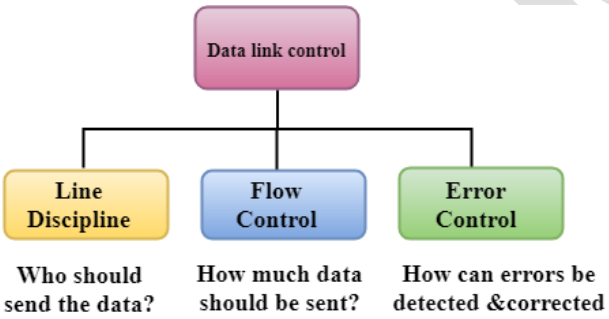
Data link control

- Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium.
- For example, In the half-duplex transmission mode, one device can only transmit the data at a time.
- If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information.
- The Data link layer provides the coordination among the devices so that no collision occurs.

The Data link layer provides three functions:

- Line discipline
- Flow Control
- Error Control



Line Discipline

- Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.
- **Line Discipline can be achieved in two ways:**
- ENQ/ACK
- Poll/select

END/ACK

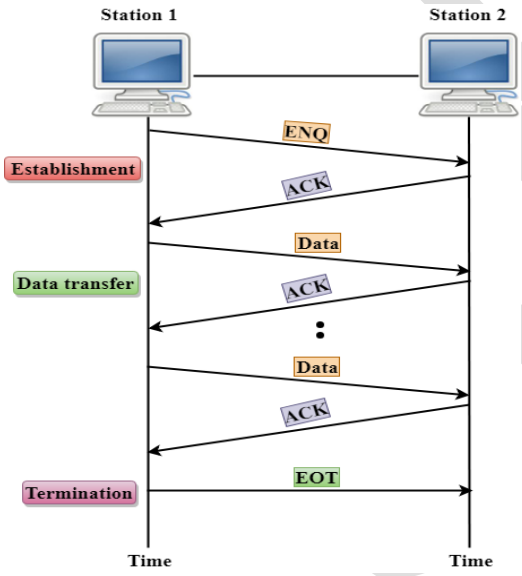
- END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one.
- END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

Working of END/ACK

- The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.
- The receiver responses either with the positive acknowledgement(ACK) or with the negative acknowledgement(NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Following are the responses of the receiver:

- If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame.
- If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.
- If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.



Poll/Select

- The Poll/Select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

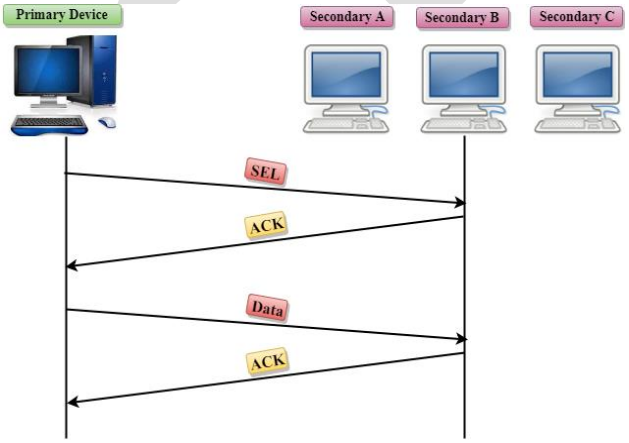
Working of Poll/Select

- In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.

- The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.
- The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.
- If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as **polling.**
- If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as **selecting.**

Select

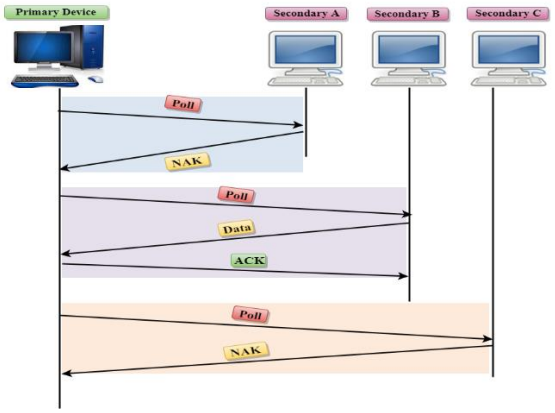
- The select mode is used when the primary device has something to send.
- When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a Select (SEL) frame, one field of the frame includes the address of the intended secondary device.
- When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.
- If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device. Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.



Poll

- The Poll mode is used when the primary device wants to receive some data from the secondary device.
- When a primary device wants to receive the data, then it asks each device whether it has anything to send.

- Firstly, the primary asks (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send.
- Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send. The secondary device can send more than one frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.



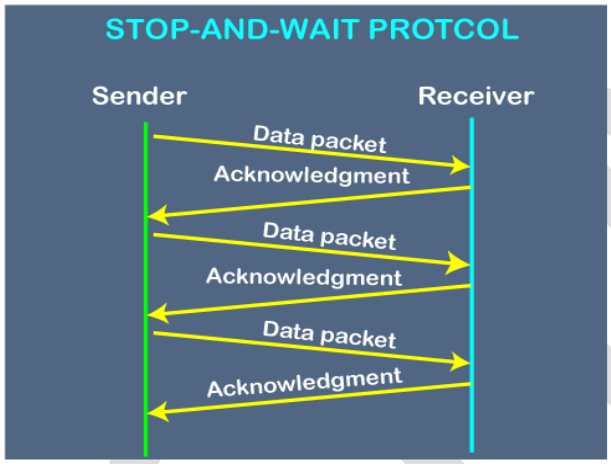
Flow Control

- It is a set of procedures that tells the sender how much data should be sent to the receiver so that it is not lost.
- This mechanism makes the sender wait for an acknowledgment before sending the next data.
- **Two methods have been developed to control the flow of data:**
- Stop-and-wait
- Sliding window

Stop-and-wait

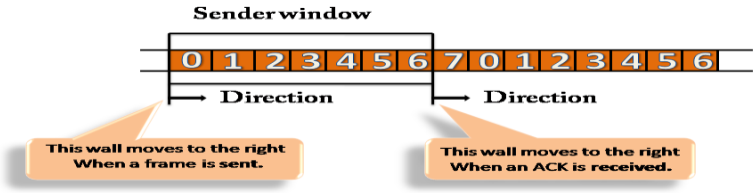
- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.
- When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame
- Suppose if any frame sent is not received by the receiver and lost.
- So the receiver will not send any acknowledgment as it has not received any frame.
- Also, the sender will not send the next frame as it will wait for the acknowledgment for the previous frame which it had sent.
- So a deadlock situation can be created here.

- To avoid any such situation there is a time-out timer.
- The sender will wait for this fixed amount of time for the acknowledgment and if the acknowledgment is not received then it will send the frame again.
- There are two types of delays while sending these frames
- **Transmission Delay:** Time taken by the sender to send all the bits of the frame onto the wire is called transmission delay.
- **Propagation Delay:** Time taken by the last bit of the frame to reach from one side to the other side is called propagation delay.
- Hence , the total time required to send a frame is
- **Total time = Td(Transmission Delay)+Tp(Propagation Delay for data frame)+Tp(Propagation Delay for acknowledgment frame)**



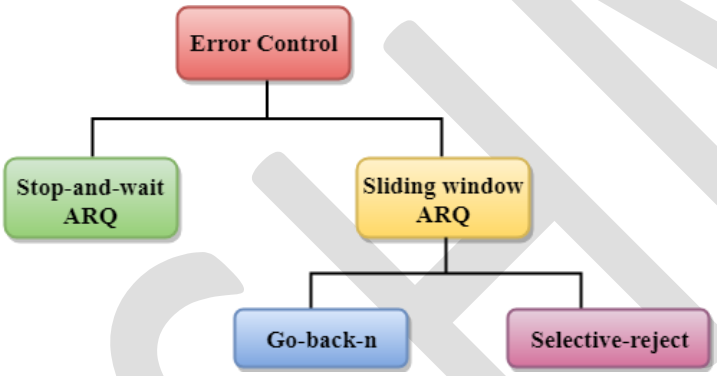
Sliding Window

- The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- A single ACK acknowledge multiple frames.
- Sliding Window refers to imaginary boxes at both the sender and receiver end.
- The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5.
- When the sender sees the ACK with the number 5, it go to know that the frames 0 through 4 have been received.



Error Control

- Error Control is a technique or error detection and retransmission.
- Error correction in the data link layer is implemented simply : anytime an error detected in an exchange, a negative acknowledgment(NAK) is returned and the specified frames are retransmitted.
- This process is called automatic repeat request (ARQ).



Stop-and-wait ARQ

- Stop-and-wait ARQ is and a form of stop-and-wait flow control extended to include retransmission of data in case of lost or damaged frames.
- For retransmission to work four features are added to the basic flow control mechanism:
- The sending device keeps a copy of the last frame transmitted until it receives an acknowledgment for that frame.
- Keeping a copy allows the sender to retransmit lost or damaged frames until they are received correctly.
- A data 0 frame is acknowledged by an ACK1 frame, indicating that the receiver has gotten data 0 and is now expecting data 1.
- This numbering allows of identification of data frames in case of duplicate transmission.

- If an error is discovered in a data frame a NAK frame is returned.
- NAK frames, which are not numbered , tell the sender to retransmit the last frame sent.

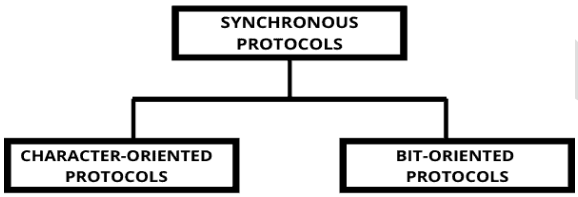
Damaged Frames

- When a frame is discovered by the receiver to contain an error, it returns a NAM frame and the sender retransmits the last frame.
- For example, the sender transmits a data frame: data 0.
- The receiver returns an ACK1, indicating that data 0 arrived undamaged and it is now expecting data 1.
- The sender transmits its next frame: data 0.
- The receiver discovers an error in data 0 and returns a NAK. The sender retransmits data 0.
- The time data 0 arrives intact, and the receiver returns ACK1.

Data link control protocols

- The speed of Synchronous transmission makes it the better choice over Asynchronous transmission. For both LAN, MAN and WAN technology, Protocols governing synchronous transmission can be divided into two classes :

1. Character – Oriented protocols
2. Bit – Oriented protocols

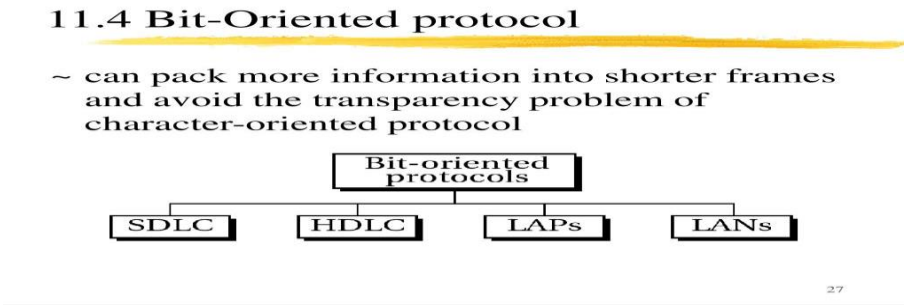


Character Oriented Protocols

- Character Oriented protocols also called Byte oriented protocols.
- It interpret a transmission frame or packet as a succession of characters, each usually composed of one byte(eight bits).

Bit-Oriented Protocols

- In a Bit-Oriented protocol the frame or packet is interpreted as a series of bits.
- It can pack more information into the shorter frame



High-level Data Link Control (HDLC)

- It is a bit-oriented data link protocol designed to support both half-duplex communication over point-to-point and multipoint links.

Synchronous Data Link Control (SDLC)

- It is primarily used in wide area networks(WANs)
- You can use SDLC in a variety of connection topologies, including direct point-to-point connections between a primary and a secondary station and multipoint connections between a primary and a group of secondary stations.

Link Access Procedure (LAP) Protocols

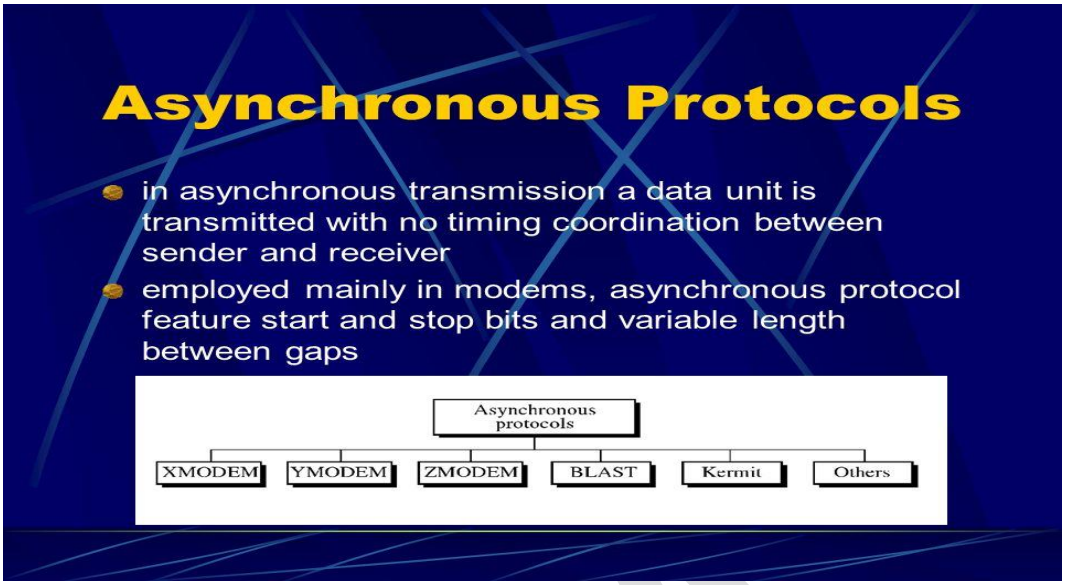
- Several protocols under the general category link access procedure(LAP) have been developed.
- Each of these protocols is a subset of HDLC tailored for a specific purpose.
- LAPB, LAPD and LAPM are the most common of these.

Link Access Procedure Balanced (LAPB) : is a simplified subset of HDLC used only for connecting a station to a network.

Link Access Procedure for D channel (LAPD): is another simplified subset of HDLC used in Integrated Services Digital Network(ISDN).

Link Access Procedure for Modem (LAPM): is a simplified subset of HDLC for modems.

- It is designed to do Asynchronous-Synchronous conversion, error detection and retransmission.
- It has been developed to apply HDLC features to modems.



Asynchronous Protocols

- Due to its inherent slowness, Asynchronous transmission at this level is being replaced by higher-speed synchronous mechanisms.
- Asynchronous protocols are not complex and are inexpensive to implement.
- In Asynchronous transmission a data unit is transmitted with no timing coordination between sender and receiver.
- A receiver does not need to know exactly when a data unit is sent, it only needs to recognize the beginning and the end of the unit.
- This is accomplished by using extra bits (start and stop bits) to frame the data unit.

XMODEM : A file transfer protocol for telephone line communication.

- This protocol is a half-duplex stop-and-wait ARQ protocol.

YMODEM : This protocol is similar to XMODEM, with the following major differences.

- The data unit is 1024 bytes
- Multiple files can be sent simultaneously.

ZMODEM

- ZMODEM is a newer protocol combining features of both XMODEM and YMODEM.

BLAST

- Blocked Asynchronous transmission (BLAST) is more powerful than XMODEM. It is full-duplex with sliding window flow control. It allows the transfer of data and binary files.

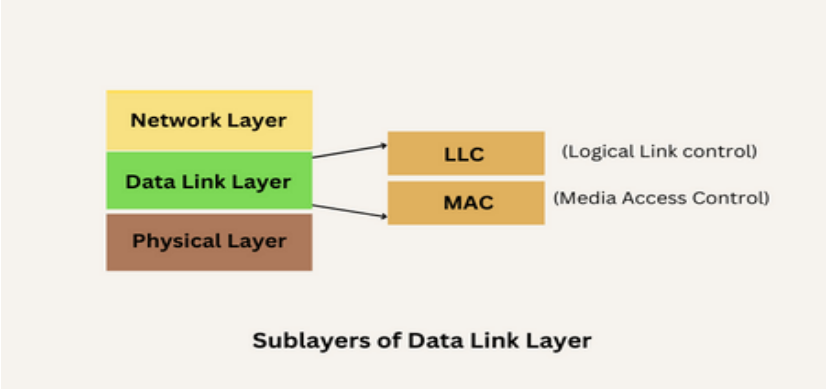
Kermit

- Most widely used Asynchronous protocol.
- This file transfer protocol is similar in operation to XMODEM

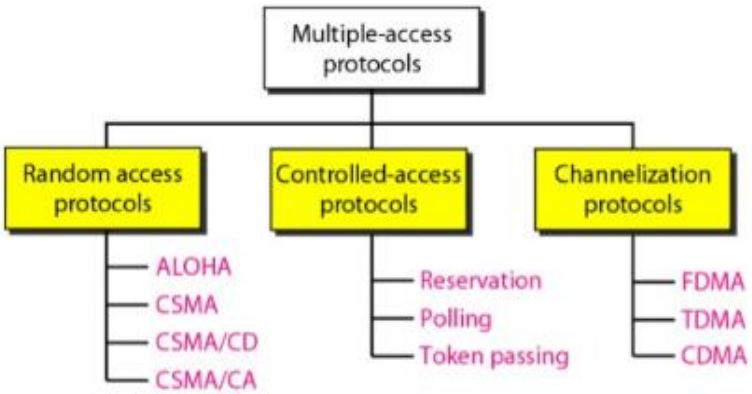
MULTIPLE ACCESS, RANDOM ACCESS

- We can consider the data link layer as two sub layers.
- The upper sub layer is responsible for data link control, and the lower sub layer is responsible for resolving access to the shared media.
- If the channel is dedicated, we do not need the lower sub layer.
- The upper sub layer that is responsible for flow and error control is called the **logical link control(LLC)** layer; the lower sub layer that is mostly responsible for multiple-access resolution is called the **media access control(MAC)** layer.

When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link



Sublayers of Data Link Layer



RANDOM ACCESS

- In random access or contention methods, no station is superior to another station and none is assigned the control over another.
- No station permits, or does not permit, another station to send.
- At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.
- This decision depends on the state of the medium(idle or busy).
- Two features give this method its name.
- First, there is no scheduled time for a station to transmit.
- Transmission is random among the stations.
- Second, no rules specify which station should send next.
- Stations compete with one another to access the medium.
- That is why these methods are also called contention methods.
- Random access method evolved from protocol known as ALOHA, which used a procedure called multiple access(MA).
- Forces the station to sense the medium before transmitting.
- This was called carrier sense multiple access.
- This method later evolved into two parallel methods:

  Carrier sense multiple access with collision detection(CSMA/CD)

  2. Carrier sense multiple access with collision avoidance(CSMA/CA)
- CSMA/CD tells the station what to do when a collision is detected.

  CSMA/CA tries to avoid the collision

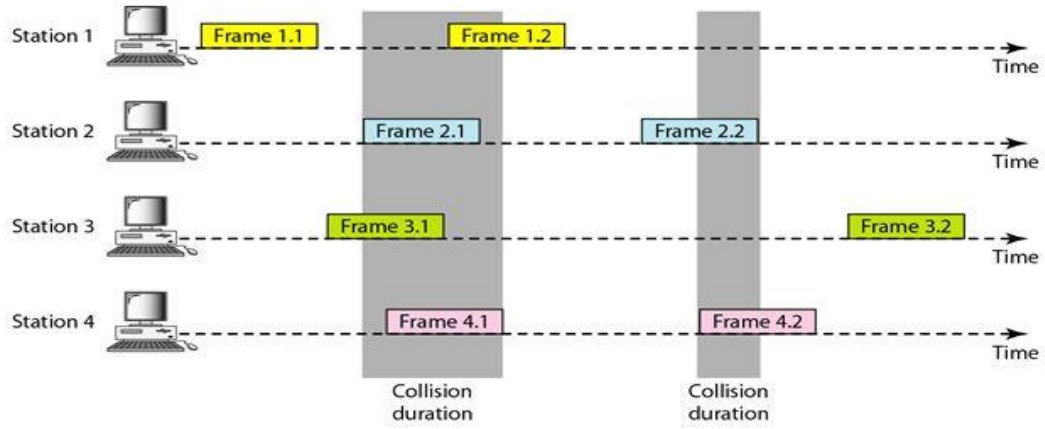
ALOHA

- ALOHA Means “Hello”
- It is implemented in satellite communication systems.
- When two or more systems seek to transmit on the same channel at the same time, a shared communication system such as ALOHA needs a way to handle collisions.
- A node in the ALOHA system transmits whenever data is ready to be sent.
- A collision takes place and the sent frames are lost if the other node transmits at the same time.
- Version of ALOHA

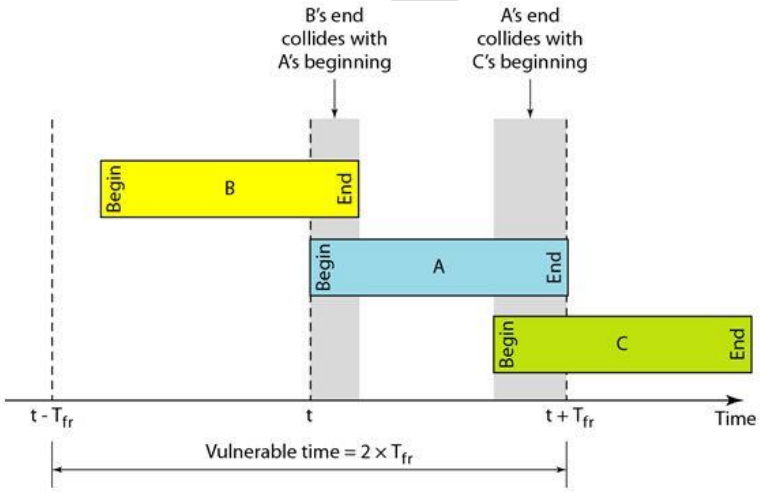
- **Pure ALOHA**
- **Slotted ALOHA**

Pure ALOHA

- The original ALOHA protocol is called pure ALOHA.
- The idea is that each station sends a frame whenever it has the frame to send.
- However, since there is only one channel to share, there is the possibility of collision between frames from different stations.
- Fig shows an example of frame collisions in pure ALOHA.

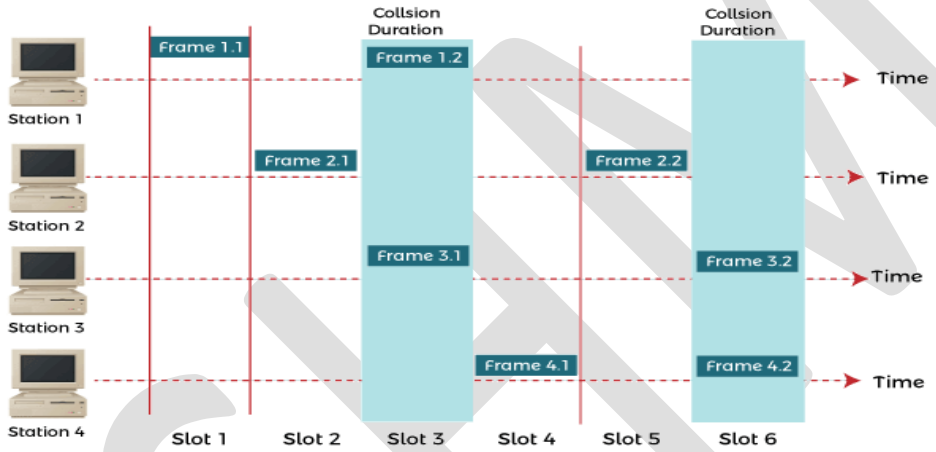


- Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged.
- Only two frames, frame 1.1 and frame frame 3.2 survive. All other frames are destroyed.
- If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.



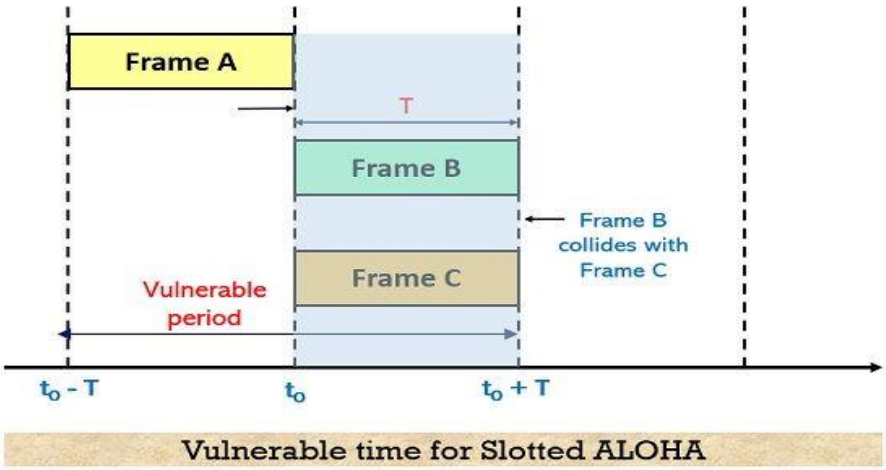
Slotted ALOHA

- Slotted ALOHA increases the capacity of pure ALOHA while reducing collisions.
- Slotted ALOHA reduces the number of collisions and doubles the capacity of pure ALOHA.
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.
- However, there can still be collisions if more than one station tries to transmit at the beginning of the same time slot.



Frames in Slotted ALOHA

- In slotted ALOHA , if any station is not able to place the frame onto the channel at the beginning of the slot. i.e. it misses the time slot then the station has to wait until the beginning of the next time slot.
- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in figure.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collisions are reduced to one-half.



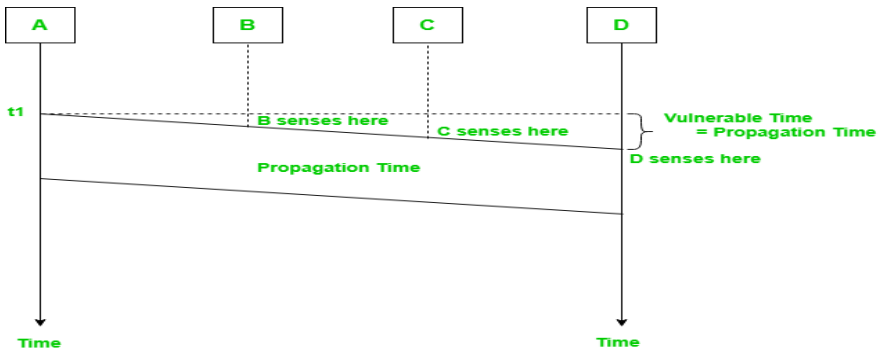
Vulnerable time for Slotted ALOHA

Carrier Sense Multiple Access (CSMA)

- This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer.
- Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.
- CSMA is based on the principle "sense before transmit" or "listen before talk".

If the channel is in use, devices wait before transmitting

- MA (Multiple Access) indicates that many devices can connect to and share the same network.
- All devices have equal access to use the network when it is clear.
- Even though devices attempt to sense whether the network is in use, there is good chance that two stations will attempt to access it at the same time.
- Vulnerable time = Propagation time (Tp)
- This is the time needed for a signal to propagate from one end of the medium to the other.
- When a station sends a frame, and any other station tries to send a frame during this time, a collision will result.



Persistence Methods

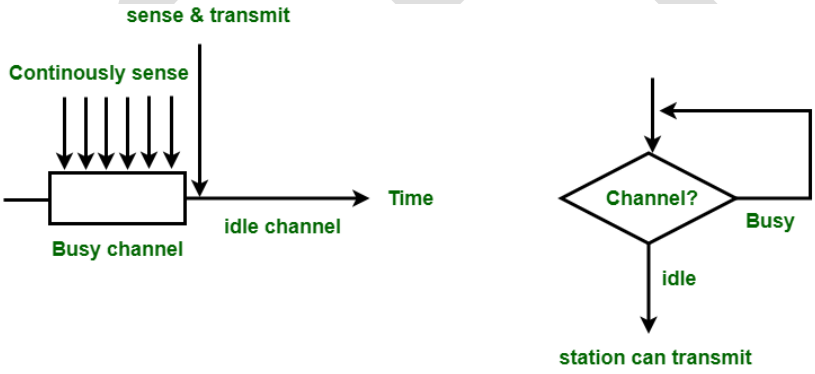
The persistence methods can be applied to help the station take action when the channel is busy/idle.

- 1-Persistent method
- Non-persistent method

P-persistent method

1-persistent CSMA: In 1-persistent CSMA, the station continuously senses the channel to check its state i.e. idle or busy so that it can transfer data or not.

- In case when the channel is busy, the station will wait for the channel to become idle.
- When station found idle channel, it transmits the frame to the channel without any delay. It transmits the frame with probability 1.
- Due to probability 1, it is called 1-persistent CSMA.
- The problem with this method is that there are a large number of chances for the collision it is because there is a chance when two or more stations found channel in idle state and the transmit frames at the same time.
- On the time when collision occurs the station has to wait for the random time for the channel to be idle and to start all again.



Non-persistent CSMA: In this method, the station that has frames to send, only that station senses for the channel.

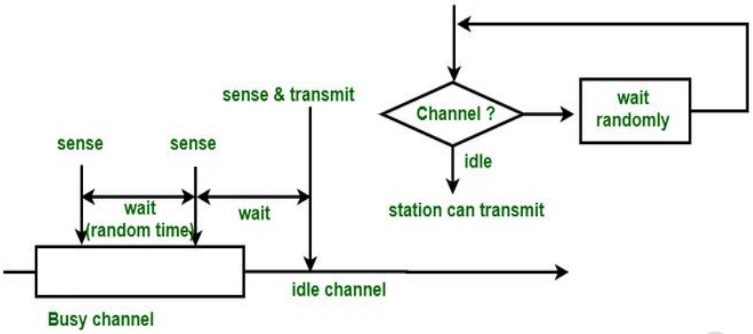
In case of an idle channel, it will send frame immediately to that channel.

In case when the channel is found busy, it will wait for the random time and again sense for the state of the station whether idle or busy.

In this method, the station does not immediately sense for the channel for only the purpose of capturing it when it detects the end of the previous transmission.

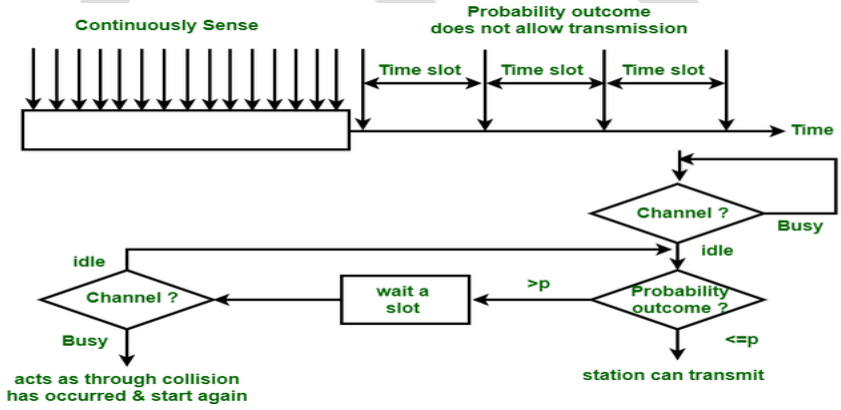
The main advantage of using this method is that it reduces the chances of collision.

The problem with this is that it reduces the efficiency of the network.



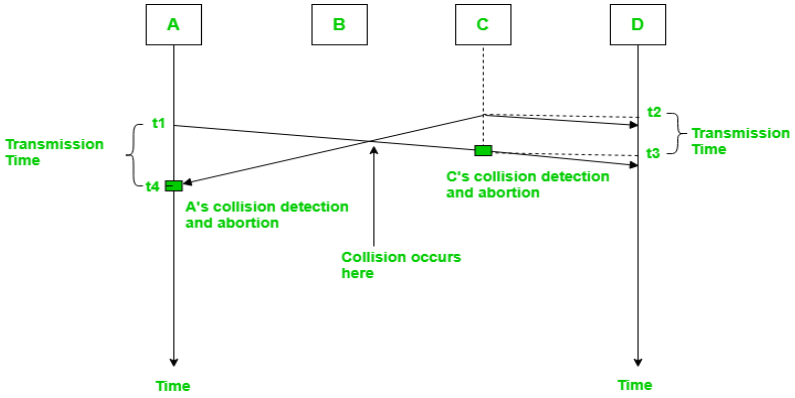
p-persistent CSMA: This is the method that is used when channel has time-slots and that time-slot duration is equal to or greater than the maximum propagation delay time.

- When the station is ready to send the frames, it will sense the channel.
- If the channel found to be busy, the channel will wait for the next slot.
- If the channel found to be idle, it transmits the frame with probability p, thus for the left probability i.e. q which is equal to 1-p the station will wait for the beginning of the next time slot.
- In case, when the next slot is also found idle it will transmit or wait again with the probabilities p and q.
- This process is repeated until either the frame gets transmitted or another station has started transmitting.



Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.
- If successful, the transmission is finished, if not, the frame is sent again.

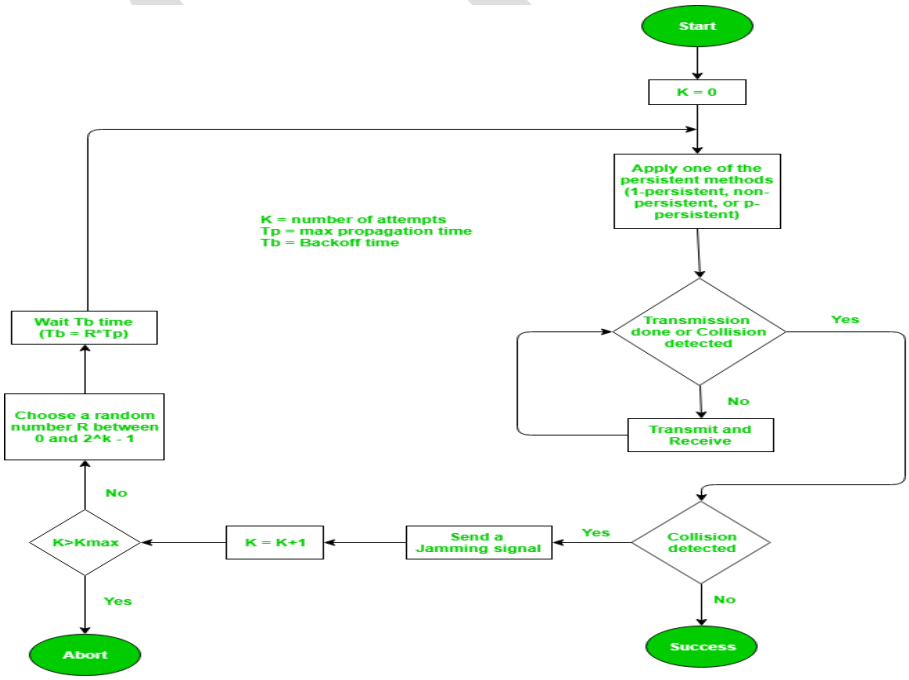


- In the diagram, *starts* sending the first bit of its frame at t1 and since C sees the channel idle at t2, starts sending its frame at t2.
- C detects A's frame at t3 and aborts transmission. A detects C's frame at t4 and aborts its transmission.

  Transmission time for C's frame is, therefore, t3-t2 and for A's frame is t4-t1
- So, the **frame transmission time (Tfr) should be at least twice the maximum propagation time (Tp)**. This can be deduced when the two stations involved in a collision are a maximum distance apart.
- **Throughput and Efficiency:** The throughput of CSMA/CD is much greater than pure or slotted ALOHA.
- For the 1-persistent method, throughput is 50% when G=1.

  For the non-persistent method, throughput can go up to 90%.

Process: The entire process of collision detection can be explained as follows:



Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- CSMA/CA use three strategies to avoid Collisions. These are three types of strategies:

1.InterFrame Space (IFS): When a station finds the channel busy it senses the channel again, when the station finds a channel to be idle it waits for a period of time called

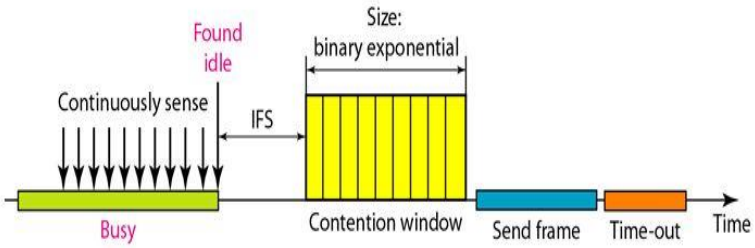
IFS time.

IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.

2.Contention Window: It is the amount of time divided into slots.

A station that is ready to send frames chooses a random number of slots as **wait time**.

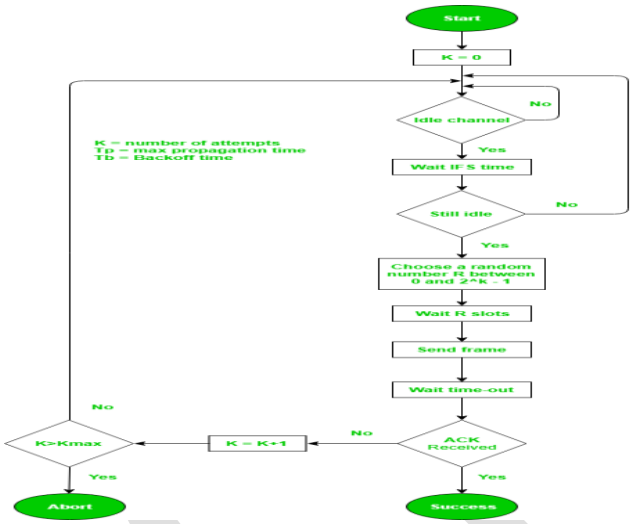
3.Acknowledgments: The positive acknowledgments and time-out timer can help guarantee a successful transmission of the frame.



Characteristics of CSMA/CA :

- **Carrier Sense**: The device listens to the channel before transmitting, to ensure that it is not currently in use by another device.
- **Multiple Access**: Multiple devices share the same channel and can transmit simultaneously.
- **Collision Avoidance**: If two or more devices attempt to transmit at the same time, a collision occurs. CSMA/CA uses random backoff time intervals to avoid collisions.
- **Acknowledgment (ACK)**: After successful transmission, the receiving device sends an ACK to confirm receipt.
- **Fairness**: The protocol ensures that all devices have equal access to the channel and no single device monopolizes it.
- **Binary Exponential Backoff**: If a collision occurs, the device waits for a random period of time before attempting to retransmit. The backoff time increases exponentially with each retransmission attempt.

- **Interframe Spacing**: The protocol requires a minimum amount of time between transmissions to allow the channel to be clear and reduce the likelihood of collisions.
- **RTS/CTS Handshake**: In some implementations, a Request-To-Send (RTS) and Clear-To-Send (CTS) handshake is used to reserve the channel before transmission. This reduces the chance of collisions and increases efficiency.
- **Wireless Network Quality**: The performance of CSMA/CA is greatly influenced by the quality of the wireless network, such as the strength of the signal, interference, and network congestion.
- **Adaptive Behavior**: CSMA/CA can dynamically adjust its behavior in response to changes in network conditions, ensuring the efficient use of the channel and avoiding congestion.
- **Process:** The entire process of collision avoidance can be explained as follows:



Controlled Access Protocols

- In controlled access, the stations consult one another to find which station has the right to send.
- A station cannot send unless it has been authorized by other stations.
- Three popular controlled-access methods are :
- **Reservation**
- **Polling**
- **Token Passing**

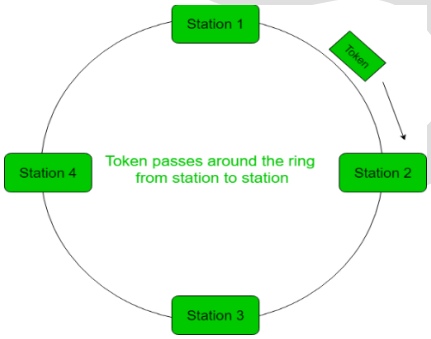
Reservation

- In the reservation method, a station needs to make a reservation before sending data.
- The timeline has two kinds of periods:

    - Reservation interval of fixed time length
    - Data transmission period of variable frames
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.

Token Passing

- In token passing scheme, the stations are connected logically to each other in form of ring and access to stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas incase of Token bus, each station uses the bus to send the token to the next station in some predefined order.
- In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.
- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbours and the other N – 1 stations to send a frame, if they have one.
- There exists problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable operation of this scheme.



Performance of token ring can be concluded by 2 parameters:-

1. **Delay**, is a measure of time between when a packet is ready and when it is delivered. So, the average time (delay) required to send a token to the next station = a/N.
2. **Throughput**, which is a measure of successful traffic.

Throughput, S = 1/(1 + a/N) for a<1

and

S = 1/{a(1 + 1/N)} for a>1.

where N = number of stations

$a = T_p/T_t$

(T_p = propagation delay and T_t = transmission delay)

Advantages of Token passing:

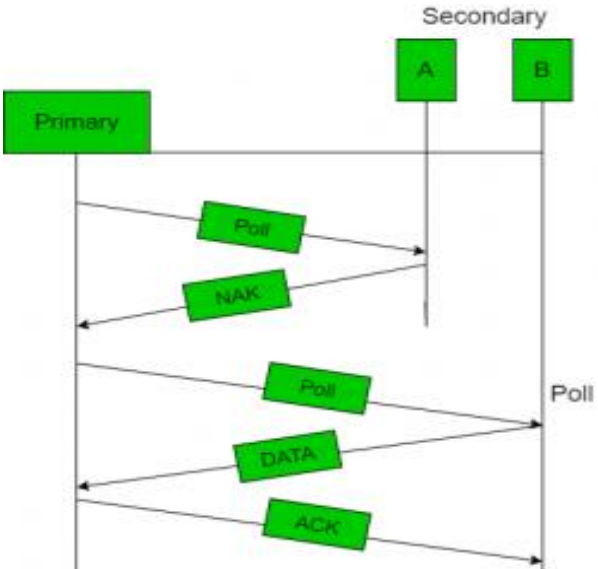
- It may now be applied with routers cabling and includes built-in debugging features like *protective relay and auto reconfiguration.*
- It provides *good throughput* when conditions of high load.

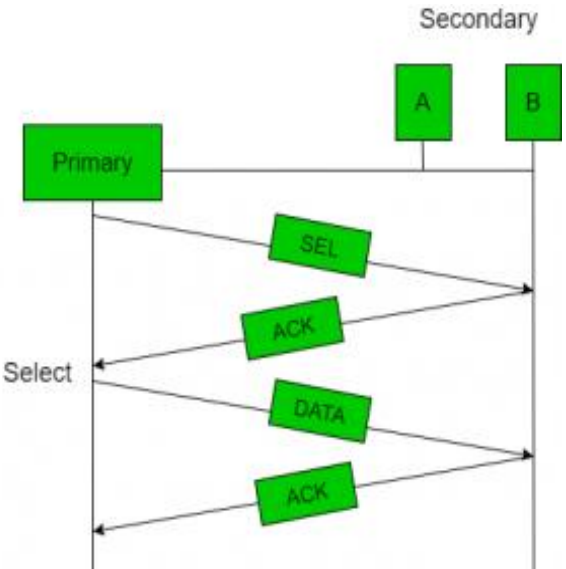
Disadvantages of Token passing:

- Its cost is *expensive.*
- Topology components are more expensive than those of other, more widely used standard.
- The hardware element of the token rings are designed to be tricky. This implies that you should choose on manufacture and use them exclusively.

Polling

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.
- Although all nodes receive the message the addressed one responds to it and sends data if any. If there is no data, usually a “poll reject”(NAK) message is sent back.
- Problems include high overhead of the polling messages and high dependence on the reliability of the controller.





Advantages of Polling:

- The maximum and minimum access time and data rates on the channel are fixed predictable.
- It has maximum *efficiency.*
- It has maximum *bandwidth.*
- No slot is wasted in polling.
- There is assignment of priority to ensure faster access from some secondary.

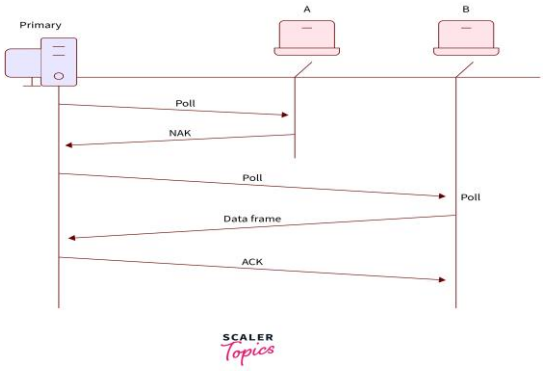
Disadvantages of Polling:

- It consume *more time.*
- Since every station has an equal chance of winning in every round, link sharing is *biased.*
- Only some station might run out of data to send.
- An increase in the turnaround time leads to a drop in the data rates of the channel under low loads.
- **Efficiency** Let T_{poll} be the time for polling and T_t be the time required for transmission of data. Then,
- Efficiency = $T_t/(T_t + T_{poll})$

Poll Function

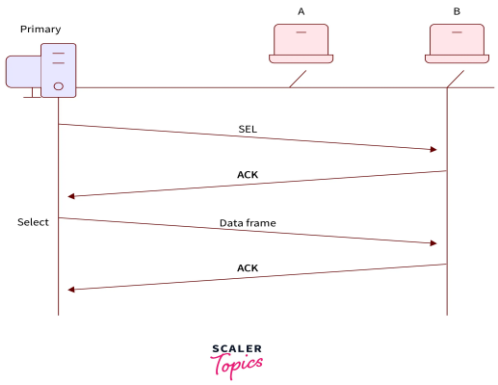
- Suppose there is a condition when the primary device wants to accept data from secondary devices, then in this condition, it generally asked from secondary devices if they want to transmit any data. This process is known as the polling function. The polling function is used by the primary device to ask for transmit the data from the secondary device.
- When the Primary device wants to get the data frame then it should ask (poll) each secondary device on that particular network if they want to transfer any data frame.
- If the secondary device has any data that it needs to transfer to the primary device then it sent the data frame although it will transmit a negative acknowledgment (NAK)
- If there is a condition when the primary device received a negative acknowledgment from one secondary device then it repeats this process with another secondary device in the same manner till it finds the secondary device that has some data to send.

- Whenever the primary device gets a positive acknowledgment i.e data frame from any secondary device, then after it, it reads the data frame and transmits a return acknowledgment (ACK).



Select Function

- Suppose there is a condition when the primary device needs to send some data to secondary devices then they tell the secondary devices so that secondary devices prepare themselves to receive the data. This process is known as the select function. The primary device generally uses a select function when it wants to send some data to secondary devices. As already mentioned above the primary device always has control over the link.
- Before transferring any data frame, there is the creation of a select (SEL) frame
- And the primary device transmits this frame to the secondary device.
- This SEL frame in its one field contains the address of the secondary device to which the primary device wants to send the data.
- There is an alert from the primary device to the secondary device for the transmission of the upcoming data packet.
- After this primary device waits for the acknowledgment(ACK) frame from the secondary device.



Advantages of Polling

- Some of the advantages of using the polling method are given below
- There are fixed and predictable data rates and the minimum and maximum access time on the channel.
- For ensuring faster access to data from the secondary device it used priority assignment.

Drawbacks

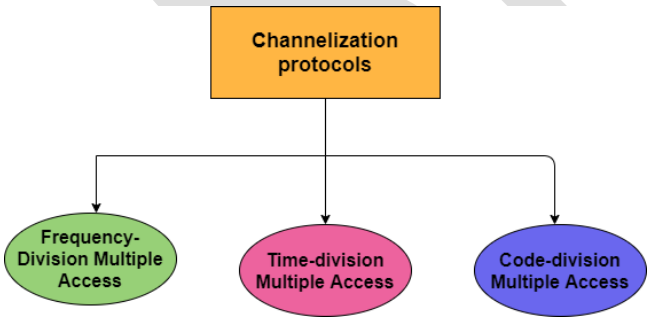
- Some of the disadvantages of using the polling method are given below:
- The dependency on the reliability of the controller is high.
- In the condition of low load, there is a decrement in the data rate of the channel due to the increment in turnaround time.
- There is so much overhead of polling messages.

Channelization Protocols

- Channelization is basically a method that provides the multiple-access and in this, the available bandwidth of the link is shared in time, frequency, or through the code in between the different stations.

Channelization Protocols are broadly classified as follows:

- FDMA(Frequency-Division Multiple Access)
- TDMA(Time-Division Multiple Access)
- CDMA(Code-Division Multiple Access)



1. Frequency-Division Multiple Access

- With the help of this technique, the available bandwidth is divided into frequency bands. Each station is allocated a band in order to send its data. Or in other words, we can say that each band is reserved for a specific station and it belongs to the station all the time.

- Each station makes use of the **bandpass filter** in order to confine the **frequencies of the transmitter.**
- In order to prevent station interferences, the allocated bands are separated from one another with the help of small **guard bands.**
- The Frequency-division multiple access mainly specifies a predetermined frequency for the entire period of communication.
- Stream of data can be easily used with the help of FDMA.

Advantages of FDMA

- Given below are some of the benefits of using the FDMA technique:
- This technique is efficient when the traffic is uniformly constant.
- In case if the channel is not in use then it sits idle.
- FDMA is simple algorithmically and the complexity is less.
- For FDMA there is no restriction regarding the type of baseband or the type of modulation.

Disadvantages of FDMA

- By using FDMA, the maximum flow rate per channel is fixed and small.

2 Time-Division Multiple Access

- Time-Division Multiple access is another method to access the channel for shared medium networks.
- With the help of this technique, the stations share the bandwidth of the channel in time.
- A time slot is allocated to each station during which it can send the data.
- Data is transmitted by each station in the assigned time slot.
- There is a problem in using TDMA and it is due to TDMA the synchronization cannot be achieved between the different stations.
- When using the TDMA technique then each station needs to know the beginning of its slot and the location of its slot.
- If the stations are spread over a large area, then there occur propagation delays; in order to compensate this guard, times are used.
- The data link layer in each station mainly tells its physical layer to use the allocated time slot.
- Some examples of TDMA are as follows;
- personal digital Cellular(PDC)

- Integrated digital enhanced network.
- Universal terrestrial radio access(UTRA)

3. Code-Division Multiple Access

- CDMA(code-division multiple access) is another technique used for channelization.
- CDMA technique differs from the FDMA because only one channel occupies the entire bandwidth of the link.
- The CDMA technique differs from the TDMA because all the stations can send data simultaneously as there is no timesharing.
- The CDMA technique simply means communication with different codes.
- In the CDMA technique, there is only one channel that carries all the transmission simultaneously.
- CDMA is mainly based upon the coding theory; where each station is assigned a code, Code is a sequence of numbers called chips.
- The data from the different stations can be transmitted simultaneously but using different code languages.

Advantages of CDMA

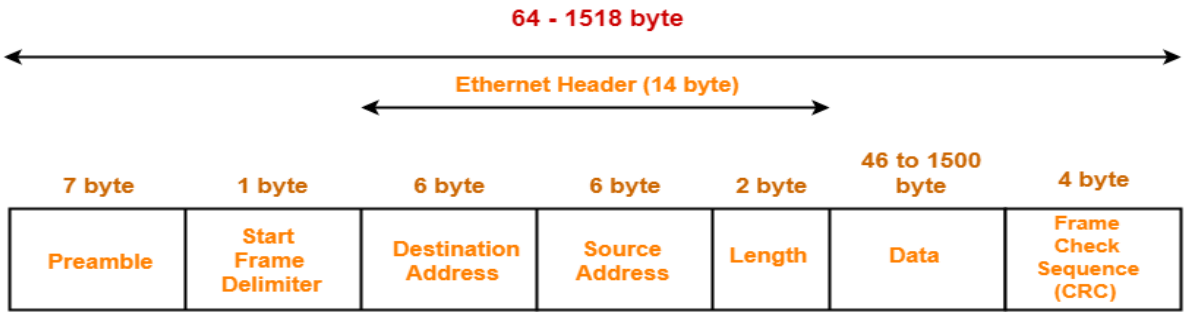
- Given below are some of the advantages of using the CDMA technique:
- Provide high voice quality.
- CDMA operates at low power levels.
- The capacity of the system is higher than the TDMA and FDMA.
- CDMA is better cost-effective.

ETHERNET : IEEE STANDARDS

- Local Area Network (LAN) is a computer network that is designed for a limited geographic area such as building or a campus.
- Ethernet is simply refers to the most common type of Local Area Network (LAN) used today.
- A standard Ethernet cable is slightly thicker than a phone cable.
- A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps).

- Wired connections are less prone to interference and are more secure than wireless ones, which is why many business and organizations still use Ethernet.
- Ethernet is also known by its technical name , IEEE 802.3".
- Computer society of IEEE (Institute Of Electrical and Electronic Engineers) started a project called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers.
- The standard was adopted by ANSI.
- The ISO also approved it as an international standard.
- The IEEE has subdivided the data link layer into two sublayers: Logical link control (LLC) and Media access control (MAC).
- In IEEE 802, flow control, error control and part of the framing duties are collected into one sub layer called the LLC.
- The LLC provides one single data link control protocol for all IEEE LANs.
- In this way the LLC is different from the media access control sublayer, which provides different protocols for different LANs.
- Media access control (MAC) defines the specific access method for each LAN.
- Example, it defines CSMA/CD as the media access method for Ethernet LANs.
- Ethernet provides connectionless service, which means each frame sent is independent of the previous or next frame.
- Ethernet has no connection establishment or connection termination phase.
- Ethernet is unreliable.

  Frame Format of Ethernet



IEEE 802.3 Ethernet Frame Format

PREAMBLE – Ethernet frame starts with a 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allow sender and receiver to establish bit synchronization

Start of frame delimiter (SFD) – This is a 1-Byte field that is always set to 10101011. SFD indicates that upcoming bits are starting the frame, which is the destination address.

Destination Address – This is a 6-Byte field that contains the MAC address of the machine for which data is destined.

Source Address – This is a 6-Byte field that contains the MAC address of the source machine. As Source Address is always an individual address (Unicast), the least significant bit of the first byte is always 0.

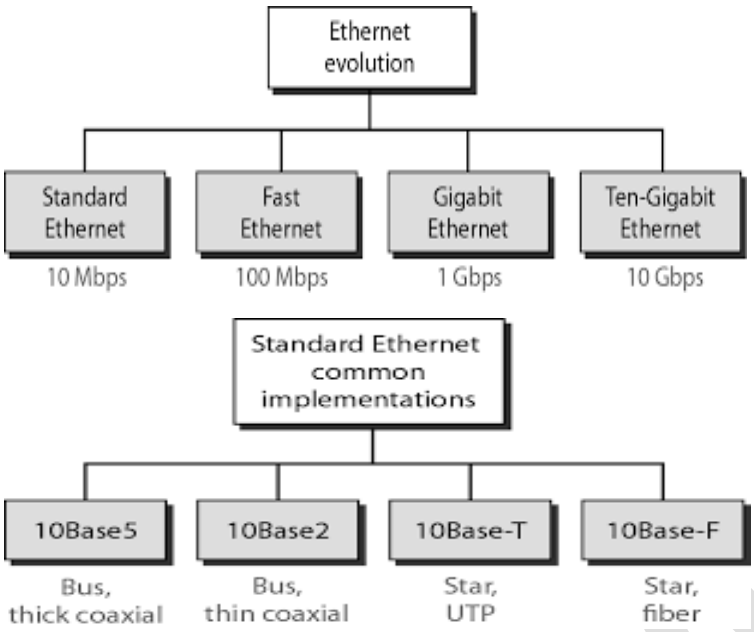
Length – Length is a 2-Byte field, which indicates the length of the entire Ethernet frame. This 16-bit field can hold a length value between 0 to 65534, but length cannot be larger than 1500 Bytes because of some own limitations of Ethernet.

Data – This is the place where actual data is inserted, also known as **Payload.** The maximum data present may be as long as 1500 Bytes. In case data length is less than minimum length i.e. 46 bytes, then padding 0's is added to meet the minimum possible length.

Cyclic Redundancy Check (CRC) – CRC is 4 Byte field. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as sent checksum value, data received is corrupted.

Addressing

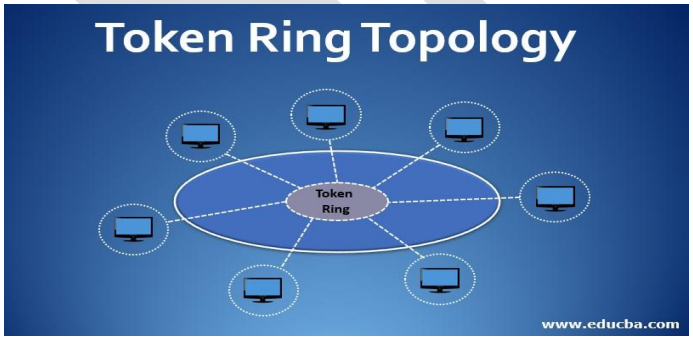
- Each station on an Ethernet network has it's own network interface card (NIC)
- NIC fits inside the station and provides the station with a link layer address.
- Ethernet address is 6 bytes(48bits) written in hexadecimal notation with a colon between the bytes.
- Eg: 4A:30:10:21:10:1A



TOKEN BUS AND TOKEN RING

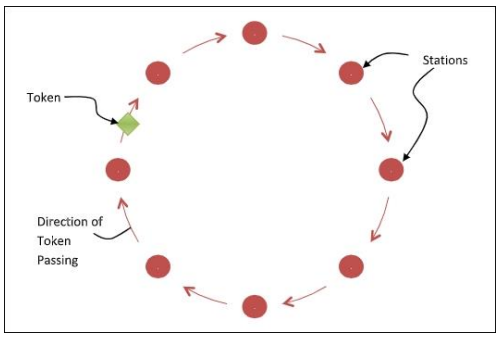
Token ring – IEEE 802.5

- Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition.
- A token is a special frame of 3 bytes that circulates along the ring of stations.
- A station can send data frames only if it holds a token.
- The tokens are released on successful receipt of the data frame.



- If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise it simply passes the token to the next station.
- Passing the token means receiving the token from the preceding station and transmitting to the successor station.
- The data flow is unidirectional in the direction of the token passing.

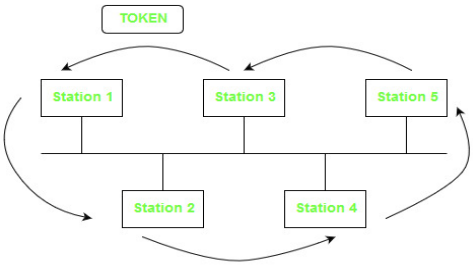
- In order that tokens are not circulated infinitely, they are removed from the network once their purpose is completed.



Token Bus (IEEE 802.4)

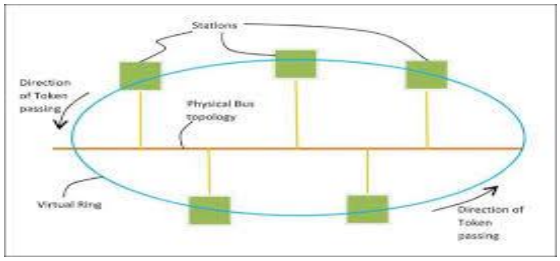
- Token bus (IEEE 802.4) is a standard for implementing token ring over virtual ring in LANs.
- The physical media has a bus or a tree topology and uses coaxial cables.
- A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring..
- Each node knows the address of its preceding station and its succeeding station.
- A station can only transmit data when it has the token.

  The working principle of token bus is similar to Token Ring.



- A token is a small message that circulates among the stations of a computer network providing permission to the stations for transmission.

If a station has data to transmit when it receives a token, it sends the data and then passes the token to the next station; otherwise, it simply passes the token to the next station

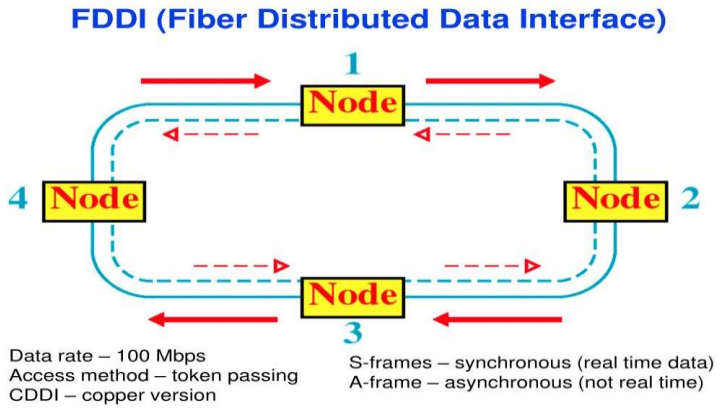


Fiber Distributed Data Interface (FDDI)

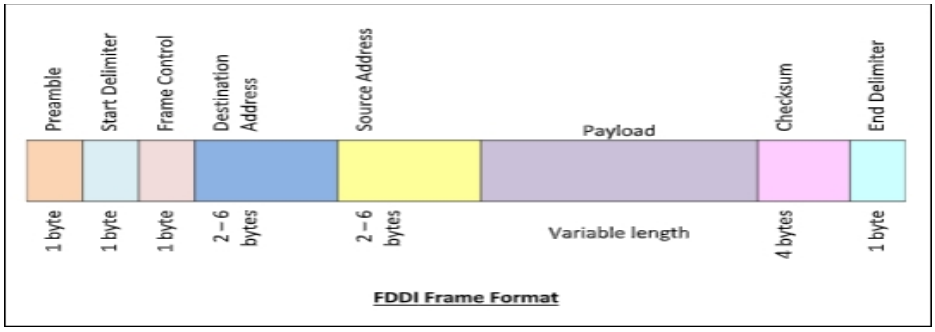
- Fiber Distributed Data Interface (FDDI) is a set of ANSI and ISO standards for transmission of data in local area network (LAN) over fiber optic cables.
- It is applicable in large LANs that can extend up to 200 kilometers in diameter.

Features

- FDDI uses optical fiber as its physical medium.
- It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.
- It provides high data rate of 100 Mbps and can support thousands of users.
- It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.
- It uses ring based token passing mechanism and is derived from IEEE 802.4 token bus standard.
- It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails.
- FDDI technology can also be used as a backbone for a wide area network (WAN).



FDDI Frame Format



The fields of an FDDI frame are −

- **Preamble:** 1 byte for synchronization.
- **Start Delimiter:** 1 byte that marks the beginning of the frame.
- **Frame Control:** 1 byte that specifies whether this is a data frame or control frame.
- **Destination Address:** 2-6 bytes that specifies address of destination station.
- **Source Address:** 2-6 bytes that specifies address of source station.
- **Payload:** A variable length field that carries the data from the network layer.
- **Checksum:** 4 bytes frame check sequence for error detection.
- **End Delimiter:** 1 byte that marks the end of the frame.

S. No.	Token Bus Network	Token Ring Network
1.	In the token bus network, the token is passed along a virtual ring.	While in the token ring network the token is passed over a physical ring.
2.	The token bus network is simply designed for large factories.	While the token ring network is designed for the offices.
3.	The token bus network is defined by the IEEE 802.4 standard.	While the token ring network is defined by the IEEE 802.5 standard.
4.	Token bus network provides better bandwidth.	While the token ring network does not provide better bandwidth as compared to the token bus.
5.	In a token bus network, Bus topology is used.	While in token ring network, Star topology is used.
6.	The maximum time it takes to reach the last station in a token bus network cannot be calculated.	While the maximum time to reach the last station in the token ring network can be calculated.
S. No.	**Token Bus Network**	**Token Ring Network**
7	In a token bus network, coaxial cable is used	In token ring network, twisted pair and fiber optic is used.
8	In a token bus network, the cable length is 200m to 500m.	In a token ring network, the cable length is 50m to 1000m.
9.	In token bus network, distributed algorithm provide maintenance.	In a token ring network, a designated monitor station performs station maintenance.
10.	The priority handling mechanism is not associated with the transmission of data through workstations with this network.	The priority handling mechanism is associated with the transmission of data through workstations with this network.
11.	These networks are not much reliable.	These networks are reliable.
12.	It does not keep routing details.	It keeps the information of routing.
13.	The network is less expensive compared to the Token Ring network.	It is expensive.

FDDI VS TOKEN RING

Similarities

- FDDI uses a rotating ring setup in the same way as the token ring protocol.

- **FDDI's ring operation is basically very similar to the Token Ring early release operation in the way that tokens are passed on the network.**

Differences

- As opposed to Token Ring's single ring, FDDI, uses two to achieve better results and less chance of failure.

- In a basic Token Ring network, at any instant there is a single active ring monitor which supplies the master clock for the ring, whereas in FDDI this approach isn't ideal because of the high data rates. Instead, each ring interface has its own local clock, and outgoing data is transmitted using this clock.

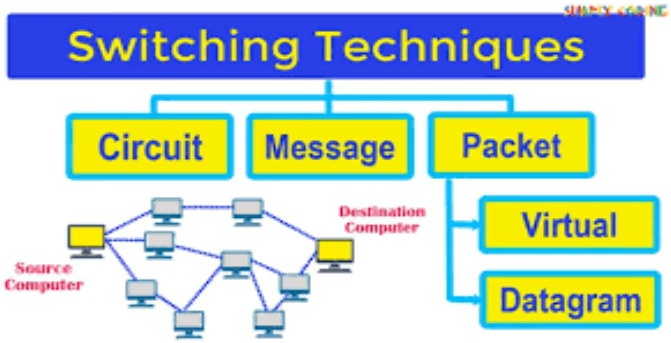
- Unlike the basic Token Ring, which is based on the use of priority and reservation bits, the priority operation of the FDDI ring uses a principle that is based on a parameter known as the Token Rotation Time, or TRT.

- FDDI uses a timed token protocol where Token Ring uses priority/reservation token access, leading to differences in frame format and how station traffic is handled

Protocol	Data Rate	Segment Length
FDDI	100	Unlimited
IEEE 802.5	4/16	250
IBM Token Ring	4/16	250

Switching techniques

- In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.
- Switching technique is used to connect the systems for making one-to-one communication.

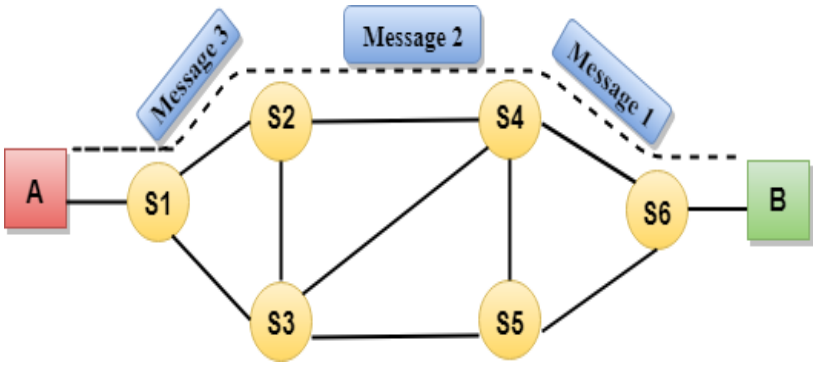


Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place..
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



Advantages Of Circuit Switching:

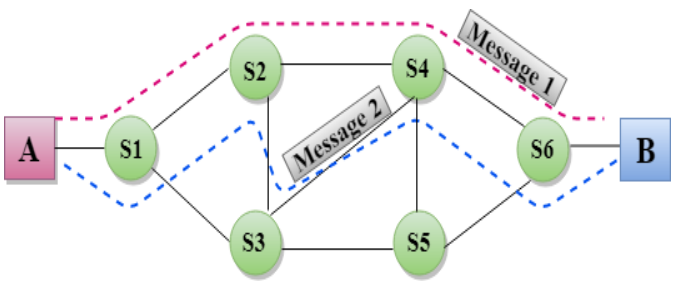
- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages Of Message Switching

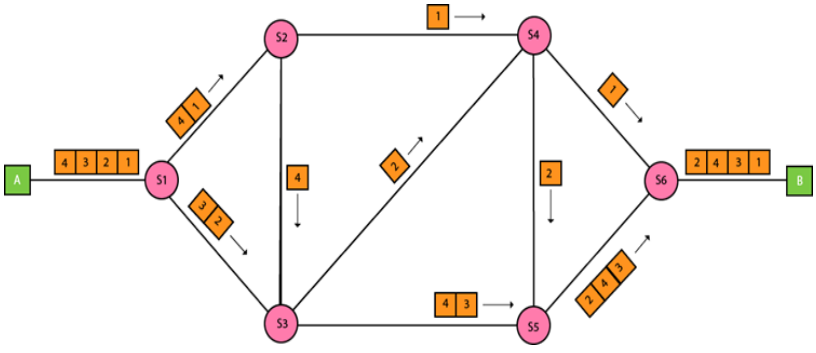
- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages Of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



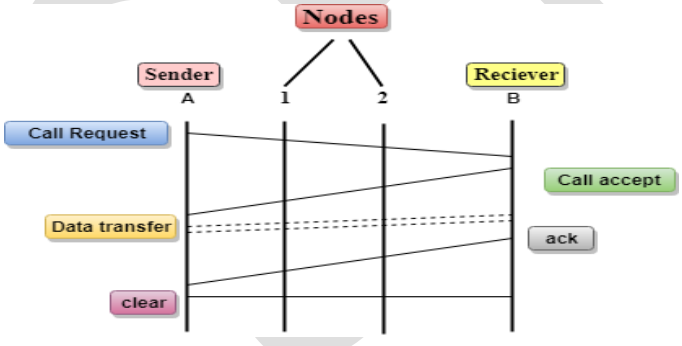
Approaches Of Packet Switching:

Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.



- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible

Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:**It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously.

Disadvantages Of Packet Switching

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.

If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered

Integrated Services Digital Network

- ISDN or Integrated Services Digital Network, is a circuit-switched telephone network system that transmits both data and voice over a digital line.
- You can also think of it as a set of communication standards to transmit data, voice, and signaling.
- These digital lines could be copper lines. It was designed to move outdated landline technology to digital.
- ISDN connections have a reputation for providing better speeds and higher quality than traditional connections. Faster speeds and better connections allow data transmissions to travel more reliably.

History of ISDN

- Analog phone networks failed constantly and proved to be unreliable for long-distance connections.Sometime in the 1960s, the system began to change over to a packet-based, digital switching system.
- The UN-based International Telecommunications Union, or ITU, started recommending ISDN in 1988 as a new system for operating companies to deliver data.
- It still took time for communication providers to begin to offer ISDN. This was mainly because both major companies at the time were on separate operating systems.
- By the 1990s, the National ISDN 1 was created.While this innovation could improve the quality of communications, an agreed-upon standard still took time to figure out.
- Finally, manufacturers like Motorola and USRobotics decided to make the transition easier for everyone.
- ISDN provided consumers with better pricing and higher-bandwidth internet access. Today, ISDN has been replaced by broadband internet access connections like DSL, WAN, and cable modems.

ISDN Services:

ISDN provides a fully integrated digital service to users. These services fall into 3 categories- bearer services, teleservices, and supplementary services.

- **Bearer Services –**
  Transfer of information (voice, data, and video) between users without the network manipulating the content of that information is provided by the bearer network. There is no need for the network to process the information and therefore does not change the content.
- **Teleservices –**
  In this, the network may change or process the contents of the data. Teleservices rely on the facilities of the bearer services and are designed to accommodate complex user needs. The user need not be aware of the details of the process. Teleservices include telephony, teletex, telefax, videotex, telex, and teleconferencing
- **Supplementary Service –**
  Additional functionality to the bearer services and teleservices are provided by supplementary services. Reverse charging, call waiting, and message handling are examples of supplementary services which are all familiar with today's telephone company services.

Advantages of ISDN:

- ISDN channels have a reliable connection.
- ISDN is used to facilitate the user with multiple digital channels.

- It has faster data transfer rate.

Disadvantages of ISDN:

- ISDN lines costlier than the other telephone system.
- It requires specialized digital devices.
- It is less flexible.