1. Star, mesh and bus topologies

Star Topology

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another.
- Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device .
- A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
- Other advantages include robustness. If one link fails, only that link is affected. All other links remain active.
- This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Bus Topology

- The preceding examples all describe point-to-point connections.
- A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network.
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.
- As a signal travels along the backbone, some of its energy is transformed into heat.
- Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Mesh

- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- The term dedicated means that the link carries traffic only between the two devices it connects.
- To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node.
- Node 1 must be connected to n - I nodes, node 2 must be connected to n – 1 nodes, and finally node n must be connected to n - 1 nodes.
- We need n(n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2.
- In other words, we can say that in a mesh topology, we need n(n -1) /2 duplex-mode links.
- To accommodate that many links, every device on the network must have n – 1 input/output (VO) ports to be connected to the other n - 1 stations.

2. Unguided and Guided transmission media

What is Guided Media?

Guided media is like a physical medium via which the signals are transmitted. The guided media is used to provide a conduit from one machine to another that can have twisted-pair, coaxial cable and fibre-optic cable. It is also known as Bounded media.

There are four types of Guided Media which are as follows:

- Open Wire
- Twisted Pair
- Coaxial Cable
- Optical Fibre

What is Unguided Media?

Unguided transmission media are techniques that allow transmission of electromagnetic waves through a wireless medium or we can say without using any physical medium. It provides a mechanism for transferring electromagnetic waves but does not direct them.

There are three types of Unguided Transmission Media which are as follows:

- Microwave Transmission
- Radio Transmission
- Infrared Transmission

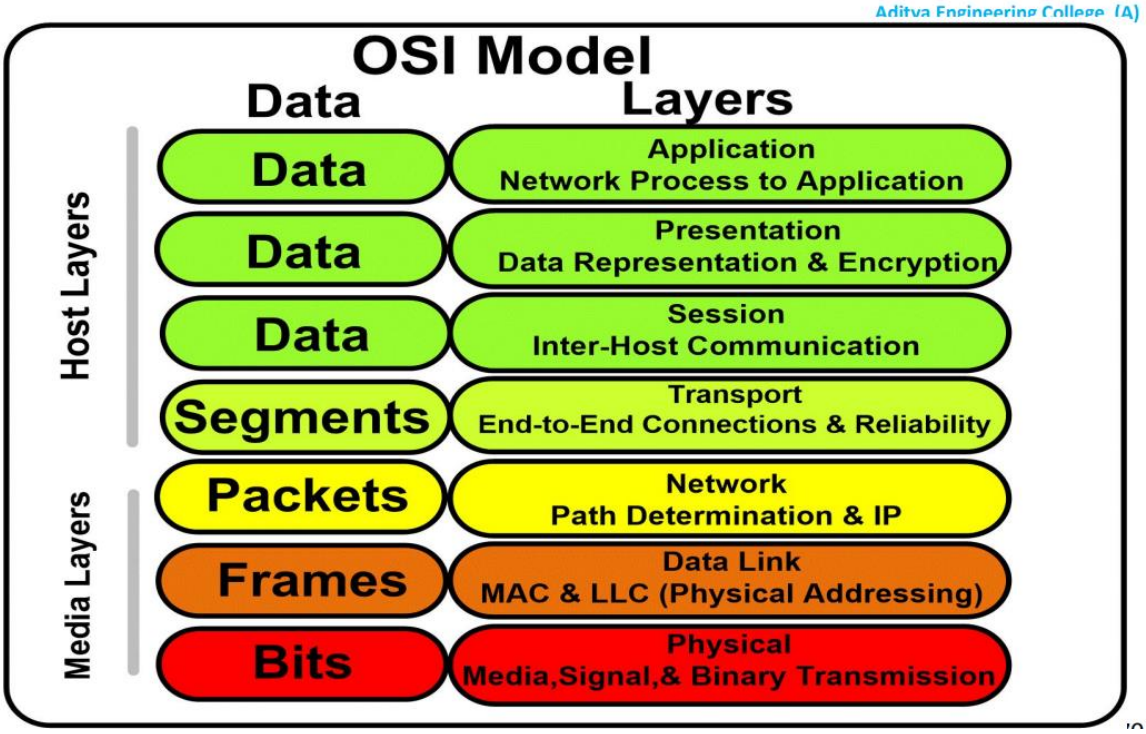
3. OSI Reference model

OSI Reference Model

- *The OSI model (minus the physical medium) is shown in Figure.*
- *This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983).*
- *It was revised in 1995 (Day, 1995).*
- *The model is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.*

• *The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:*

1. *A layer should be created where a different abstraction is needed.*
2. *Each layer should perform a well-defined function.*
3. *The function of each layer should be chosen with an eye toward defining internationally standardized protocols.*
4. *The layer boundaries should be chosen to minimize the information flow across the interfaces.*
5. *The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.*



4. Comparison of OSI and TCP/IP models

TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical model
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Protocols are not strictly defined	Stricter boundaries for the protocols
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard

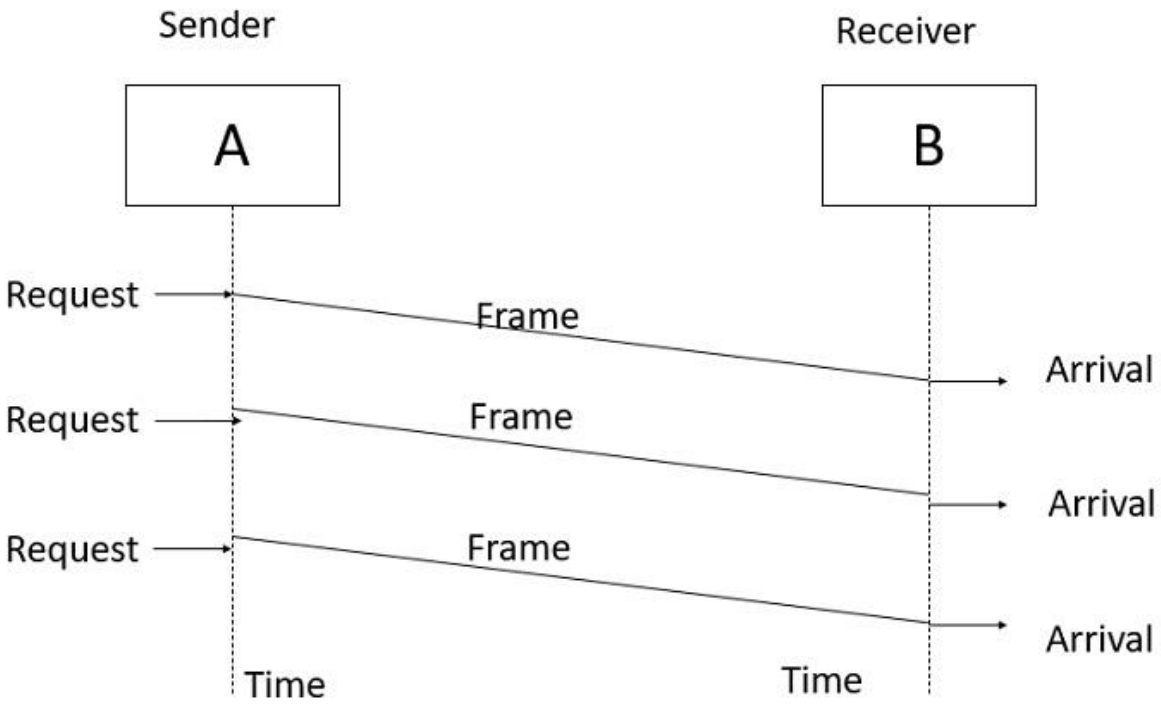
5. Elementary Data Link Layer protocols

Elementary Data Link protocols are classified into three categories, as given below −

- Protocol 1 − Unrestricted simplex protocol
- Protocol 2 − Simplex stop and wait protocol
- Protocol 3 − Simplex protocol for noisy channels.

Unrestricted Simplex Protocol

Data transmitting is carried out in one direction only. The transmission (Tx) and receiving (Rx) are always ready and the processing time can be ignored. In this protocol, infinite buffer space is available, and no errors are occurring that is no damage frames and no lost frames.


Sender
Receiver
A
B
Request
Frame
Arrival
Request
Frame
Arrival
Request
Frame
Arrival
Time
Time

Simplex Stop and Wait protocol

In this protocol we assume that data is transmitted in one direction only. No error occurs; the receiver can only process the received information at finite rate. These assumptions imply that the transmitter cannot send frames at rate faster than the receiver can process them.

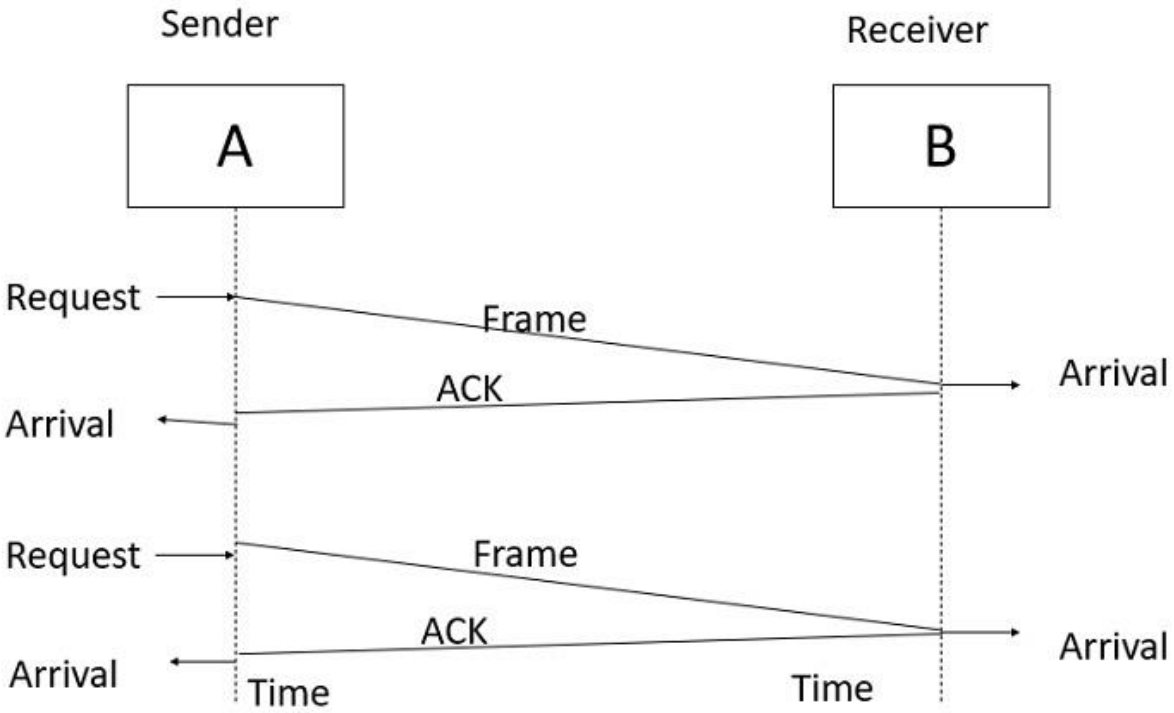
The main problem here is how to prevent the sender from flooding the receiver. The general solution for this problem is to have the receiver send some sort of feedback to sender, the process is as follows −

Step1 − The receiver send the acknowledgement frame back to the sender telling the sender that the last received frame has been processed and passed to the host.

Step 2 − Permission to send the next frame is granted.

Step 3 − The sender after sending the sent frame has to wait for an acknowledge frame from the receiver before sending another frame.

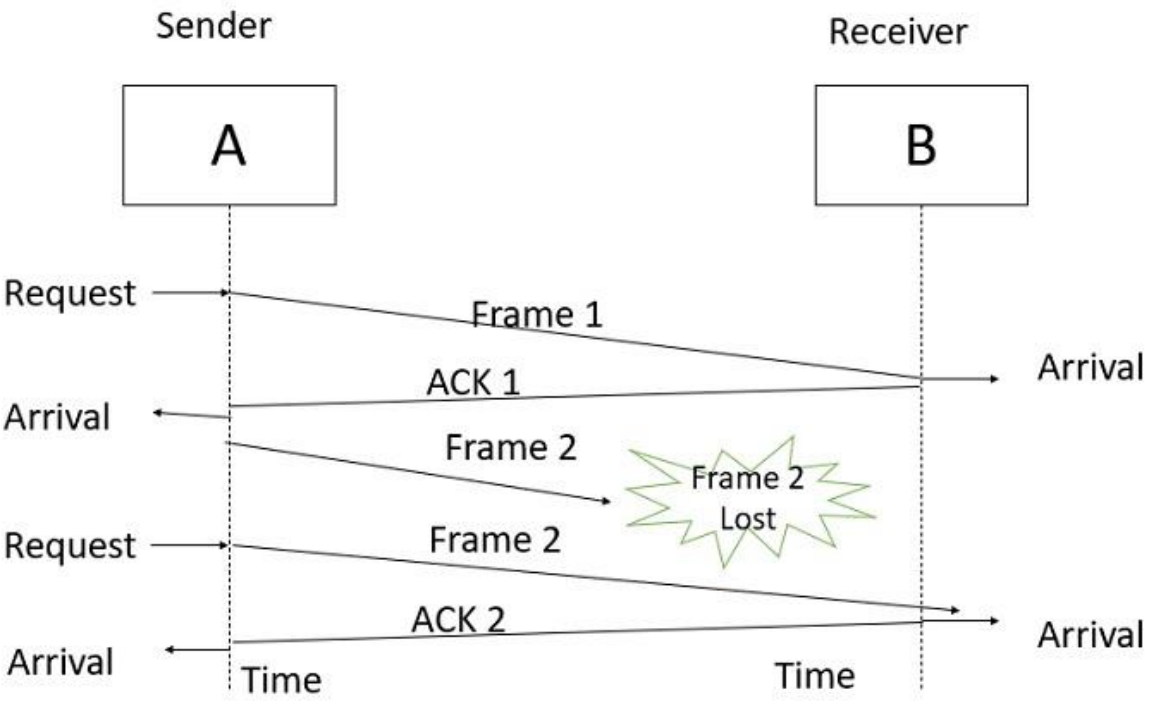
This protocol is called Simplex Stop and wait protocol, the sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame.



Simplex Protocol for Noisy Channel

Data transfer is only in one direction, consider separate sender and receiver, finite processing capacity and speed at the receiver, since it is a noisy channel, errors in data frames or acknowledgement frames are expected. Every frame has a unique sequence number.

After a frame has been transmitted, the timer is started for a finite time. Before the timer expires, if the acknowledgement is not received , the frame gets retransmitted, when the acknowledgement gets corrupted or sent data frames gets damaged, how long the sender should wait to transmit the next frame is infinite.



6. Sliding window protocols

Sliding Window Protocol

← Prev Next →

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Sliding Window Protocols

- *A One-Bit Sliding Window Protocol*
- *A Protocol Using Go-Back-N*
- *A Protocol Using Selective Repeat*

One Bit Sliding Window Protocol

- The window size in this protocol is 1.
- Such a protocol uses stop-and-wait since the sender transmits a frame and waits for its acknowledgement before sending the next one.

Go Back N

- It uses the concept of pipelining.
- Pipelining: A task is often begin before the previous task ended is known as pipelining(i.e. sending multiple frames before receiving the acknowledgment for the first frame.)
- The maximum number of frames that can be sent depends upon the size of the sending window. If the acknowledgment of a frame is not received within an agreed upon time period, all frames starting from that frame are retransmitted.

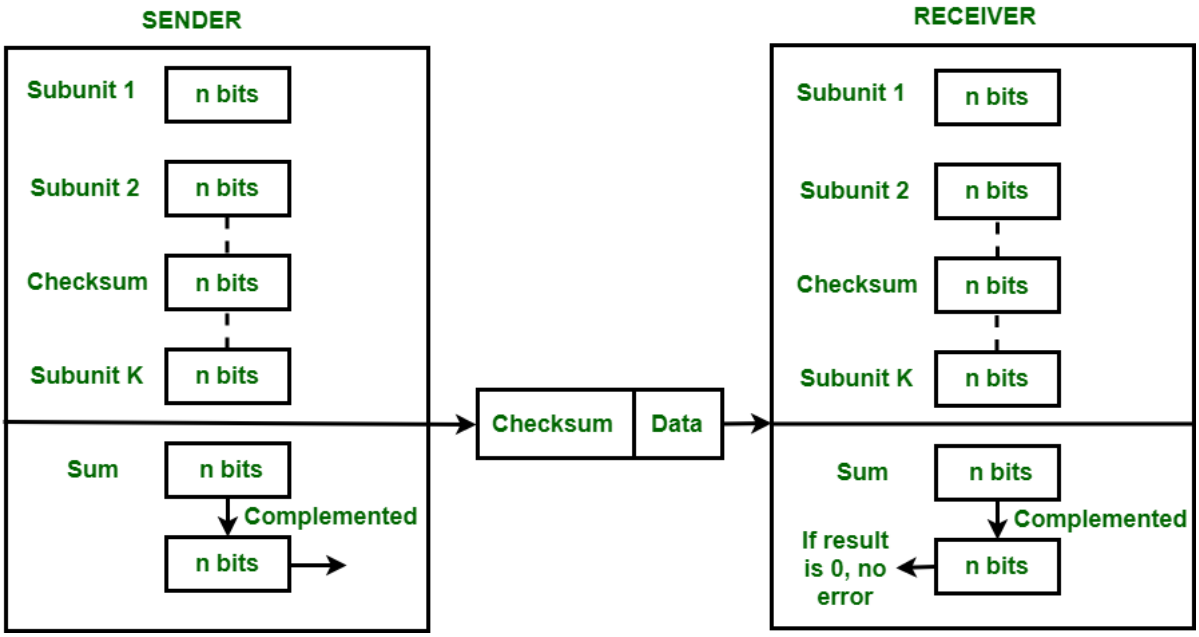
Selective Repeat

- The go-back-n protocol works well if errors are rare, but if the line is poor it wastes a lot of bandwidth on retransmitted frames.
- Selective Repeat protocol provides for sending multiple frames depending upon the availability of frames in the sending window, even if it does not receive acknowledgement for any frame.
- The receiver records the sequence number of the earliest incorrect or un-received frame. It then fills the receiving window with the subsequent frames that it has received. It sends the sequence number of the missing frame along with ever acknowledgement frame.
- Once, Sender has sent all the frames in the window, it retransmits the frame whose sequence number is given by the acknowledgements. It then continues sending the other frames.

7. Checksum

Checksum is the error detection method used by upper layer protocols and is considered to be more reliable than LRC, VRC and CRC. This method makes the use of **Checksum Generator** on Sender side and **Checksum Checker** on Receiver side.

At the Sender side, the data is divided into equal subunits of n bit length by the checksum generator. This bit is generally of 16-bit length. These subunits are then added together using one's complement method. This sum is of n bits. The resultant bit is then complemented. This complemented sum which is called checksum is appended to the end of original data unit and is then transmitted to Receiver.



8. Hamming code

Hamming codes

- *Given any two codewords that may be transmitted or received—say, 10001001 and 10110001—it is possible to determine how many corresponding bits differ.*
- *In this case, 3 bits differ. To determine how many bits differ, just XOR the two codewords and count the number of 1 bits in the result.*

10001001
10110001
00111000

- *The number of bit positions in which two codewords differ is called the **Hamming distance** (Hamming, 1950).*
- *Its significance is that if two codewords are a Hamming distance d apart, it will require d single-bit errors to convert one into the other.*

- Consider a message having four data bits (D) which is to be transmitted as a 7-bit codeword by adding three error control bits. This would be called a (7,4) code. The three bits to be added are three EVEN Parity bits (P), where the parity of each is computed on different subsets of the message bits as shown below.

7	6	5	4	3	2	1	
D	D	D	P	D	P	P	7-BIT CODEWORD
D	-	D	-	D	-	P	(EVEN PARITY)
D	D	-	-	D	P	-	(EVEN PARITY)
D	D	D	P	-	-	-	(EVEN PARITY)

9. Static channel allocation (Traditional) problems

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, then Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

These are explained as following below:

1. Static Channel Allocation in LANs and MANs:
It is the classical or traditional approach of allocating a single channel among multiple competing users Frequency Division Multiplexing (FDM). if there are N users, the bandwidth is divided into N equal sized portions each user being assigned one portion. since each user has a private frequency band, there is no interface between users.

It is not efficient to divide into fixed number of chunks.

Most real-life network situations have a variable number of users, usually large in number with bursty traffic. If the value of N is very large, the bandwidth available for each user will be very less. This will reduce the throughput if the user needs to send a large volume of data once in a while.

It is very unlikely that all the users will be communicating all the time. However, since all of them are allocated fixed bandwidths, the bandwidth allocated to non-communicating users lies wasted.

If the number of users is more than N, then some of them will be denied service, even if there are unused frequencies.

10. Assumption in dynamic channel allocation

2. Dynamic Channel Allocation:
Possible assumptions include:

1. **Station Model:**
   Assumes that each of N stations independently produce frames. The probability of producing a packet in the interval IDt where I is the constant arrival rate of new frames.

2. **Single Channel Assumption:**
   In this allocation all stations are equivalent and can send and receive on that channel.

3. **Collision Assumption:**
   If two frames overlap in time-wise, then that's collision. Any collision is an error, and both frames must re transmitted. Collisions are only possible error.

4. **Time** can be divided into Slotted or Continuous.

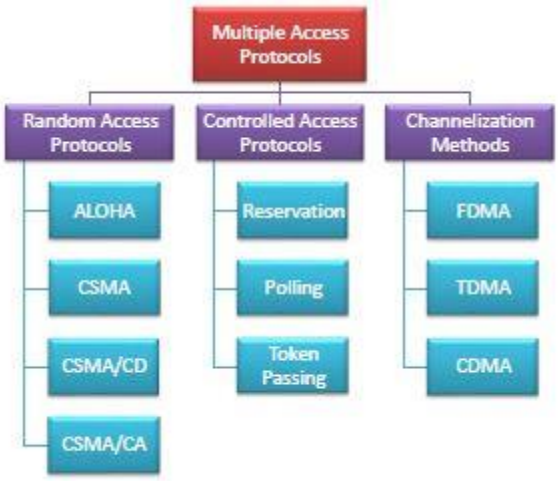
5. **Stations** can sense a channel is busy before they try it.

- N independent stations.
- A station is blocked until its generated frame is transmitted.
- probability of a frame being generated in a period of length Dt is IDt where I is the arrival rate of frames.
- Only a single Channel available.
- Time can be either: Continuous or slotted.
- **Carrier Sense:** A station can sense if a channel is already busy before transmission.
- **No Carrier Sense:** Time out used to sense loss data.

11. Explain how Media(multiple) access control protocol are classified

Multiple access protocols are a set of protocols operating in the Medium Access Control sublayer (MAC sublayer) of the Open Systems Interconnection (OSI) model. These protocols allow a number of nodes or users to access a shared network channel. Several data streams originating from several nodes are transferred through the multi-point transmission channel.

The objectives of multiple access protocols are optimization of transmission time, minimization of collisions and avoidance of crosstalks.



Random Access Protocols

Random access protocols assign uniform priority to all connected nodes. Any node can send data if the transmission channel is idle. No fixed time or fixed sequence is given for data transmission.

Controlled Access Protocols

Controlled access protocols allow only one node to send data at a given time.Before initiating transmission, a node seeks information from other nodes to determine which station has the right to send. This avoids collision of messages on the shared channel.

Channelization

Channelization are a set of methods by which the available bandwidth is divided among the different nodes for simultaneous data transfer.

12. Explain about Multiplexing

What is Multiplexing?

Multiplexing is the sharing of a medium or bandwidth. It is the process in which multiple signals coming from multiple sources are combined and transmitted over a single communication/physical line.

- The process of sharing of channels by multiple signals
- Can use a single wire to carry several signals than to install a separate wire for every signal
- Frequency Division Multiplexing
- Time Division Multiplexing
- Code Division Multiplexing

FDM

- takes advantage of passband transmission to share a channel
- divides the spectrum into frequency bands
- each user having exclusive possession of some band in which to send their signal
- AM : 500 – 1500kHz
- FM : 88 – 108 MHz

Time Division Multiplexing

- The users take turns (in a round-robin fashion), each one periodically getting the entire bandwidth for a little burst of time
- **Bits** from each input stream are **taken** in a **fixed time slot** and output to the aggregate stream
- the **streams** must be **synchronized** in time
- Small intervals of **guard time (**analogous to a frequency guard band) may be added to accommodate small timing variations

Code Division Multiplexing

- a form of **spread spectrum communication** in which a narrowband signal is spread out over a wider frequency band
- more tolerant of interference
- multiple signals from different users share the same frequency band