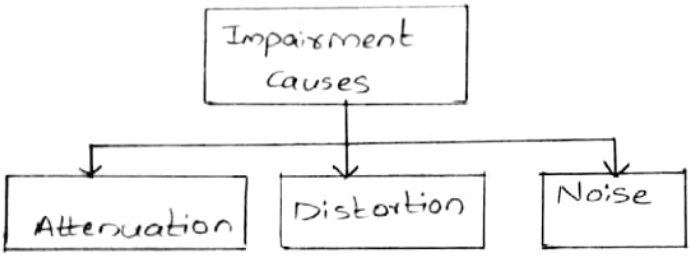
1) Explain about Transmission Impairments and write features of Protocols.

Transmission Impairment :-

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. Three causes of impairment are attenuation, distortion and noise.



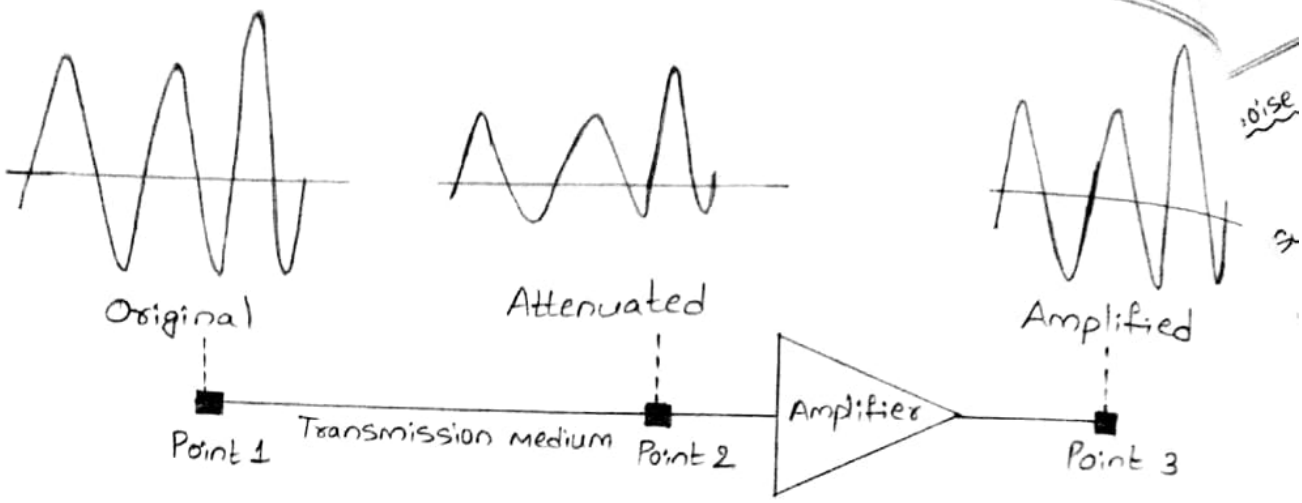
Attenuation :-

Attenuation means loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

To show that a signal has lost or gained strength, engineers use the unit of decibel. The decibel (dB) measures the relative strengths of two signals or one signal at two different points.

$$dB = 10 \log_{10} \frac{P_2}{P_1}$$

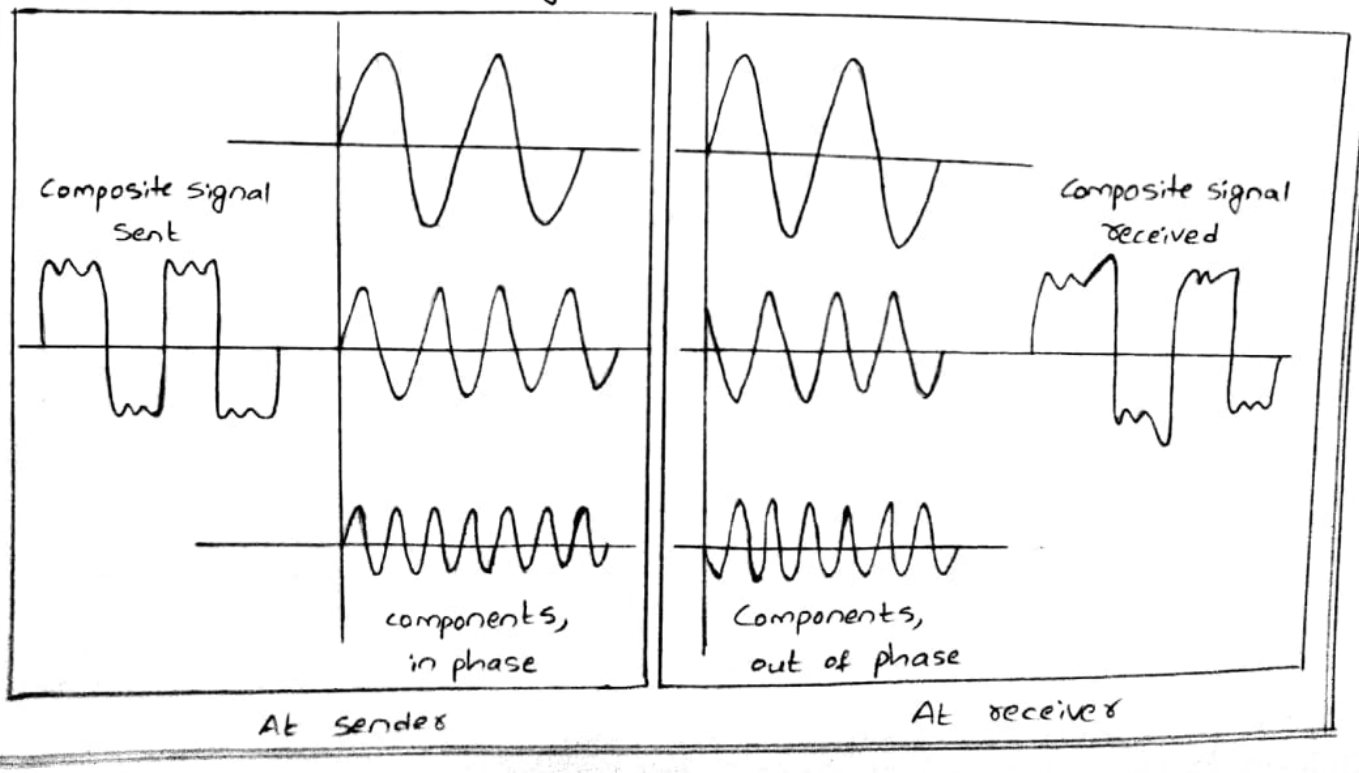
P_2, P_1 are powers of signal at points 2 and 1 respectively



The decibel is negative if a signal is attenuated and positive if a signal is amplified.

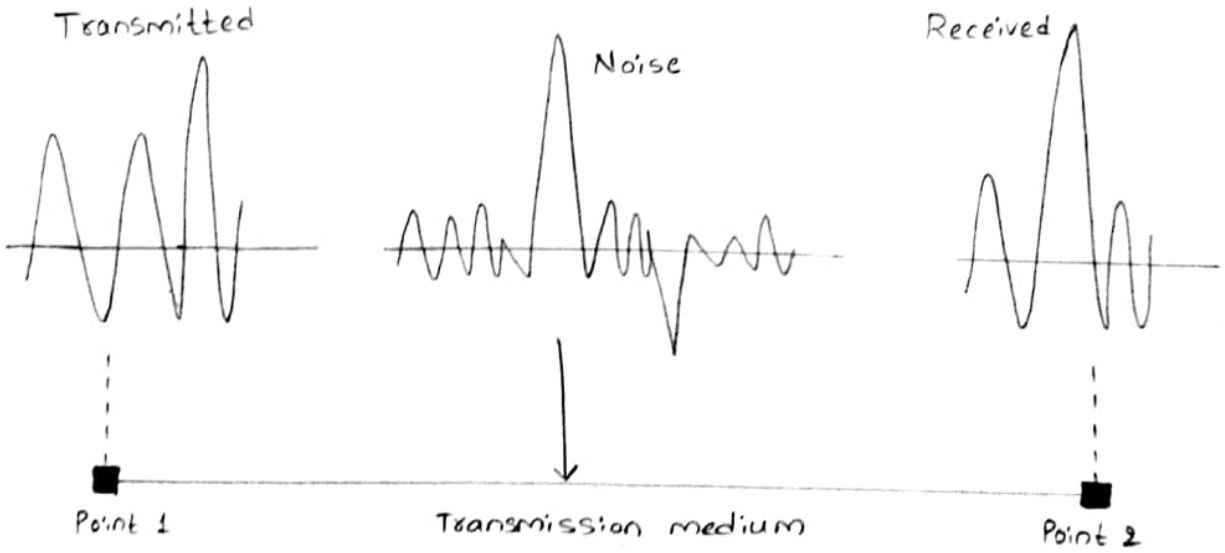
Distortion :-

Distortion means that the signal changes its form or shape. It can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as period duration. In other words, signal components at the receiver have phases different from what they had at the sender.



Noise :-

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk and impulse noise may corrupt the signal. Thermal noise is random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter. Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna and transmission medium acts as a receiving antenna. Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as receiving antenna. Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning and so on.



Protocols :-

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications.

The key elements of a protocol are syntax, semantics and timing.

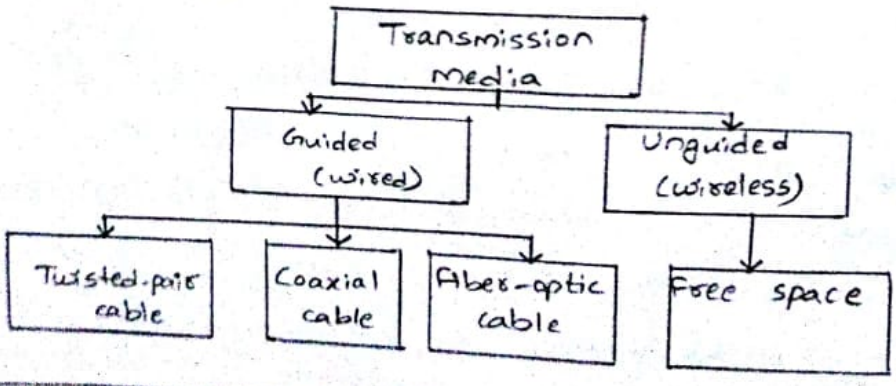
Syntax :- The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver and the rest of the stream to be the message itself.

Semantics :- The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

Timing :- The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

) Explain guided transmission media and unguided media in detail with applications.

A transmission medium can be broadly defined as anything that can carry information from a source to a destination.



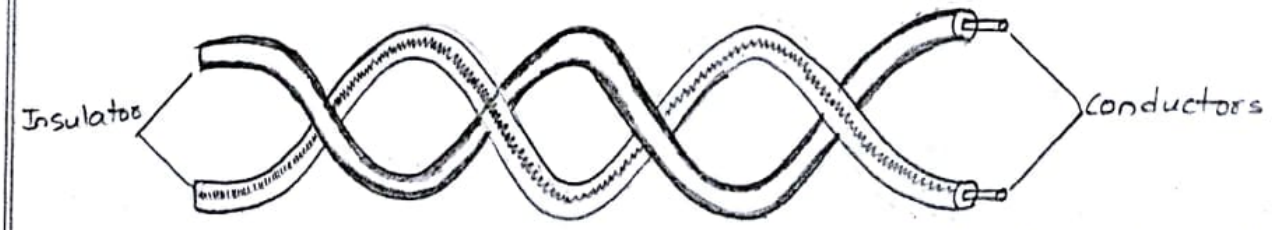
Guided Media :-

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable and fiber-optic cable. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

1) Twisted-pair cable :-

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together. One of the wires is used to carry signals to the receiver and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

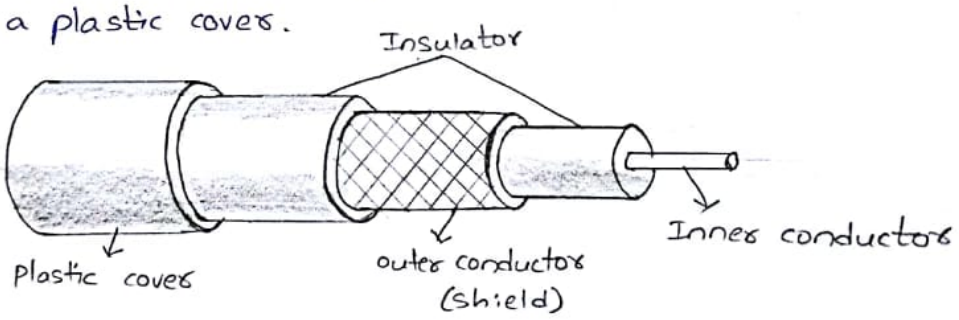
If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources. This results in a difference at the receiver.



Applications :- Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop - the line that connects subscribers to the central telephone office - commonly consists of unshielded twisted-pair cables. Local area networks such as 10 Base-T and 100 Base-T use twisted-pair cables.

2) Coaxial cable :-

Coaxial cable carries signals of higher frequency range than those in twisted-pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or standard wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath and the whole cable is protected by a plastic cover.

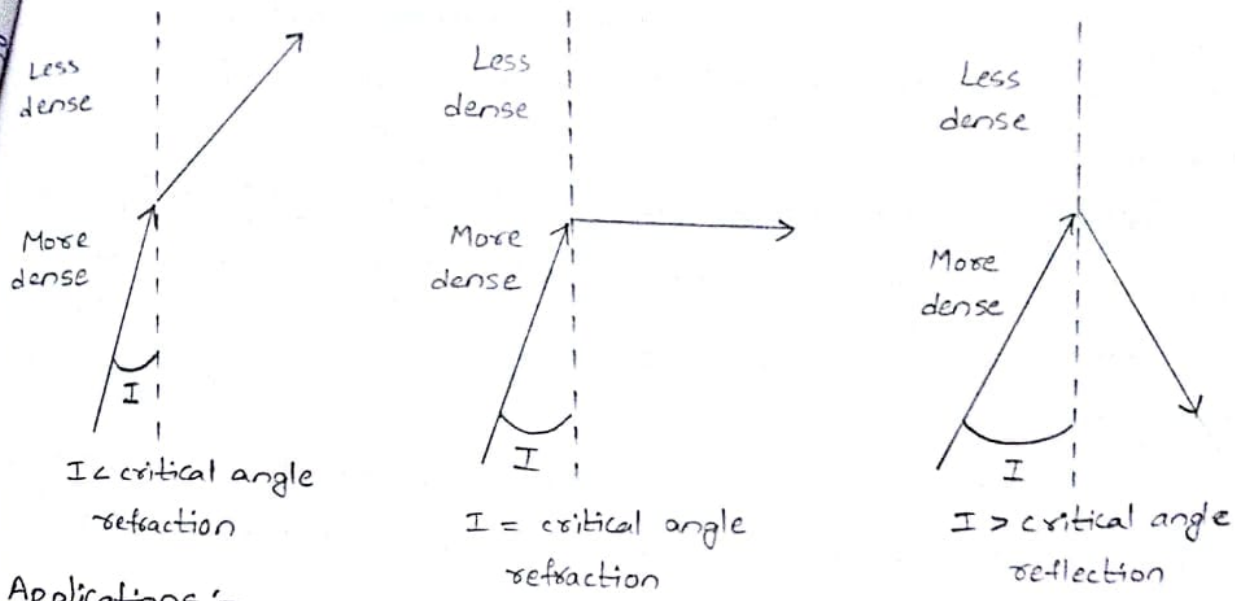


Applications :-

Coaxial cable was widely used in analog telephone networks where a single coaxial cable (network) could carry 10,000 voice signals. Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps. Cable TV networks also use coaxial cables. Another common application of coaxial cable is in traditional Ethernet LANs.

3) Fibre-Optic cable :-

A fibre-optic cable is made of glass or plastic and transmits signals in the form of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light travelling through one substance suddenly enters another substance (of a different ray), the ray changes direction.



Applications :-

Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate of 1600 Gbps. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network.

Local-area networks such as 100 Base-FX network and 1000 Base-X also use fiber-optic cable.

Unguided media (Wireless) :-

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

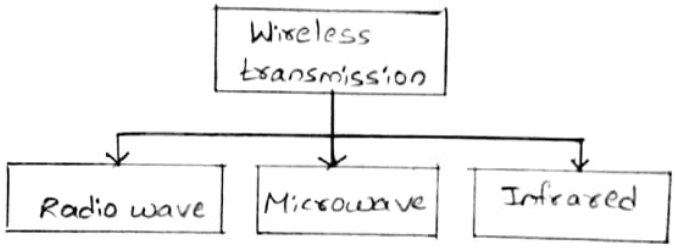
Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation and line-of-sight propagation.

In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna

and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance.

In sky propagation, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to earth. This type of transmission allows for greater distances with lower output power.

In line-of-sight propagation, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth.

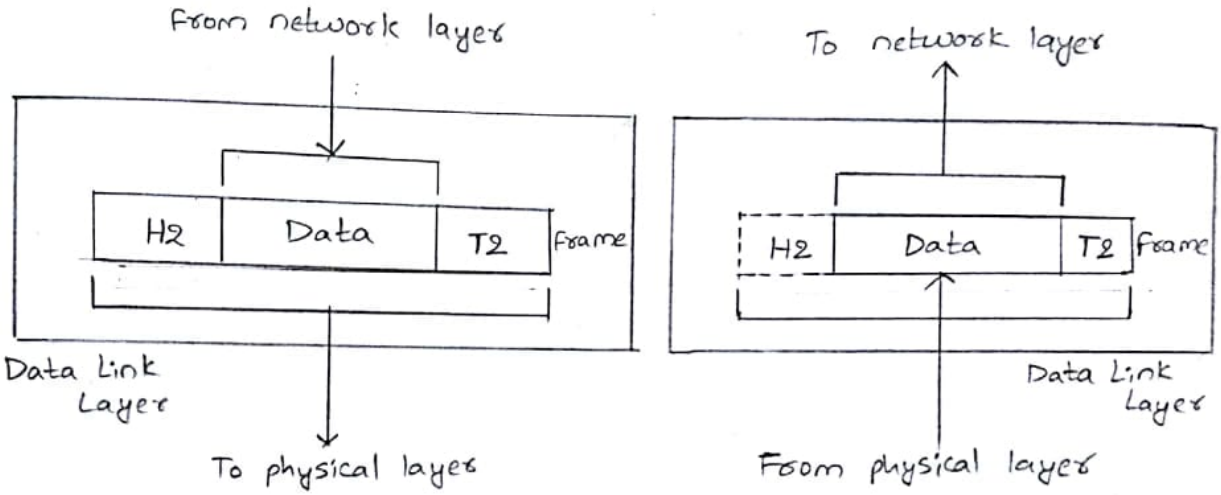


Band	Range	Propagation	Application
VLF (Very Low Frequency)	3-30 kHz	Ground	long-range radio navigation
LF (low frequency)	30-300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz-3 MHz	Sky	AM radio
HF (high frequency)	3-30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30-300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (Ultra high frequency)	300 MHz-3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (Super high frequency)	3-30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30-300 GHz	Line-of-sight	Radar, Satellite

What are the functions of data link layer and write advantages of layered approach.

Data Link Layer :-

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer.



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

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

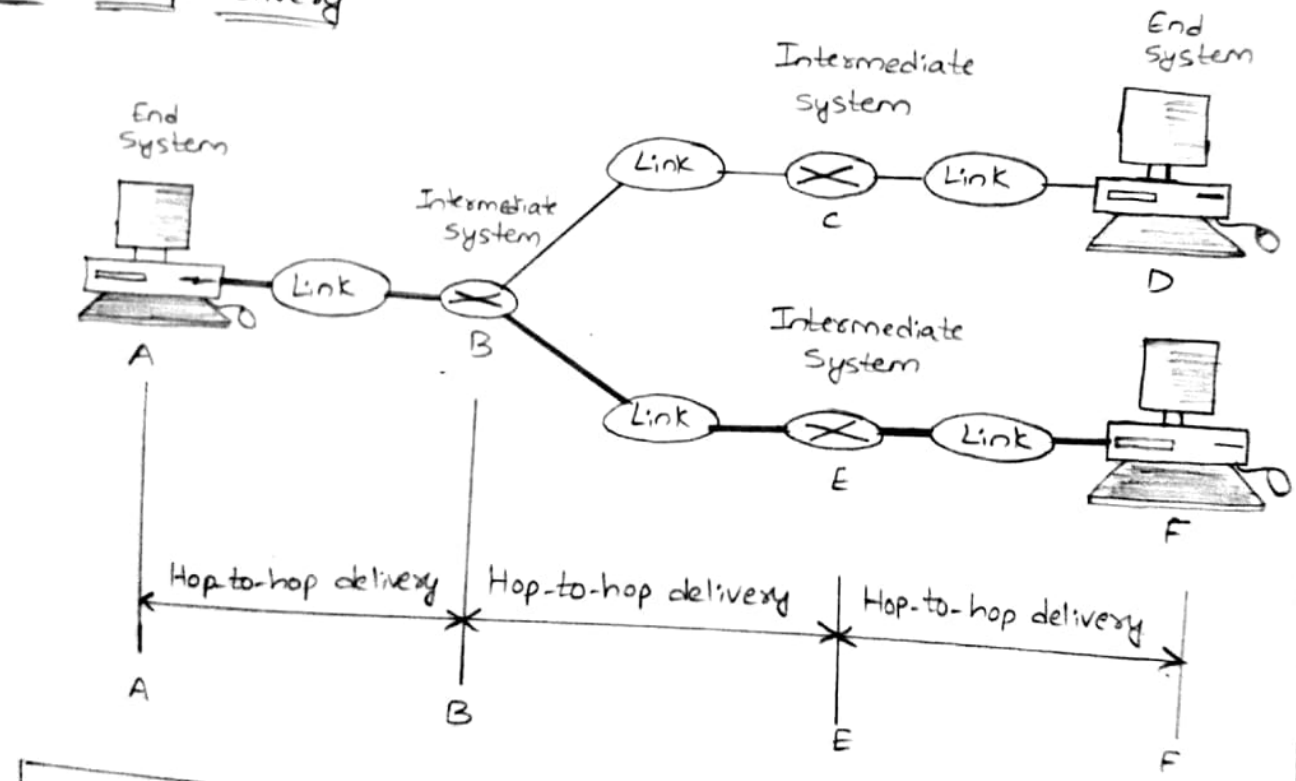
Physical addressing :- If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the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

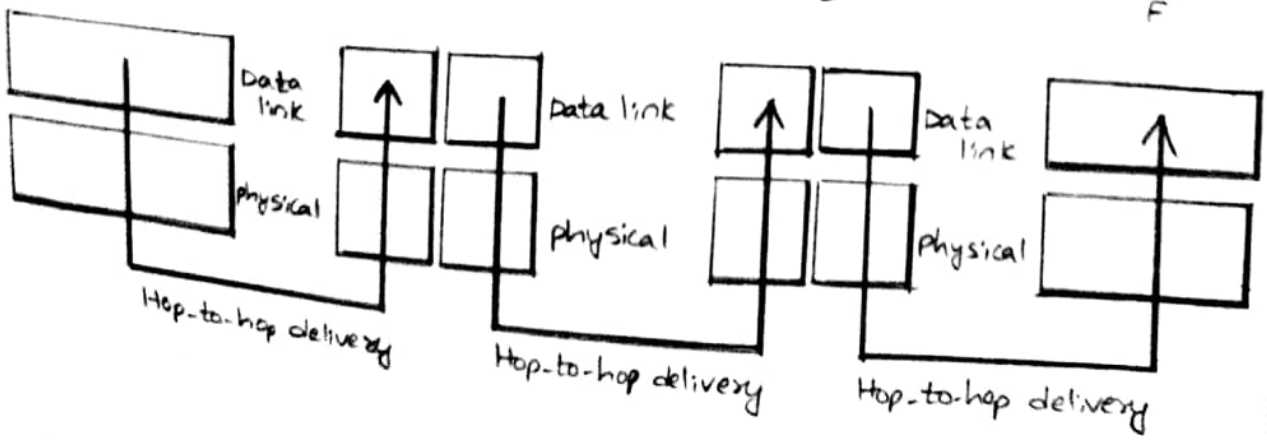
Flow control :- If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Error control :- The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

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

Hop-to-hop delivery





Advantages of layered approach :-

Layered architecture in a network increases flexibility, maintainability, and scalability. In a layered architecture we separate the user interface from the business logic and the business logic from the data access logic. Separation of concerns among these logical layers and components is easily achieved with the help of layered architecture.

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. The OSI model allows complete interoperability between otherwise incompatible systems. Another aspect of data communications in the OSI model is encapsulation.

A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5 and so on. In other words, the data portion of a packet at level N-1 carries the whole packet (data and header and maybe trailer) from level N. The concept is called encapsulation.

The major advantages of layered approach are :-

1) To translate, encrypt and compress data
2) To transmit bits over a medium; to provide mechanical and electrical specifications.
3) To organize bits into frames; to provide hop-to-hop delivery
4) To move packets from source to destination; to provide internetworking.
5) To provide reliable process-to-process message delivery and error recovery.
6) To establish, manage and terminate sessions.

7) To allow access to network resources.

⇒ Multiple applications can reuse the components. Different components of the application can be independently deployed, maintained and updated on different time schedules.

⇒ Layered architecture makes it possible to configure different levels of security to different components deployed on different boxes.

⇒ Layered architecture also helps to test the components independent of each other.

⇒ It allows good maintenance, where changes can be made without affecting layer interfaces.

⇒ It is decomposable and therefore effects separation of concerns and different abstraction levels.

---

4) Define IP protocol. Explain in detail about TCP header with neat diagram.

Internetworking Protocol (IP) :-

The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol - a best-effort delivery service. The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no

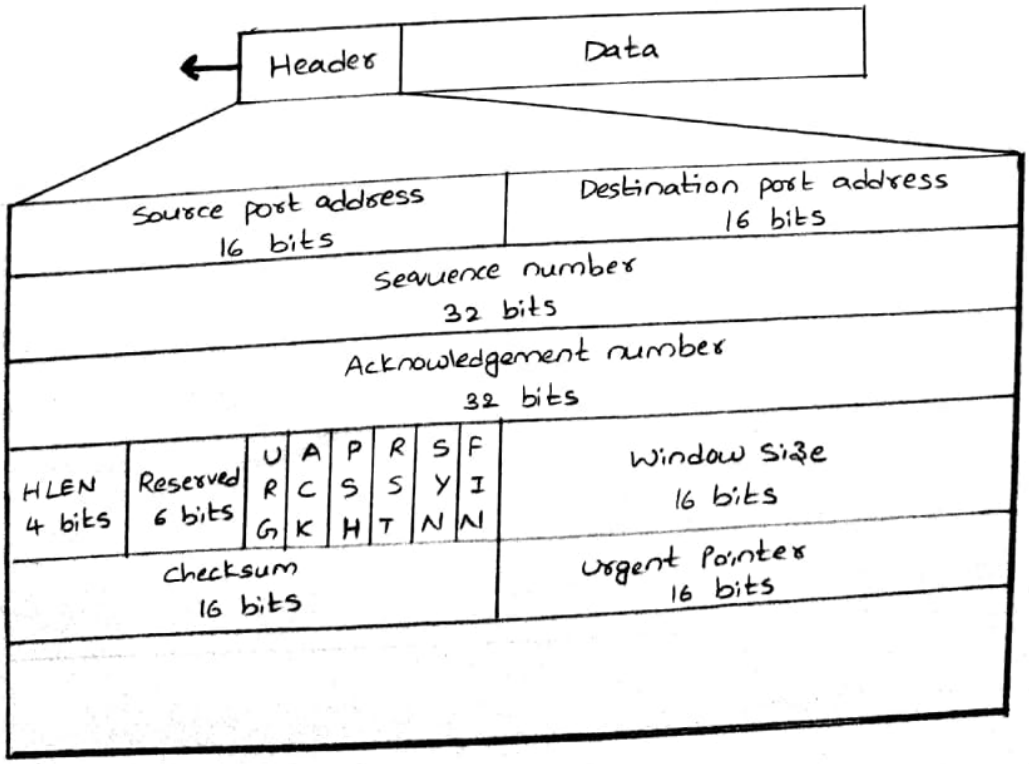
facility for reordering datagrams once they arrive at their destination.

The limited functionality of IP should not be considered as a weakness, however. IP provides base-bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency.

Transmission Control Protocol (TCP):-

It provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream means connection-oriented. A connection must be established between both ends of a transmission before either can transmit data. It adds connection-oriented and reliability features to the services of IP.

TCP segment format



A packet in TCP is called a segment. The segment consists of a 20 to 60-byte header, followed by data from the application program. The header is 20 bytes if there are no options and up to 60 bytes if it contains options.

Source port address :- This is a 16-bit field that defines the port number of the application program in the host that is sending the segment. This serves the same purpose as the source port address in the UDP header.

Destination port address :- This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment. This serves the same purpose as the destination port address in the UDP header.

Sequence number :- This 32-bit field defines the number assigned to the first byte of data contained in this segment. A TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. The sequence number tells the destination which byte in this sequence comprises the first byte in the segment. During connection establishment, each party uses a random number generator to create an initial sequence number (ISN) which is usually different in each direction.

Acknowledgement number :- This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party. If the receiver of the segment has successfully received byte number x from the other party, it defines x+1 as the acknowledgement number. Acknowledgement and data can be piggybacked together.

Header length :- This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes. Therefore, the value of this field can be between 5 (5×4=20) and 15 (15×4=60).

Reserved :- This is a 6-bit field reserved for future use.

Control :- This field defines 6 different control bits or flags. One or more of these bits can be set at a time.

URG : Urgent pointer is valid
ACK : Acknowledgement is valid
PSH : Request for push
RST : Reset the connection
SYN : Synchronize sequence numbers
FIN : Terminate the connection

URG	ACK	PSH	RST	SYN	FIN

These bits enable flow control, connection establishment and termination, connection abortion, and the mode of data transfer in TCP. A brief description of each bit is shown in the table.

Flag	Description
URG	The value of urgent pointer field is valid
ACK	The value of acknowledgement field is valid
PSH	push the data
RST	Reset the connection
SYN	Synchronize sequence numbers during connection
FIN	Terminate the connection

Window Size :- This field defines the size of the window, in bytes, that the other party must maintain. The length of this field is 16 bits, which means that the maximum size of the window is 65,535 bytes. This value is normally referred to as the receiving window (rwnd) and is determined by the receiver. The sender must obey the dictation of the receiver in this case.

Checksum :- This 16-bit field contains the checksum. The calculation of the checksum for TCP follows the same procedur as the one described for UDP. However, the inclusion of the checksum in the UDP datagram is optional, whereas the inclusion of checksum for TCP is mandatory.

Urgent pointer :- This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines the number that must be added to the sequen number to obtain the number of last urgent byte in the data section of the segment.

Options :- There can be up to 40 bytes of optional information in the TCP header.

5) List the major disadvantages with the layered approach to protocols.

1) There might be a negative impact on the performance as we have the extra overhead of passing through layers instead of calling a component directly.
2) Development of user-intensive applications can sometime take longer if the layering prevents the use of user interface components that directly interact with the database.
3) The use of layers helps to control and encapsulate the complexity of large applications, but adds complexity to simple applications.
4) Changes to lower level interfaces tend to percolate to higher levels, especially if the relaxed layered approach is used.
5) Layered architecture doesn't define any particular protocol.
6) It may find sometimes difficult to fit a new protocol in this model. This is because this model was created before the

invention of any of these protocols.

7) The session layer is used for session management. Presentation layer deals with user interaction. Though they are useful, not as much as other layers in the OSI model.

8) There is some duplication in services at various layers. Such as, both transport and data link layer have error control mechanisms.

9) There is also interdependence among the layers. These layers can not work in parallel. They have to be in wait to receive data from its predecessor.

* Perhaps the major disadvantage is the processing and data overhead. There is processing overhead because as many as seven modules (OSI model) are invoked to move data from the application through the communications software.

There is data overhead because of the appending of multiple headers to the data. Another possible disadvantage is that there must be at least one protocol standard per layer. With so many layers, it takes a long time to develop and promulgate the standards.

⇒ It is difficult to exactly assign of functionalities to the correct and appropriate layer because of having too many layers, performance of the system is degraded.

⇒ some functions (like FDDI station management) really need to access and operate at multiple layers.

→ Poorly conceived layers can lead to awkward and complex interfaces.