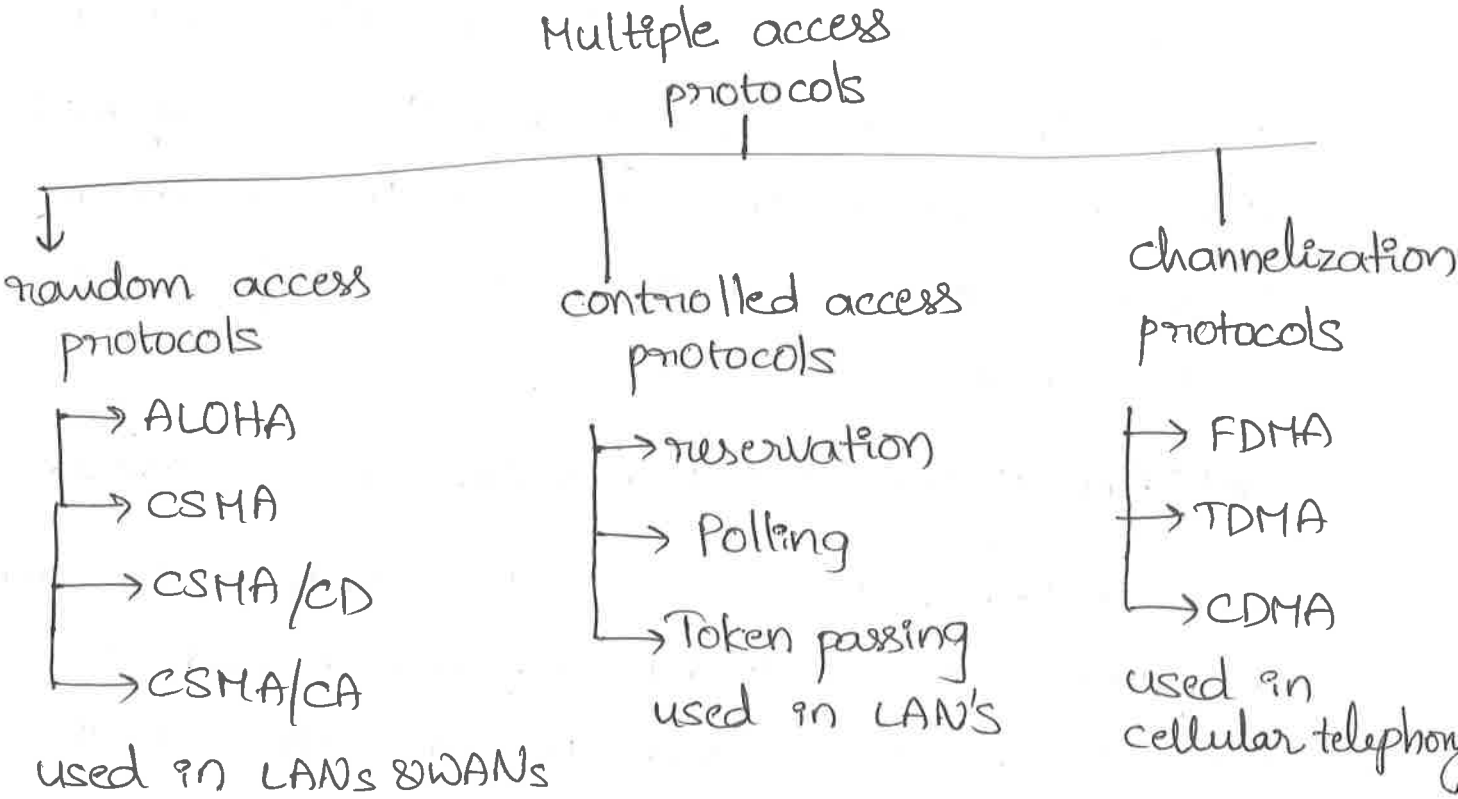
Media Access Control UNIT-3

When nodes ~~are~~ & stations are connected and use a common link, called a multipoint & broadcast link, we need a multiple access protocol to coordinate access to the link. Many protocols have been devised to handle access to a shared link. All of these protocols belong to a sub layer in the data link layer called media access control (MAC).

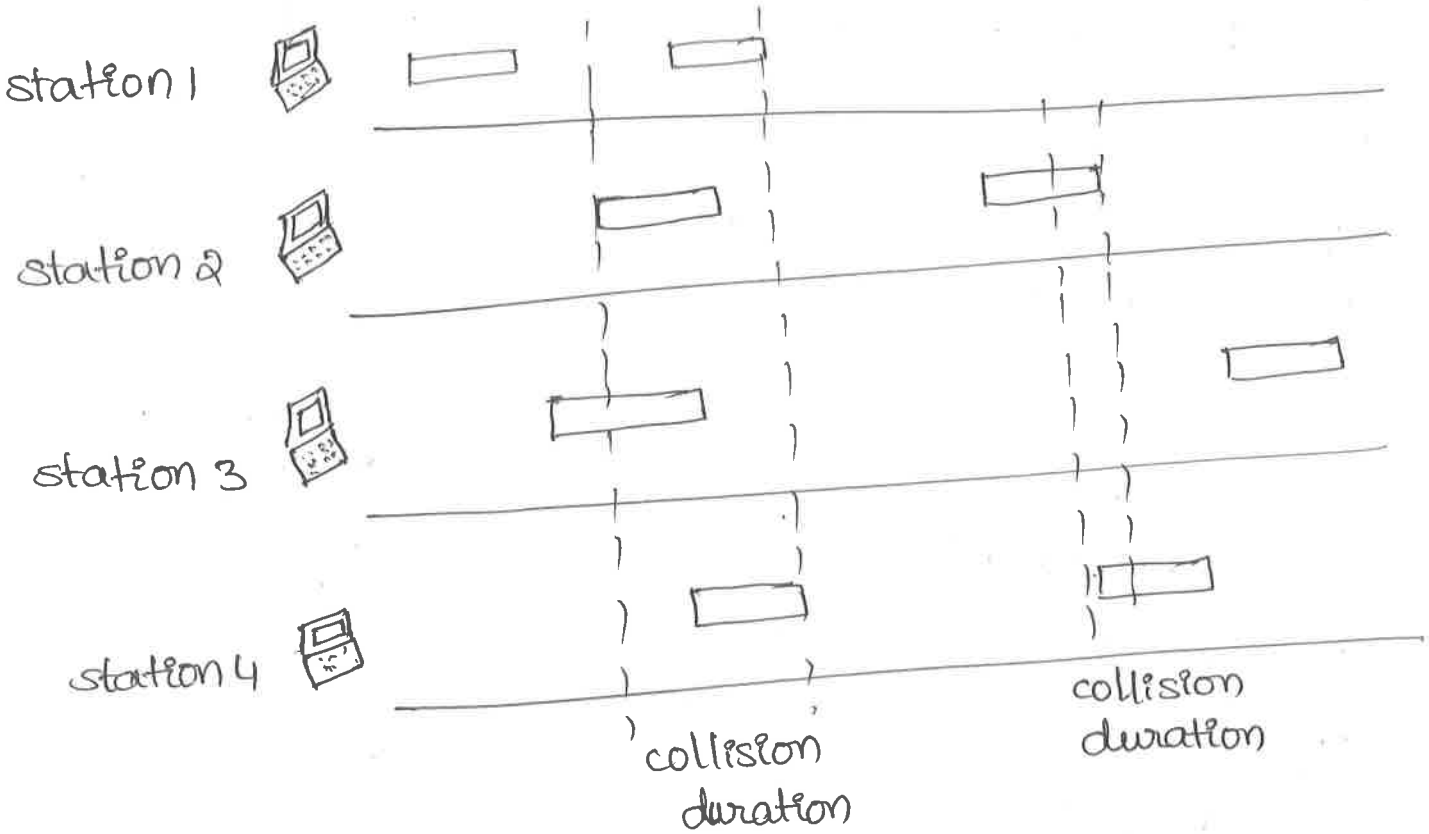


Random Access: In random access & contention methods, no station is superior to another station and none is assigned control over another.

Each station can transmit when it desires on the condition that it follows the predefined procedure including testing the state of the medium (idle, 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. This is why these methods are called random access. Second, no rules specify which station should send next, stations compete with one another to access the medium. That is why these methods are called contention methods. However, if more than one station tries to send, there is an access conflict - collision and the frames will be either destroyed or modified.

ALOHA : the earliest random access method.

Pure ALOHA : The idea is that each station sends a frame whenever it has a frame to send. Since, there is only one channel to share, there is the possibility of collision between frames from different stations.



→ 4 stations, each 2 frames, total 8 frames
→ only two frames survive
→ Pure ALOHA protocol relies on acknowledgements from the receiver. If the ack does not arrive after a time out period, the station assumes that the frame (or ack) has been destroyed and resends the frame. A collision involves two or more stations. If all these stations try to resend after the time out, the frames will collide again. Pure ALOHA dictates that when the time out period passes, each stations waits a random amount of time before resending its frame. We will call this is the back off time T_B.

Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum no. of retransmission attempts K_{max}, a station must give up and try later.

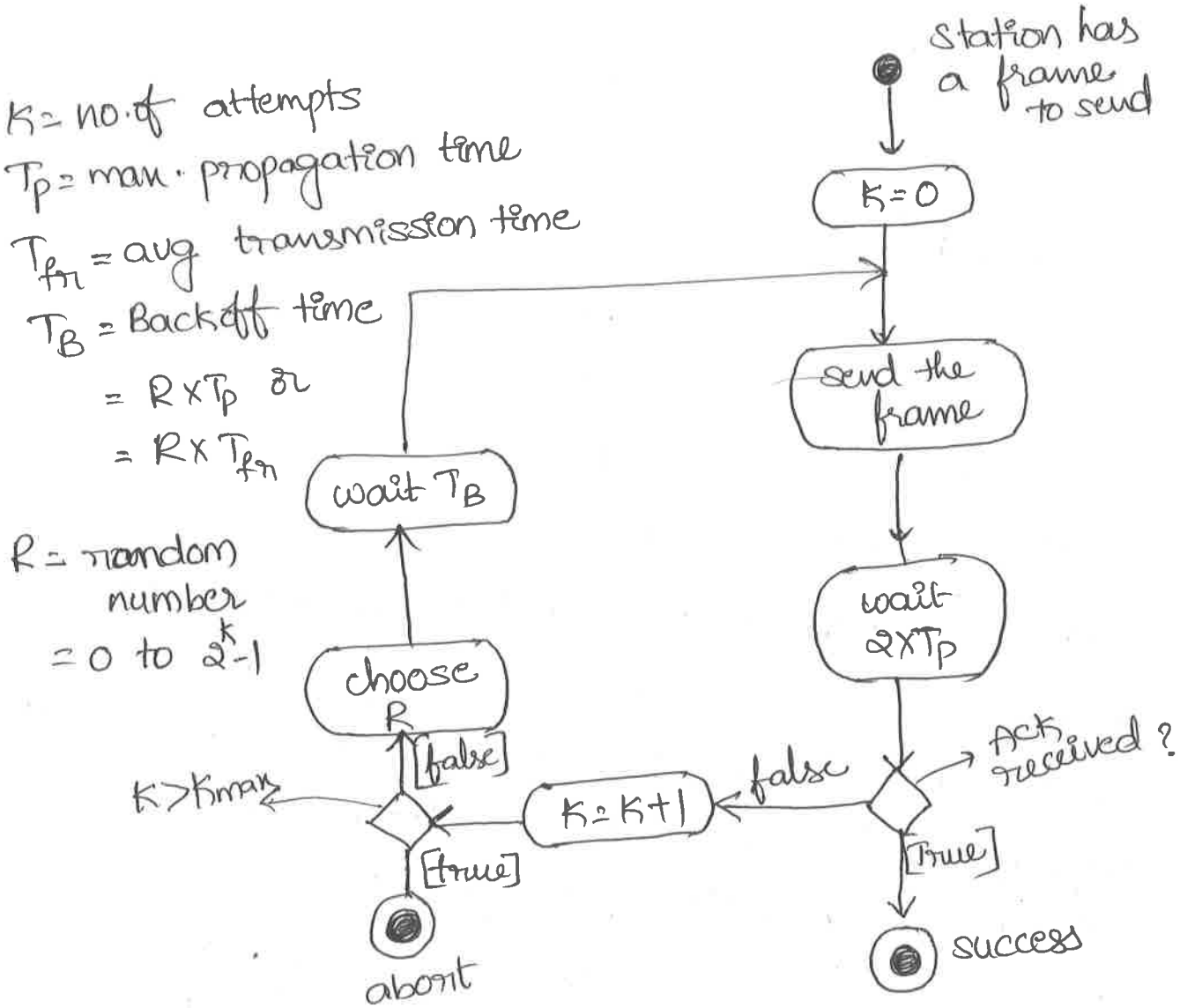


fig: Procedure for pure ALOHA protocol

The time out period is equal to the maximum possible round trip propagation delay. The backoff time T_B is a random value that depends on K (the no. of attempted unsuccessful transmissions)

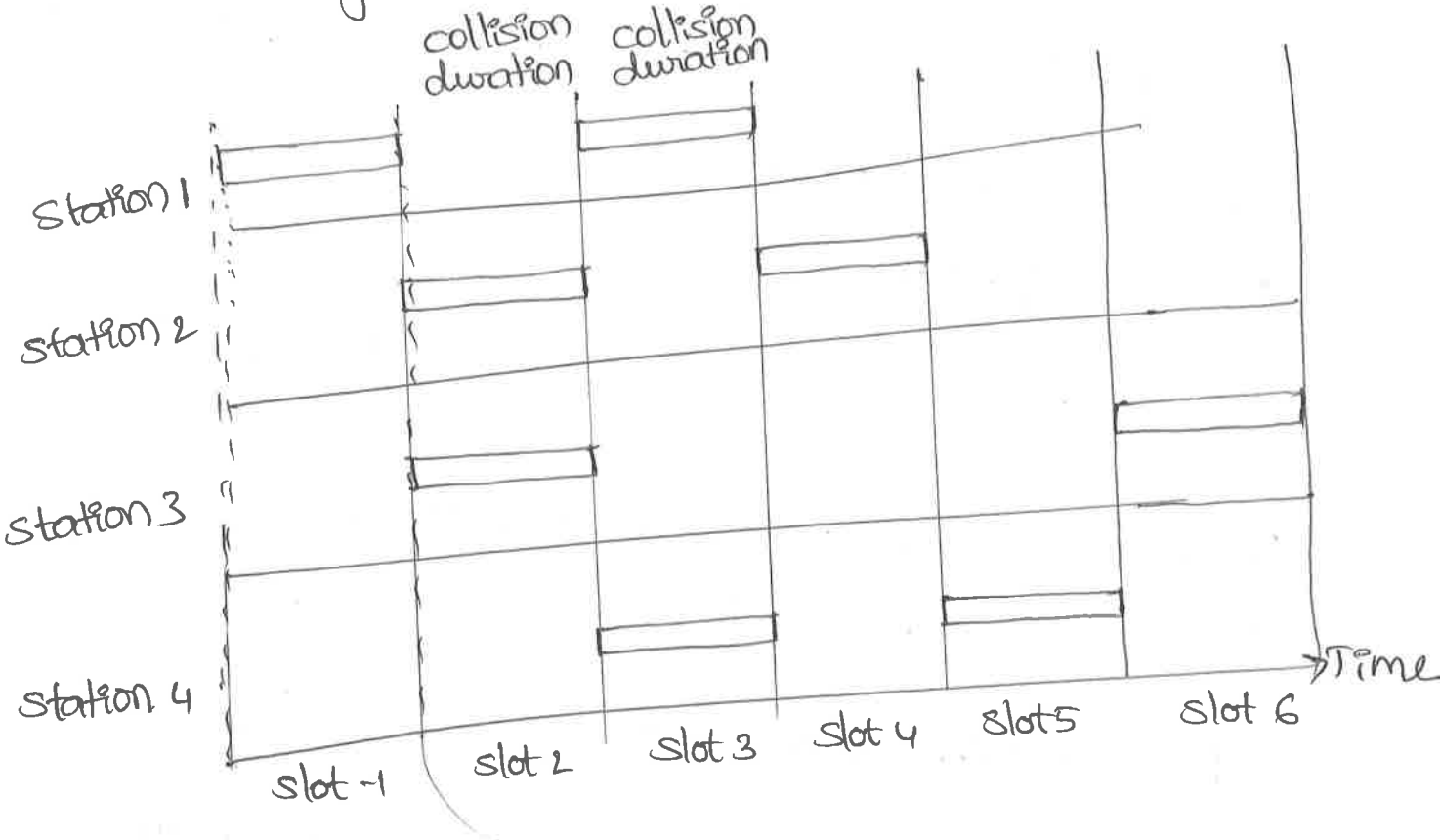
The formula for T_B is binary exponential backoff. In this method, for each retransmission a multiplier $R = 0$ to $2^K - 1$ is randomly chosen and multiplied by T_p (max propagation time) or T_{fr} (avg time required to send out a frame) to find T_B. The range of the random numbers increases after each collision. $K_{max} = 15$ usually

Vulnerable time : The length of time in which there is a possibility of collision.

Pure ALOHA Vulnerable time = $2 \times T_{fr}$

Throughput : G is the avg no. of frames generated by the system during one frame transmission time. The avg no. of successfully transmitted frames for pure ALOHA is $S = G \times e^{-2G}$. The max. throughput S_{max} is 0.184 for $G = 1/2$. ∴ If a station generates only one frame in this vulnerable time, (no other generati a frame during this time) the frame will reach its destination successfully.

Slotted ALOHA : In this, we divide the time into slots of T_{fr} seconds & force the station to send only at the begining of the time slot.



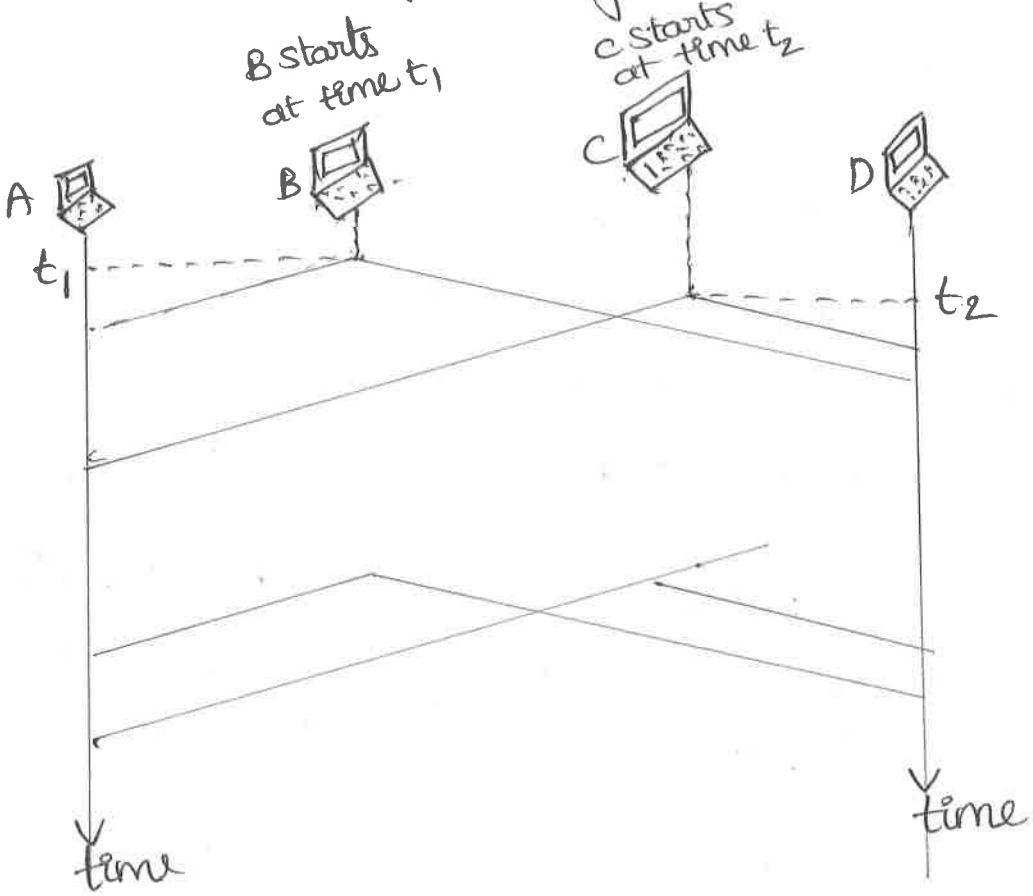
There is still the possibility of collision if two stations try to send at the beginning of the same time slot. The vulnerable time is now reduced to one half, ~~one~~ equal to T_{fr}.

$$\text{Vulnerable time} = T_{fr}$$

Throughput : The max throughput $S_{max} = 0.368$ when $G = 1$. In other words if one frame is generated during one frame transmission time, then 36.8% of these frames reach their destination successfully.

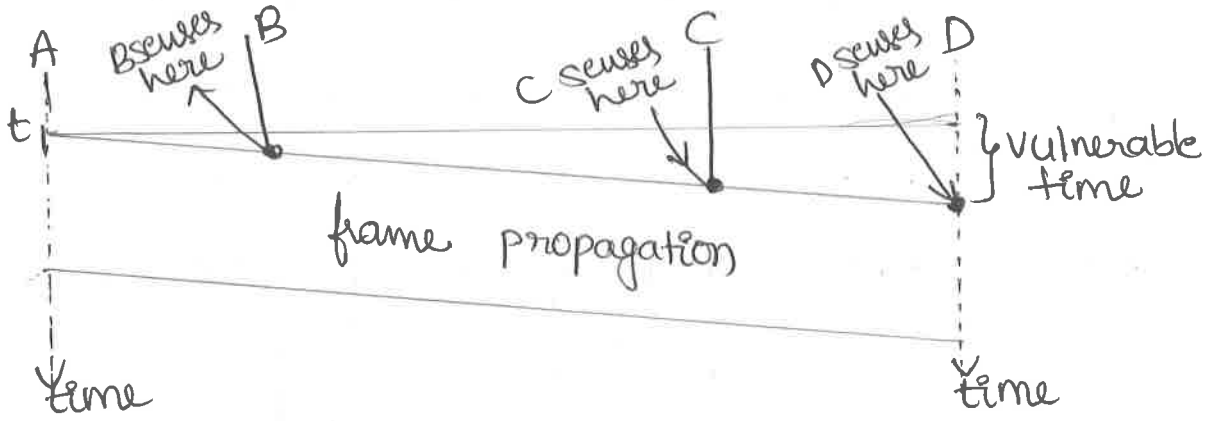
CSMA : To minimize the chance of collision. hoo means, If a station senses the medium before trying to use it. Carrier Sense Multiple Access requires that each station first listen to the medium before sending.

The possibility of collision still exists because of propagation delay. when a station sends a frame, it still takes time for the first bit to reach every station and for every station to sense it.



At time t_1, station B senses the medium and finds it idle, so it sends a frame. At time t_2 ($t_2 > t_1$) station C senses the medium and finds it idle because at this time, the first bits from station B have not reached station C. station C also sends a frame. Two collide & destroyed.

Vulnerable time : Vulnerable time for CSMA is the propagation time T_p. 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 :

what should a station do if the channel is busy or idle? Three methods to answer this question

① 1-persistent ② non persistent ③ P-persistent

1-persistent : In this method, if the line is idle, the station sends its frame immediately (with probability 1). This method has high chance of collision

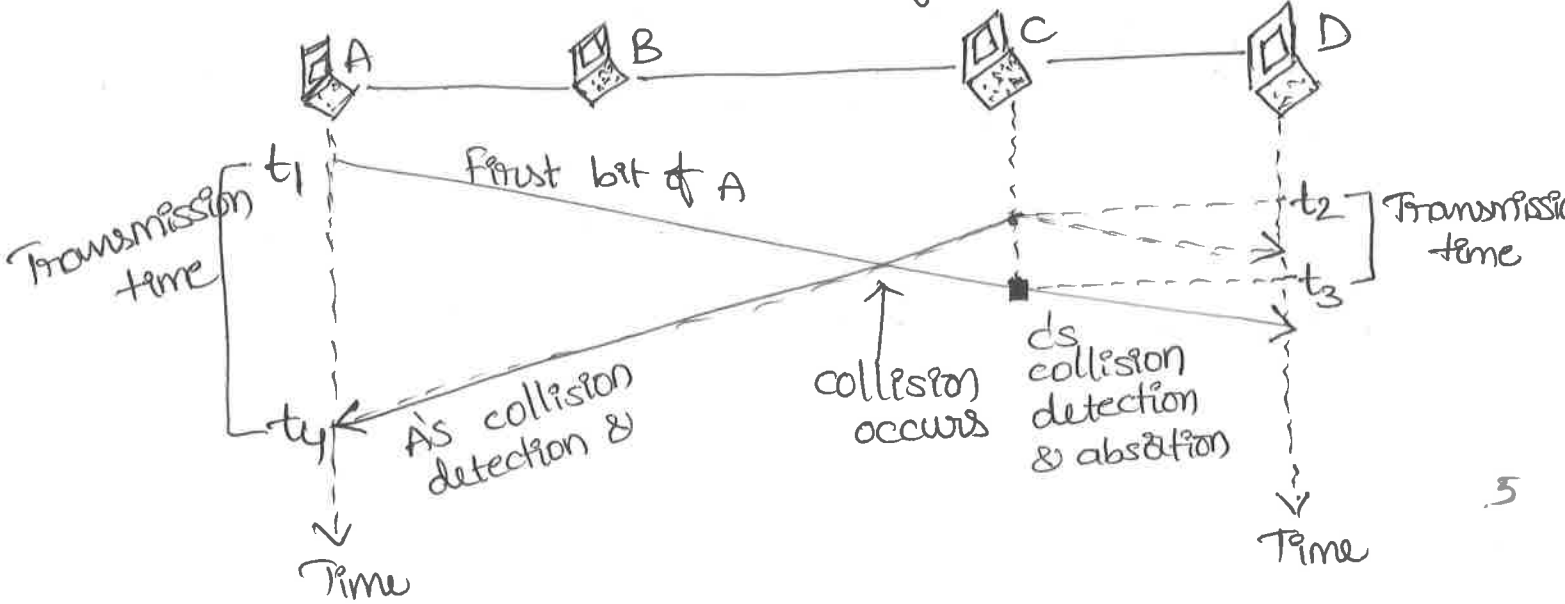
Non-persistent : In this method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. reduces chance of

collision. reduces efficiency of the networks.

P-persistent : this approach combines the advantages of the two strategies. reduces the chance of collision & improves efficiency. In this method, after the station finds the line idle it follows these steps.

1. with probability P, the station sends its frame
2. with probability $q = 1-P$, the station waits for the beginning of the next time slot and checks the line again
   a. if the line is idle, it goes to step 1
   b. if the line is busy, it acts as though a collision has occured and uses the backoff procedure.

CSMA/CD : In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.



At time t_1, station A has executed its persistence procedure and starts sending the bits of its frames. At time t_2, station C has not yet sensed the first bit sent by A. station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs some time after time t_2. Station C detects a collision at time t_3 when it receives the first bit of A's frame. Station C immediately aborts transmission. Station A detects collision at time t_4 when it receives the first bit of C's frame, it also immediately aborts transmission.

Minimum frame size: For CSMA/CD to work, we need a restriction on the frame size The frame transmission time T_{fr} must be atleast two times the max. propagation time T_p.

Procedure: It is similar to the one for the ALOHA protocol, but there are differences.

The first difference is the addition of the persistence process. The 2nd difference is the frame transmission. In ALOHA, we first transmit the entire frame and then wait for an acknowledgement. In CSMA/CD, transmission and collision detection are continuous processes. The station transmits and receives continuously and simultaneously. We constantly monitor in order to detect one of two conditions; either transmission is finished & a collision is detected. Either event stops transmission. The third difference is the sending of a short jamming signal to make sure that all other stations become aware of the collision.

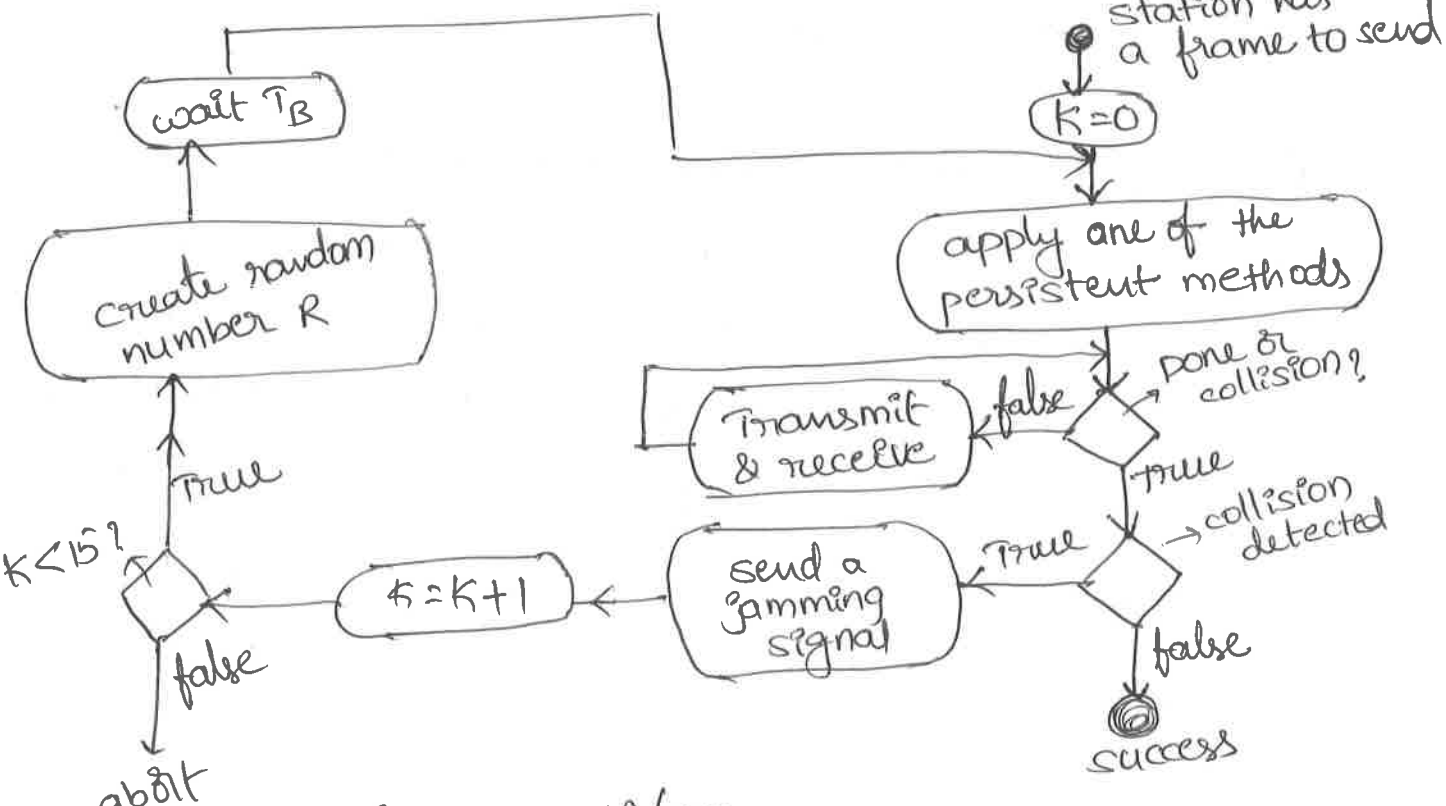


fig: CSMA/CD

T_{fm} = Frame average transmission time

K = no. of attempts

R = random number = 0 to $2^K - 1$

T_B = Backoff time = $R \times T_{fm}$

Energy level: level of energy in a channel can have three values

zero – channel is idle

normal – a station has successfully captured the channel and is sending its frame

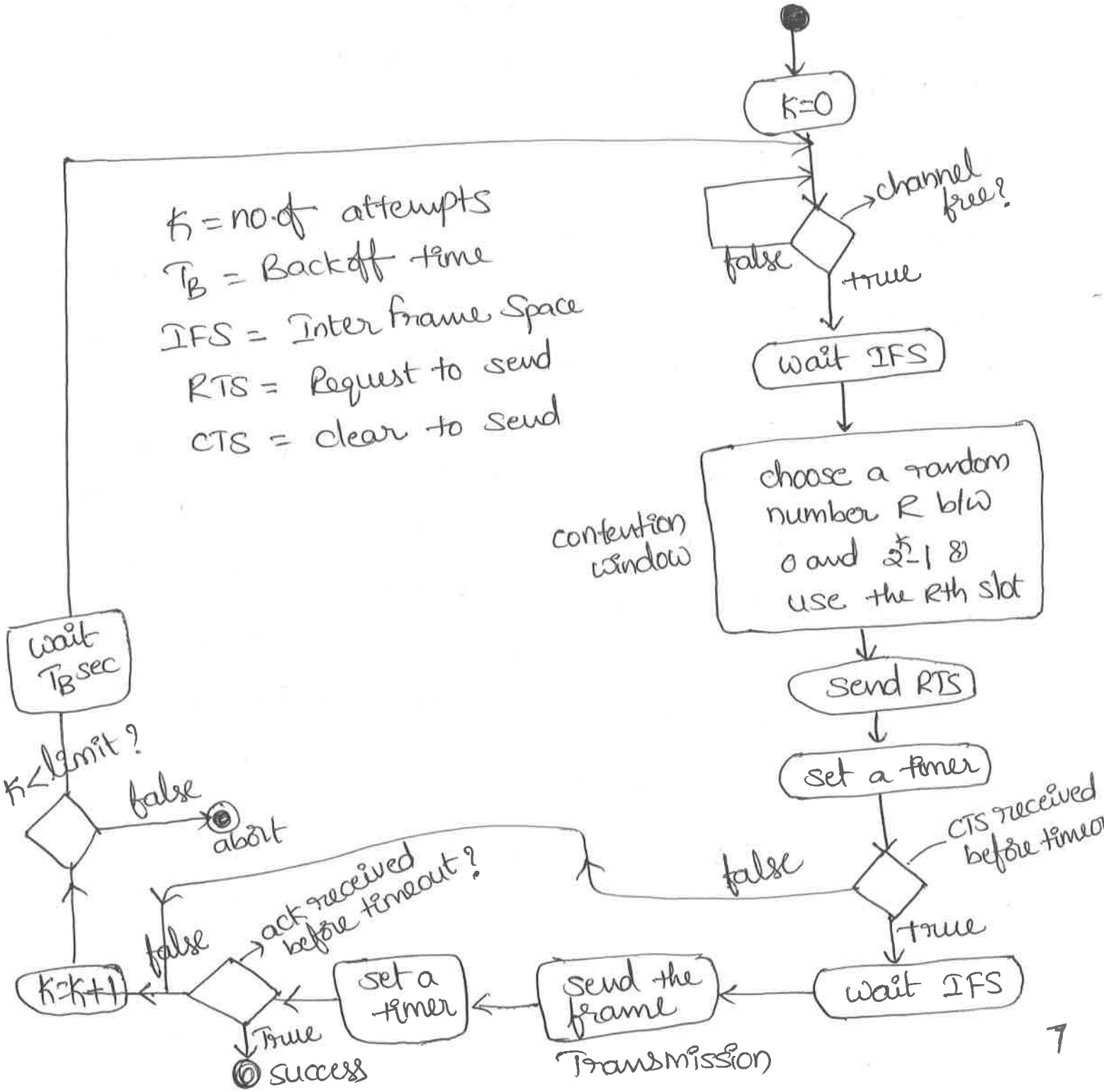
abnormal – there is a collision & the level of energy is twice the normal level.

A station that has a frame to send needs to monitor the energy level to determine if the channel is idle, busy or in collision state.

Throughput: The maximum throughput occurs at a different value of G and is based on the persistence method & the value of p in the p-persistent approach. For the 1-persistent method, the max throughput is around 50% when G=1. For the non persistent method, the max. throughput can go upto 90% when G is between 3 and 8 i.e G = 3 to 8.

CSMA/CA : CSMA/CA was invented for wireless networks. collisions are avoided through the use of CSMA/CA's three strategies.

1. The interframe space
2. The contention window
3. Acknowledgment



Inter Frame Space : When an idle channel is found, the station does not send immediately. It waits for a period of time called the IFS. Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting. After waiting an IFS time if the channel is still idle, the station can send, but it still needs to wait a time equal to the contention window.

Contention window : The contention window is an amount of time divided into slots. A station that is ready to send choose a random no. of slots as its wait time. The no. of slots in the window changes according to the binary exponential backoff strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time. The station needs to ~~send~~ sense the channel after each time slot. However, if the station finds the channel busy, it does not restart the process, it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.

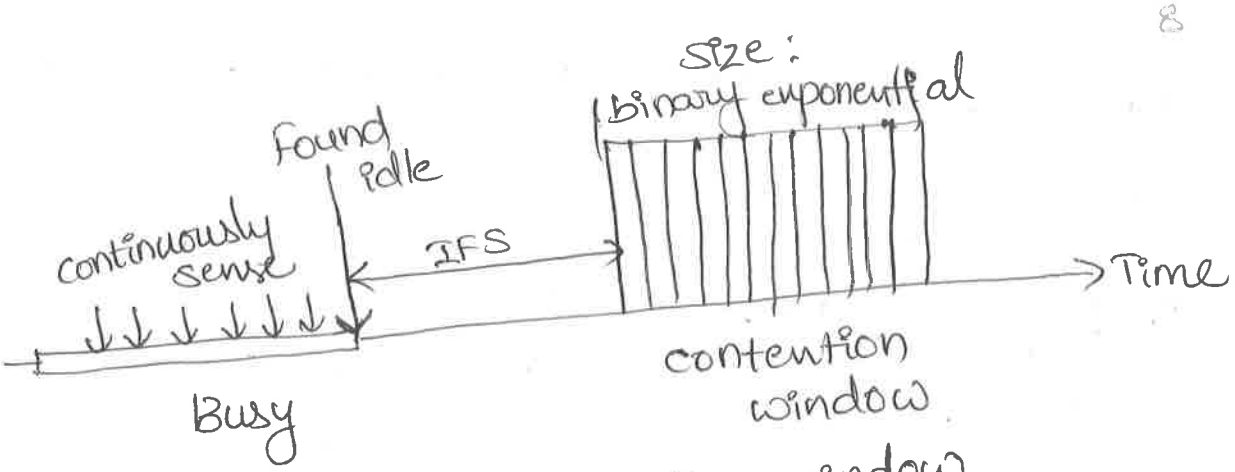
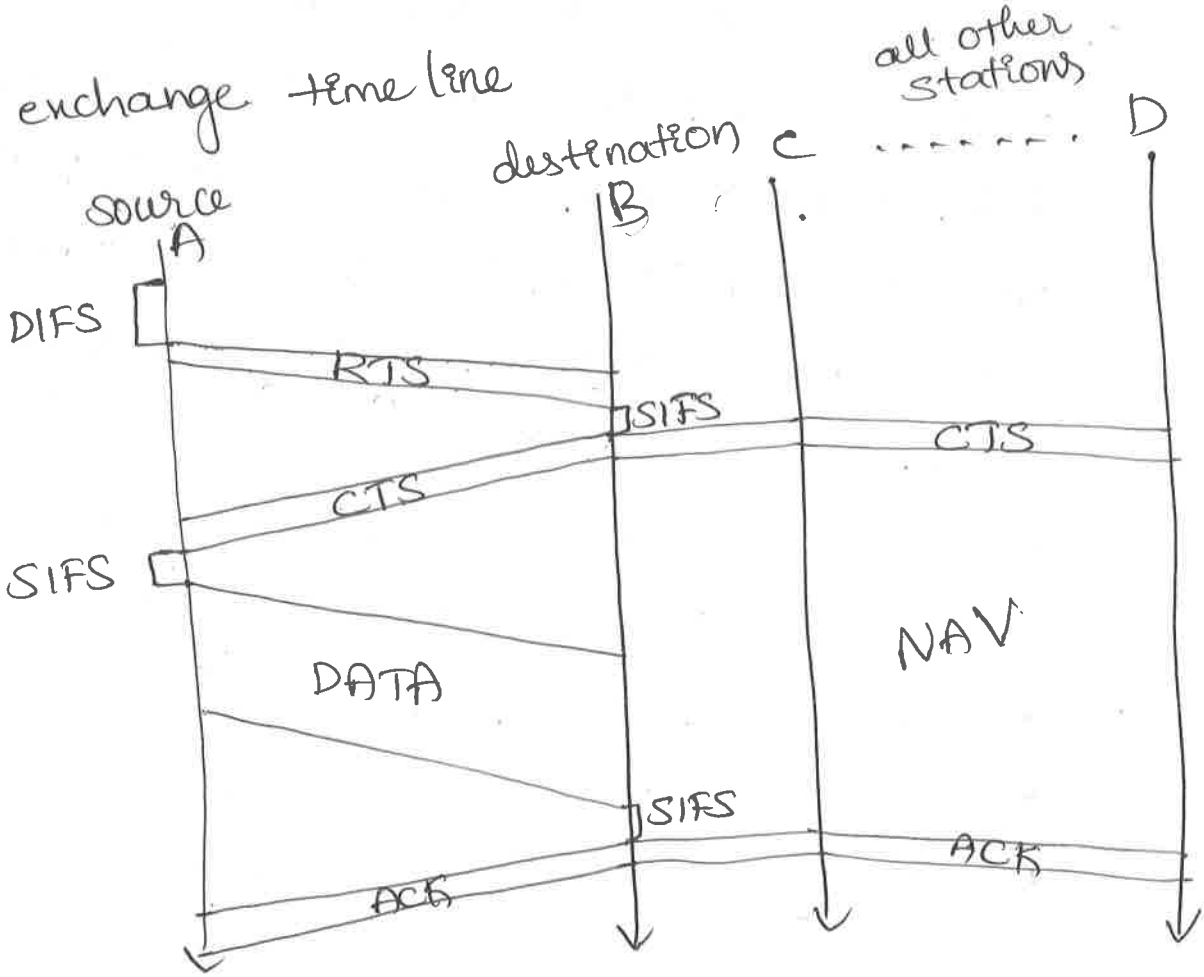


fig: contention window

Acknowledgement: With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The +ve acknowledgment and the time out timer can help guarantee that the receiver has received the frame.

Frame exchange time line



Above figure shows the exchange of data and control frames in time.

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
   a) the channel uses a persistence strategy with backoff until the channel is idle.
   b) After the station is found to be idle, the station waits for a period called the DCF IFS (DIFS); then the station sends a control frame called the request to send (RTS).
2. After receiving the RTS and waiting a period of time called the short IFS (SIFS), the destination station sends a control frame, called clear to send (CTS), to the source station. This control frame indicates that the destination is ready to receive data.
3. The source station sends data after waiting an amount of time equal to SIFS.
4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received.

Network Allocation Vector :

How collision avoidance accomplished ?

when a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness. Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

collision during handshaking

what happens if there is a collision during the time when RTS or CTS control frames are in transition, often called the handshaking period? Two or more stations may try to send RTS frames at the same time. These control frames may collide. However because there is no mechanism for collision detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver. The backoff strategy is employed, and the sender tries again.

Hidden station problem :

Figure shows that the RTS message from B reaches A, but not C. However, because both B and C are within the range of A, the CTS message from B to A reaches C. Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

Controlled access : In this, 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.

Reservation : In the reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.

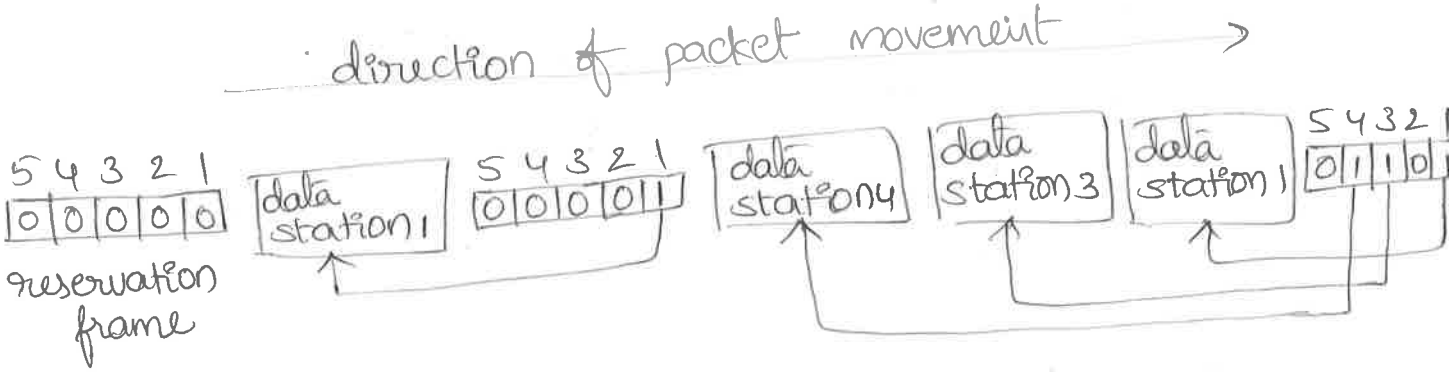


Figure shows a situation with five stations and five minislot reservation frame. In the first interval, only stations 1, 3 and 4 have made reservations. In the 2nd interval, only station 1 has made a reservation.

Polling : Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device. The primary device controls the link, the secondary devices follow its instructions. It is upto the primary device to determine which device is allowed to use the channel at a given time. This method uses poll and select functions to prevent collisions. The drawback is if the primary station fails, the system goes down.

Select : the select function is used whenever the primary device has something to send.

If the primary is neither sending nor receiving data, it knows the link is available. If it has something to send, the primary device sends it. The primary must alert the secondary to the upcoming transmission and wait for an acknowledgement of the secondary's ready status. Before sending data, the primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary.

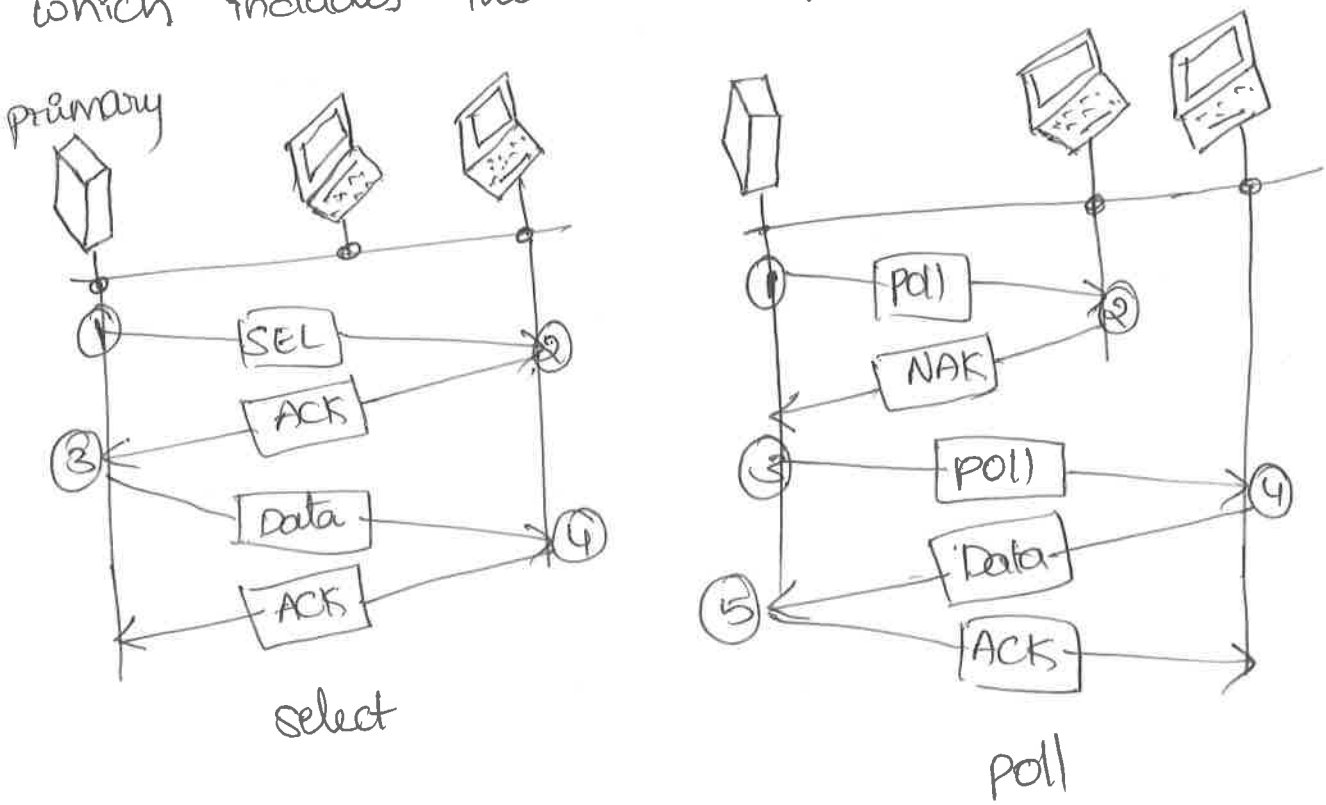


fig: select and poll functions

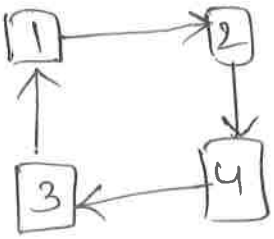
Poll: The poll function is used by the primary device to request transmissions from the secondary

device. when the primary is ready to receive data, it must ask each device in turn if it has anything to send. when the first secondary is approached, it responds either with a NAK frame if it has nothing to send or with data if it does. If the response is negative, then the primary polls the next secondary in the same manner until it finds one with data to send. when the response is positive, the primary reads the frame and returns an ack, verifying its receipt.

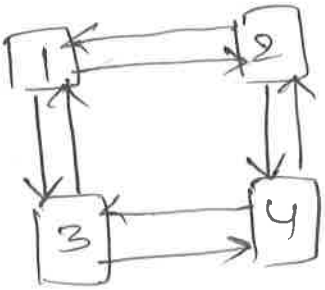
Token Passing: In the token passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a predecessor and a successor. the predecessor is the station which is logically before the station in the ring, the successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now

In this method, a special packet called a token circulates through the ring. the possession of the token gives the station the right to access the channel and send its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. Token management is needed for this access method. The token must be monitored to ensure it has not been lost or destroyed.

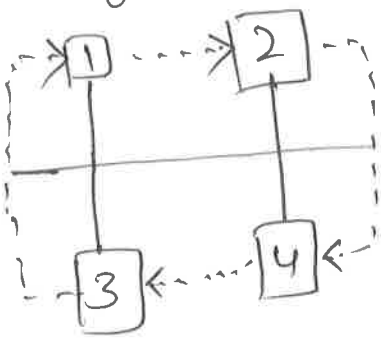
Logical Ring: In a token passing network, stations do not have to be physically connected in a ring, the ring can be a logical one.



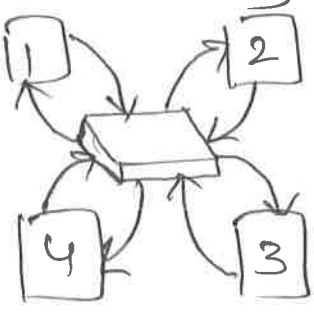
physical ring



Dual ring



bus ring or token bus



Star ring

In the physical ring topology, when a station sends the token to its successor, the token cannot be seen by other stations. This means that the token does not have to have the address of the next successor. problem with this is that if one of the links fails, the whole system fails.

The dual ring topology uses a second ring which operates in the reverse direction compared with the main ring. If one of the links in the main ring fails, the system automatically combines the two rings to form a temporary ring. After the failed link is restored, the auxiliary ring becomes idle again. For this topology to work, each station needs to have two transmitter ports and two receiver ports. The high speed token ring networks called FDDI, CDDI (Fiber distributed data copper Interface) use this topology.

In the bus ring topology, the stations are connected to a single cable called a bus. They however, make a logical ring, because each station knows ~~when a station has finished~~ the address of its successor (and also predecessor) when a station has finished sending its data, it releases the token and inserts the address of its successor in the token. The token bus LAN, standardized by IEEE, uses this topology.

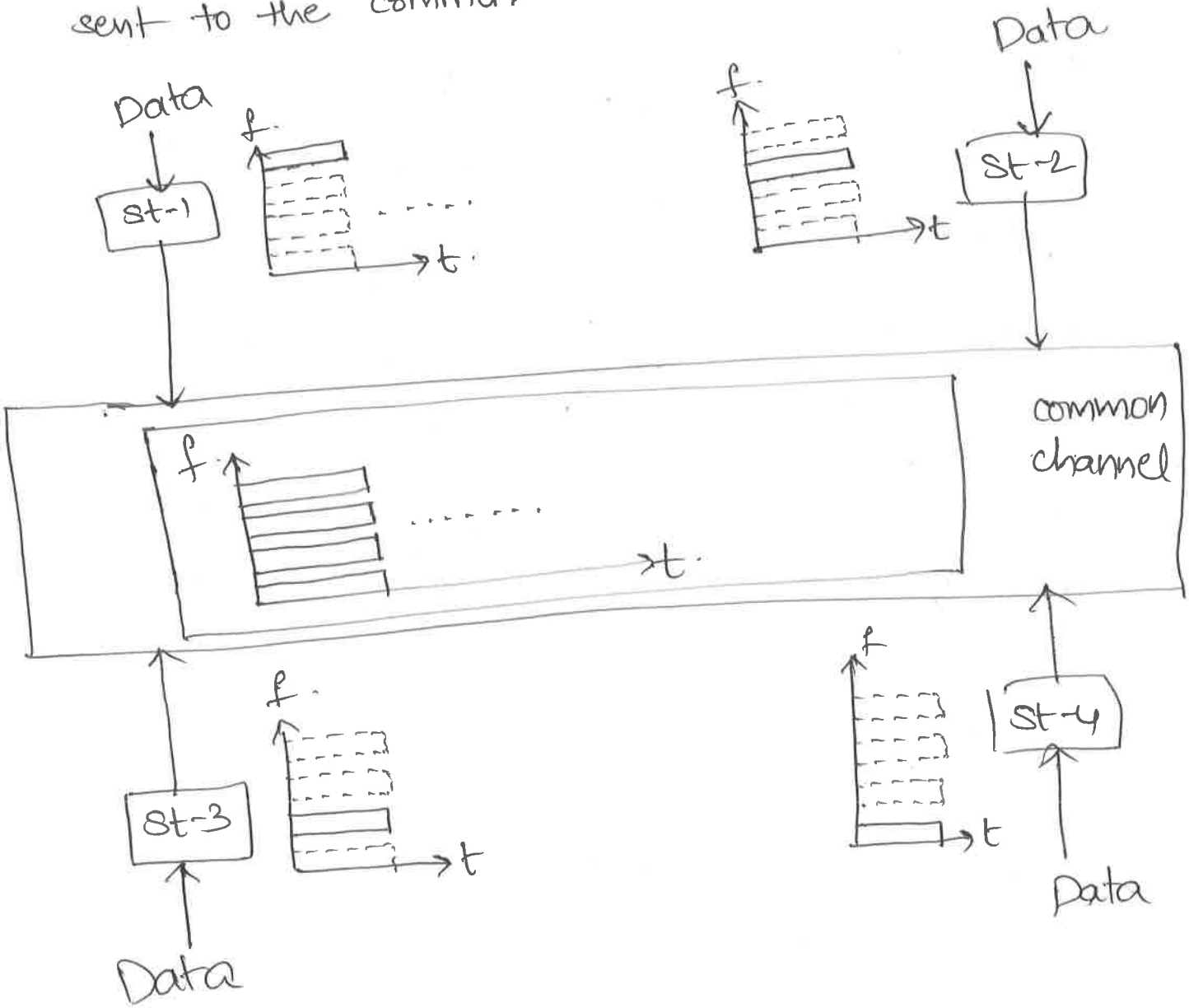
In a star ring topology, there is a hub, that acts as the connector. The wiring inside the hub makes the ring, the stations are connected to this ring through the two wire connections. This topology less prone to failure, bcz if a link goes down, it will be bypassed by the hub and the rest of the stations can operate. Also adding & removing stations from the ring is easier. This topology is used in the token ring LAN designed by IBM.

Channelization: It is a multiple access method in which the available bandwidth of a link is shared in time, freq & code among different stations.

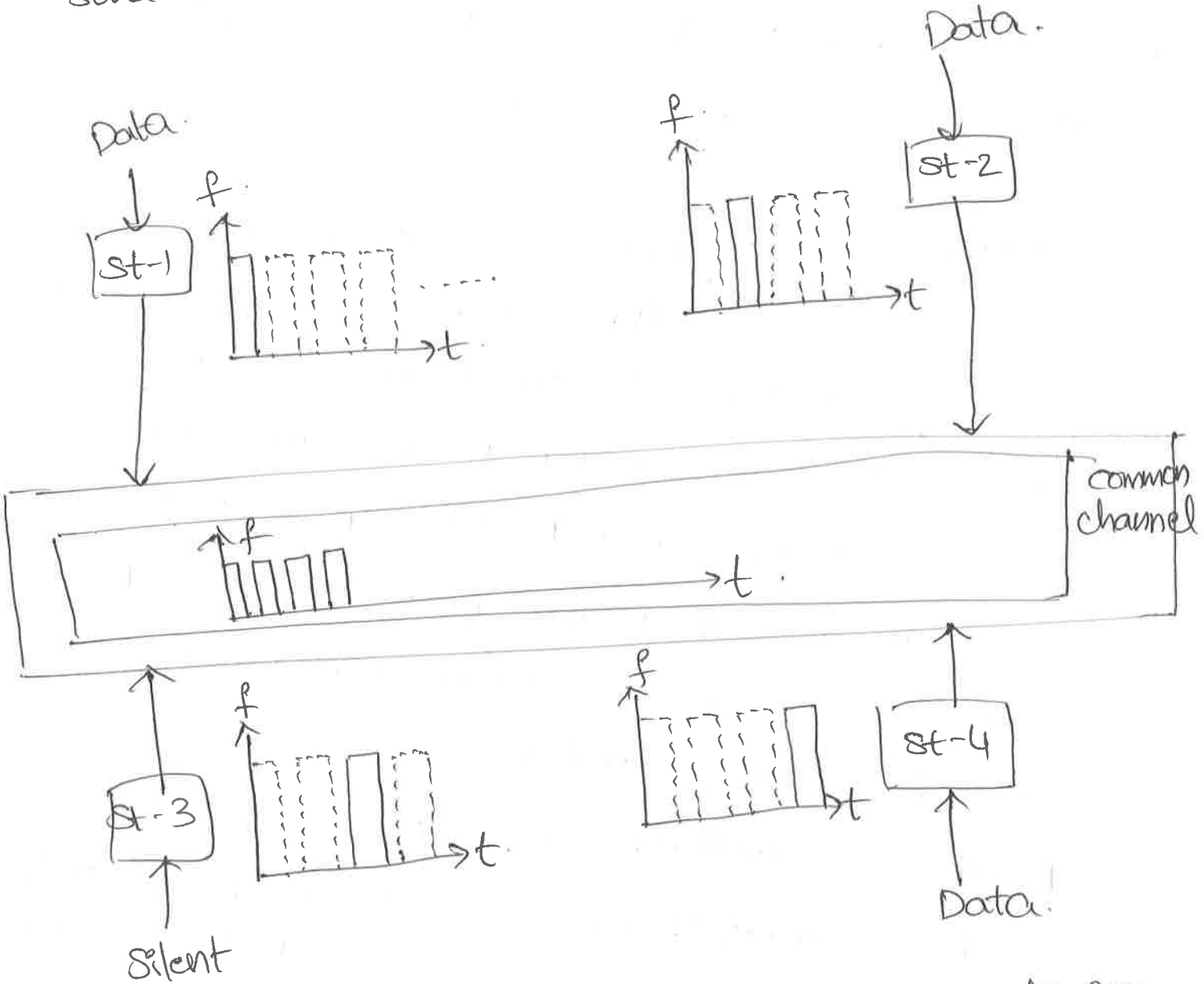
FDMA: In FDMA, the available bandwidth is divided into frequency bands. Each band is reserved for a specific station, and it belongs to the station all the time. Each station also uses a bandpass filter to confine the transmitter frequencies, to prevent station interferences, the allocated bands are separated from one another by small guard bands.

FDMA specifies a predetermined frequency band for the entire period of communication. FDM is a physical layer technique that combines the loads from low bandwidth channels and transmits them by using a high bandwidth channel. The channels that are combined are low pass. The multiplexer modulates the signals, combines them, and creates a bandpass signal. The bandwidth of each channel is shifted by the multiplexer.

FDMA, is an access method in the data link layer. The data link layer in each station tells its physical layer to make a bandpass signal from the data passed to it. The signal must be created in the allocated band. There is no physical multiplexer at the physical layer. The signals created at each station are automatically band pass filtered. They are mixed when they are sent to the common channel.



TDMA : In TDMA, the stations share the bandwidth of the channel in time. Each station is allocated a time slot during which it can send data.



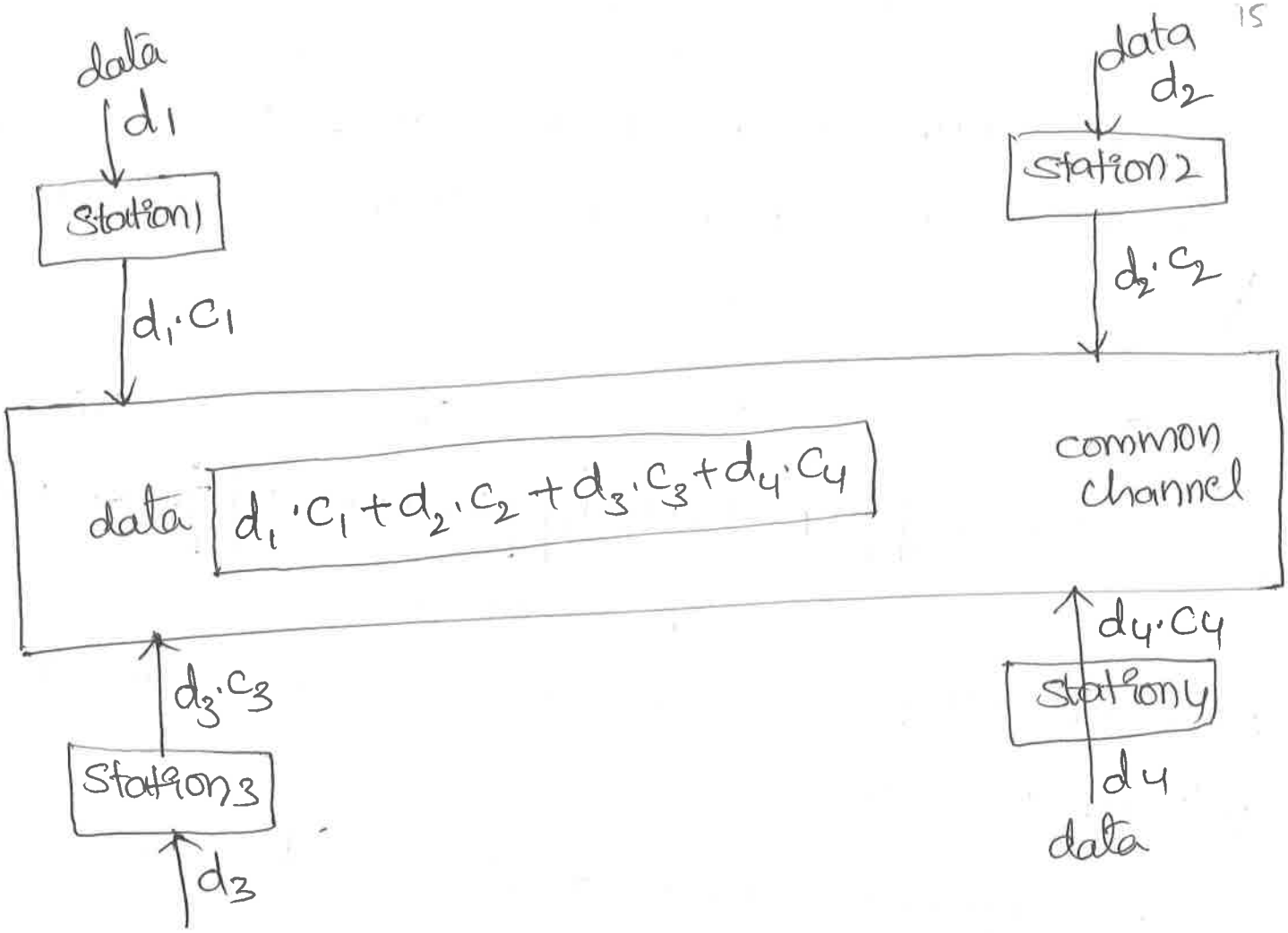
The main problem with TDMA lies in achieving synchronization between the different stations. Each station needs to know the beginning of its slot and the location of its slot. This may be difficult

because of propagation delays introduced in the system if the stations are spread over a large area. To compensate for the delays, we can insert guard times. Synchronization is accomplished by having preamble bits at the beginning of each slot.

CDMA : In CDMA, one channel carries all transmissions simultaneously. CDMA means communication with different codes. Let us assume we have four stations 1, 2, 3, 4 connected to the same channel. The data from station 1 are d_1, 2 are d_2 ..... The codes assigned to the first station is c_1, second is c_2 ..... we assume that the assigned codes have two properties.

1. If we multiply each code by another, we get 0
2. If we multiply each code by itself, we get 4. (no. of stations)

Let us see how the above four stations can send data using the same common channel.



station 1 multiplies its data by its code to get $d_1 \cdot c_1$. station 2 multiplies its data by its code to get $d_2 \cdot c_2$ ..... Any station that wants to receive data from one of the other three multiplies the data on the channel by the code of the sender

ex: suppose stations 1 and 2 are talking to each other. station 2 wants to hear what station 1 is saying. It multiplies the data on the channel by c_1, the code of station 1

$(\because c_2 \cdot c_1 = c_3 \cdot c_1 = c_4 \cdot c_1 = 0)$

$$\text{data} = (d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4)\, c_1$$

$$= d_1 c_1 \cdot c_1 + \underbrace{d_2 c_2 \cdot c_1}_{=0} + \underbrace{d_3 \cdot c_3 \cdot c_1}_{=0} + \underbrace{d_4 \cdot c_4 \cdot c_1}_{=0}$$

$$= 4 d_1 + 0$$

chips: CDMA is based on coding theory. Each station is assigned a code, which is a sequence of numbers called chips.

c_1	c_2	c_3	c_4
[+1 +1 +1 +1]	[+1 -1 +1 -1]	[+1 +1 -1 -1]	[+1 -1 -1 +1]

chip sequences

They are called orthogonal sequences and have the following properties.

1. Each sequence is made of N elements, where N is the no. of stations.
2. multiplication of a sequence by a scalar

$$2 \cdot [+1 \ +1 \ -1 \ -1] = [+2 \ +2 \ -2 \ -2]$$

3. If we multiply two equal sequences, element by element and add the results, we get N. This is called the inner product of two equal sequences.

$$[+1 \ +1 \ -1 \ -1] \cdot [+1 \ +1 \ -1 \ -1] = 1+1+1+1 = 4.$$

4. If we multiply two different sequences, element by element, and add the results, we get 0. This is called the inner product of two different sequences.

$[+1\ +1\ -1\ -1] \cdot [+1\ +1\ +1\ +1] = 1+1-1-1 = 0$

5. Adding two sequences means adding the corresponding elements. The result is another sequence.

$[+1\ +1\ -1\ -1] + [+1\ +1\ +1\ +1] = [+2\ +2\ 0\ 0]$

Data representation: We follow these rules for encoding. If a station needs to send a

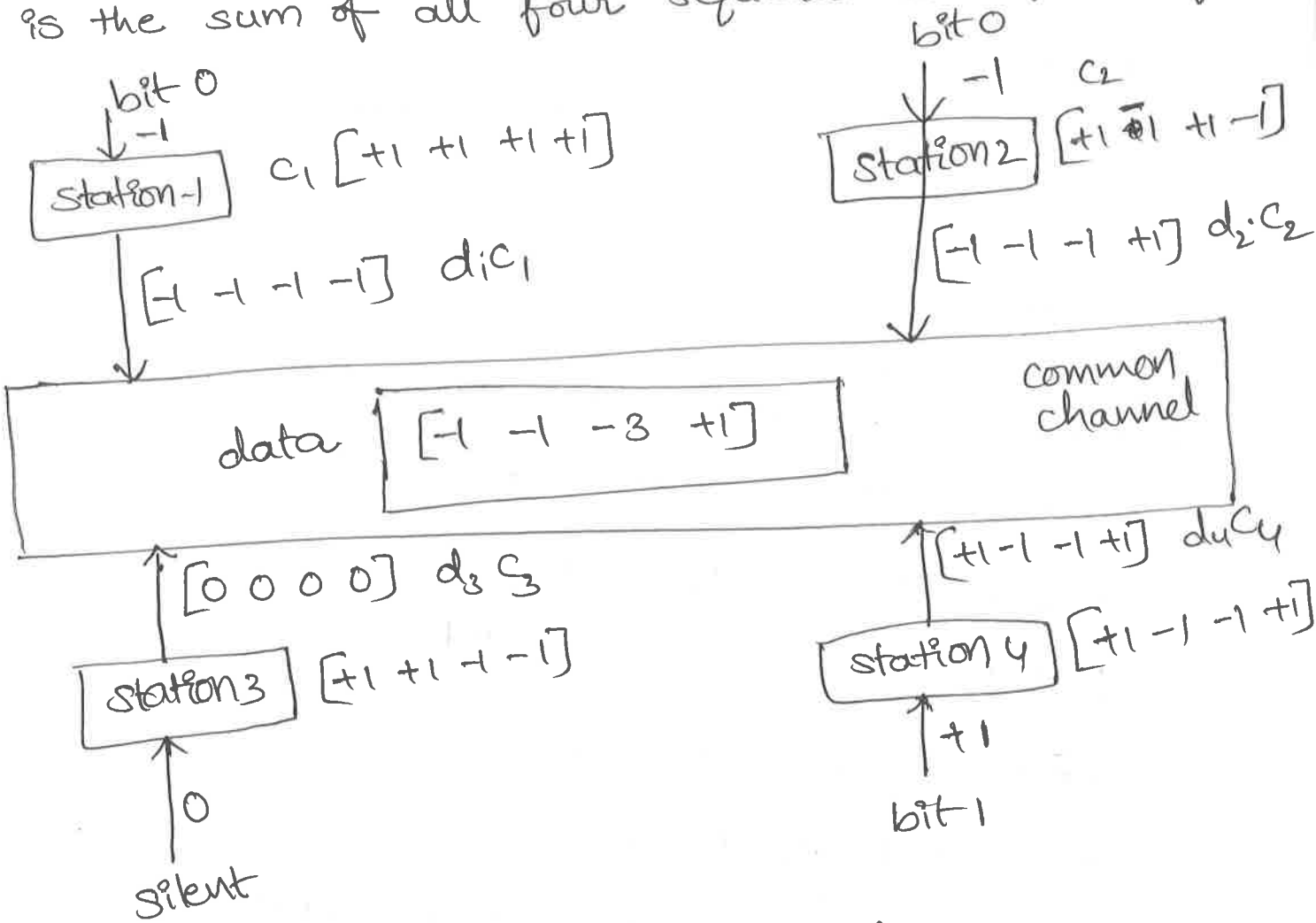
0 bit, it encodes it as −1.

1 bit, " " +1

station is idle, it sends no signal, which interpreted as a 0.

encoding and decoding: As a simple example, we show how four stations share the link during a 1-bit interval. We assume that stations 1 and 2 are sending a 0 bit and channel 4 is sending a 1 bit. Station 3 is silent. the data at the sender site are translated to −1 −1 0 and +1. Each station multiplies the corresponding number by its chip. The result is a new sequence which is sent to the channel. For simplicity, we assume that all stations send the resulting sequences

at the same time. The sequence on the channel is the sum of all four sequences as defined before.



sharing channel in CDMA

Now imagine that station 3, which we said is silent, is listening to station 2. Station 3 multiplies the total data on the channel by the code for station 2, which is [+1 -1 +1 -1], to get

$$[-1 \ -1 \ -3 \ +1] \cdot [+1 \ -1 \ +1 \ -1] = \frac{-4}{4} = -1 \rightarrow \text{bit 1}$$

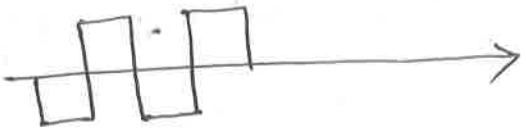
Signal level : The figure shows the corresponding signals for each station (using NRZ-L) and the signal that is on the common channel.

bit 0

station-1 [-1 -1 -1 -1]

bit 0

station-2 [-1 +1 -1 +1]

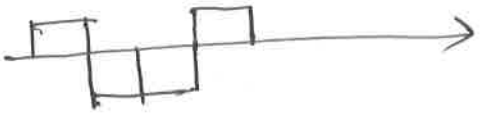


Silent

station-3 [0 0 0 0]

bit -1

station -4 [+1 -1 -1 +1]



Data on the channel

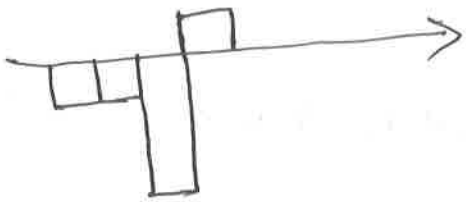


Fig shows how station 3 can detect the data sent by station 2 by using the code for station 2. The total data on the channel are multiplied by the signal representing station 2 chip code to get a new signal. The station then integrates & adds the area under the signal, to get the value -4, which is divided by 4 and interpreted as bit 0.

Sequence generation: To generate chip sequences, we use a walsh table with an equal no. of rows and columns as shown below.

$$W_1 = [+1] \Rightarrow W_{2N} = \begin{bmatrix} W_N & W_N \\ W_N & \overline{W}_N \end{bmatrix}$$

$$W_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix} \Rightarrow$$

$$W_4 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$$

In the walsh table, each row is a sequence of chips. W_1 for a one chip sequence has one row and one column. We can choose -1 or +1 for the chip for this trivial table. (choose +1)

According to walsh, if we know the table for N sequences W_N, we can create the table for 2N sequences W_{2N} as shown in above fig.

Wired LANs : Ethernet

Ethernet Protocol:

TCP/IP accepts any protocol at these two layers (physical, datalink) that can provide services to the network layer. In 1980's & 1990's several different types of LAN's were used. All of these LANS used a media access method to solve the problem of sharing the media. The ethernet used the CSMA/CD approach. The token ring, token bus & FDDI (Fiber distribution data interface) used the token passing approach.

Almost every LAN except Ethernet has disappeared from the marketplace because Ethernet was able to update itself to meet the needs of the time. The ethernet protocol was designed so that it could evolve with the demand for higher transmission rates.

IEEE project 802 : In 1985, the computer society of IEEE started a project, called project 802 to set standards to enable intercommunication among equipment from a variety of manufacturers. It does not seek to replace OSI or TCP/IP, instead, it is a way of specifying functions of

the physical layer and the data link layer of major CAN protocols.

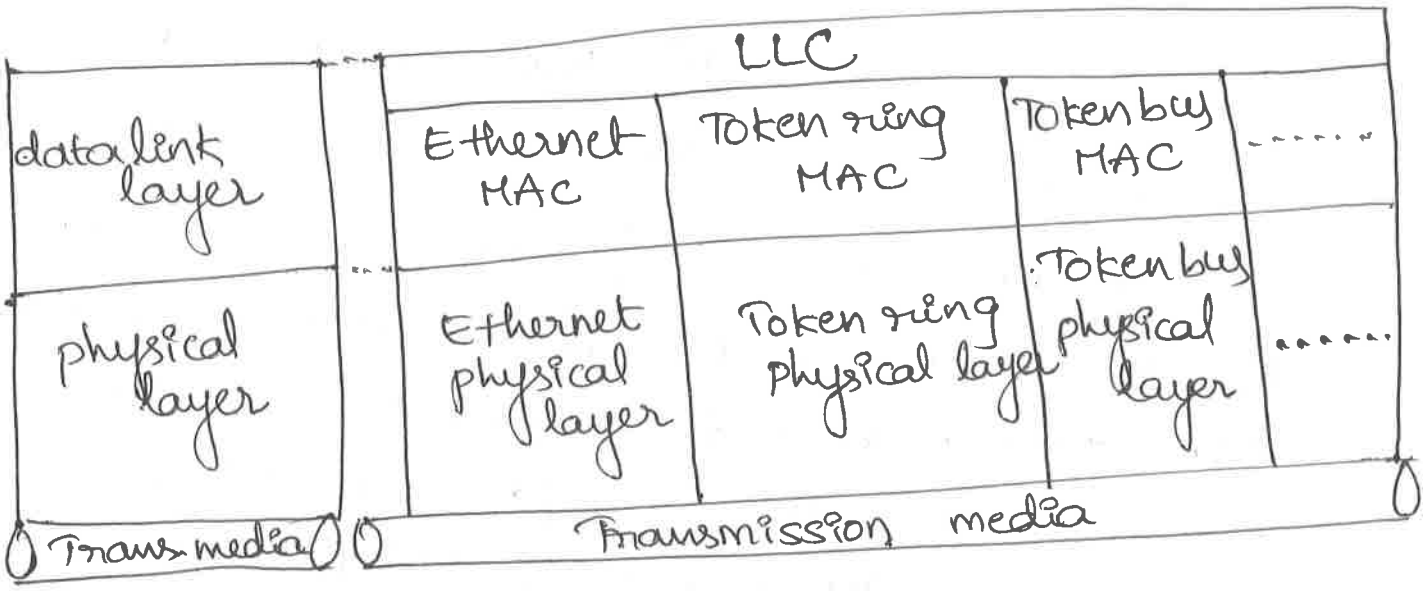


fig: IEEE standard for LANs.

The IEEE has subdivided the data link layer into two sublayers: logical link control (LLC) and media access control (MAC)

LLC: data link control handles framing, flow control and error control. In IEEE project 802, flow control, error control & part of framing duties are collected into one sublayer called the logical link control. Framing is handled in both LLC & MAC sub layer.

MAC : IEEE project 802 has created a sublayer called media access control that defines the specific access method for each LAN. It defines CSMA/CD as the media access method for Ethernet LANs.

Ethernet evolution : Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs. Four generations.

1. Standard ethernet (10Mbps)
2. Fast ethernet (100Mbps)
3. Gigabit ethernet (1Gbps)
4. 10 Gigabit ethernet (10Gbps)

Standard ethernet :

characteristics :

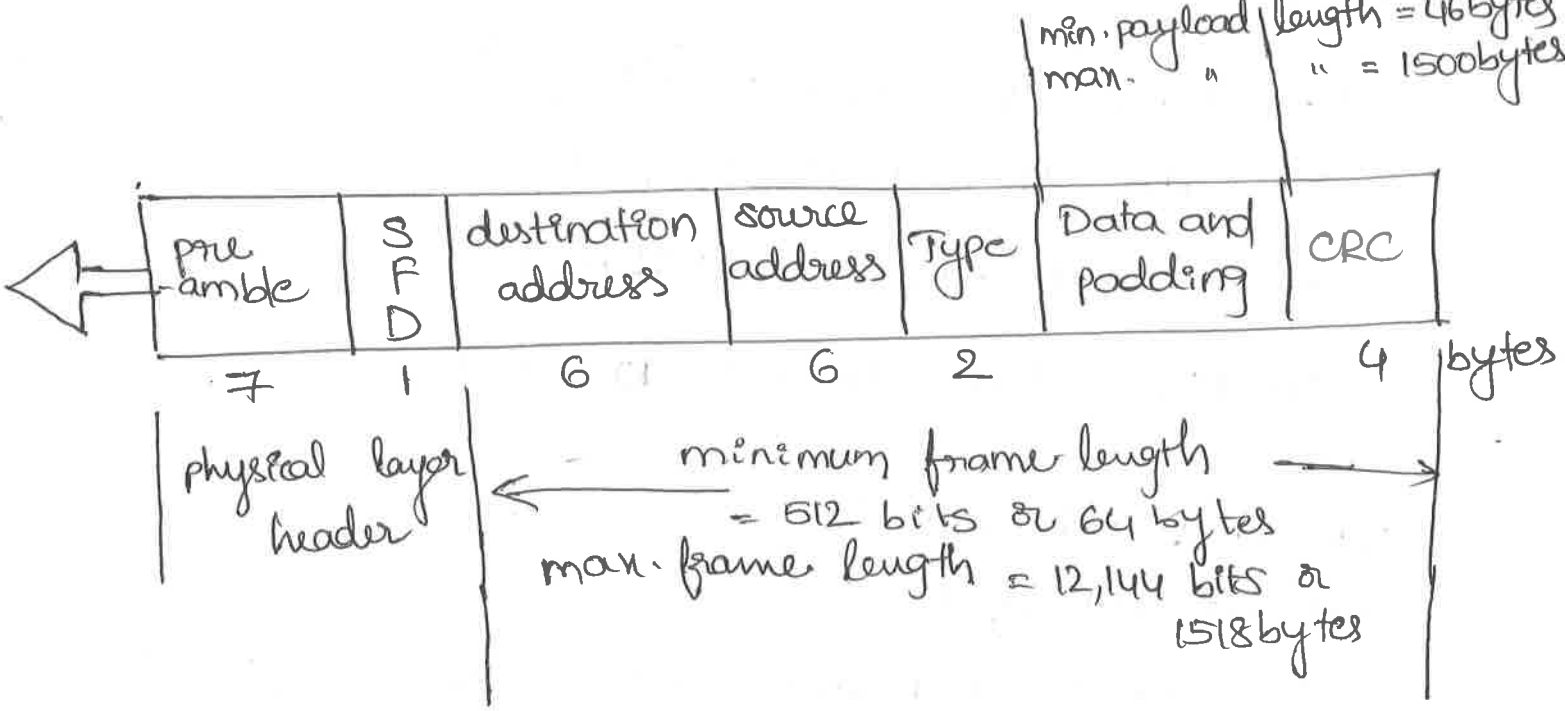
connectionless and unreliable service : Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next frame. Ethernet has no connection establishment & connection termination phases. The sender sends a frame whenever it has it. The receiver may or may not be ready for it.

Ethernet is also unreliable like IP and UDP. If a frame is corrupted during transmission and the receiver finds out about the corruption, which has a high level of probability of happening because of the CRC-32, the receiver drops the frame silently.

Frame format.

preamble : 56 bits of alternating 1's and 0's

SFD : start frame delimiter, (10101011), flag.



preamble : It alert the receiving system to the coming frame and enable it to synchronize its clock if its out of synchronization.

SFD : It signals the beginning of the frame. SFD warns the stations that this is the last chance for synchronization.

The last 2 bits are $(11)_2$ and alert the receiver that the next field is the destination address. An ethernet frame is a variable length frame. It needs a flag to define the beginning of the frame. The SFD field is also added at the physical layer.

Destination address : contains the link layer address of the destination station or stations to receive the packet.

Source address : contains the link layer address of the sender of the packet.

Type : This field defines the upper layer protocol whose packet is encapsulated in the frame. This protocol can be IP, ARP, OSPF....

Data : This field carries data encapsulated from the upper layer protocols. If the data is more than 1500 bytes, it should be fragmented and encapsulated in more than one frame. If it is less than 46 bytes, it needs to be padded with extra 0's.

CRC : The last field contains error detection information, in this case a CRC-32. The CRC is calculated over the addresses, types and data field.

Frame length : Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame. The minimum length restriction is required for the correct operation of CSMA/CD. The maximum length restriction has two historical reasons. First, memory was very expensive when ethernet was designed, a maximum length restriction helped to reduce the size of the buffer. Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

Addressing : Each station on an ethernet network has its own network interface card (NIC). The NIC fits inside the station and provides the station with a link layer address. The Ethernet address is 6 bytes, written in hexadecimal notation, with a colon between the bytes : Ex : 4A:30:10:21:10:1A

Transmission of address bits : The transmission is left to right byte by byte, however, the LSB bit is sent first and MSB bit is sent last This bit means that the bit that defines an address as unicast or multicast arrives first at the receiver. This helps the receiver to immediately know if the packet is unicast & multicast.

Unicast, multicast & broadcast addresses : If the LSB bit of the first byte in a destination address is 0, the address is unicast, otherwise multicast. The broadcast address is a special case of the multicast address, the recipients are all the stations on the LAN. A broadcast destination address is 48 is.

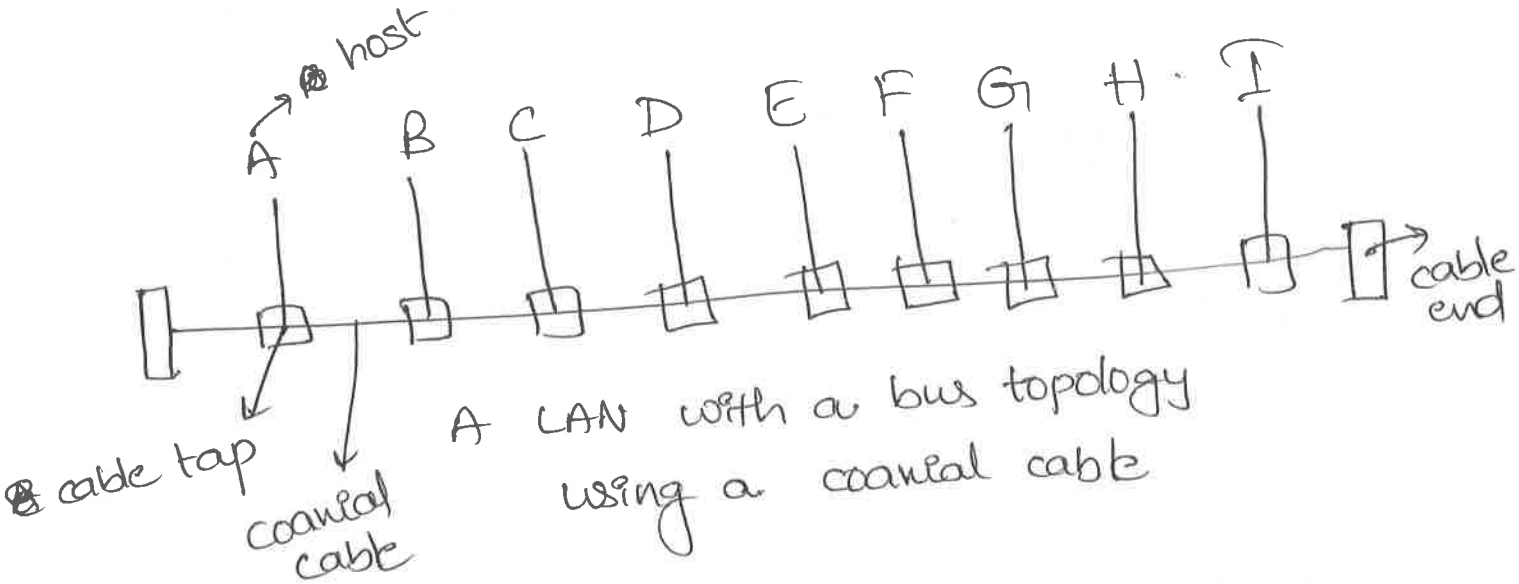
Distinguish between Unicast, multicast & broadcast transmission : Standard Ethernet uses a coaxial cable or a set of twisted pair cables with a hub. How the actual unicast, multicast, and broadcast transmissions are distinguished from each other.

* In a unicast transmission, all stations will receive the frame, the intended recipient keeps and handles the frame, the rest discard it.

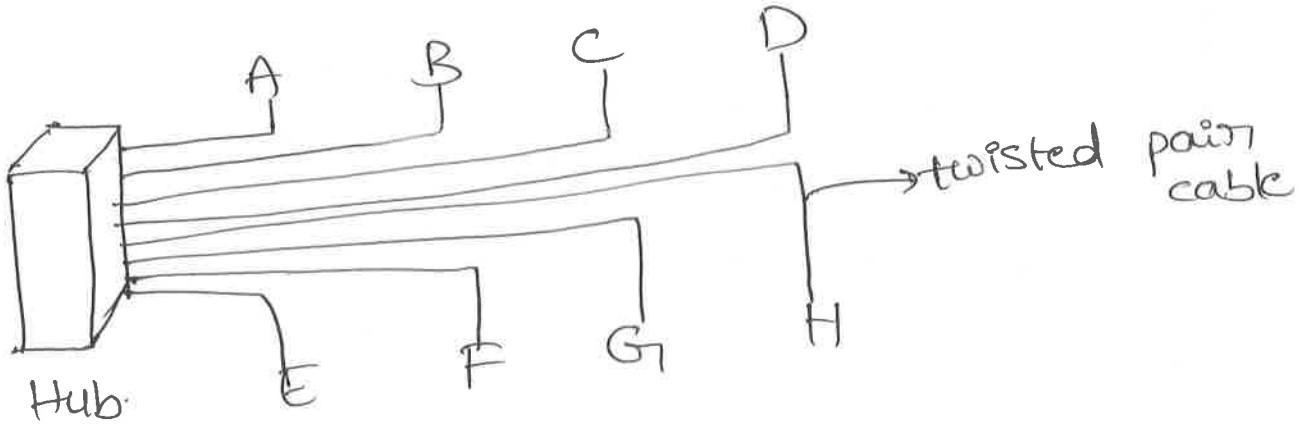
* In a multicast transmission, all stations will receive the frame, the stations that are members of the group keep and handle it, the rest discard it.

* In a broadcast transmission, all stations will receive the frame and all stations keep and handle it.

Access method: the standard ethernet choose CSMA/CD with 1-persistent method.



A LAN with a bus topology using a coaxial cable



A LAN with a star topology using a hub

Efficiency of a standard Ethernet: It is defined as the ratio of the time used by a station to send data to the time the medium is occupied by this station.

$$\text{Efficiency} = \frac{1}{1+(6.4)a}$$

a = no. of frames that can fit on the medium.

$$a = \frac{\text{Propagation delay}}{\text{transmission delay}}$$

If a↓ efficiency↑ ⇒ for a=0 efficiency = 100%

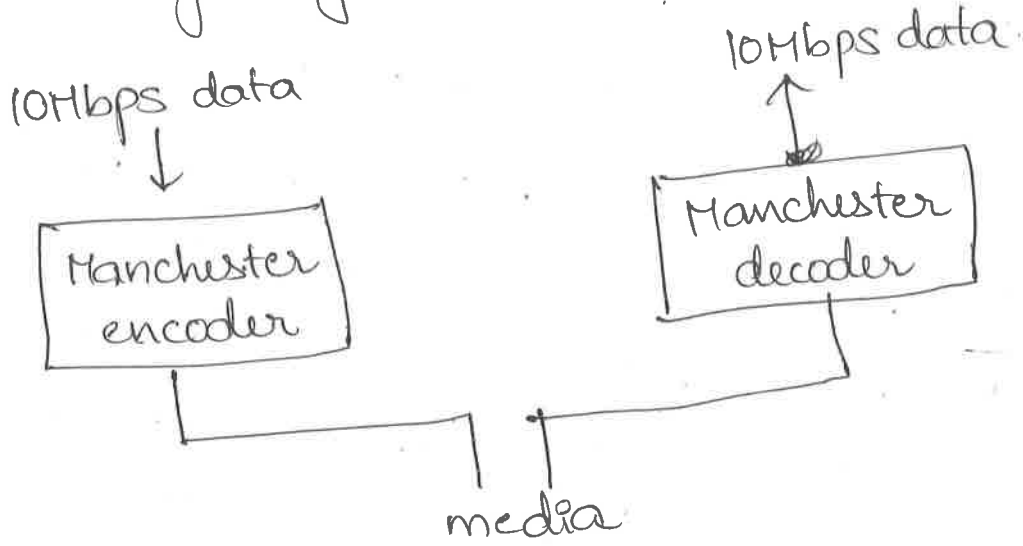
Implementation:

Implementation	medium	medium length	encoding
10 base 5	thick coax	500m	Manchester
10 base 2	Thin coax	185m	"
10 base-T	2 UTP	100m	"
10 base-F	2 Fiber	2000m	"

In the nomenclature 10 baseX, the number defines the data rate (10Mbps), the term base means baseband signal, and X approximately defines either the maximum size of the cable in 100 meters or the type of cable.

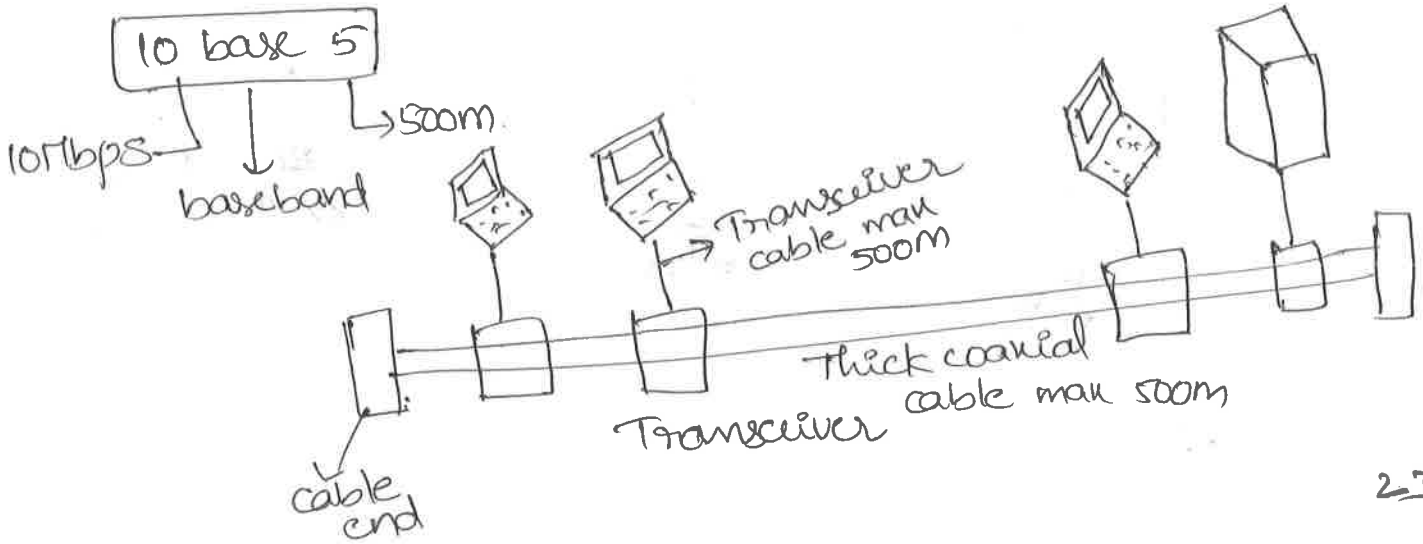
T for unshielded twisted pair cable (UTP) &
F for fiber optic.

Encoding & decoding : All standard implementations use digital signaling at 10Mbps.



10 base 5 : Thick ethernet

The first implementation is called 10 base 5, thick ethernet or thicknet. 10 base 5 was the 1st ethernet specification to use a bus topology with an external transceiver connected via a tap to a thick coaxial cable.

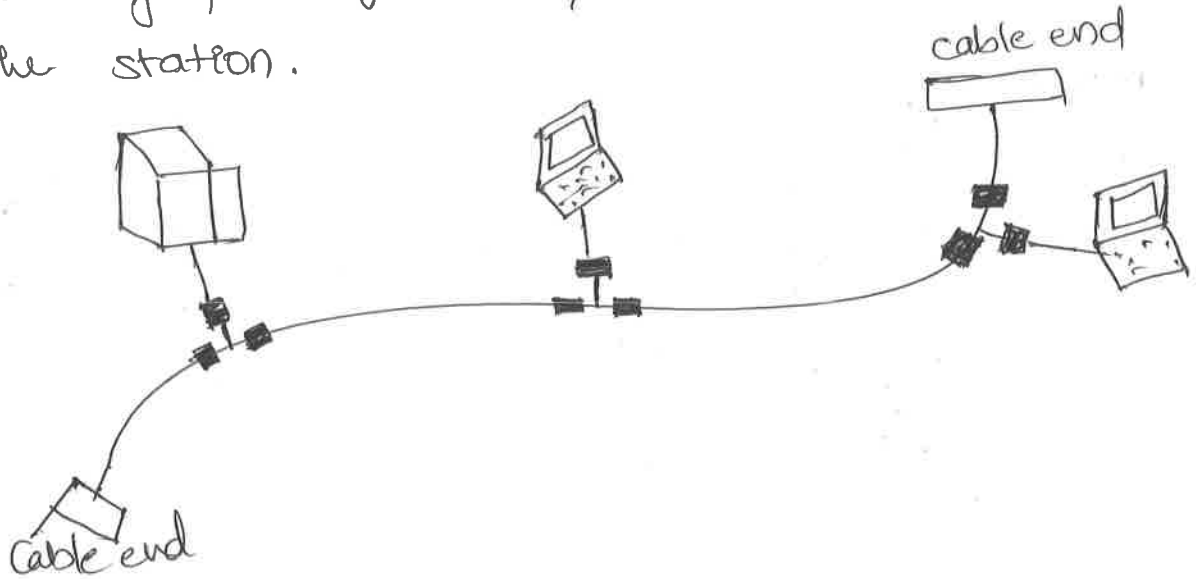


The transceiver is responsible for transmitting, receiving and detecting collisions. The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable.

The max. length is only 500m, otherwise there is excessive degradation of the signal. If a length of more than 500m is needed, upto 5 segments, each a maximum of 500m, can be connected using repeaters.

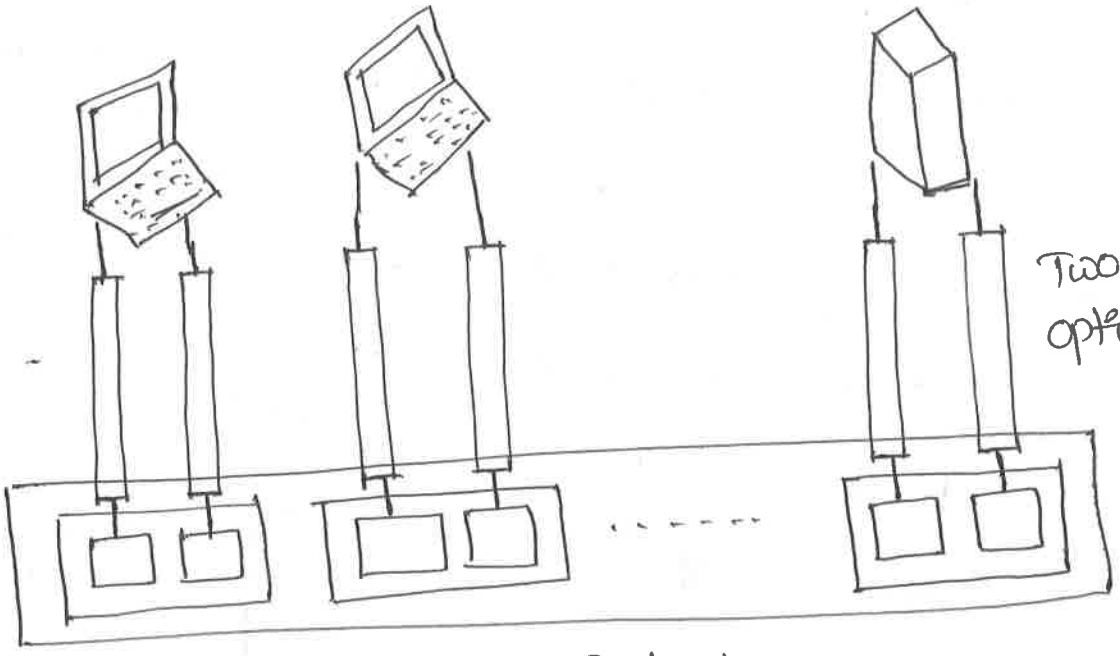
10 base 2 : Thin ethernet

The 2nd implementation is called 10 base 2, thin ethernet & cheapernet. 10 base 2 also uses a bus topology, but the cable is much thinner and more flexible. In this case, the transceiver is normally part of NIC, which is installed inside the station.



10 base F : Fiber ethernet

10 base F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber optic cables.



10 base-F hub

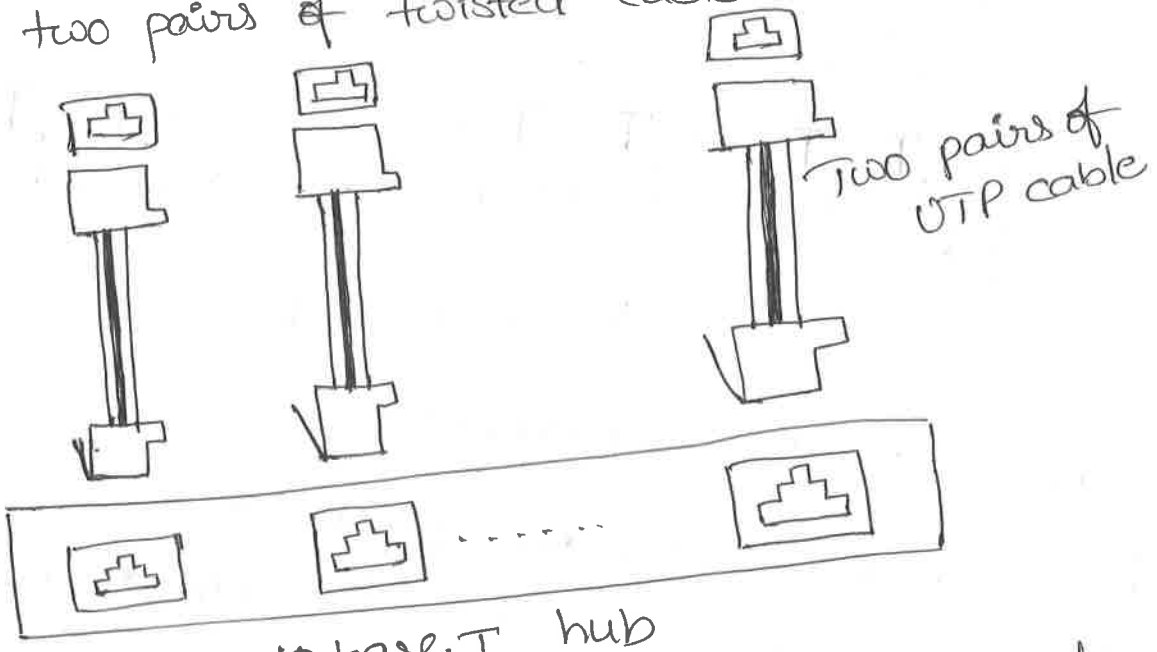
Changes in the standard:

bridged ethernet: The first step in the Ethernet evolution was the division of a LAN by bridges. Bridges have two effects on an ethernet LAN: They raise the B.W & they separate collision domains.

collision here occurs in the thin coaxial cable This implementation is more cost effective than 10base5 because of less expensive & the tee connections are much cheaper than taps. Installation is simpler bcz very flexible.

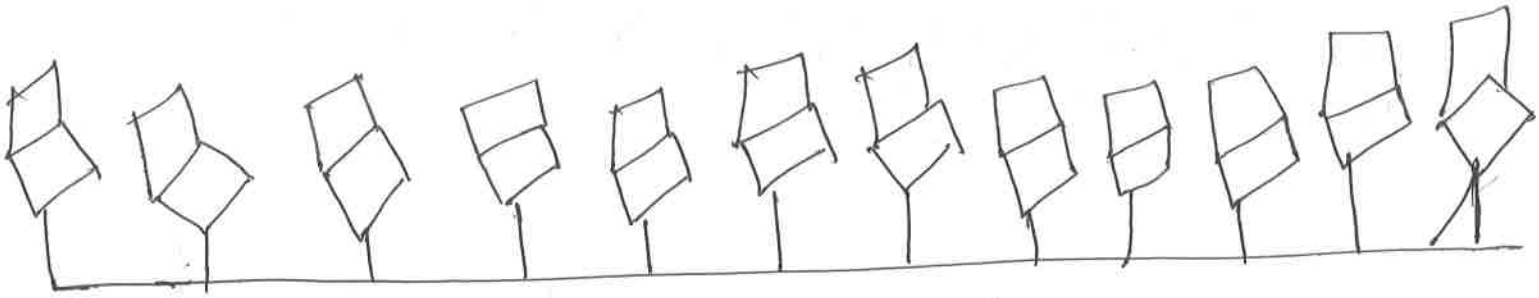
10 base T : Twisted pair ethernet

The 3rd implementation is called 10 base T or twisted pair ethernet. 10 base T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable as shown below.

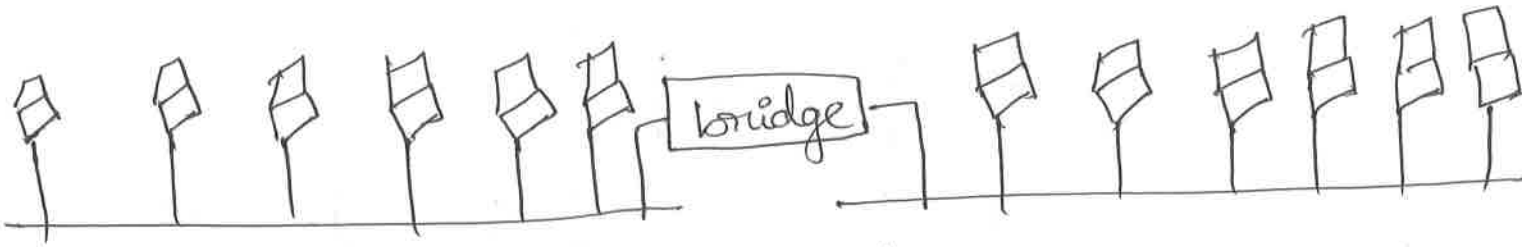


Two pairs of twisted cable create two paths between the station and the hub. Any collision here happens in the hub. The max. length of the twisted pair cable is 100m, to minimize the effect of attenuation in the twisted cable.

Raising the bandwidth: In an unbridged Ethernet network, the total capacity is shared among all stations with a frame to send. A bridge divides the network into two or more networks. Bandwidth wise each network is independent.



without bridging

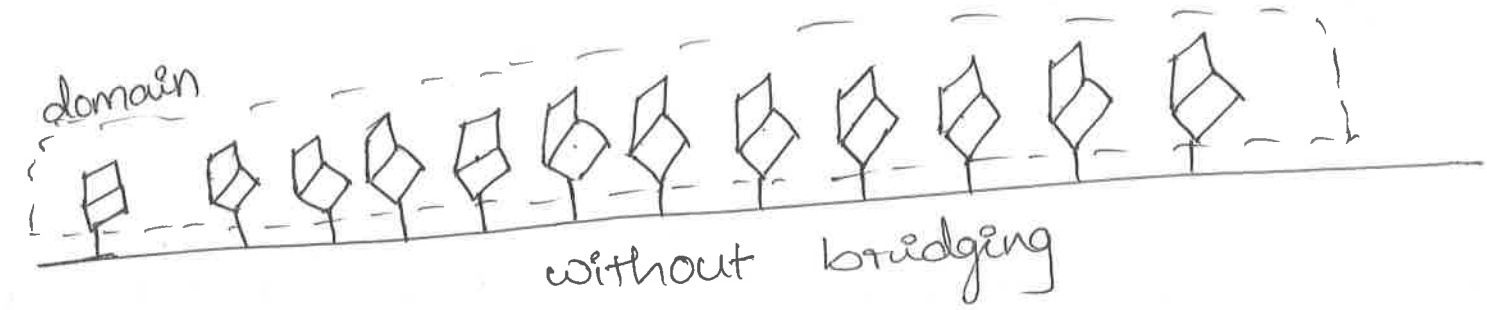


with bridging

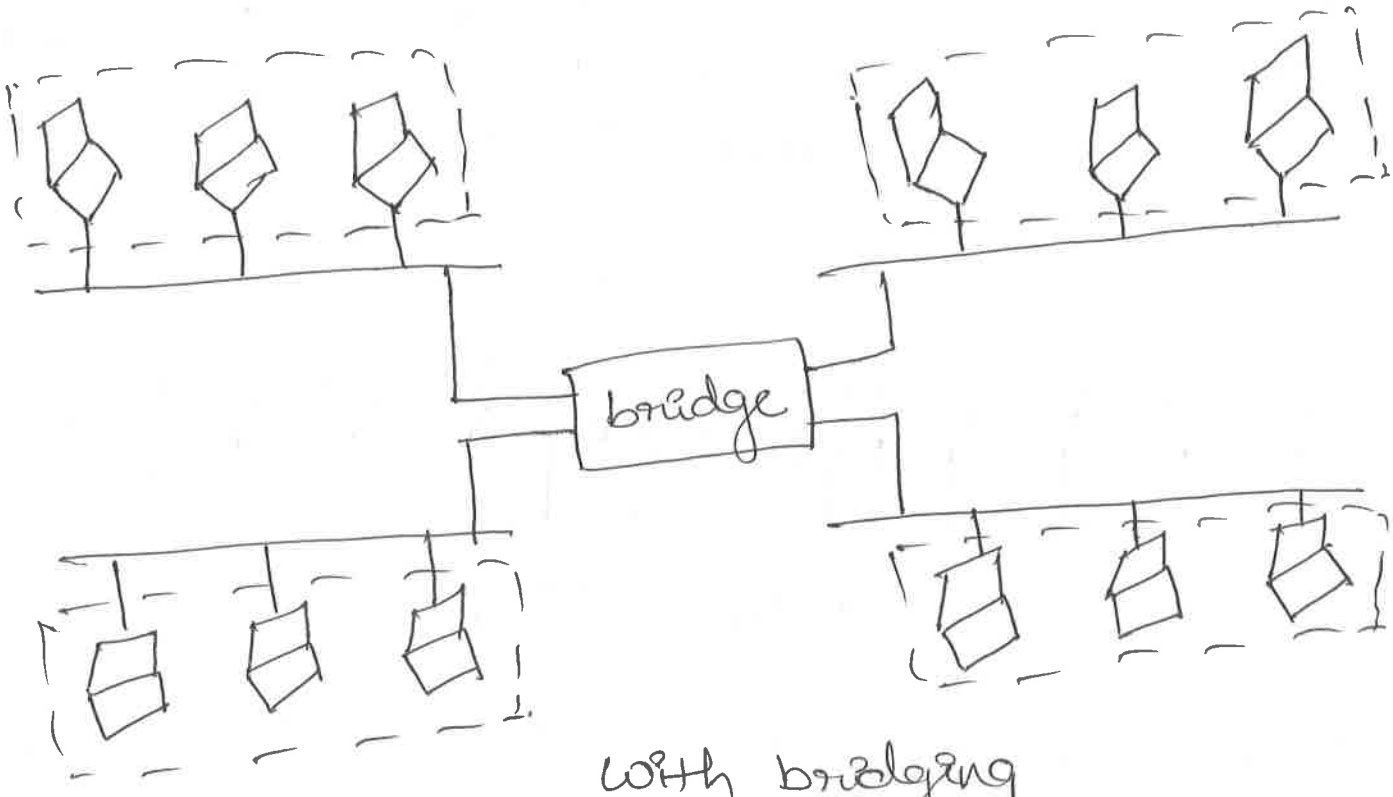
In above figure, a network with 12 stations is divided into two networks, each with 6 stations. The 10Mbps capacity in each segment is now shared between 6 stations (actually 7 bcz the bridge acts as a station in each segment) not 12 stations. In a network with heavy load, each

station is offered 10/7 Mbps instead of 10/12 Mbps. If we use a four port bridge, each station is now offered 10/4 Mbps.

Separating collision domains:



without bridging

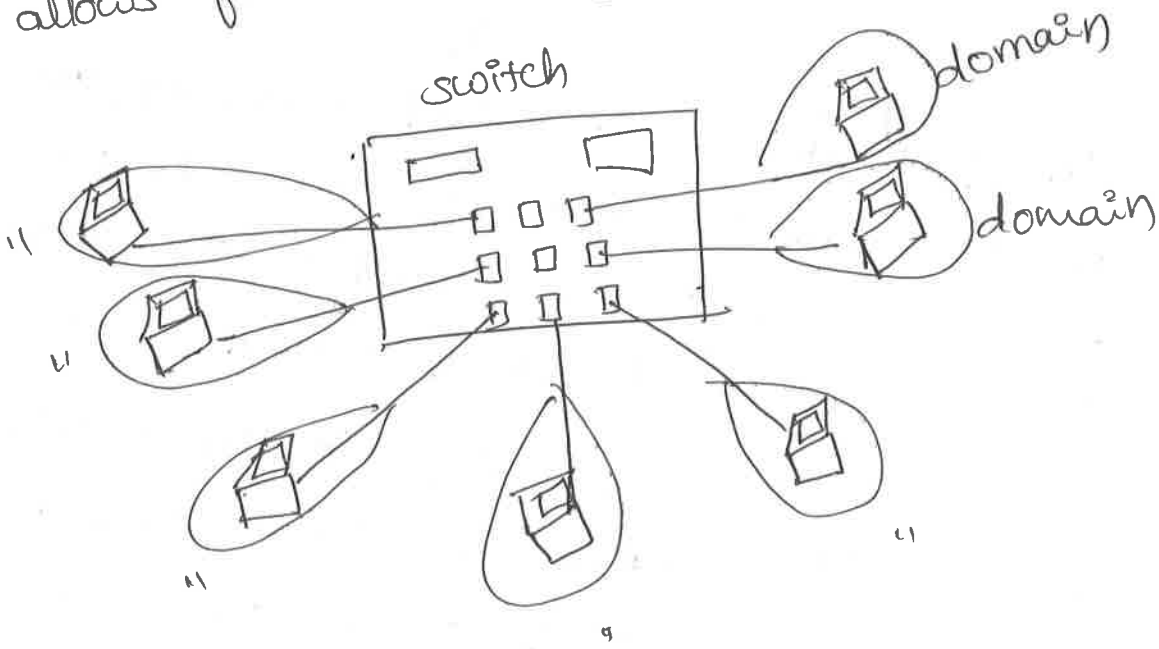


with bridging

Figure shows the collision domains for an unbridged and a bridged network. Without bridging 12 stations contend for access to the medium, with bridging only 3 stations contend for access

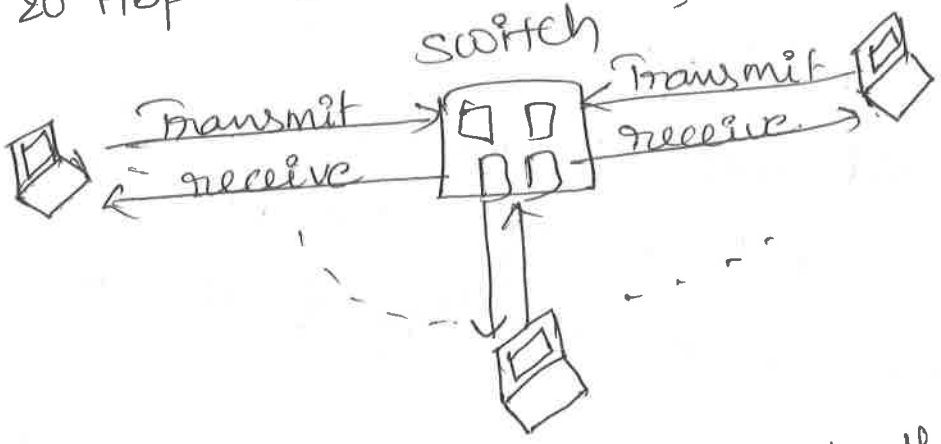
to the medium.

Switched Ethernet : The idea of a bridged LAN can be extended to a switched LAN. If we can have a multiple port bridge, why not have an N port switch ? In this way, the bandwidth is shared only between the station and the switch. In addition, the collision domain is divided into N domains. A layer-2 switch is an N-port bridge with additional sophistication that allows faster handling of the packets.



switched ethernet

Full duplex ethernet: One of the limitations of 10base5 and 10base2 is that communication is half duplex. The next step in the evolution was to move from switched ethernet to full duplex switched ethernet. The full duplex mode increases the capacity of each domain from 10 to 20 Mbps. ~~Instead of~~



In full duplex switched ethernet, there is no need for the CSMA/CD method. because each station is connected to the switch via two separate links. Each station & switch can send and receive independently without worrying about collision. the carrier sensing and collision detection functionalities of the MAC sublayer can be turned off.

MAC control layer: standard ethernet was designed as a connectionless protocol at the MAC sub layer. There is no explicit flow control or error control & acknowledgment. To provide for flow and error control in full duplex switched ethernet, a new sublayer, called the MAC control is added between the LLC sublayer and the MAC sub layer.

Fast ethernet: The designers of the fast ethernet needed to make it compatible with standard ethernet. The MAC sublayer was left unchanged, which meant the frame format & the max & min size could also remain unchanged

The goals of fast ethernet are

* upgrade the data rate to 100Mbps
* make it compatible with standard ethernet
* keep the same frame format & 48 bit address

Access method: The proper operation of the CSMA/CD depends on the transmission rate, the minimum size of the frame and the maximum network length.

The max length of the n/w should be changed i.e if the minimum frame size is still 512bits and it is transmitted 10 times faster, the collision needs to be detected 10 times sooner, which means the max length of the n/w should be 10 times shorter. So the fast ethernet came with two solutions

1. to drop the bus topology and use a passive hub and star topology but makes the max size of the network 250 meters instead of 2500m as in the standard ethernet.

2. to use link layer switch with a buffer to store frames and a full duplex connection to each host to make the transmission medium private for each host. In this case, there is no need for CSMA/CD because the hosts are not competing with each other.

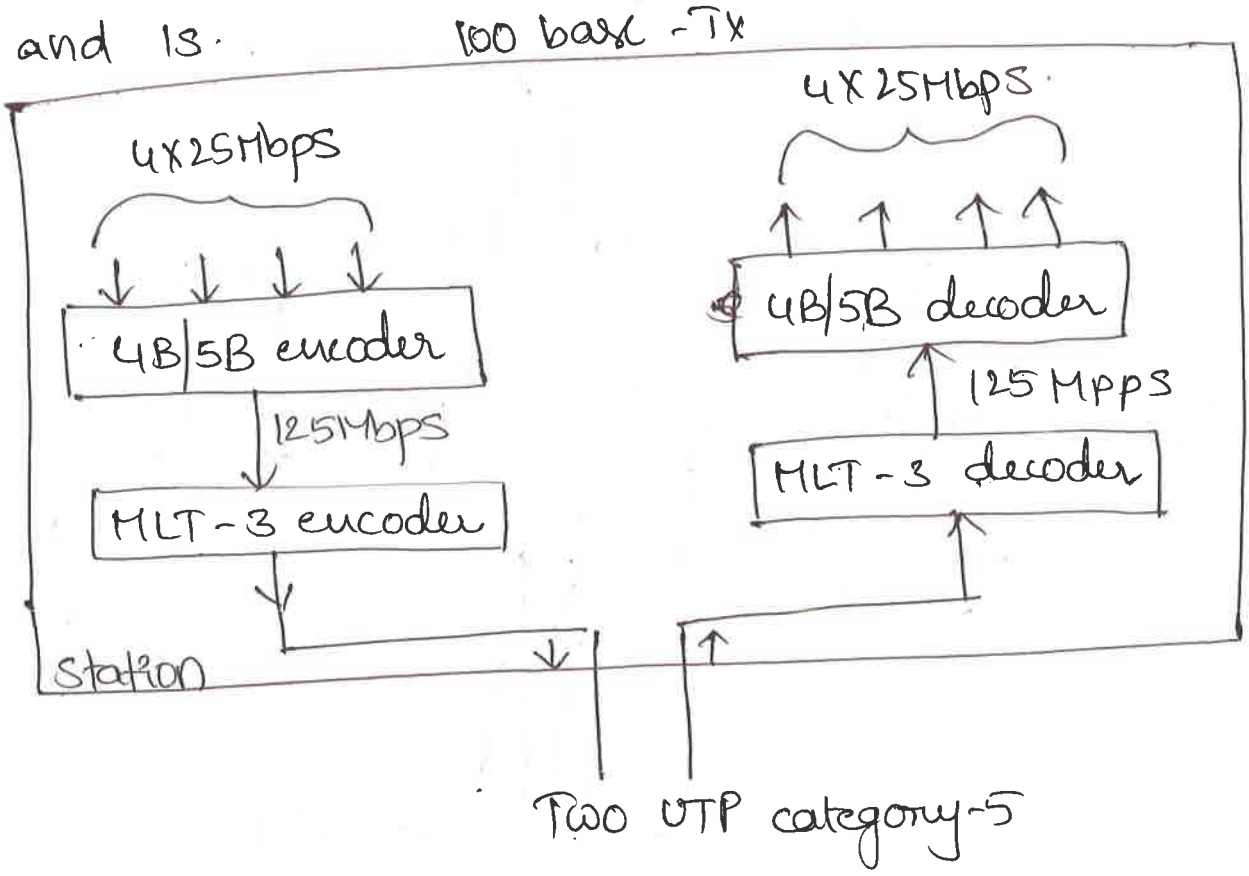
Autonegotiation : It allows two devices to negotiate the mode or data rate of operation. It was designed particularly to allow incompatible devices to connect to one another.

physical layer : changes in physical layer

Topology : If there are only two stations, they can be connected point to point. Three or more stations need to be connected in a star topology with a hub or a switch.

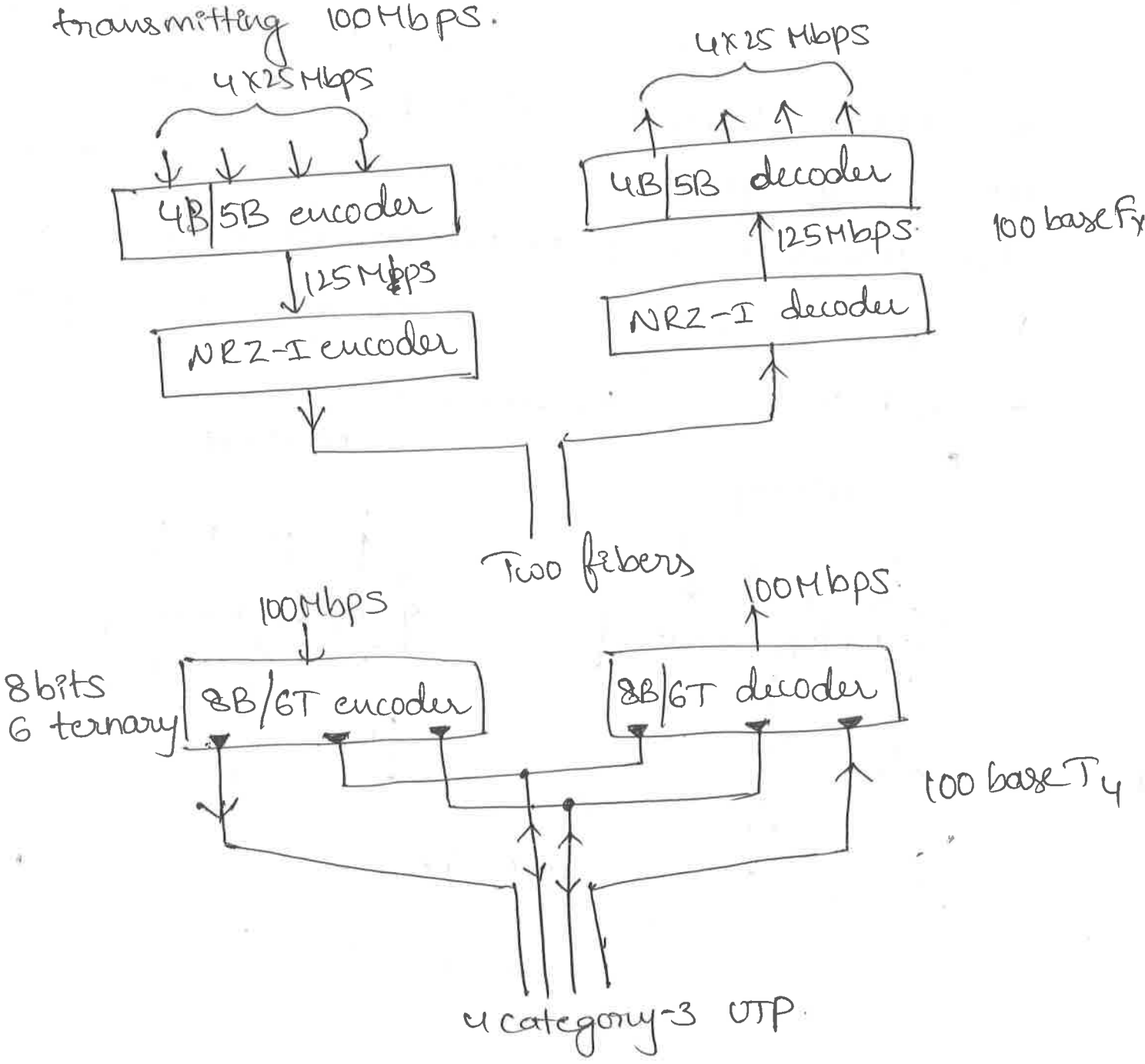
Encoding : (Multi level Transmit)

100 base-Tx uses two pairs of twisted pair cable (either category 5 UTP or STP). For this implementation the MLT-3 scheme was selected, since MLT-3 is not a self synchronous line coding scheme, 4B/5B block coding is used to provide bit synchronization by preventing the occurrence of a long seq of 0's and 1's.



100 base Fx uses two pairs of feber optic cables. The designers selected the NRZ-I encoding scheme for this implementation. However NRZ-I has a bit synchronization problem, to overcome this the designers used 4B/5B block coding.

100 base T4 uses category 3 or higher UTP, the implementation uses four pairs of UTP for transmitting 100Mbps.



Implementation	Medium	Medium length	wires	encoding
100 base-Tx	UTP & STP	100m	2	4B5B+MLT-3
100 base-Fx	fiber	185m	2	4B5B+NRZ-I
100 base-T4	UTP	100m	4	Two 8B/6T

8 bits as 6 Ternary signals

Gigabit ethernet:

MAC sublayer : Gigabit ethernet has two approaches for medium access : half duplex & full duplex. Mostly full duplex.

Full duplex mode : there is a central switch connected to all computers or other switches. In this mode, for each input port, each switch has, buffers in which data are stored until they are transmitted. CSMA/CD is not used. Max length of the cable is determined by the signal attenuation in the cable, not by the CD process.

Half duplex mode : In this case, a switch can be replaced by a hub, which acts as the common cable in which a collision might occur. It uses CSMA/CD. The max length of the network in this approach is totally dependent on the minimum frame size. three methods have been defined traditional, carrier extension & frame bursting.

Traditional: In this we keep the min length of the frame as in traditional ethernet (512 bits)

Standard - 10Mbps i.e $1S \rightarrow 10 \times 10^6$ bits

$? \leftarrow 512$ bits

$$\frac{512}{10 \times 10^6} = 51.2 \mu s.$$

Gigabit - 1000Mbps i.e $1S \rightarrow 1000 \times 10^6$ bits

$? \leftarrow 512$ bits

$$\frac{512}{1000 \times 10^6} = 0.512 \mu s.$$

The reduced slot time means that collision is detected 100 times earlier. This means that the max length of the n/w is 25m. i.e with in room

Carrier extension: The carrier extension approach defines the min length of a frame as 512 bytes. i.e the min length is 8 times longer. This method forces a station to add extension bits to any frame that is lessthan 4096 bits.

Frame bursting: Instead of adding an extension to each frame, multiple frames are sent. To make these multiple frames look like one frame padding is added between the frames, so that the channel is not idle.

physical layer

Topology :

If two stations → point to point

morethan two → star with hub & switch

another configuration is to connect several star topologies & let one star topology be part of another.

Implementation

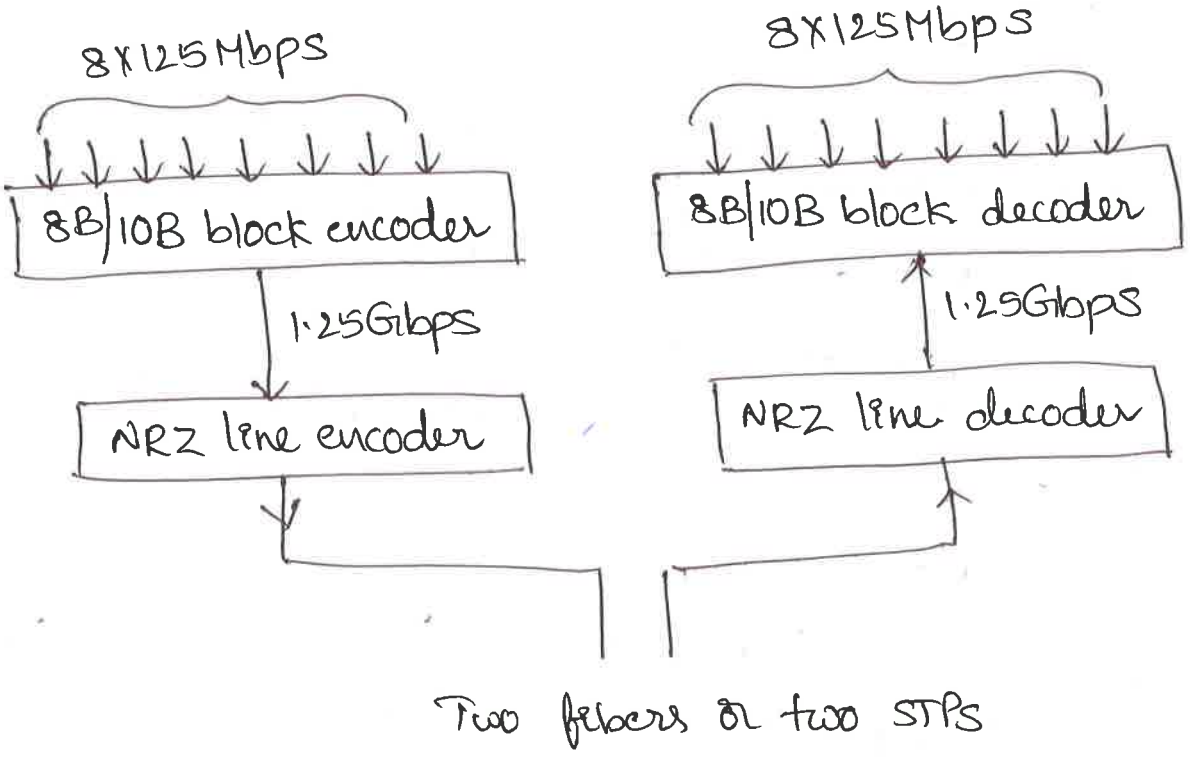
1000 base - SX (short wave) } Two wire optical
- LX (long wave) } fiber cable
- CX (STP) → shielded twisted pair cable

1000 base - T - four wire category - 5 twisted pair cable

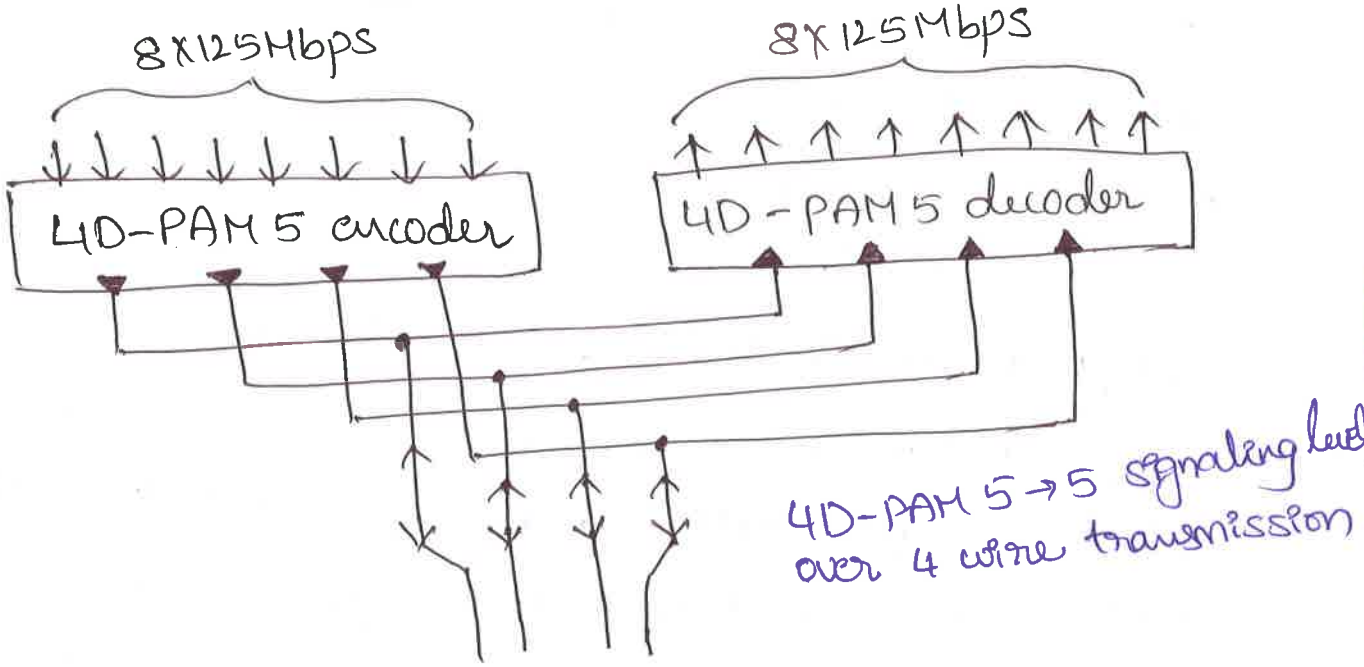
Encoding : cannot use manchester.

The two wire use an NRZ scheme along with 8B/10B block coding. In the four wire implementation it is not possible to have 2 wires for input and 2 for output, because each wire would need to carry 500Mbps, which exceeds the capacity for category 5 UTP. As a solution 4D-PAM5 encoding is used to reduce the bandwidth. Thus, all four wires are involved in both input and output, each wire carries 250Mbps, which is in the range for category 5 UTP cable.

1000 base-SX, 1000 base-LX and 1000 base-CX



1000 base-T



Implementation	Medium	Medium length	wires	encoding
1000 base -SX	Fiber S-W	550m	2	8B/10B + NRZ
1000 base -LX	Fiber L-W	5000m	2	"
1000 base -CX	STP	25m	2	"
1000 base -T4	UTP	100m	4	4D-PAM5

10 Gigabit ethernet: The idea is to extend the technology, the data rate and the coverage distance so that the ethernet can be used as LAN and MAN. This data rate is possible only with fiber optic technology. The standard defines ~~to support existing~~ two types of physical layers LAN PHY and WAN PHY.

The first is designed to support existing LANS.

The 2nd actually defines a WAN with links connected through SONET OC-192

Implementation: 10 Gigabit ethernet operates only in duplex mode, there is no need for contention. CSMA/CD is not used in 10 Gigabit ethernet.

Implementation	Medium	Medium length	no. of wires	encoding
10 Gi base-SR	Fiber 850nm	300m	2	64B66B
10Gi base-LR	Fiber 1310nm	10km	2	64B66B
10Gi base-EW	Fiber 1350nm	40km	2	SONET
10Gi base-X4	Fiber 1310nm	300m-10km	2	8B10B

SR/SW SR → LAN short Reach & short range
SW → WAN

LR/LW LR → Long Range, Long Reach

ER/EW ER → Extended Reach, Extended range

SONET → Synchronous optical network