KEY ELEMENTS

OF

COMPUTER NETWORK

Authors:

Mr. Chetan N. Rathod [M.C.A., M.Phil.]

VIVEKANAND COLLEGE FOR ADVANCED COMPUTER & INFORMATION SCIENCE, SURAT

Mr. Sagar V.Fegade [M.C.A.]

M.L.PARMAR COLLEGE OF COMPUTER SCIENCE & I.T, SURAT

Ms. Bhumika K. Charnanand [M.C.A., M.Phil.]

PRABHU B.C.A. COLLEGE, UMRA, SURAT

Jump2Learn

Unit - 2

The layering Models and Data Communication

Jump2Learn

2.1 Introduction to OSI model with all layers

OSI Model

- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.
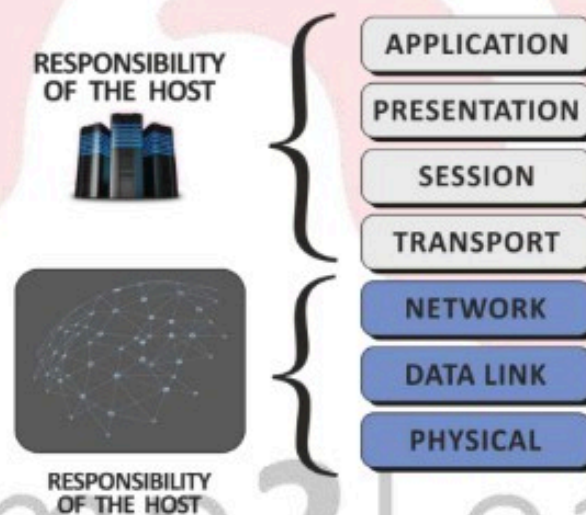
Characteristics of OSI Model:

Figure 2.1

- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

Functions of the OSI Layers

There are the seven OSI layers. Each layer has different functions. Lists of seven layers are given below:

1) Physical Layer
2) Data-Link Layer
3) Network Layer
4) Transport Layer
5) Session Layer

5) Session Layer
6) Presentation Layer
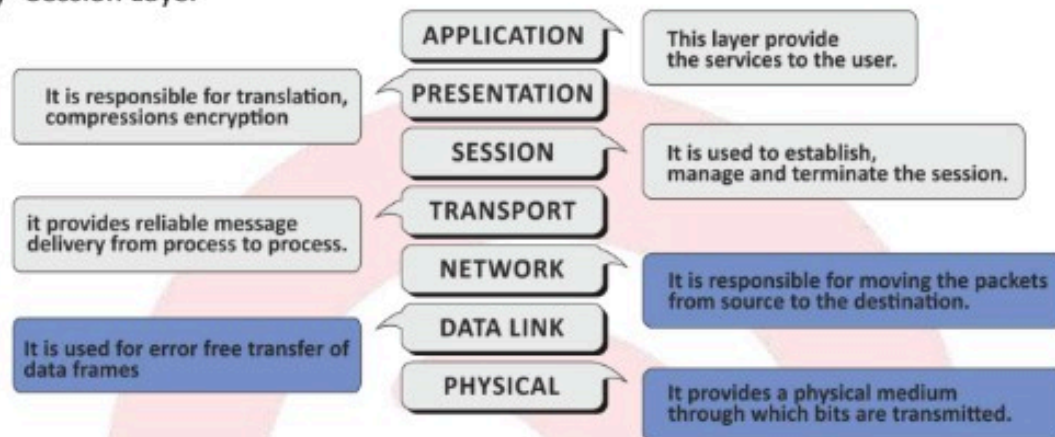7) Application Layer

Figure 2.2

Physical layer :-

1. The physical layer responsible for sending bits from one computer to another .
2. The physical layer is not concerned with the meaning of the bits but it deals with physical connection to the network and with transmission and reception of signals.
3. The physical level is used to defined physical and electrical such as what will represent a 1 or a 0 how many pins network will have, how data will be synchronized and when the network adapter may or may not transmit the data.
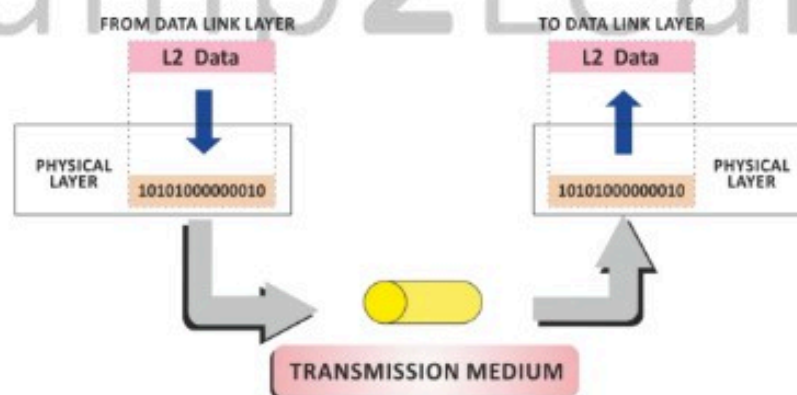4. The position of the physical layer with respect to transmission medium and the data link layer
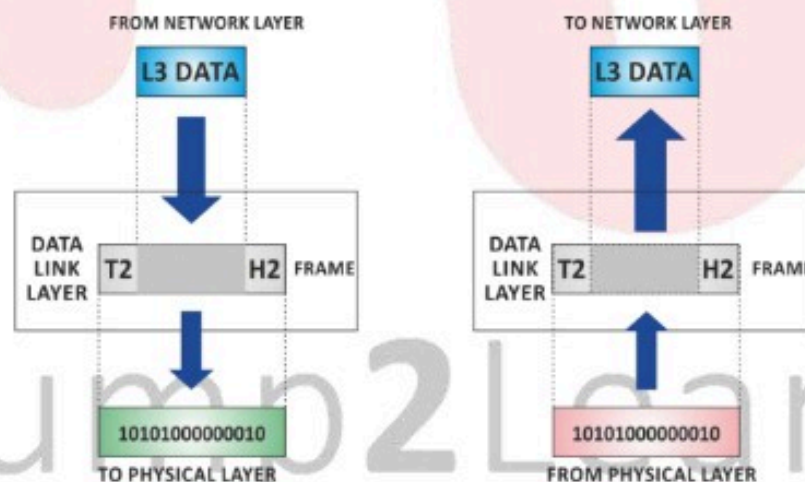

FIGURE 2.3

Following are the function of the physical layer:-

1. To defined the typed of encoding i.e. how 0's and 1's are changed to signals.
2. To defined the transmission rate i.e. the number of bits transmitted per second.
3. To deal with the synchronization of the transmitter and receiver.
4. To deal with network connection types, including multipoint and point to point connection.
5. To deal with physical topologies i.e. bush, star, ring or mesh.
6. To deal with media bandwidth i.e. baseband broadband transmission .
7. Multiplexing which deals with combining several data channels into one.
8. To defined characteristics between the device and the transmission medium.
9. To defined the transmission mode between to device i.e. whether it should be simplex, half duplex or full duplex.

Data Link Layer :-

It is responsible for reliable node to node delivery of the data. It accepts packets from the network layer form frames give it to the physical layer.

FIGURE 2.4

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- 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:

Logical Link Control Layer

- It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
- It identifies the address of the network layer protocol from the header.
- It also provides flow control.

Media Access Control Layer

- A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
- It is used for transferring the packets over the network.

Functions of the Data-link layer

- Framing: The data link layer translates the physical's raw bit stream into packets known as 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.

Header	Packet	Trailer
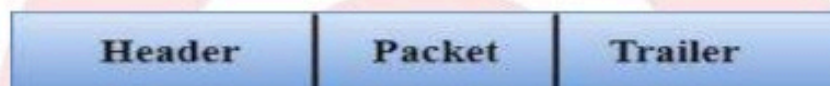
- Physical Addressing: The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- Flow Control: Flow control is the main functionality of the Data-link layer. It is the technique through which the 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.
- Error Control: Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- Access Control: When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.
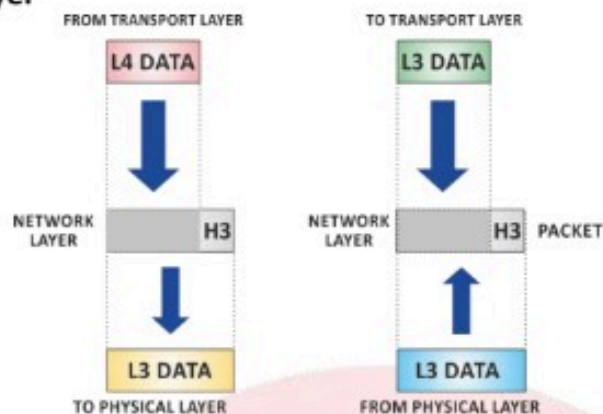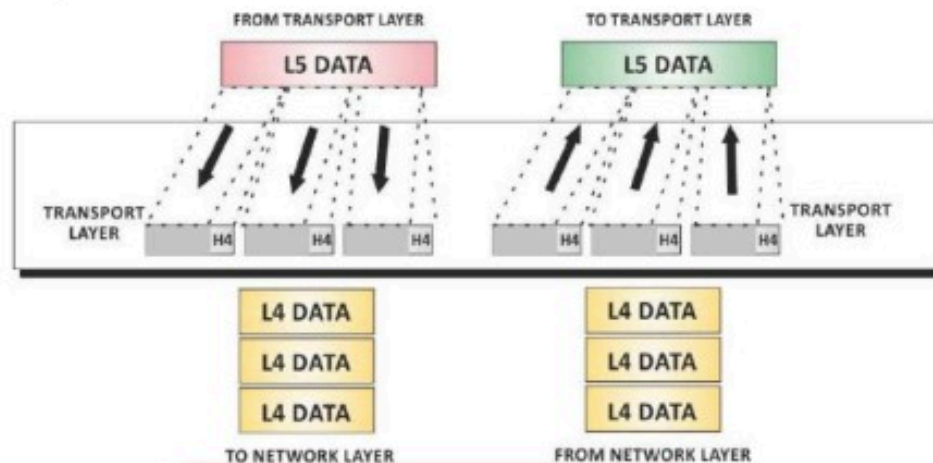
Network Layer

FIGURE 2.5

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **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.
- **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).

Transport Layer:

FROM TRANSPORT LAYER | TO TRANSPORT LAYER

L5 DATA | L5 DATA

TRANSPORT LAYER | H4 | H4 | H4 | H4 | H4 | H4 | TRANSPORT LAYER

L4 DATA | L4 DATA
L4 DATA | L4 DATA
L4 DATA | L4 DATA

TO NETWORK LAYER | FROM NETWORK LAYER

FIGURE 2.6

- 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.

The two protocols used in this layer are:
- **Transmission Control Protocol**
    - It is a standard protocol that allows the systems to communicate over the internet.
    - It establishes and maintains a connection between hosts.
    - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

- **User Datagram Protocol**
    - User Datagram Protocol is a transport layer protocol.
    - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

- **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. 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.

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

- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.
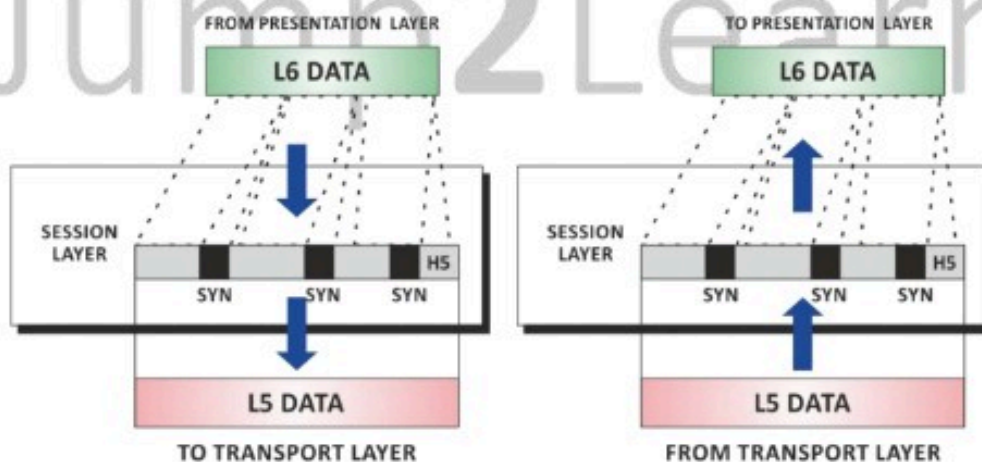
Session Layer:

FIGURE 2.8

- It is a layer 3 in the OSI model.

- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. 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.
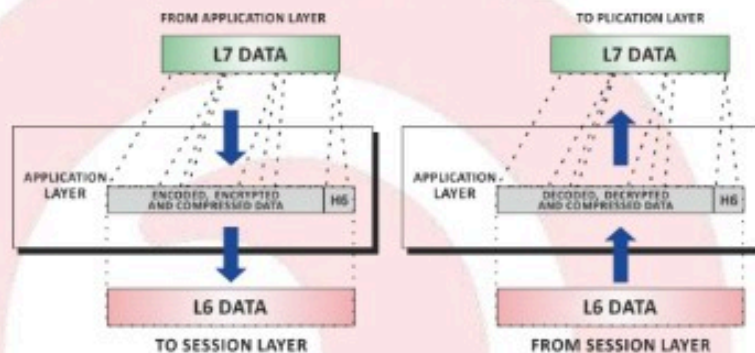
Presentation Layer

FIGURE 2.8

- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.

- It acts as a data translator for a network.

- This layer is a part of the operating system that converts the data from one presentation format to another format.

- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- Translation: The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

- Encryption: Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- 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.
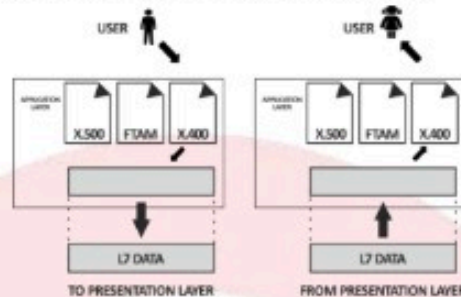
Application Layer

FIGURE 2.9

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.

- This layer provides the network services to the end-users.

Functions of Application layer:
- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- **Directory services:** An application provides the distributed database sources and is used to provide that global information about various objects.

CP/IP model
- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four

10

layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.

- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:
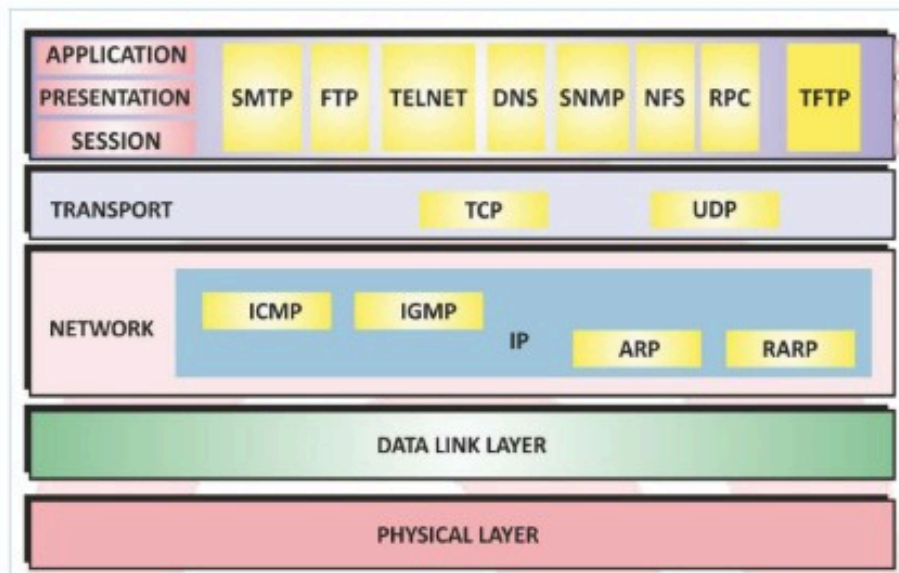
FIGURE 2.10

Network Access 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 protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.

11

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.

Following are the protocols used in this layer are:

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:

- **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.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for Address Resolution Protocol.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- The two terms are mainly associated with the ARP Protocol:
    - ARP request: When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
    - ARP reply: Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- ICMP stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram 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.
- An ICMP protocol mainly uses two terms:
    - ICMP Test: ICMP Test is used to test whether the destination is reachable or not.
    - ICMP Reply: ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. 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.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being   sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission**

Control protocol.

- **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.
    - **UDP consists of the following fields:** Source port address: The source port address is the address of the application program that has created the message.
    - **Destination port address:** The destination port address is the address of the application program that receives the message.
    - **Total length:** It defines the total number of bytes of the user datagram in bytes.
    - **Checksum:** The checksum is a 16-bit field used in error detection.
- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.
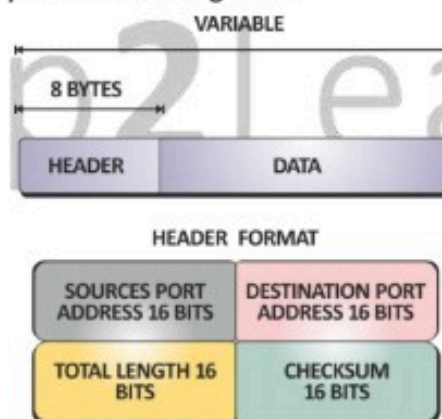

FIGURE 2.11

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.
- 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.

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.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using HTTP protocol to interact with the network where HTTP protocol is an application layer protocol.

Following are the main protocols used in the application layer:
- **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.

- **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.

2.2 Differences between OSI Model & TCP/IP model

OSI(Open System Interconnection)	TCP/IP (Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.

7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

2.3 Data Communication Model, Digital and Analog data and signals (Chapter-1)

bit rate, baud, bandwidth, Nyquist bit rate

Bit rate

Bit rate is defined as the transmission of number of bits per second.

Bit rate is also defined as per second travel number of bits.

Bit rate emphasized on computer efficiency.

The formula of **Bit Rate** is: = baud rate x the number of bit per baud

Bit rate is not used to decide the requirement of bandwidth for transmission of signal.

Baud Rate

Baud rate is defined as the number of signal units per second.

Baud rate is also defined as per second number of changes in signal.

While baud rate emphasized on data transmission.

The formula of Baud Rate is: = bit rate / the number of bit   While baud rate is used to decide the requirement of bandwidth for transmission of signal.

Bandwidth

In computer networking, the term bandwidth is refers to as the measure of the capacity of a medium to transmit 'data. A medium that has a high capacity, has high bandwidth, whereas a medium that has limited capacity has low bandwidth. Bandwidth can be best- understood by comparing it to its hose. If half-inch garden hose can carry water from a trickle up two gallons per minute, that hose can be said to have a bandwidth gallons per minute. A four-inch fire hose, however, might have a bandwidth that exceeds 100 gallons per minute.

Data transmission rates are frequently stated in terms of bits that can be transmitted per second. An Ethernet LAN theoretically can transmit 10 - million bits per second and has a bandwidth of 10 megabits per second (Mbps).

The bandwidth that a cable can accommodate is determined in part by the cable's length. A short cable generally can accommodate greater bandwidth than a longer cable, which is one reason why all cable designs specify maximum length for cable runs. Beyond those limits, the highest-frequency signals can deteriorate, and errors begin to occur in data signals.

The two ways to allocate the capacity of transmission media are with baseband and broadband transmissions. Baseband devotes the entire capacity of the medium to one communication channel. Broadband lets two or more communication channels share the bandwidth of the communication medium. Baseband is the most common mode of operation. Most LANs function in baseband mode, for Sample baseband signaling can be accomplished with both analog digital signals.

Although you might not realize it, you have a great deal of experience with broadband transmission. Consider for example, that the TV cable coming into your house from an antenna or cable provider is a broadband medium. Many television signals, can share the bandwidth of cable because each signal is modulated using a separately assigned frequency. You can use the television tuner to choose the channel you want to watch by selecting its frequency, This technique of dividing bandwidth into frequency band is called as frequency division multiplexing (FDM) and works only with analog signals. Another technique, called time division multiplexing (TDM), also supports digital signals.

Nyquist bit rate:

Nyquist gives the upper bound for the **bit rate** of a **transmission** system by calculating the bit rate directly from the number of **bits** in a symbol (or signal levels) and the bandwidth of the system (assuming 2 symbols/per cycle and first harmonic).