reduce the bandwidth of the data to be transmitted (the primary goal of data compression is to reduce the number of bits which is to be transmitted).
- ▶ This layer is responsible for interoperability (ability of computers to exchange and make use of information) between **encoding methods** as different computers use different encoding methods.

Functions

- ▶ This layer is responsible for interoperability (ability of computers to exchange and make use of information) between **encoding methods** as different computers use different encoding methods.
- ▶ This layer encodes the message from the user-dependent format to the common format and vice-versa.
- ▶ This layer deals with the **syntax and semantics** of the messages.
- ▶ This layer also ensures that the messages which are to be presented to the upper as well as the lower layer should be **standardized as well as in an accurate format** too.
- ▶ Presentation layer is also responsible **for translation, formatting, and delivery** of information for processing or display.

- ▶ **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted.
- ▶ Data compression is very important in multimedia such as text, audio, video.
- ▶ **Encryption/ Decryption:** Data encryption translates the data into another form or code.
- ▶ The encrypted data is known as the ciphertext and the decrypted data is known as plain text.
- ▶ A key value is used for encrypting as well as decrypting data.

Application layer



Application layer

- ▶ At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications.
- ▶ These applications produce the data, which has to be transferred over the network.

This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

- ▶ Example: Application – Browsers, Skype Messenger, etc.

Application Layer

- ❑ Application layer interacts with application programs and is the highest level of OSI model. It provide
- ❑ Network Virtual Terminal(NVT)
- ❑ File Transfer and Access Management(FTAM)
- ❑ Mail Services
- ❑ Directory Services.
- ❑ Examples of application layer are applications such as file transfer, electronic mail, remote login etc.

▶ **Function:-**

- ▶ **Network Virtual Terminal:** It allows a user to log on to a remote host.
- ▶ **FTAM-** File transfer access and management : This application allows a user to access file in a remote host, retrieve files in remote host and manage or control files from a remote computer.
- ▶ **Mail services:** An application layer provides the facility for email forwarding and storage.

Protocol supported at each layer

Layer	Name	Protocols
Layer 7	Application	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	MPEG, ASCH, SSL(Secure Sockets Layer) and TLS (Transport Layer Security)
Layer 5	Session	NetBIOS, RPC
Layer 4	Transport	TCP, UDP
Layer 3	Network	IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	RAPA, PPP(Point-to-Point Protocol), Frame Relay, ATM(Asynchronous Transfer mode), Fiber Cable, etc.

OSI Model

7. Application	User interface	Data	Gateways
6. Presentation	Data Presentation, encryption, compression, encoding.	Data	Gateways
5. Session	Maintaining sessions	Data	Gateways
4. Transport	Process to process communication, port nos.	Segments	Gateways
3. Network	Logical addressing, source to destination delivery.	Packets	Routers
2. Data-Link	Physical addressing, Node to Node delivery.	Frames	Switches, Bridges
1. Physical	Moves bits between devices	Bits	Hubs, Repeaters

TCP/IP MODEL

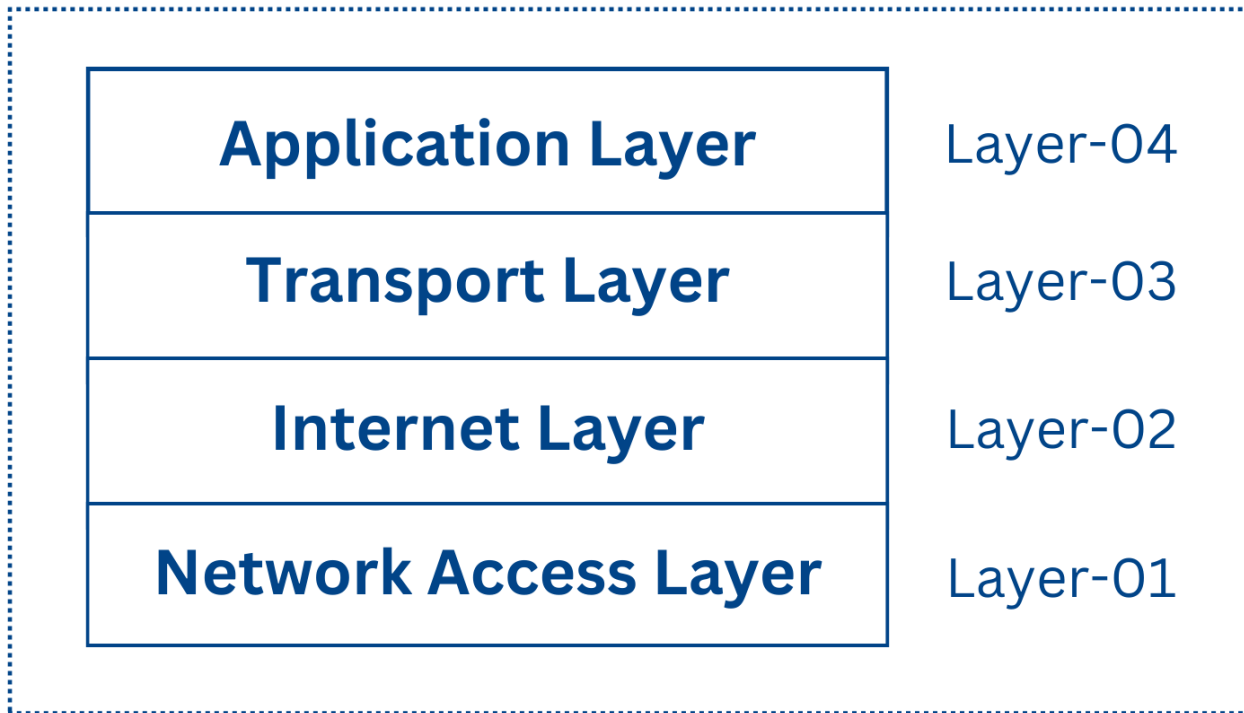
- ▶ TCP/IP stands for **Transmission Control Protocol/Internet Protocol** and is a suite of communication protocols used to interconnect network devices on the internet.
- ▶ TCP/IP is also used as a communications protocol in computer network.
- ▶ The entire IP suite -- a set of rules and procedures -- is commonly referred to as TCP/IP.
- ▶ TCP and IP are the two main protocols, though others are included in the suite.
- ▶ TCP/IP was designed and developed by the Department of Defense (DoD) in the 1970s and is based on standard protocols and adopted as the protocol standard for Internet in 1983.

- ▶ Transmission Control Protocol/Internet Protocol is the set of communication protocols used in the internet and similar computer networks.
- ▶ It provides end-to-end data communication.

Layers in TCP/IP Model

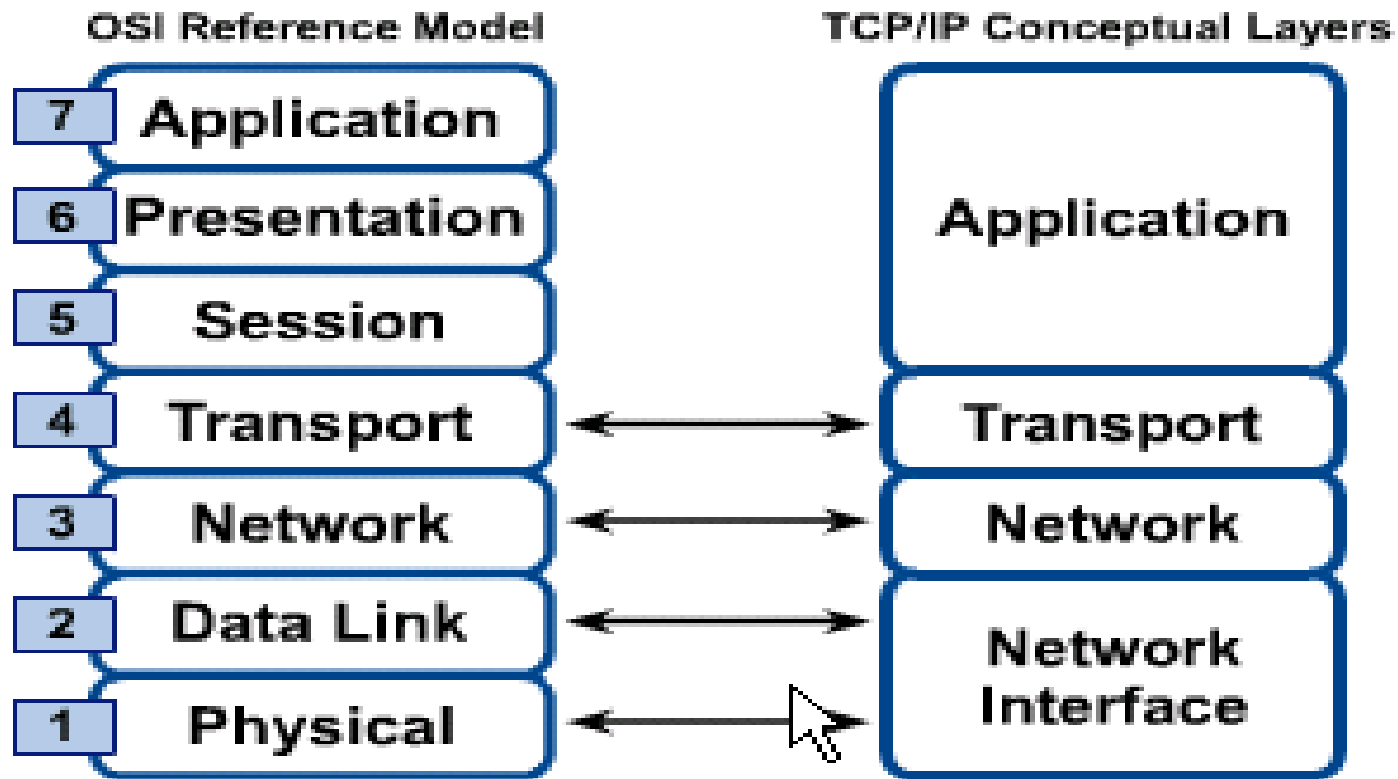
- ▶ The TCP/IP model generally consists of four essential layers
 - Application Layer
 - Host-To-Host Layer/Transport Layer
 - Internet Layer/Network Layer
 - Network Access Layer/Link Layer/Host to network layer

TCP/IP model



- ▶ According to the four-layered architecture, the TCP/IP model divides the data into packets.
- ▶ The TCP/IP model provides both efficiency and standardization, and it is one of the biggest reasons why the TCP/IP model always works.

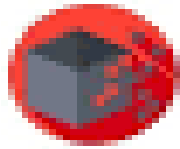
OSI & TCP/IP Models



How does TCP/Ip wprk

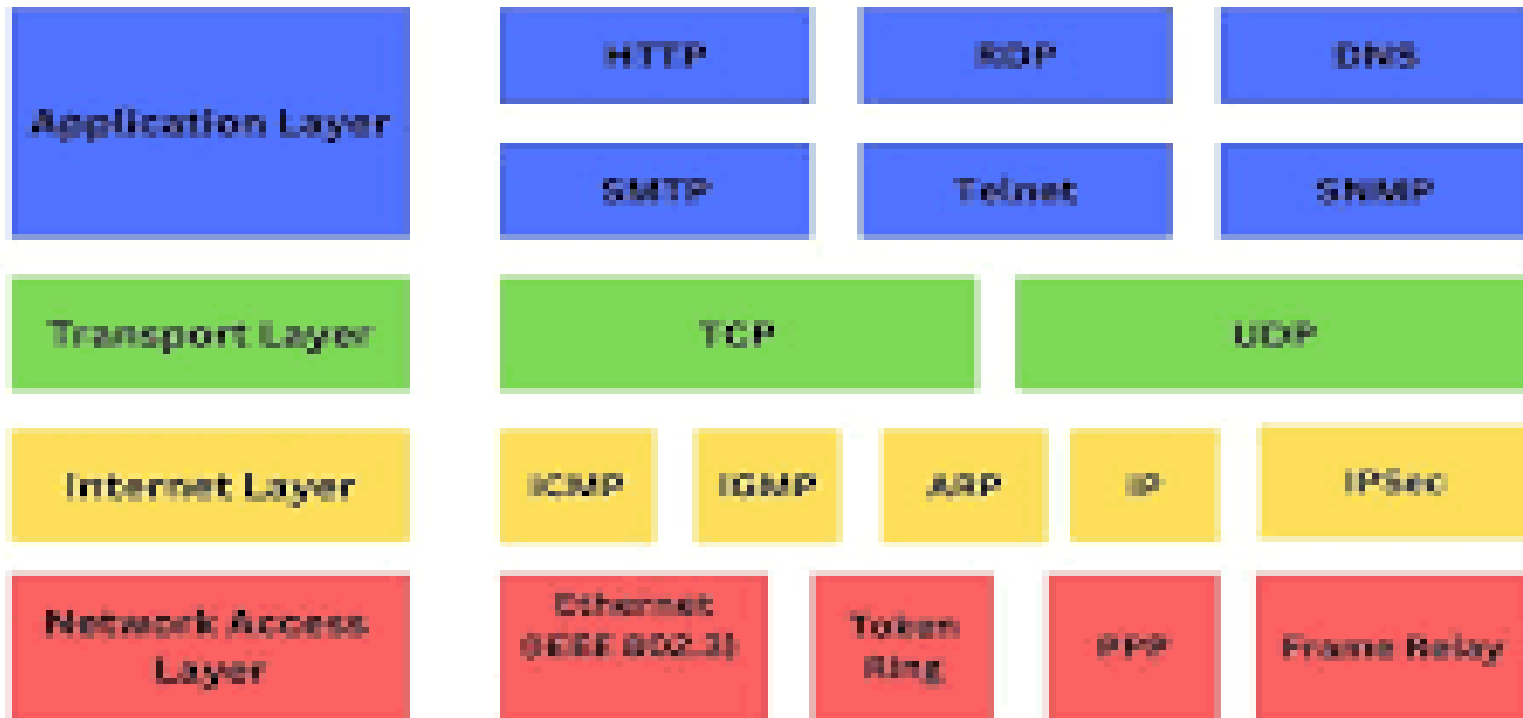
- ▶ The main work of TCP/IP is to transfer the data of a computer from one device to another.
- ▶ The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender.
- ▶ To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.

TCP/IP Model



TCP/IP Layers

Protocols (Examples)



Functions of TCP/IP layers:

- ▶ Functions of **TCP/IP layers:**

 - Network layer**

- ▶ A network layer is the lowest layer of the TCP/IP model.
- ▶ A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- ▶ It defines how the data should be sent physically through the network.
- ▶ This layer is mainly responsible for the transmission of the data between two devices on the same network.

- ▶ The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of **IP addresses into physical addresses**.
- ▶ The technologies used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.

2)Internet Layer

- ▶ An internet layer is the second layer of the TCP/IP model.
- ▶ An internet layer is also known as the **network layer**.
- ▶ The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- ▶ The main **protocols** residing at this layer are as follows:

- ▶ **IP Protocol:** IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.
- ▶ Following are the responsibilities of this protocol:
 - 1) **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
 - 2) **Host-to-host communication:** It determines the path through which the data is to be transmitted.

- ▶ **APR:**–ARP stands for **Address Resolution Protocol**.
- ▶ ARP is a network layer protocol which is used to find the physical address from the known IP address.
- ▶ **AARP:-Reverse Address Resolution Protocol**
- ▶ AARP is a network layer protocol which is used to find the IP address(logical) from the known physical address

ICMP:-

- ▶ ICMP stands for **Internet Control Message Protocol**.
- ▶ It is a mechanism used by the hosts or routers to send notifications regarding datagram (packet) problems back to the sender.
- ▶ A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.

- ▶ The core responsibility of the ICMP protocol is to report the problems. The responsibility of the correction lies with the sender.
- ▶ ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

IGMP

- ▶ IGMP stands for **Internet Group Management Protocol**. It is a protocol that allows several devices to share one IP address so they can all receive the same data. Specifically, IGMP allows devices to join a multicast group.

Transport Layer

- ▶ The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error.
- ▶ End-to-end communication is referred to as such.
- ▶ **Transmission Control Protocol (TCP)** and **User Datagram Protocol (UDP)** are transport layer protocols at this level.

1) Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission. It is connection oriented protocol.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.

- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

2) User Datagram Protocol (UDP)

- User Datagram Protocol (UDP)
- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.

TCP vs UDP: Differences between the protocols

Factor	TCP	UDP
Connection type	Requires an established connection before transmitting data	No connection is needed to start and end a data transfer
Data sequence	Can sequence data (send in a specific order)	Cannot sequence or arrange data
Data retransmission	Can retransmit data if packets fail to arrive	No data retransmitting. Lost data can't be retrieved
Delivery	Delivery is guaranteed	Delivery is not guaranteed
Check for errors	Thorough error-checking guarantees data arrives in its intended state	Minimal error-checking covers the basics but may not prevent all errors
Broadcasting	Not supported	Supported
Speed	Slow, but complete data delivery	Fast, but at risk of incomplete data delivery

TCP vs UDP: Differences between the protocols

Factor	TCP	UDP
Reliability	TCP is more reliable as it provides error checking support and also guarantees delivery of data to the destination router.	UDP, on the other hand, provides only basic error checking support using checksum. So, the delivery of data to the destination cannot be guaranteed in UDP as in case of TCP.
Header size	TCP uses a variable-length (20–60) bytes header.	UDP has a fixed-length header of 8 bytes.
Speed	TCP is comparatively slower than UDP.	UDP is faster as compared to TCP.
Acknowledgment segments	TCP has Acknowledgement segments.	UDP does not have any Acknowledgement segments.
Stream	The connection is a byte stream	Connection is message stream.
Protocols	TCP is used by HTTP ,	UDP is used by DNS , DHCP , ⁸⁸

Application Layer

- ▶ An application layer is the topmost layer in the TCP/IP model.
- ▶ It is responsible for handling high-level protocols, issues of representation.
- ▶ This layer allows the user to interact with the application.

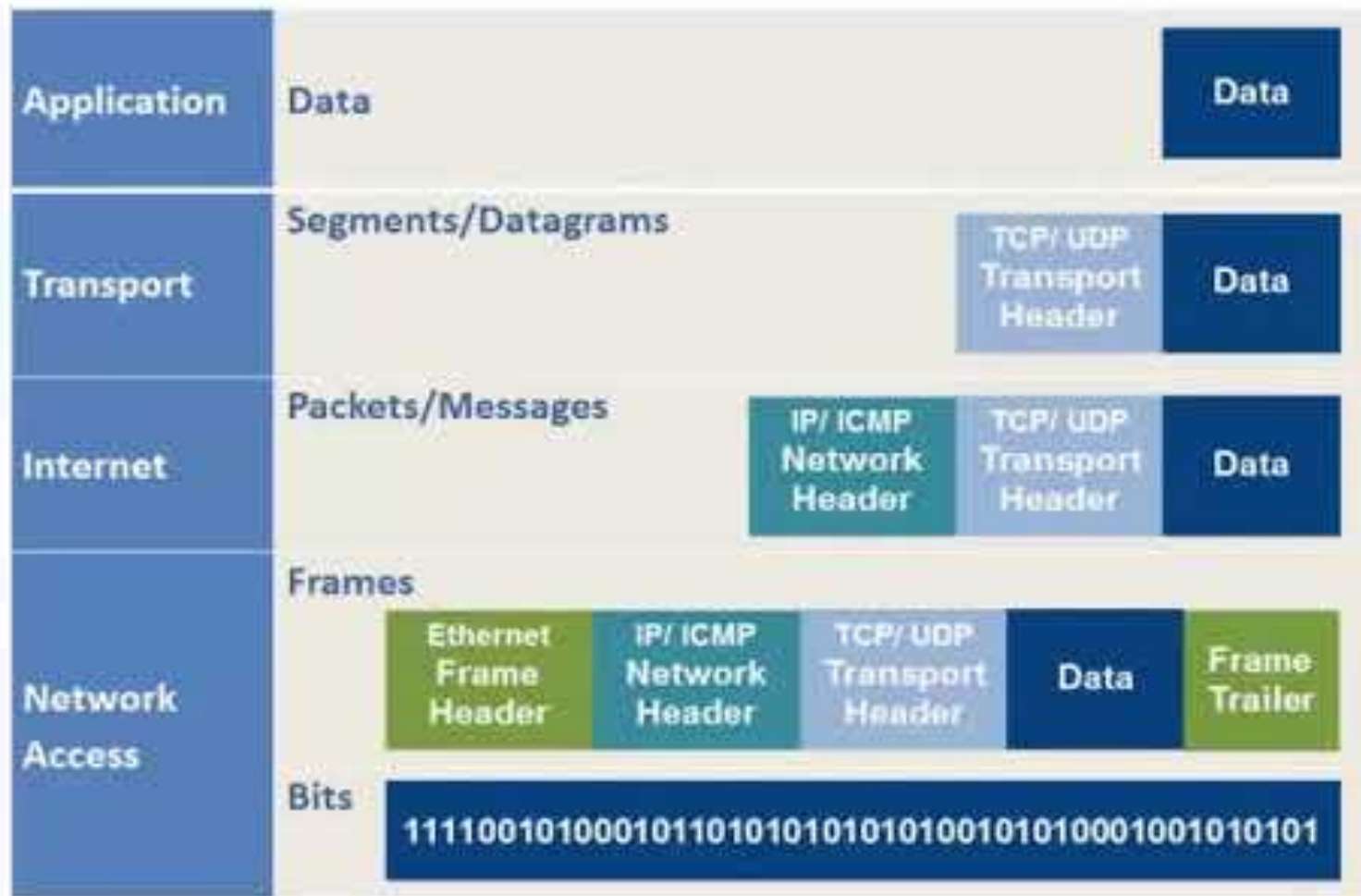
Application Layer protocol

- ▶ **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video.
- ▶ It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- ▶ **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

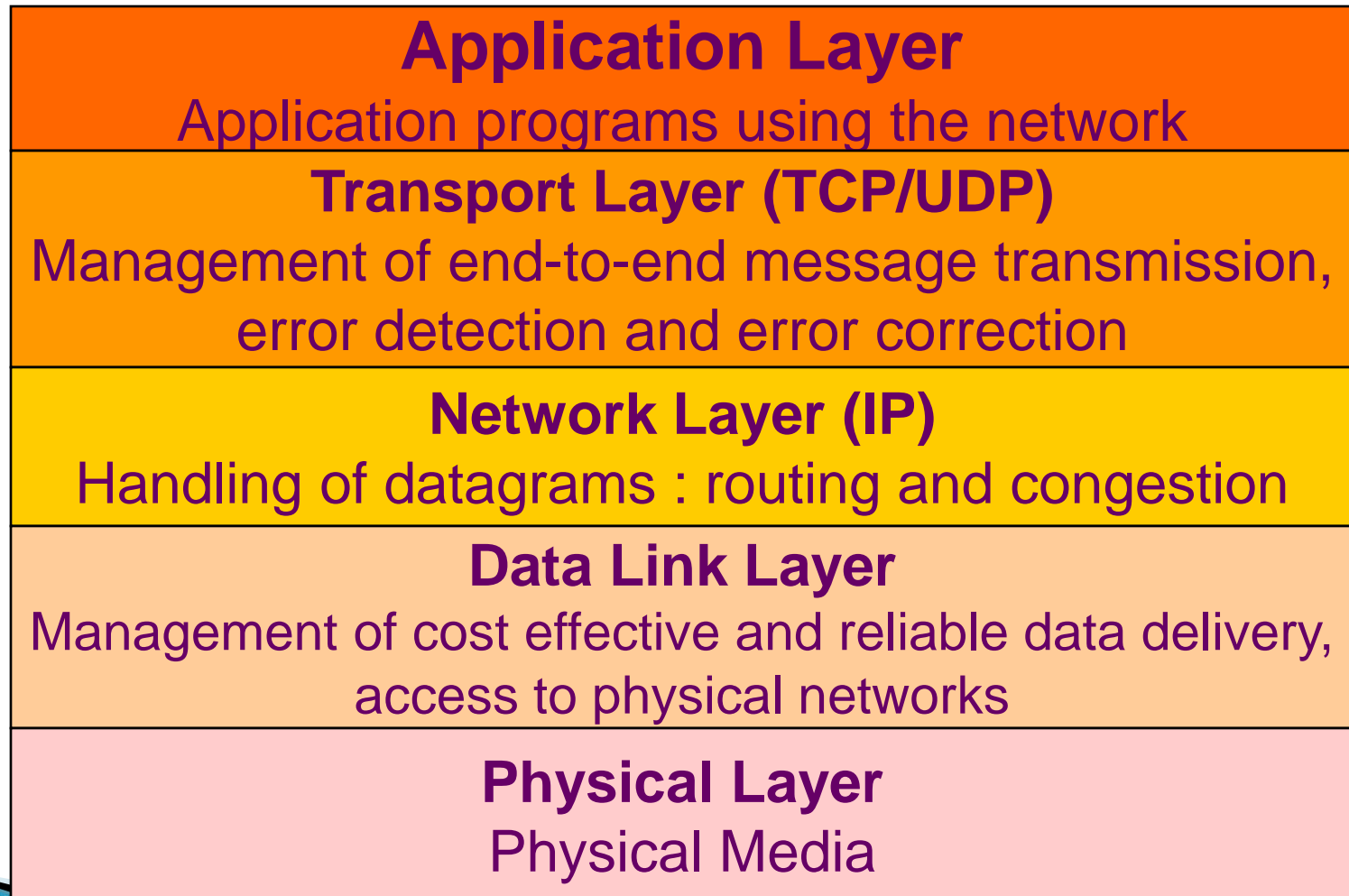
Application Layer

- ▶ **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- ▶ **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

- ▶ **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- ▶ **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.



TCP/IP Model



The advantages of TCP/IP protocol suite are

- ▶ It is an industry–standard model that can be effectively deployed in practical networking problems.
- ▶ It is interoperable, i.e., it allows cross-platform communications among heterogeneous networks.
- ▶ It is an open protocol suite. It is not owned by any particular institute and so can be used by any individual or organization.
- ▶ It is a scalable, client-server architecture. This allows networks to be added without disrupting the current services.
- ▶ It assigns an IP address to each computer on the network, thus making each device to be identifiable over the network. It assigns each site a domain name. It provides name and address resolution services.

The disadvantages of the TCP/IP model are

- ▶ It is not generic in nature. So, it fails to represent any protocol stack other than the TCP/IP suite. For example, it cannot describe the Bluetooth connection.
- ▶ It does not clearly separate the concepts of services, interfaces, and protocols. So, it is not suitable to describe new technologies in new networks.
- ▶ It does not distinguish between the data link and the physical layers, which has very different functionalities. The data link layer should concern with the transmission of frames. On the other hand, the physical layer should lay down the physical characteristics of transmission. A proper model should segregate the two layers.

- ▶ It was originally designed and implemented for wide area networks. It is not optimized for small networks like LAN (local area network) and PAN (personal area network).
- ▶ Among its suite of protocols, TCP and IP were carefully designed and well implemented. Some of the other protocols were developed ad hoc and so proved to be unsuitable in long run. However, due to the popularity of the model, these protocols are being used even 30–40 years after their introduction.

Comparison between TCP/IP and OSI Model

OSI Model	TCP/IP Model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI layers have seven layers.	TCP/IP has four layers.
In the OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are a part of the OSI model.	There is no session and presentation layer in the TCP model.

It is defined after the advent of the Internet.	It is defined before the advent of the internet.
It provides standardization to the devices like router, motherboard, switches, and other hardware devices.	It does not provide the standardization to the devices. It provides a connection between various computers.
In this model, the network layer provides both connection-oriented and connectionless service.	The network layer provides only connectionless service.