Chapter-1 Introduction MIMP Questions

Q.1 Define Following Term: (May-2016)

Ans:

1. Protocol

A protocol is a standard set of rules that allow electronic devices to communicate with each other. These rules include what type of data may be transmitted, what commands are used to send and receive data, and how data transfers are confirmed.

2. Half Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.

3. end to end delay

End-to-end delay or one-way delay refers to the time taken for a packet to be transmitted across a network from source to destination.

End-to-end-delay in networks comes from several sources including

- transmission delay
- propagation delay
- processing delay
- queuing delay

4. Internet

The internet is a globally connected network system that uses TCP/IP to transmit data via various types of media. The internet is a network of global exchanges – including private, public, business, academic and government networks – connected by guided, wireless and fiber-optic technologies

5. Throughput

Throughput is the data per second that can be transferred by a network connection at a point in time.

Q.2 Explain working of packet switched networks. (Nov-2016)

Ans:

- Packet switching was designed to provide a more efficient facility than circuit-switching for bursty data traffic.
- With packet switching, a station transmits data in small blocks, called packets.
- At each node packets are received, stored briefly (buffered) and passed on to the next node.
  1. **Store and forward mechanism**
- Each packet contains some portion of the user data plus control info needed for proper functioning of the network.

- A key element of packet-switching networks is whether the internal operation is datagram or virtual circuit (VC).

  1. With internal VCs, a route is defined between two endpoints and all packets for that VC follow the same route.

  2. With internal diagrams, each packet is treated independently, and packets intended for the same destination may follow different routes.
- Examples of packet switching networks are X.25, Frame Relay, ATM and IP.
- Station breaks long message into packets. Packets sent one at a time to the network.
- Packets handled in two ways:
  1. **Datagram**
     - Each packet treated independently
     - Packets can take any practical route
     - Packets may arrive out of order
     - Packets may go missing
     - Up to receiver to re-order packets and recover from missing packets
  2. **Virtual Circuit**
     - Preplanned route established before any packets sent.
     - Once route is established, all the packets between the two communicating parties follow the same route through the network
     - Call request and call accept packets establish connection (handshake)
     - Each packet contains a Virtual Circuit Identifier (VCI) instead of destination address.
     - No routing decisions required for each packet
     - Clear request to drop circuit
     - Not a dedicated path
  3. **Message Switching**
     - This technique was somewhere in middle of circuit switching and packet switching.
     - In message switching, the whole message is treated as a data unit and is transferred in its entirety.
     - A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop.
       a. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.

Q.3 Explain Dial up, DSL and FTTH in brief

Ans:

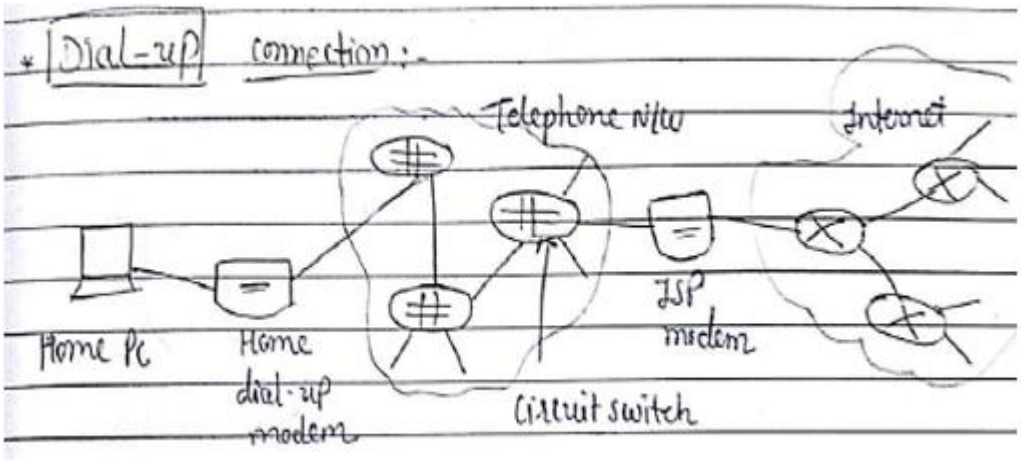
Dial Up:

A dial-up is a connection that is established using a modem. To make the dial-up connection the modem must be connected to an active phone line that is not in use. When connecting the modem will pick up the phone and dial a number that is attached to another computer. After the connection has been made the computer can check e-mail, browse the Internet, and share files.

Drawback of Dial up connection

- It is extremely slow, Maximum speed provides only 56 kbps
- It will connect with phone line so that only one task can be performed at a time either user can access internet or phone calls.
- During accessing internet if phone call comes then internet will be disconnect.

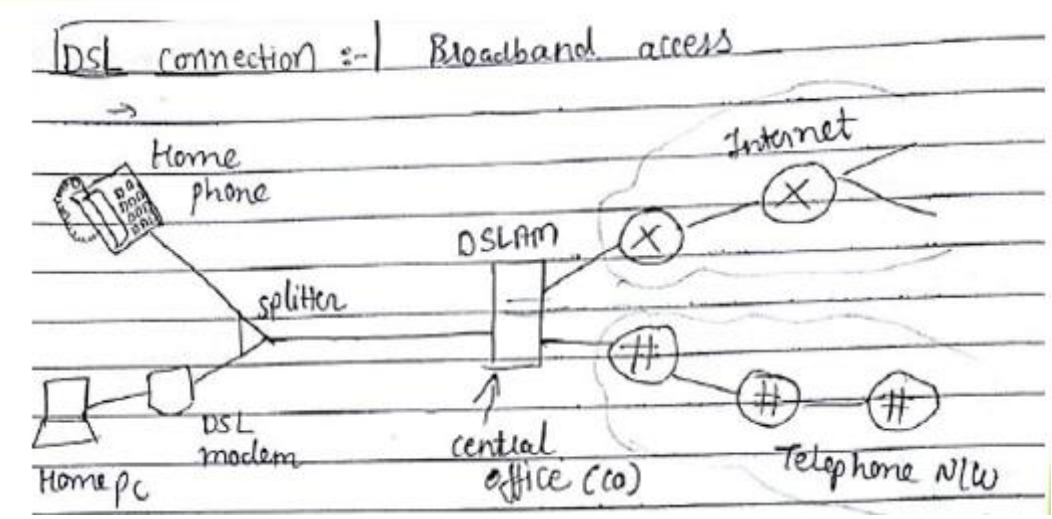
- User can only attempt phone call or use internet at a time.



Dial up Connection

DSL

- DSL: Digital Sub Scriber Line
- It uses existing telephone line (twisted pair) to exchange data with DSLAM (Digital Subscriber Line Access Multiplexer.
- Telephone line carries both data and telephone signals with different frequencies.
- Due to frequency division telephone and internet can share connection at the same time.
- User can use both internet and phone calls at a time.



DSL Connection

Advantages of DSL Connection

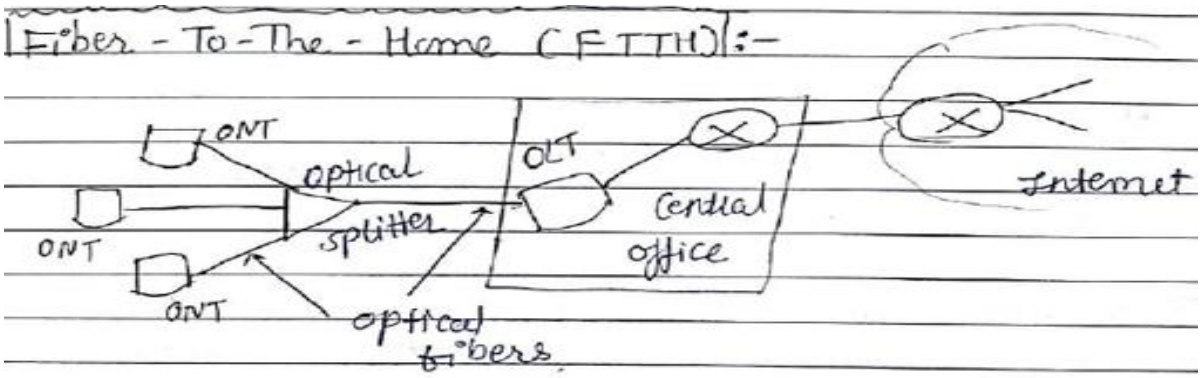
- Transmit and receive data at much higher rates
- Phone calls and internet can be accessed simultaneously
- “Always on” means permanent connection

FTTH

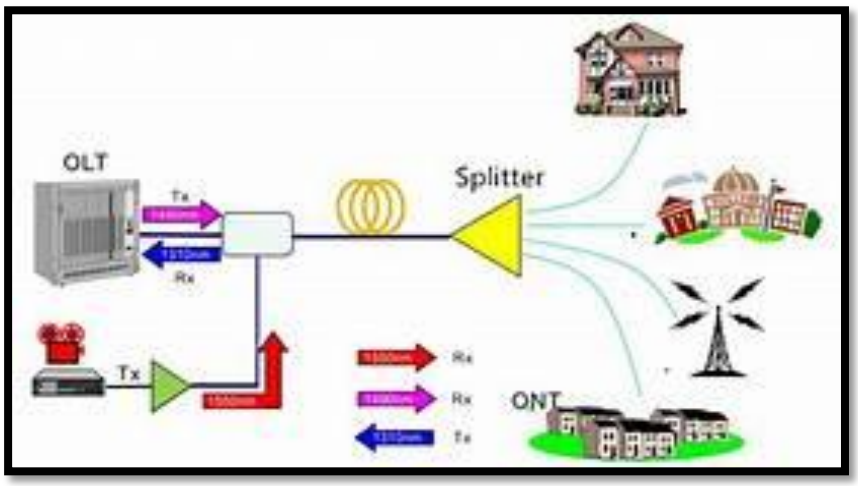
- Fiber to the home (FTTH), also called "fiber to the premises" (FTTP), is the installation and use optical fiberfrom a central point directly to individual buildings such as residences, apartment buildings and businesses to provide unprecedented high-speed Internet access.
- FTTH dramatically increases the connection speeds available to computer users compared with technologies now used in most places.
- While FTTH promises connection speeds of up to 100 megabits per second (Mbps) -- 20 to 100 times as fast as a typic cable modem or DSL (Digital Subscriber Line) connection -- implementing

FTTH on a large scale will be costly because it will require installation of new cable sets over the "last links" from existing optical fiber cables to individual users.

- Some communities currently enjoy "fiber to the curb" (FTTC) service, which refers to the installation and use of optical fiber cable to the curbs near homes or businesses, with a "copper" medium carrying the signals between the curb and the end users.



ONT: Optical Network Terminal
OLT: Optical Line Terminal



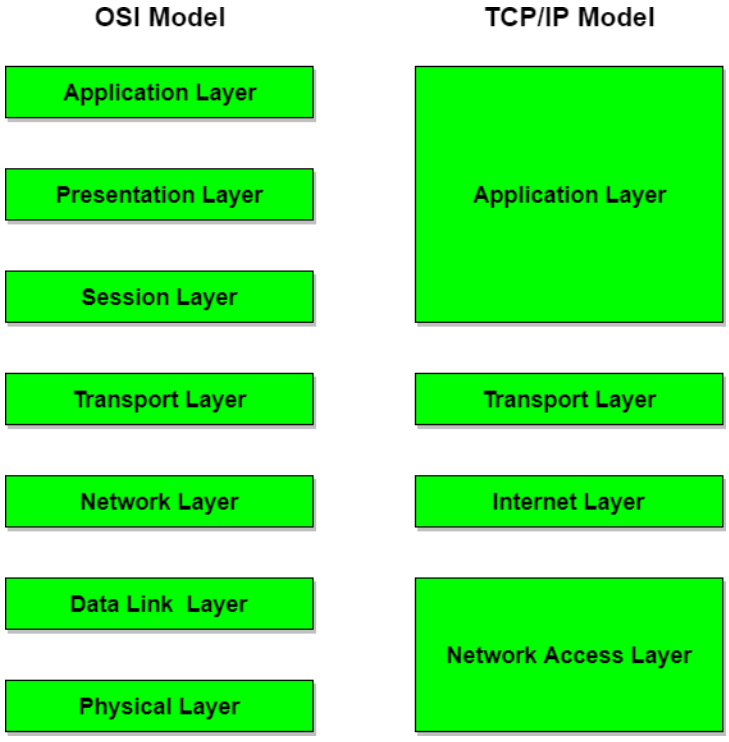
FTTH Connection

Q.4 Differentiate TCP/IP stack and OSI reference model. (Nov-2016)

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

Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model



Q.5 How encapsulation is helpful in data transmission? Explain with example on layered architecture of computer networks. (Nov-2016)

Ans:

- Data encapsulation refers to sending data where the data is augmented with successive layers of control information before transmission across a network.

- The reverse of data encapsulation is decapsulation, which refers to the successive layers of data being removed (essentially unwrapped) at the receiving end of a network.
- Different type of encryption techniques are used to protect the data or any other information from leaking and from illegal use. So another important technique is used to protect the data during transmission is called as data encapsulation.
- Literally encapsulation means to wrap up or hide so in data encapsulation different type of protocol layers are used to hide the specifications and the personal information is called as data encapsulation. It is also called as the data hiding because in this data is hiding and then transfer from one device to another with the help of protocols layers.
- When a network device sends a message, the message will take the form of a packet. Each OSI (open system interconnection) model layer adds a header to the packet.
- The packet is then covered with some information directing it onward to a destination; this is analogous to the address on a letter in which the actual message is carried inside the envelope.
- Similarly, the message in the packet is encapsulated with some information such as the address of next node, protocol information, the type of data and the source and destination addresses.

Data Encapsulation Process:

- The process of the data encapsulation has different steps at different layers of OSI model. These steps of process of data encapsulation are as follows:

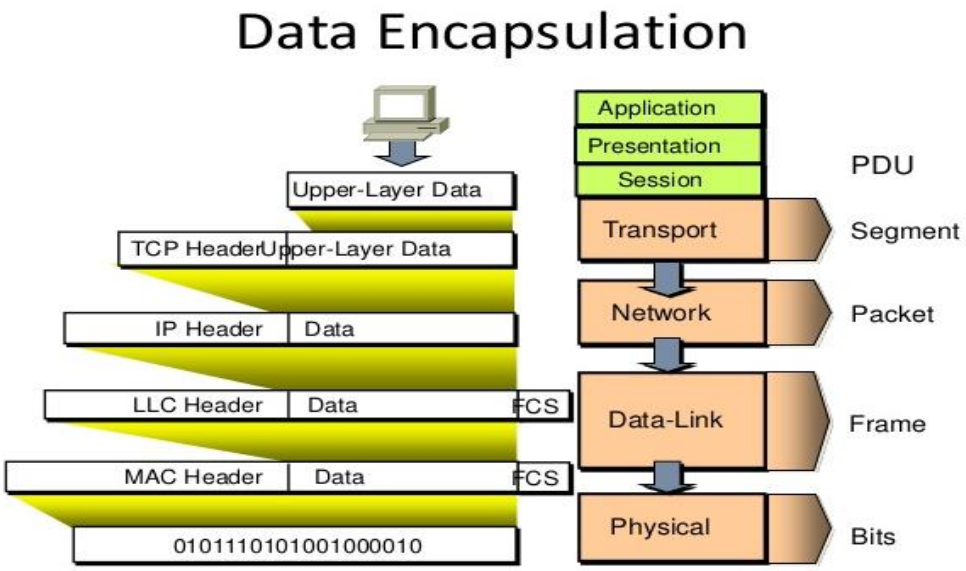
1. Encapsulate TCP Header(Application Layer)
2. Encapsulate IP Header(Network Layer)
3. MAC Header Encapsulation(Data Link Layer)
4. Physical Layer Encapsulation

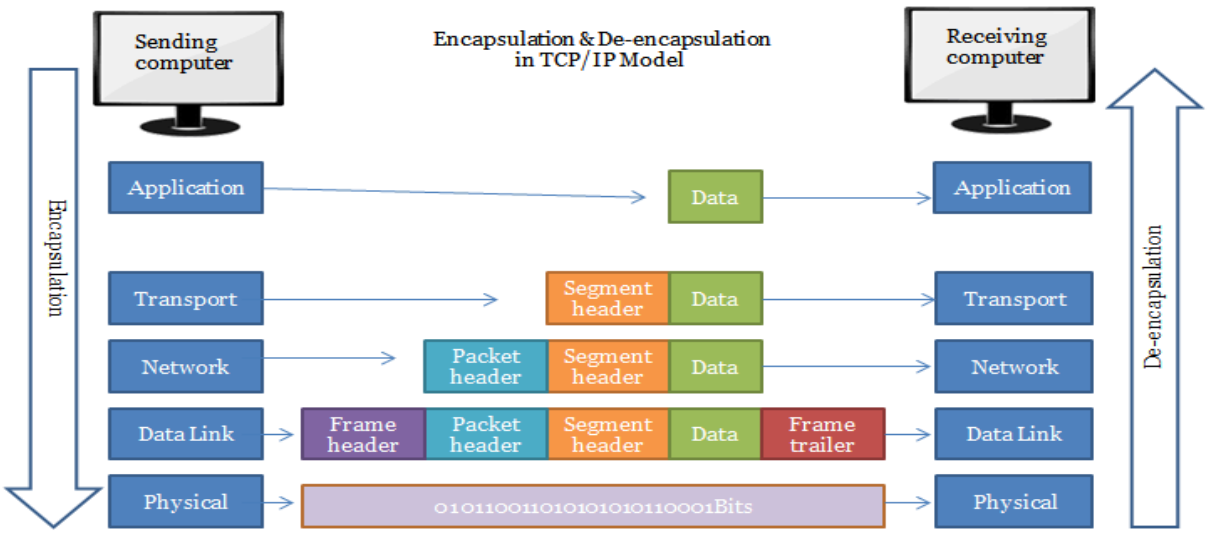
Reasons of Data Encapsulation:

- Every programming has to be done on the basis of some reasons so, data encapsulation also have some reasons which are listed below:

1. trying to use the object again
2. for the sake of independent message or information
3. Keep the architecture legal of object.

- The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. The original version of the model defined seven layers.
- A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that comprise the contents of that path. Two instances at the same layer are visualized as connected by a horizontal connection in that layer.





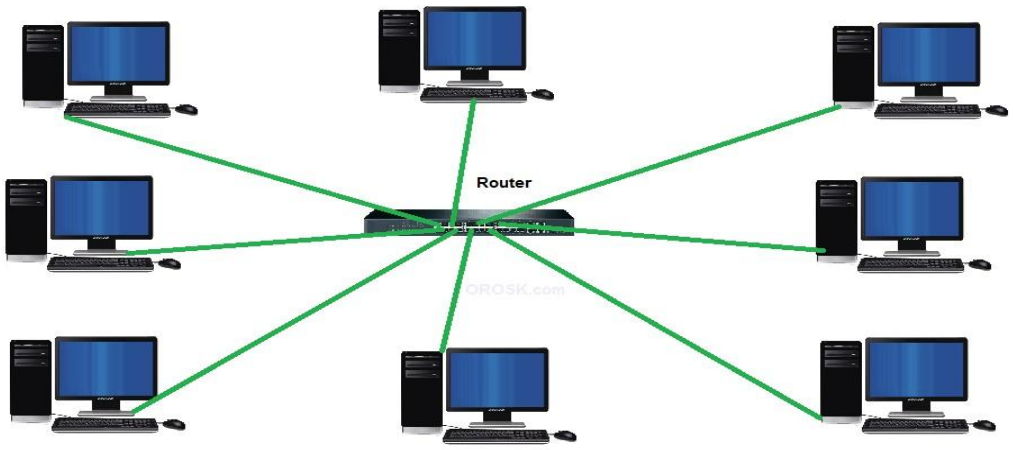
Q.6 What is topology? Explain star topology in brief. (May-2016, June-2017, Nov-2017)

Ans:

- In the bus network topology, every workstation is connected to a main cable called the bus. Therefore, in effect, each workstation is directly connected to every other workstation in the network.
- In the star network topology, there is a central computer or server to which all the workstations are directly connected. Every workstation is indirectly connected to every other through the central computer.
- In the ring network topology, the workstations are connected in a closed loop configuration. Adjacent pairs of workstations are directly connected. Other pairs of workstations are indirectly connected, the data passing through one or more intermediate nodes.
- If a Token Ring protocol is used in a star or ring topology, the signal travels in only one direction, carried by a so-called token from node to node.
- The mesh network topology employs either of two schemes, called full mesh and partial mesh. In the full mesh topology, each workstation is connected directly to each of the others. In the partial mesh topology, some workstations are connected to all the others, and some are connected only to those other nodes with which they exchange the most data.

- The tree network topology uses two or more star networks connected together. The central computers of the star networks are connected to a main bus. Thus, a tree network is a bus network of star networks.

Star topology



- Alternatively referred to as a star network, star topology is one of the most common network setups. In this configuration, every node connects to a central network device, like a hub, switch, or computer.
- The central network device acts as a server and the peripheral devices act as clients. Depending on the type of network card used in each computer of the star topology, a coaxial cable or an RJ-45 network cable is used to connect computers together.
- The picture to the right shows how this network setup gets its name, as it is shaped like a star.

Advantages of star topology:

- Centralized management of the network, through the use of the central computer, hub, or switch.
- Easy to add another computer to the network.
- If one computer on the network fails, the rest of the network continues to function normally.

Disadvantages of star topology:

- May have a higher cost to implement, especially when using a switch or router as the central network device.
- The central network device determines the performance and number of nodes the network can handle.
- If the central computer, hub, or switch fails, the entire network goes down and all computers are disconnected from the network.

Q7. Explain following terms: (May-2015, Dec-2015, May-2016)

1) Processing Delay
2) Transmission Delay
3) Queuing Delay
4) Propagation Delay

Ans:

1) Processing Delay:

- It is also known as Nodal Processing.

- Time required examining packets header & determining where to send the packets is a part of processing delay.
- In other words, starting time taken to check destination address or bit level error is known as processing delay means delay from the beginning of the process.
- For ex: Train is late by 2 hours from its arrival time.

2) Transmission Delay:

- This is the amount of time required to push the entire packet into the link.
- In other words, amount of time to require all the packets which is in queue to go to the link.
- For ex: Time to leave all the compartments of the train will be leave the platform or time required all the train which is in queue leave the platform.
- If the length of packet is L bits and transmission rate is R bit/second then,
- Delay=L/R second

3) Queuing Delay:

- Time required to wait for transmission on the link is a part of queuing delay.
- If Queue is empty when packet arrives than there will be 0 delay and if there is heavy traffic then Queuing Delay will be more.
- In other words, if packet needs to wait for transmission due to traffic is known as Queuing delay.
- For ex: Due to delay in arrival time in 1st train other train will be late & it will stand in Queue to reach the platform and wait for train when it leaves the platform & signals for next train.

4) Propagation Delay:

- The time required to send packet from one of link to the next node is known as propagation delay.
- In other words , time taken by packet from one mode to another mode
- Distance between 2 router/speed = d/2

Q.8 Define and explain following terms: (june-2017)

a) Delay
b) Throughput
c) Loss

Ans:

a) Delay:

- The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another.
- It is typically measured in multiplies or fractions of second.
- Delay may differ slightly, depending on the location of the specific pair of communicating nodes.
    - **Types of delay**
        - There are four types of delay.
        - Processing Delay or Nodal Processing
        - Queuing Delay
        - Transmission Delay
        - Propagation Delay

b) Throughput

- Throughput or Network Throughput is the rate of successful message delivery over a communication channel.

- The data these messages belong to may be delivered over a physical or logical link or it can pass through a certain network node.
- Throughput is usually measured in bits per second(bits or bps),and sometimes in data packets per second (p/s or pps)or data packets per time slot.

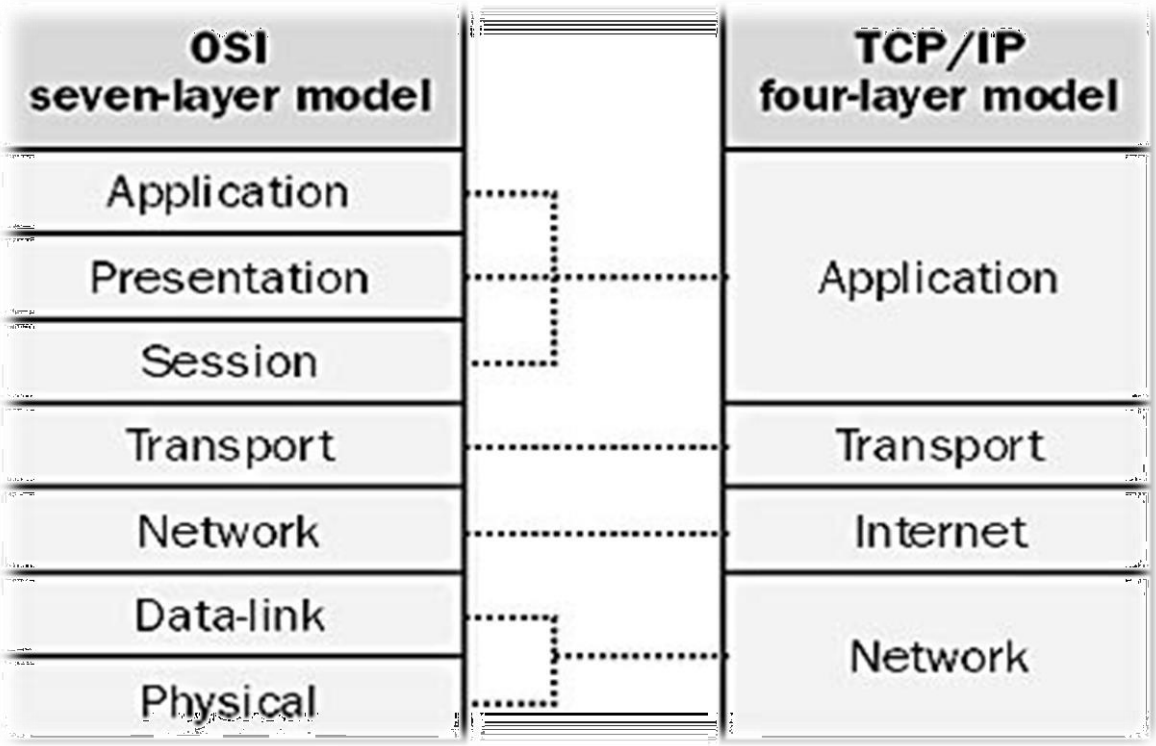
c) Packet Loss

- Packet loss is the failure of one or more transmitted packets to arrive at their destination.
- This event can cause noticeable effects in all types of digital communications.
- The loss of data packets depends on the switch queue.
- The loss of data packets increases with the increase in the traffic intensity.
- It affects the performance of the network.

Q.9 Draw the layered architecture of TCP/IP model and write at least two services provided by each layer of the model.

Ans.

- TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network.
- The TCP/IP model has five layers.
    - Application Layer
    - Transport Layer
    - Internet Layer
    - Network Interface



Application Layer:

- The application layer is the topmost layer of the four-layer TCP/IP model.
- The application layer is present on the top of the Transport layer Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

- Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP(Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol),
- DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Transport Layer:

- The purpose of the Transport layer is to permit devices on the source and destination hosts to carry on a conversation.
- Transport layer defines the level of service and status of the connection used when transporting data.
- The transport layer provides the end-to-end data transfer by delivering data from an application to its remote peer.
- The most-used transport layer protocol is the Transmission Control Protocol (TCP), which provides:
    - Reliable delivery data
    - Duplicate data suppression
    - Congestion control
    - Flow control
- Another transport layer protocol is the User Datagram Protocol (UDP), which provides:
    - Connectionless
    - Best-effort service
    - Unreliable
- UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.
- Transport layer defines the level of service and status of the connection used when transporting data.
- The transport layer provides the end-to-end data transfer by delivering data from an application to its remote peer.
- The most-used transport layer protocol is the Transmission Control Protocol (TCP), which provides:
    - Reliable delivery data
    - Duplicate data suppression
    - Congestion control
    - Flow control
- Another transport layer protocol is the User Datagram Protocol (UDP), which provides:
    - Connectionless
    - Best-effort service
    - Unreliable
- UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.

Internet Layer:

- The internet layer also called the network layer.

- Internet layer pack data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks.
- The Internet layer is also responsible for the routing of IP datagrams. Internet Protocol (IP) is the most important protocol in this layer.
- It is a connectionless protocol that does not assume reliability from lower layers. IP does not provide reliability, flow control or error recovery.
- IP provides a routing function that attempts to deliver transmitted messages to their destination.
- These message units in an IP network are called an IP datagram. Example: IP, ICMP, IGMP, ARP, and RARP.

Network Interface:

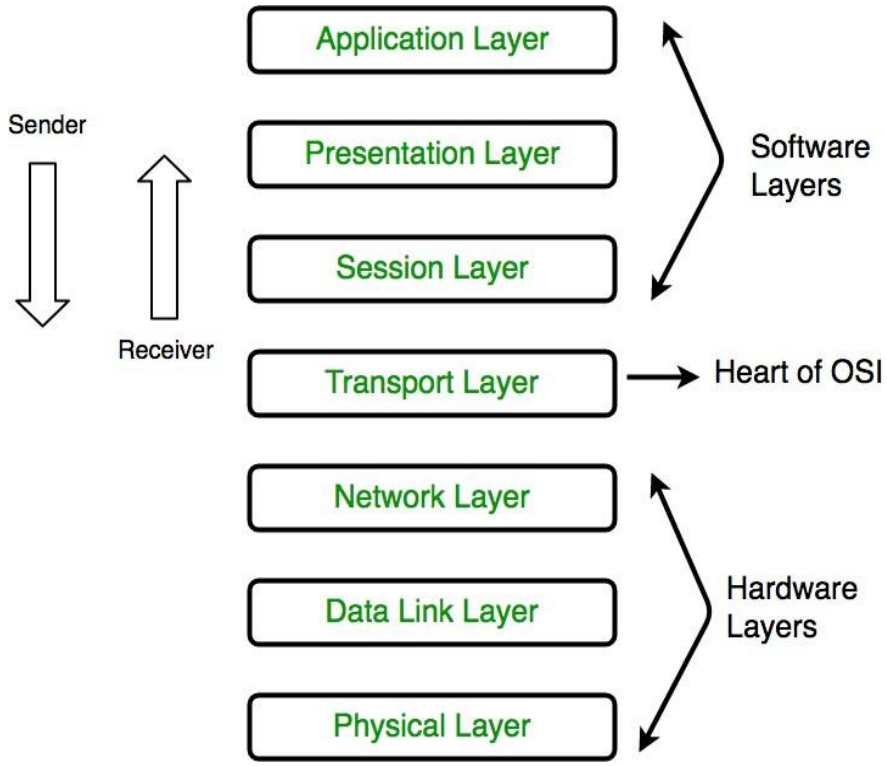
- Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signalled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.
- The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

Q. 10 Draw the layered architecture of OSI reference model and write the at least two services provided by each layer of the model. (May-2015, Nov-2017)

Ans.:

OSI stands for Open Systems Interconnection.

- It has been developed by ISO – 'International Organization of Standardization', in the year 1974. It is 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.



1. Physical Layer (Layer 1):

- The functions of the physical layer are :
- Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
- Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
- Transmission mode: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full- duplex.
- Hub, Repeater, Modem, Cables are Physical Layer devices.
- Network Layer, Data Link Layer and Physical Layer are also known as Lower Layers or Hardware Layers.

2. Data Link Layer (DLL) (Layer 2):

- The functions of the data Link layer are :
- Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- Physical addressing: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
- Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- Flow Control: The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates that amount of data that can be sent before receiving acknowledgement.
- Access control: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.
- Packet in Data Link layer is referred as Frame.

3. Network Layer (Layer 3):

- Routing: The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
- Logical Addressing: In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.
- Segment in Network layer is referred as Packet.

4. Transport Layer (Layer 4):

- The services provided by transport layer :
- Connection Oriented Service: It is a three-phase process which include

    - Connection Establishment
    - Data Transfer
    - Termination / disconnection
- In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
- Connection less service: It is a one phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.
- Data in the Transport Layer is called as Segments.
- Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
- Transport Layer is called as Heart of OSI model.

5. Session Layer (Layer 5):

- The functions of the session layer are :
- Session establishment, maintenance and termination: The layer allows the two processes to establish, use and terminate a connection.
- Synchronization: This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re- synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full-duplex.
- All the below 3 layers(including Session Layer) are integrated as a single layer in TCP/IP model as “Application Layer”.

6. Presentation Layer (Layer 6):

- The functions of the presentation layer are :
- Translation: For example, ASCII to EBCDIC.
- Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- Compression: Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7):

- The functions of the Application layer are :
    - Network Virtual Terminal
    - FTAM-File transfer access and management
    - Mail Services
    - Directory Services
- OSI model acts as a reference model and is not implemented in Internet because of its late invention. Current model being used is the TCP/IP model.

Q. 11 A Network with bandwidth of 10Mbps can pass only an average of 12,000 Frames per minute with each frame carrying an average of 10,000 bits. What is the

Throughput of this Network? (May-2016)

SOLUTION:

= (12,000*10,000) /60

Throughput =2 Mbps