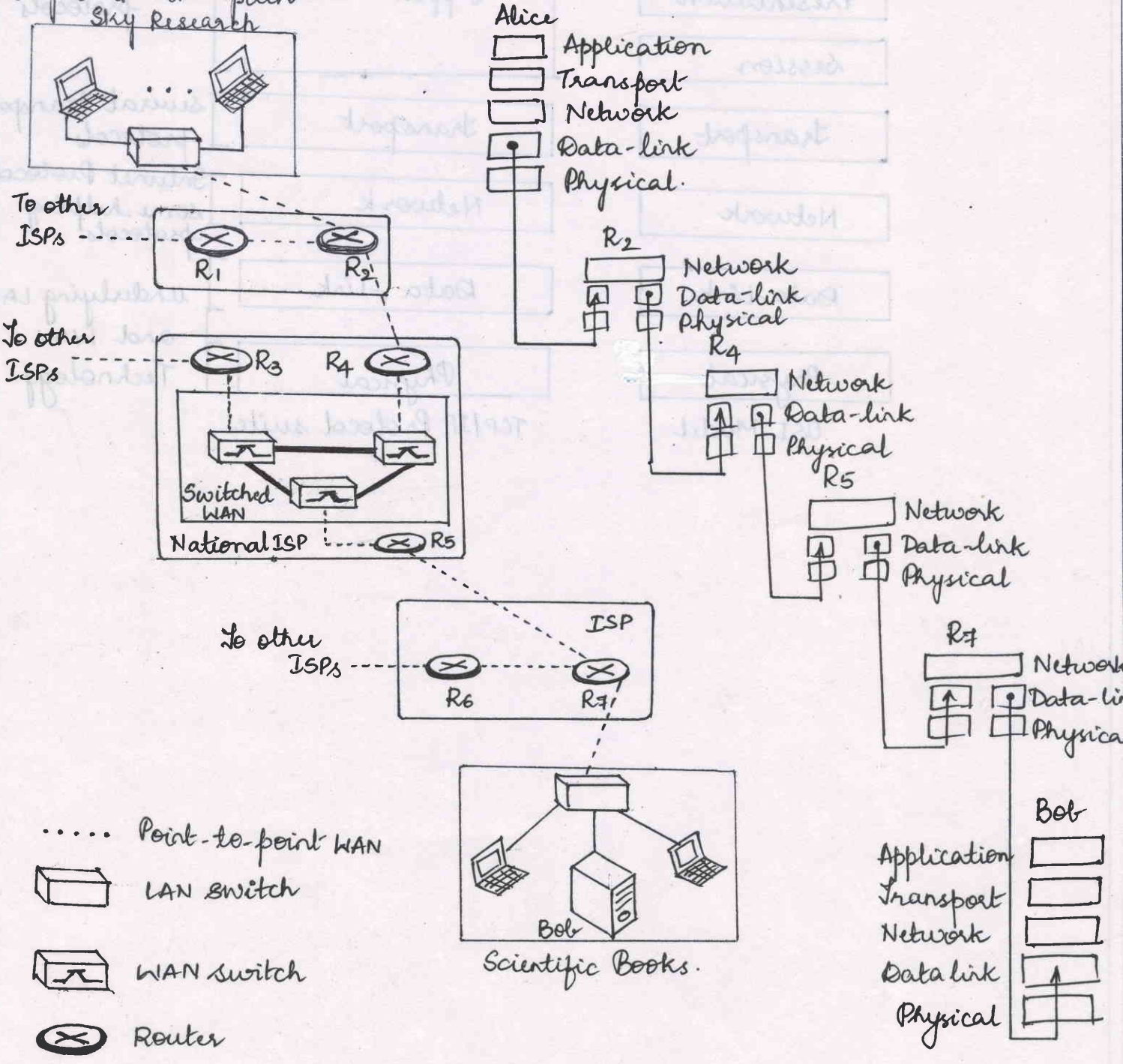
DATA-LINK LAYER:

INTRODUCTION:

The Internet is a combination of networks glued together by connecting devices (routers or switches). If a packet is to travel from a host to another host, it needs to pass through these networks. The figure shows the same scenario. Communication at the data link layer is made up of five separate logical connections between the data-link layers in the path.

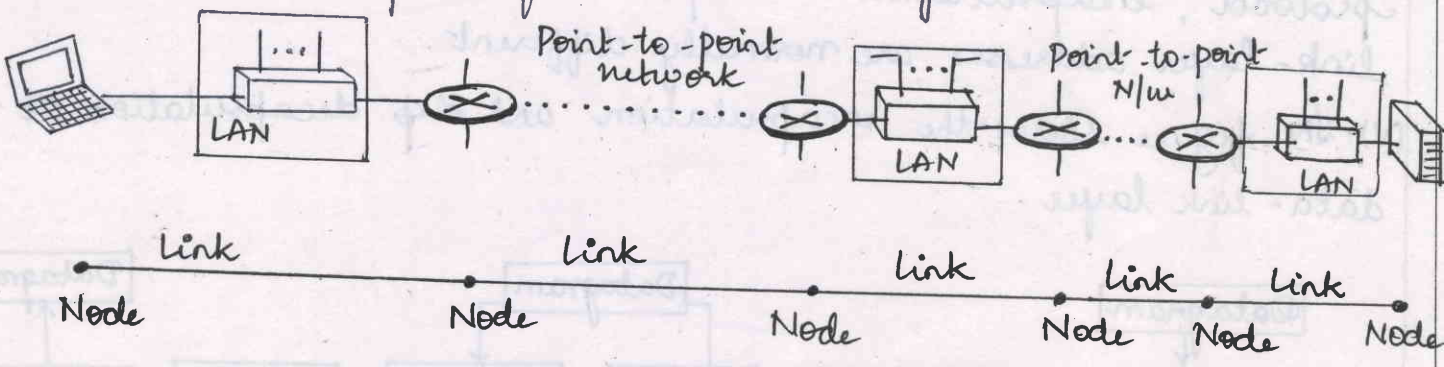


(i) The data link layer at Alice's computer communicates with the data link layer at router R_2.
(ii) The data-link layer at router R_2 communicates with the data-link layer at router R4, and so on. Finally, the data-link layer at router R7 communicates with the data link layer at Bob's computer.
(iii) Only one data-link layer is involved at the source or the destinatio-n, but two data-link layers are involved at each router.
(iv) The reason is that Alice's and Bob's computers are each connected to a single network, but each router takes input from one network and sends output to another network.

Nodes and Links :-

Communication at the data-link layer is node-to-node. A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point.

These LANs and WAN's are connected by routers. It is customary to refer two end hosts and the routers as nodes and the networks in between as links. The figure shows the simple representation of links and nodes when the path of data unit is only six nodes.



The first node is the source host; the last node is the destination host. The other four nodes are four routers. The first, the third, and the fifth links represent the three LAN's, the second and the fourth links represent the two WANs.

P.T.O.

Services:-

(i) The data-link layer is located between the physical and the network layers. The data-link layers provides services to the network layer, it receives services from the physical layer.

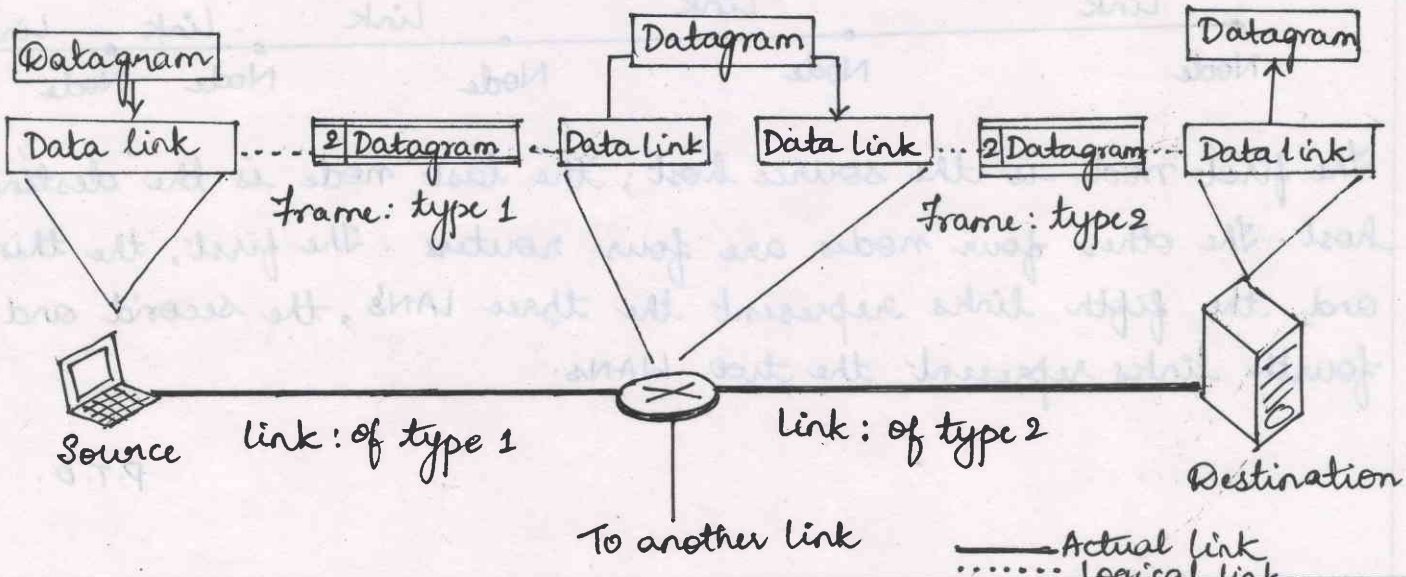
(ii) The duty scope of data-link layer is node-to-node. When a packet is travelling in the Internet, the data-link layer of a node is responsible for delivering a datagram for the next node in the path.

(iii) The data-link layer of the sending node needs to encapsulate the datagram received from network in a frame, and the data-link layer of the receiving node needs to decapsulate the datagram from the frame.

i.e. the data-link layer of source host needs only to encapsulate, the data-link layer of destination host needs to decapsulate, but each intermediate node needs to both encapsulate and decapsulate.

(iv) Intermediate nodes needs both encapsulation and decapsulation because each link may be using a different protocol with a different frame format. Even if one link and the next are using the same protocol, encapsulation & decapsulation are needed because the link-layer addresses are normally different.

(v) The figure shows the encapsulation and ~~dep~~ decapsulation at the data-link layer.



Assume that we have only one router between the source and destination.

The datagram received by the data-link layer of the source host is encapsulated in a frame. The frame is logically transported from the source host to the router. The frame is decapsulated at the data-link layer of the router and encapsulated to another frame. The new frame is logically transported from the router and to the destination host. Although we have shown only two data-link layers at the router, the router actually has three data-link layers because it is connected to three physical links.

From the figure, we can list the services provided by a data-link layer;

(i) Framing :-

The first service provided by data-link layer is 'framing'. The data-link layer at each node needs to encapsulate the datagram (packet received from the network layer) in a frame before sending it to the next node. The node also needs to decapsulate the datagram from the frame received on the logical channel. Different data-link layers have different formats for framing.

(ii) Flow Control :-

Whenever we have a producer and a consumer, we need to think about 'flow control'. If produces produces items that cannot be consumed, accumulation of items occur. The sending data-link layer at the end of a link is producer of frames; the receiving data-link layer at the other end of a link is a consumer.

If the rate of produced frames is higher than the rate of consumed frames, frames at the receiving end need to be buffered while waiting to be consumed (processed). This can be done using two ways;

(i) Let the receiving data-link layer drop the frames if its buffer is full.

(ii) Let the receiving data-link layer send a feedback to the sending data-link layer to ask it to stop or slow down.

(iii) Error Control :-

At the sending node, a frame in a data-link layer needs to be changed to bits, transformed to electromagnetic signals, and transmitted through the transmission media. At the receiving node, electromagnetic signals are received, transformed to bits, and put together to create a frame. Since electromagnetic signals are susceptible to error a frame is susceptible to error. The error ~~finds to~~ needs to be detected. After detection, it needs to be either corrected at the receiver node or discarded and retransmitted by the sending node.

(iv) Congestion Control:-

Although a link may be congested with frames, which may result in frame loss, most data-link layer protocols do not directly use a congestion control to alleviate congestion, although some wide-area networks do.

Categories of Link :

Although two nodes are physically connected by a transmission medium such as cable or air, data-link controls how the medium is used.

We can have a data-link layer that uses the whole capacity of the medium we can also have a data link layer that uses only part of the capacity of the link. i.e. we can have a point-to-point link or a broadcast link.

In a point-to-point link, the link is dedicated to two devices; in a broadcast link, the link is shared between several pairs of devices.

Sublayers :-

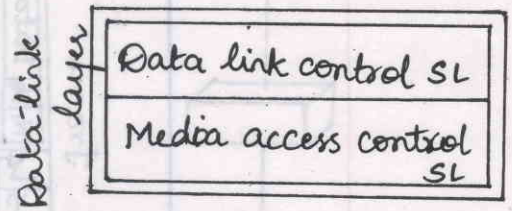
To understand the functionality of and services provided by the link layer, we can divide the data-link layer into two sublayers.

(i) Data link Control (DLC)

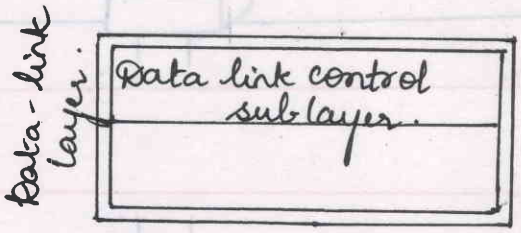
(ii) Media Access Control (MAC).

The data link control layer deals with all issues common to both point-to-point and broadcast links.

The media access control sublayer deals only with issues specific to broadcast links



(a) Data-link layer of a broadcast link



(b) Data-link layer of a point-to-point link

LINK LAYER ADDRESSING :-

In a connectionless internetwork such as the Internet, we cannot make a datagram reach its destination using on IP addresses. because each datagram in the Internet, from the same source host to the same destination host, may take a different path.

The source and destination IP addresses define the two ends but cannot define which links the datagram should pass through.

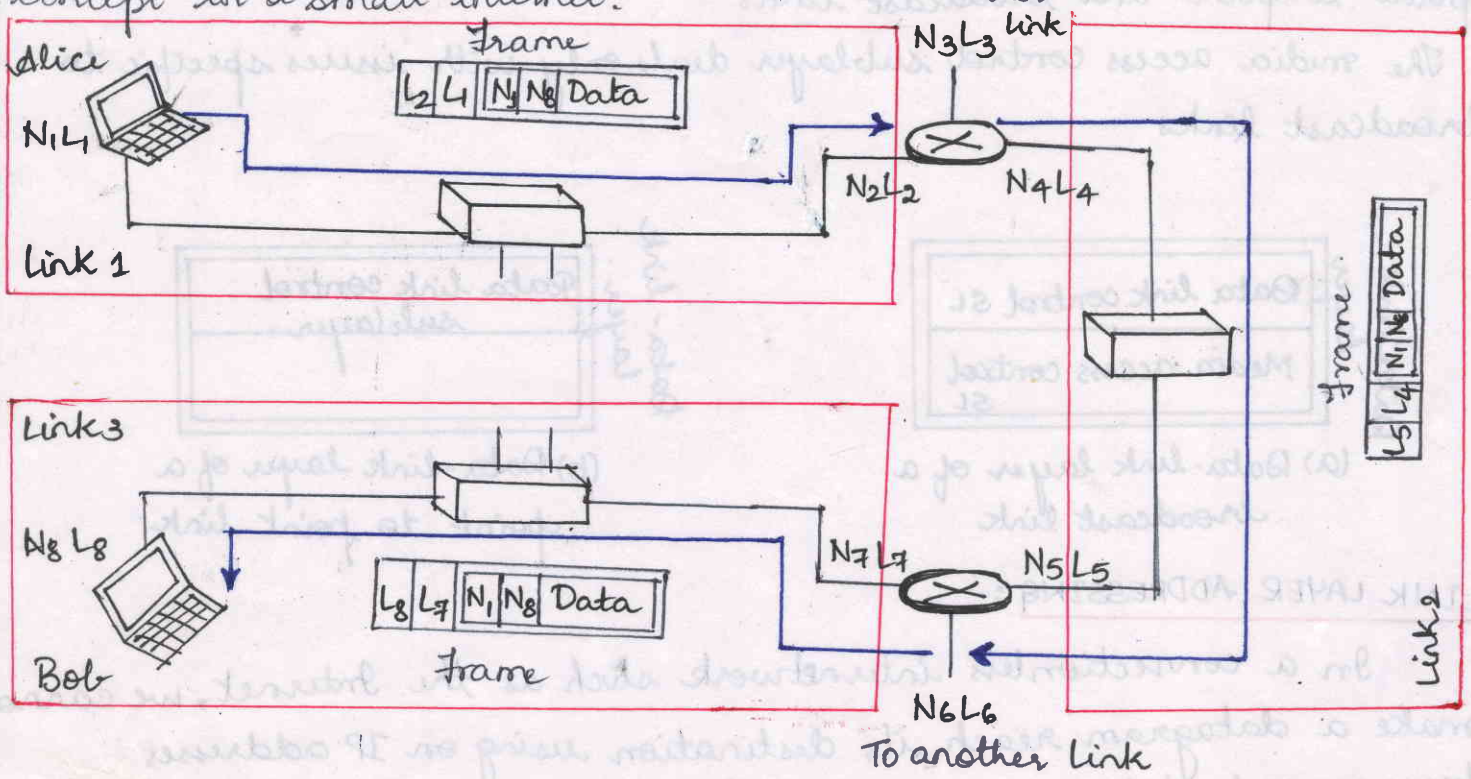
If the destination address in a datagram changes, the packet never reaches its destination ; if the source IP address in a datagram changes, the destination host or a router can never communicate with the source if a response needs to be sent back or error needs to be reported to the source.

Therefore we need another addressing mechanism in a connection-less internetwork : the link-layer addresses of the two nodes. A link-layer address is called 'link address' or 'physical address' or 'MAC address'

Since the link is controlled at the data-link layer, the addresses need to belong to data-link layer.

When a datagram passes from the network layer to the data link layer it will be encapsulated in a frame and two data-link addresses are added to the frame header. These 2 addresses are changed every time

the frame moves from one link to another. The figure represents the concept in a small internet.



IP ADDRESSES AND LINK-LAYER ADDRESSES IN A SMALL INTERNET.

N: IP Address
L: Link-layer address.

Order of address;
IP addresses : source-destination
Link-layer address: destination to source.

* In the internet depicted above, we have three links and two routers And two hosts: Alice (source) and Bob (destination).
* For each host we have two addresses., the IP address (N) and the link-layer address (L). The router has as many pairs of addresses as the number of links the router is connected to. There are three frames, one for each link.
* Each frame carries the same datagram with the same source and destination addresses (N_1 and N_8), but the link-layer addresses of the frame change from link to link.
* In link 1, the link layer addresses are L_1 and L_2. In link 2, they are L_4 and L_5. In link 3, they are L_7 and L_8.
* For IP addresses the source address comes before the destination address; for link-layer address, the destination address comes before the source.

Types of Addresses :-

Some link-layer protocols define three types of addresses :-

(i) Unicast Address :

Each host or each interface of a router is assigned a unicast address. 'Unicasting' means one-to-one communication. A frame with a unicast address destination is destined only ~~for~~ for one entity in the link.

Ex:-

The unicast link-layer addresses in the most common LAN, Ethernet, are 48 bits (six bytes) that are presented as 12 hexadecimal digits separated by colons;

The link-layer address of a computer is;

A3:34:45:11:92:F1

(ii) Multicast Address :

'Multicasting' means one-to-many communication. However the jurisdiction is local (inside the link).

Ex:-

The multicast link-layer address in most common LAN, Ethernet, are 48 bits (six bytes) that are presented as 12 hexadecimal digits separated by colons. The second digit, needs to be an even number in hexadecimal.

A2:34:45:11:92:F1.

(iii) Broadcast Address :

'Broadcasting' means one-to-all communication. A frame with a destination broadcast address is sent to all ~~entitities~~ entities in the link.

Ex:-

The broadcast link-layer addresses in the most common LAN, Ethernet, are 48 bits, all 1's, that are presented as 12 hexadecimal digits separated by colons.

FF:FF:FF:FF:FF:FF.

(P.T.O)

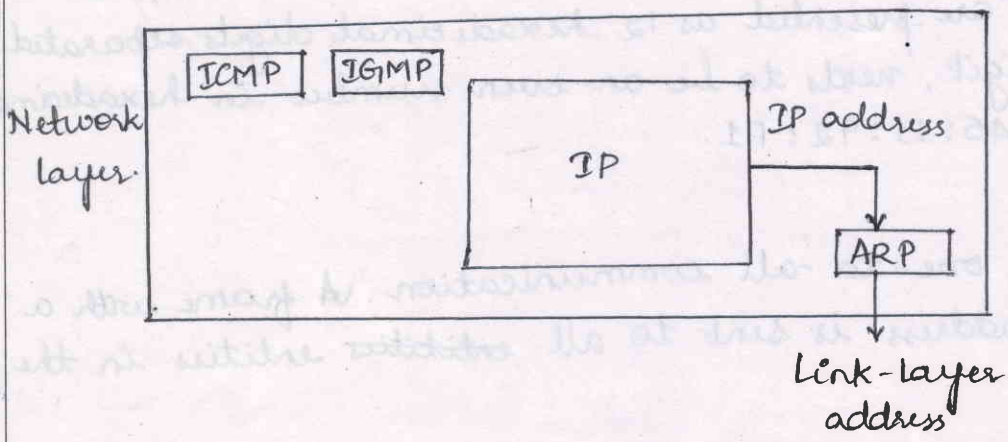
Address Resolution Protocol (ARP):-

When a node has an IP datagram to send to another node in a link, it has the IP address of the receiving node. The source host knows the IP address of the default router. Each router except the last one in the path gets the IP address of the next router by using its forwarding table. The last router knows the IP address of the destination host.

However, the IP address of the next router or node is not helpful in moving a frame through a link; we need the link-layer address of the next node. Address Resolution Protocol (ARP) is used for this purpose.

The ARP protocol is one of the Auxiliary protocols defined in the network layer. It belongs to the network layer, but it is discussed here because it maps an IP address to a logical-link address. ARP accepts an IP address from the IP protocol, maps the address to the corresponding link-layer address, and passes it to the data-link layer.

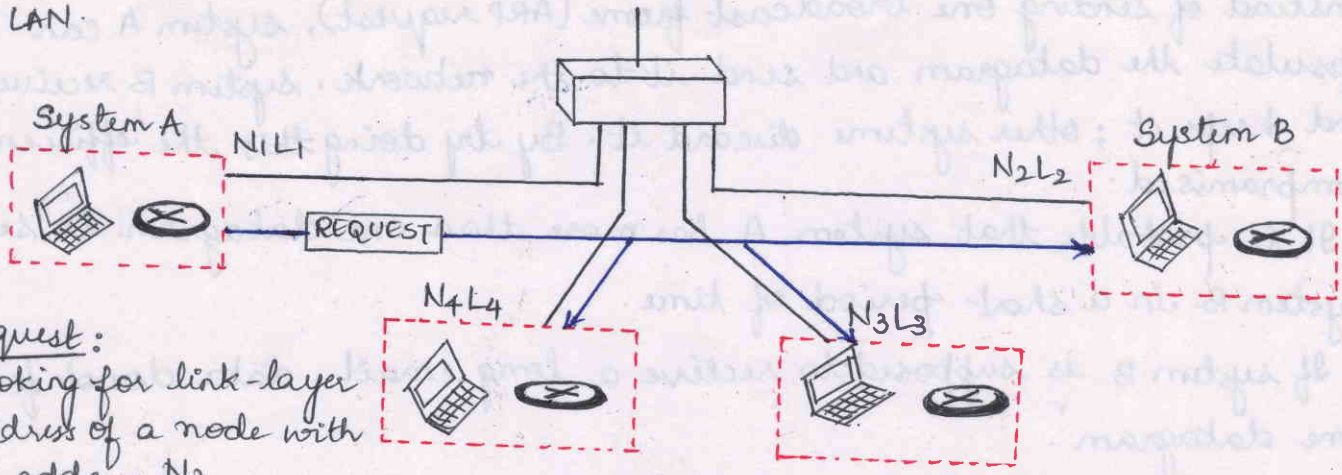
POSITION OF ARP IN TCP/IP PROTOCOL SUITE:-



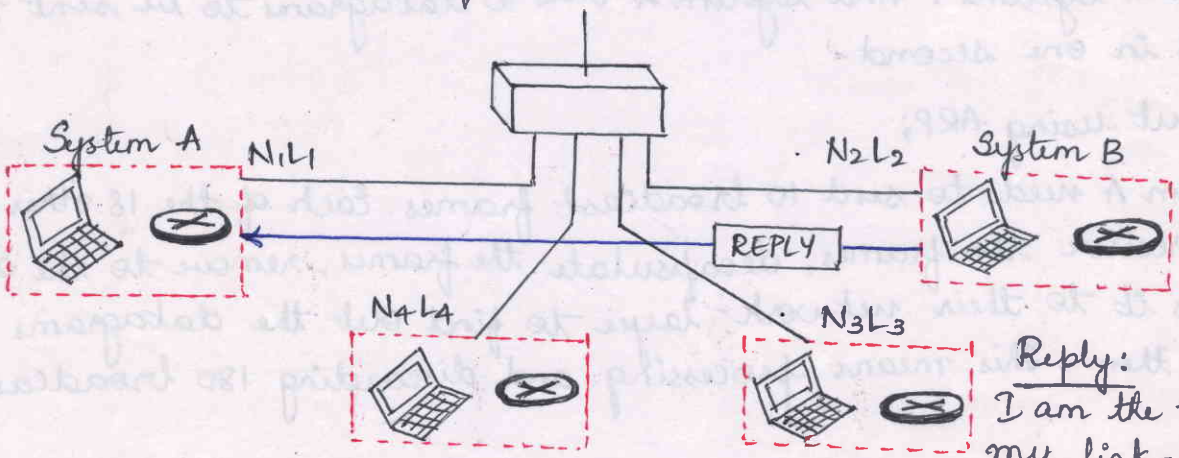
When a host or a router needs to find the link-layer address of another host or router in its network, it sends an ARP request packet. The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver.

Since the sender does not know the link-layer address of the receiver, the query is broadcast ~~over~~ address. Every host or router on the network receives and processes the ARP request packet, but only intended recipient recognizes its IP address and sends back the ARP response packet.

The response packet contains the recipient IP's and link-layer addresses. The packet is unicast directly to the node that sent the request packet.



(a) ARP request is broadcast.



(b) ARP reply is unicast

In the figure (a), the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address N2. System A needs to pass the packet to its data-link layer for actual delivery, but it does not know the physical address of the recipient. It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IP address of N2.

This packet is received by every system on the physical network, but only system B will answer it as shown in figure(b). System B sends an ARP reply packet that includes the physical address. Now system A can send

all the packets it has to this destination using the received physical address.

Caching :-

Instead of sending one broadcast frame (ARP request), system A can encapsulate the datagram and send it to the network. System B receives it and keeps it ; other systems discard it. By by doing this the efficiency is compramised.

It is probable that system A has more than one datagram to send to system B in a shat period of time.

Ex:- If system B is supposed to receive a long email, data donot fit in one datagram.

Assume 20 systems connected to network # link : system A, system B and 18 other systems. And system A has 10 datagrams to be sent to system B in one second.

* Without using ARP;

System A needs to send 10 broadcast frames. Each of the 18 other systems need to receive the frames, decapsulate the frames, remove to the datagram and pass it to their network-layer to find out the datagrams do not belong to them. This means processing and discarding 180 broadcast frames.

* Using ARP ;

System A needs to send only on broadcast frame. Each of the 18 other systems need to receive the frames, decapsulate the frames, remove the ARP message and pass the message to their ARP protocol to find that the frame must be discarded. This means processing and discarding only 18 broadcast frames.

After system B responds with its own data-link address, system A can store the link-layer address in the cache memory. The rest of the nine frames are only unicast. Since processing broadcast frames is expensive (time-consuming), the first method is preferable.

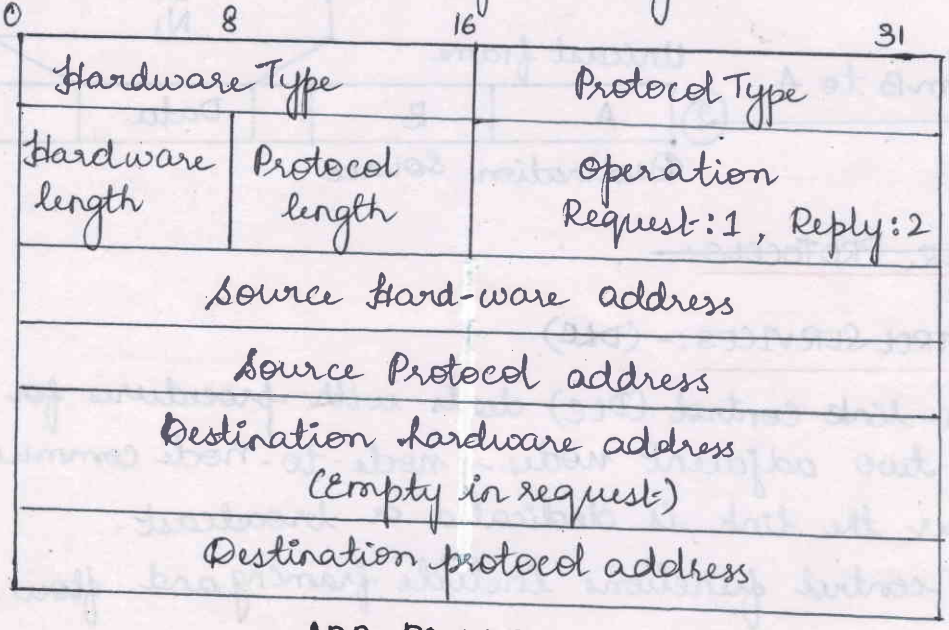
Packet Format :-

The figure shows the format of an ARP packet. The hardware type field defines the type of the link-layer protocol; Ethernet is given type 1. The protocol type field defines the network-layer protocol: IPv4 protocol is $(0800)_{16}$.

The source hardware and source protocol addresses are variable-length fields defining the link-layer and network-layer addresses of sender.

The destination hardware address and destination protocol address fields define the receive link-layer and network-layer addresses.

An ARP packet is encapsulated directly into a data-link frame. The frame needs to have a field to show that the payload belongs to the ARP and not to the network-layer datagram.

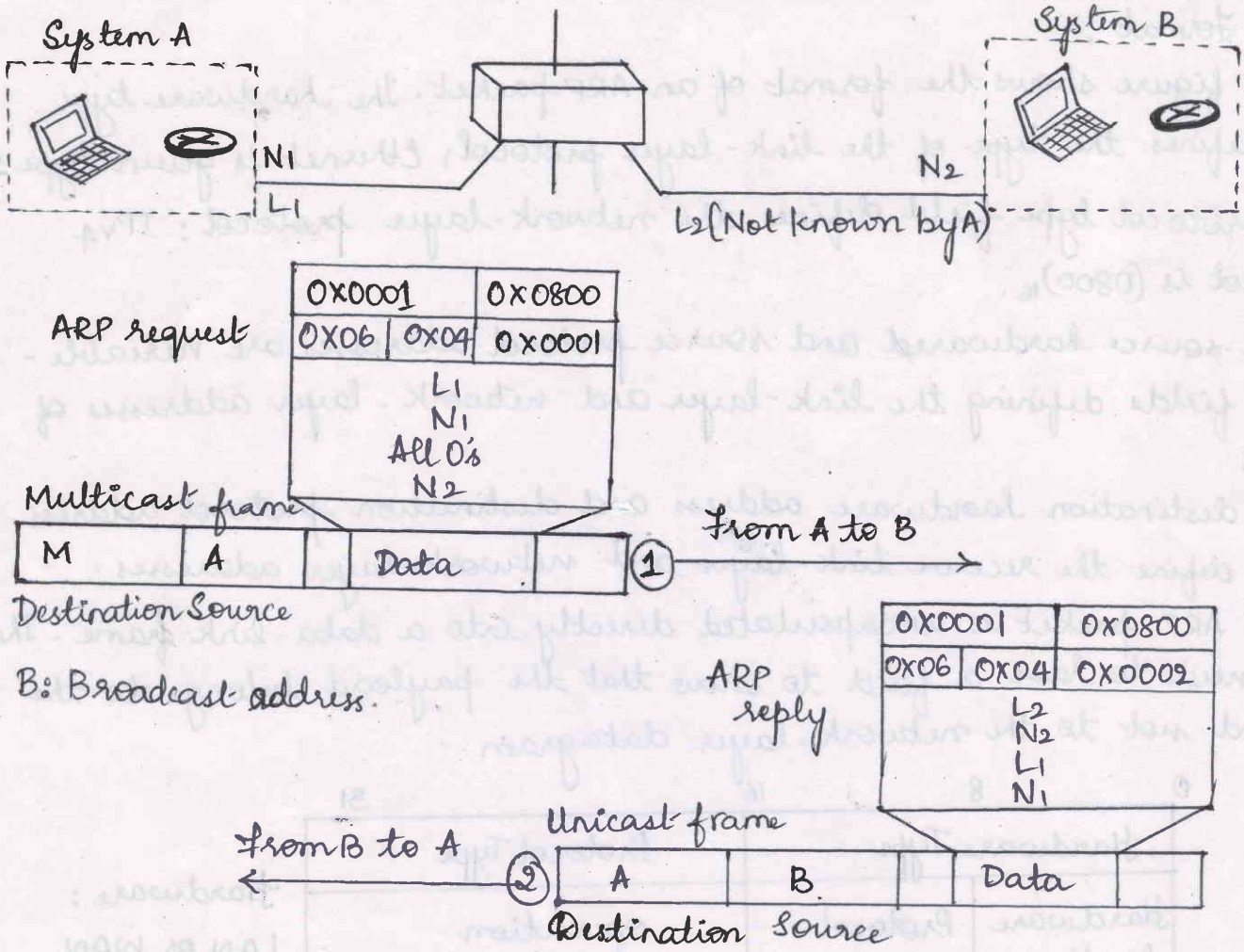


ARP PACKET

Ex:- A host with IP address N1 and MAC address L1 has a packet to send to another host with IP address N2 and physical address L2 (which is unknown to the first host). The two hosts are on the same network.

The figure shows the ARP request and response messages.

(P.T.O.)



~~DATA-LINK LAYER PROTOCOLS:-~~

DATA-LINK CONTROL SERVICES:- (DLC)

The Data-link control (DLC) deals with procedures for communication between two adjacent nodes - node-to-node communication - no matter whether the link is dedicated or broadcast.

Data-link control functions include framing and flow & error control.

Framing:-

Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination.

The physical layer provides bit synchronization to ensure that the sender and the receiver use same bit durations & timing.

The data-link layer needs to pack the bits into frames, so each frame is distinguishable from another.

Framing in data-link layer separates a message from one source to a destination by adding a sender address and a destination address.

The destination addess defines where a packet is to go; the sender address helps the recipient aknowledge the ~~receipt~~. receipt.

Though the whole message could be packed in one frame, it is not normally done because a frame can be very large, making flow and error contrd very inefficient.

When a message is carried in one very large frame, even a single bit error would require the retramission of the whole frame. When a message is divided into smaller frames, a single-bit error affects only that small frame.

Frame Size:-

Frames can be of fixed and variable size. In fixed-size framing there is no need for defining the boundaries of the frame; size is used as delimiter

Ex:- Framing in ATM WAN, which uses frames of fixed size called cells

In variable-size framing, we need to define the end of one frame and the beginning of the next. Two approaches are used for this purpose.

(i) Character-oriented framing:

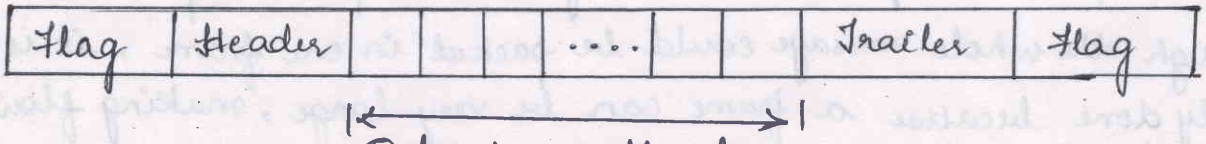
In character-oriented (byte-oriented) framing, data to be carried are 8-bit characters from a coding system such as ASCII.

The header, normally carries the source and destination addresses and other control information, and the trailer, which carries error detection redundant bits, are also multiples of 8 bits.

To separate one frame and the next, an 8-bit (1 byte) flag is added at the beginning and end of a frame.

The flag, composed of protocol-dependent special characters, signals the start or end of the frame.

Figure shows the format of a frame in a character-oriented protocol.



(a) A frame in a character-oriented protocol.

Character-oriented framing is used when only text was exchanged by the data-link layers.

Flag could be selected to be any character not used for text communication.

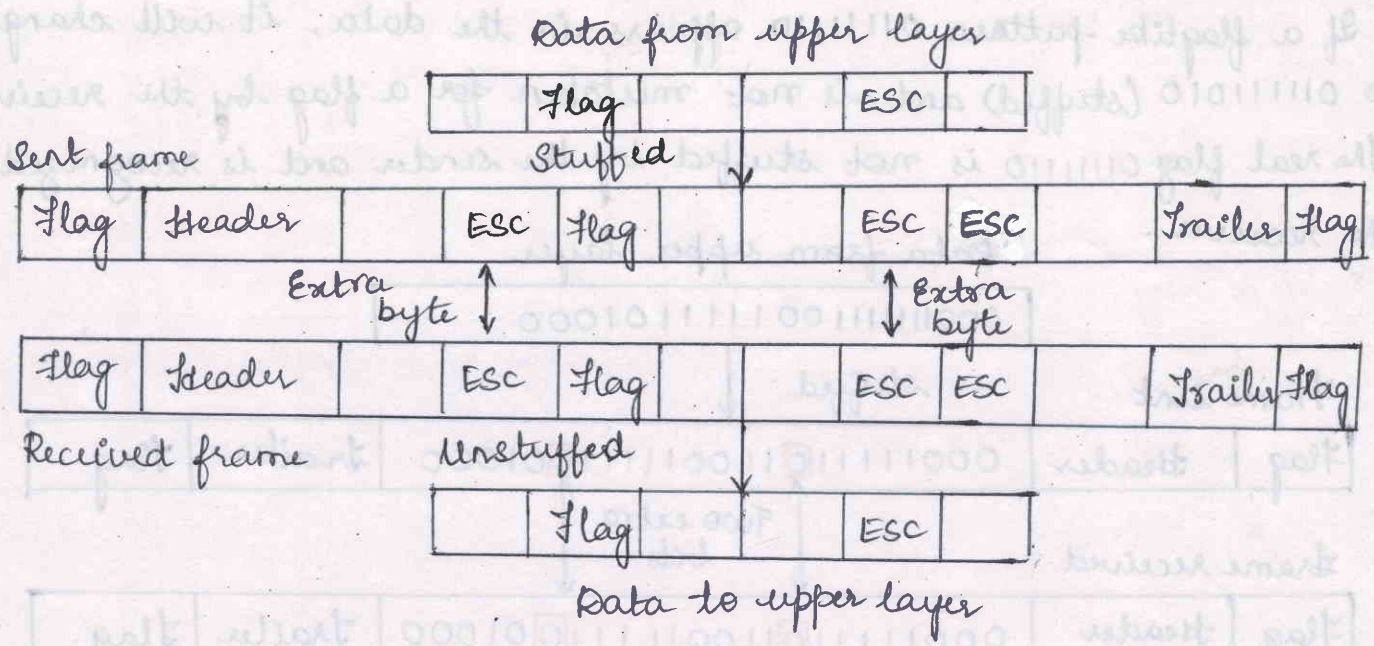
If we send information such as graphs, audio and video; any character used for the flag could also be part of the information. When the receiver encounters this pattern in the middle of the data, it believes it has reached the end of the frame.

To fix this problem, byte stuffing strategy was added to character oriented framing.

In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.

The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC) as has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not as a delimiting flag.

Byte stuffing is the process of adding one extra byte whenever there is a flag or escape character in the text.

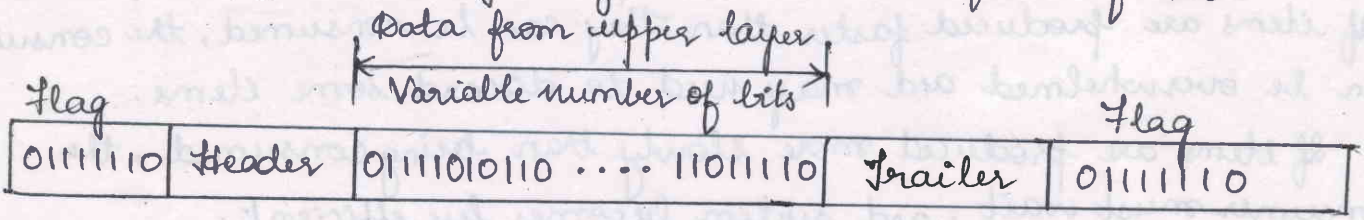


BYTE STUFFING AND UNSTUFFING.

(ii) Bit-Oriented Framing:

In bit-oriented framing, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video and so on. In addition to headers, a delimiter to separate one from another is needed.

Most protocols use a special 8-bit pattern flag, 01111110, as a delimiter to define the beginning and the end of the frame.



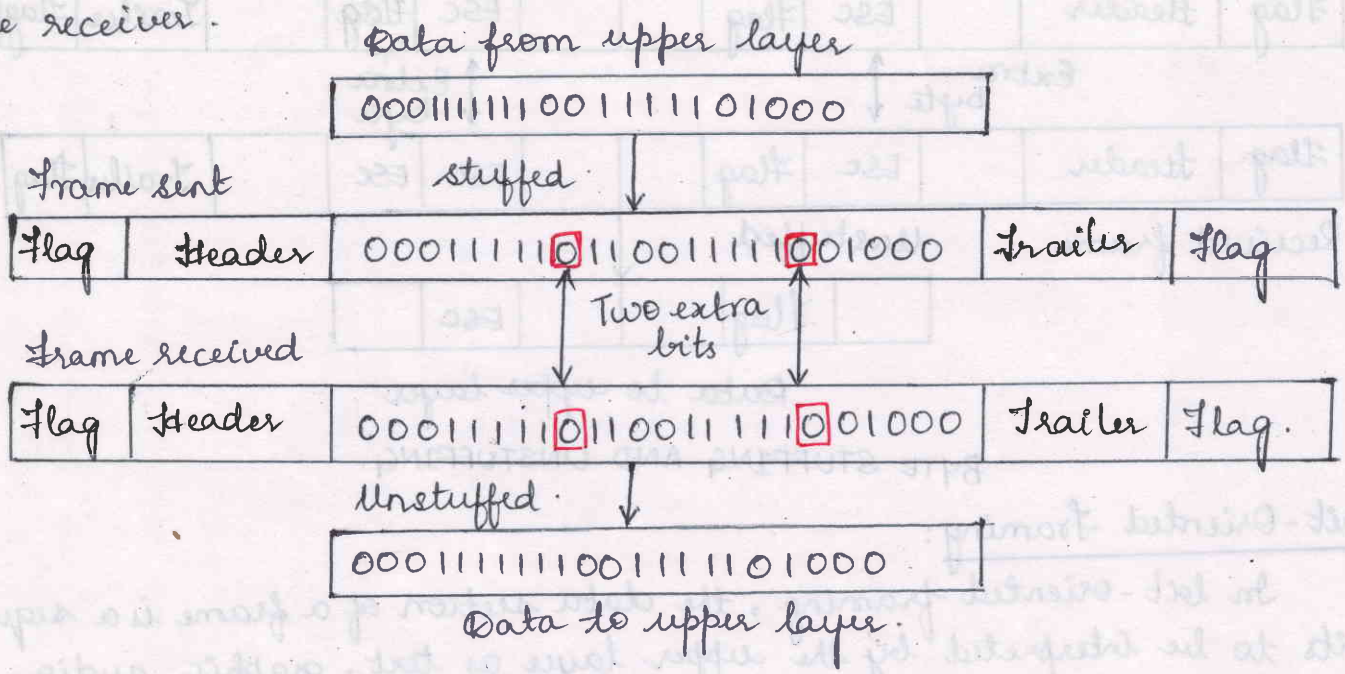
If the flag pattern appears in the data, the receiver must be informed that this not the end of the frame.

So to overcome this, bit stuffing (stuffing 1 single bit instead of 1 byte) is done to prevent the pattern from looking like a flag.

Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 01111110 for a flag.

The figure shows bit stuffing at the sender and bit removal at the receiver.

If a flaglike pattern 01111110 appears in the data, it will change to 011111010 (stuffed) and is not mistaken for a flag by the receiver. The real flag 01111110 is not stuffed by the sender and is recognized by the receiver.



Flow and Error Control :-

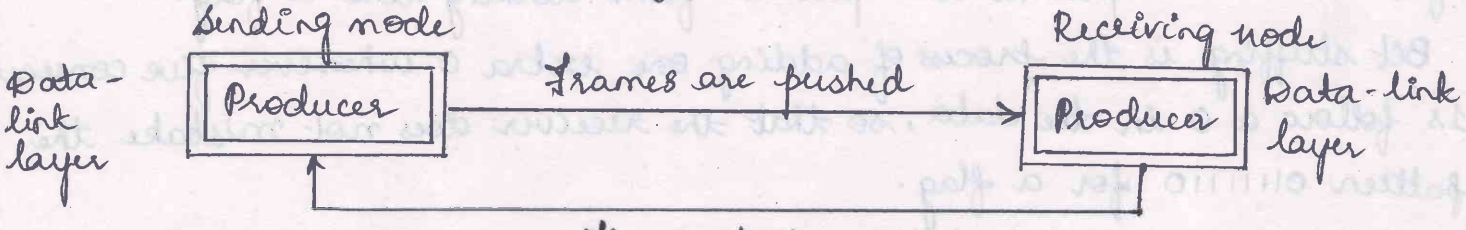
Flow Control :

When an entity produces items and another entity consumes them, there should be a balance between production and consumption rates.

If items are produced faster than they can be consumed, the consumer can be overwhelmed and may need to discard some items.

If items are produced more slowly than being consumed, the consumer must wait, and system becomes less efficient.

In communication at the data-link layer, there are four entities: network and data-link layers at the sending node and network and data-link layers at the receiving node.



The figure shows that the data-link layer at the sending node tries to push frames towards the data-link layer at the receiving end/node. If the receiving end cannot process and deliver the packet to its network at the same rate that the frames arrive, it becomes overwhelmed with frames.

Flow control in this case can be feedback from the receiving node to the sending node to stop or slow down pushing frames.

Buffers:

Flow control can be implemented in many ways, one such solution is to use two buffers; One at the sending data-link layer and the other at the receiving data-link layer.

A buffer is a set of memory locations that can hold packets at the sender and receiver.

The flow control communication can occur by sending signals from the consumer to the producer. When the buffer of receiving data-link layer is full, it informs the sending data-link layer to stop pushing frames.

Error Control:

Since the underlying technology at the physical layer is not fully reliable, error control needs to be implemented at the data-link layer to prevent the receiving node from delivering corrupted packets do its network layer

Error control at the data-link layer is normally very simple and implemented using one of the following methods; in both the cases a CRC is added to the frame header by the sender and checked by the receiver.

(i) In first method; if the frame is corrupted, it is silently discarded, if it is not corrupted, the packet is delivered to the network layer. This method is used mostly in wired LANs such as Ethernet.

(ii) In second method; if the frame is corrupted, it is silently discarded; if it is not corrupted, an acknowledgement is sent (for the purpose of both flow and error control) to the sender.

Combination of Flow and Error Control:

Flow and error control can be combined. In a simple situation; the acknowledgement that is sent for flow control can be used for error control to tell the sender the packet has arrived uncorrupted.

The lack of acknowledgement means that there is a problem in the sent frame.

A frame that carries an acknowledgement is normally called an ACK to distinguish it from the data frame.

DATA-LINK LAYER PROTOCOLS:-

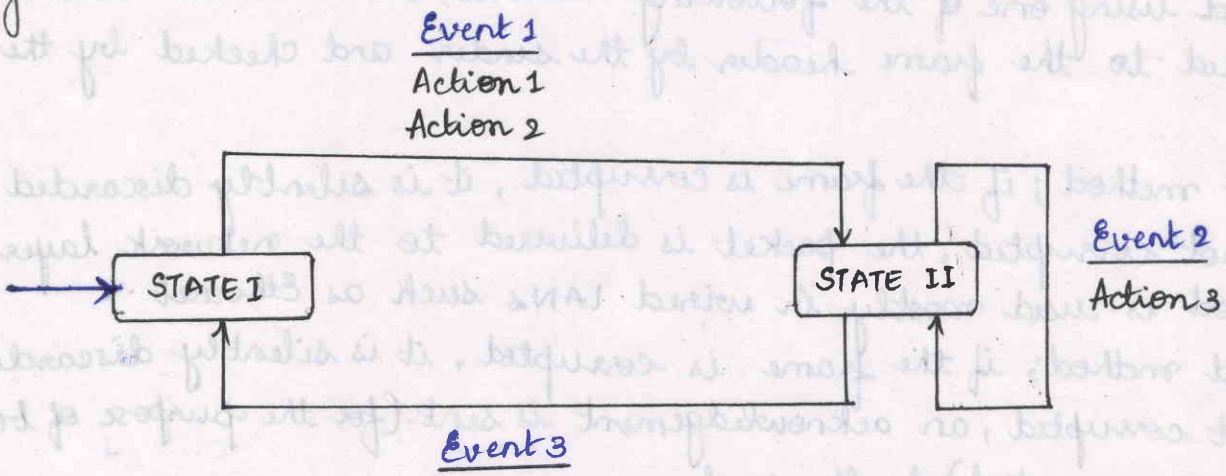
SIMPLE PROTOCOL and STOP & WAIT PROTOCOL

The behavior of a data-link layer protocol can be shown as a finite state machine (FSM). An FSM is thought of as machine with a finite number of states

The machine is always in one of the states until an event occurs. Each event is associated with two reactions : defining the list (possibly empty) of actions to be performed and determining the next state (which can be the same as the current state).

One of the states must be defined as the initial state, the state in which the machine starts when it turns on. The figure shows an example of a machine using FSM.

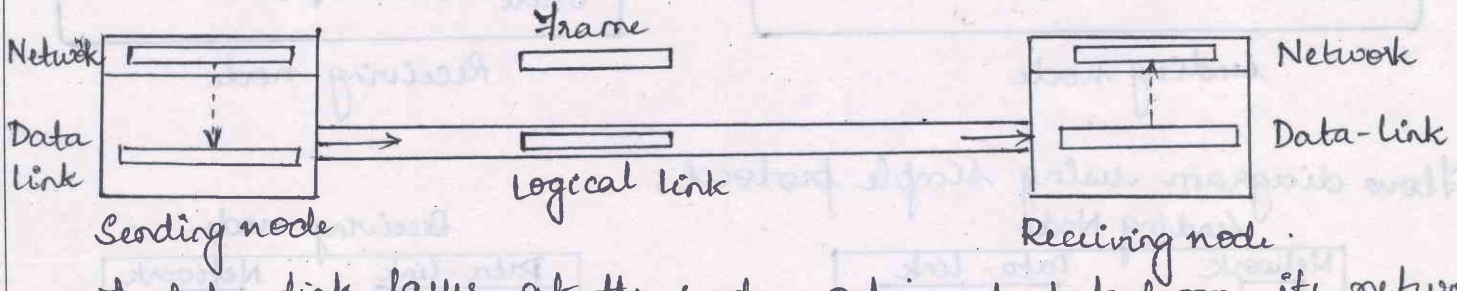
Rounded-rectangular blocks show states, horizontal line is used to separate the event from actions, colored text show events and regular black text shows actions.



The figure shows a machine with three states. The are only three possible events and three possible actions. The machine starts in state 1 occurs, the machine performs actions 1 and 2 and moves to state 2. When the machine is in state 2, two events may occur. If event 1 occurs, the machine performs action 3 and remains in the same state, state 2. If event 3 occurs, the machine performs no action, but move to state 1.

Simple Protocol :-

Simple Protocol does not have neither flow nor error control. Assume that the receiver can immediately handle any frame it receives. i.e. the receiver can never be ~~over~~ overwhelmed with incoming frame The figure shows the layout for this protocol.



The data-link layer at the sender gets a packet from its network layer, makes a frame of it and sends the frame.

The data-link layer at the receiver receives a frame from the link, extracts the packet from the frame, and delivers the packet to its network layer. The data-link layers of the sender and receiver provide transmission services for their network layers.

FSMs for the simple protocol:

The sender site should not send a frame until its network layer has a message to send. The receiver site cannot deliver a message to its network layer until a frame arrives. We can depict it using 2 FSMs

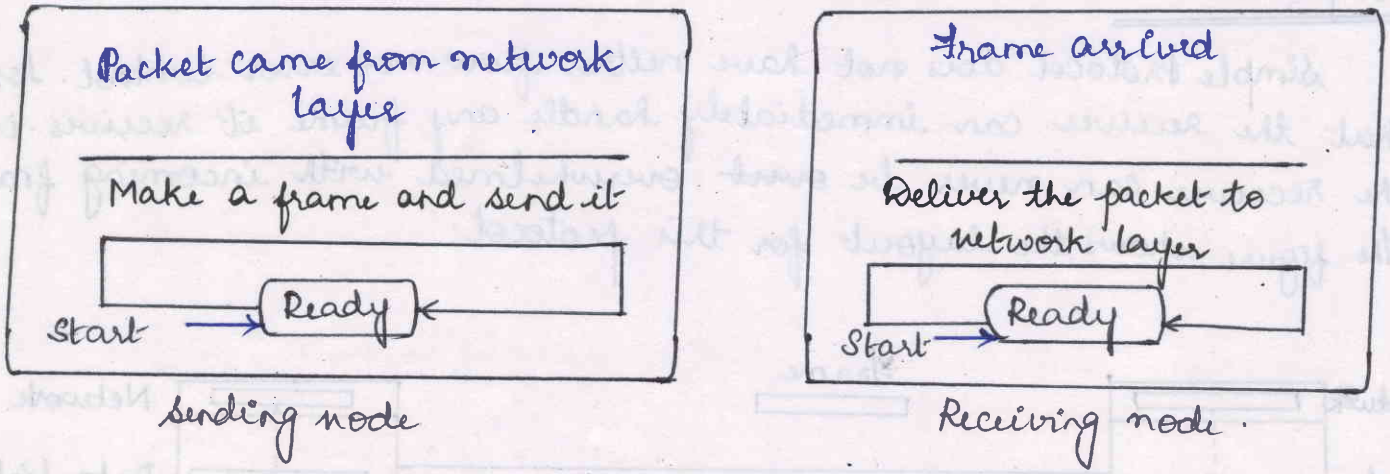
Each FSM has only one state, the 'ready' state. The sending machine remains in the ready state until a request comes from the process in the network layer.

when this event occurs, the sending machine encapsulates the message in a frame and sends it to the receiving machine.

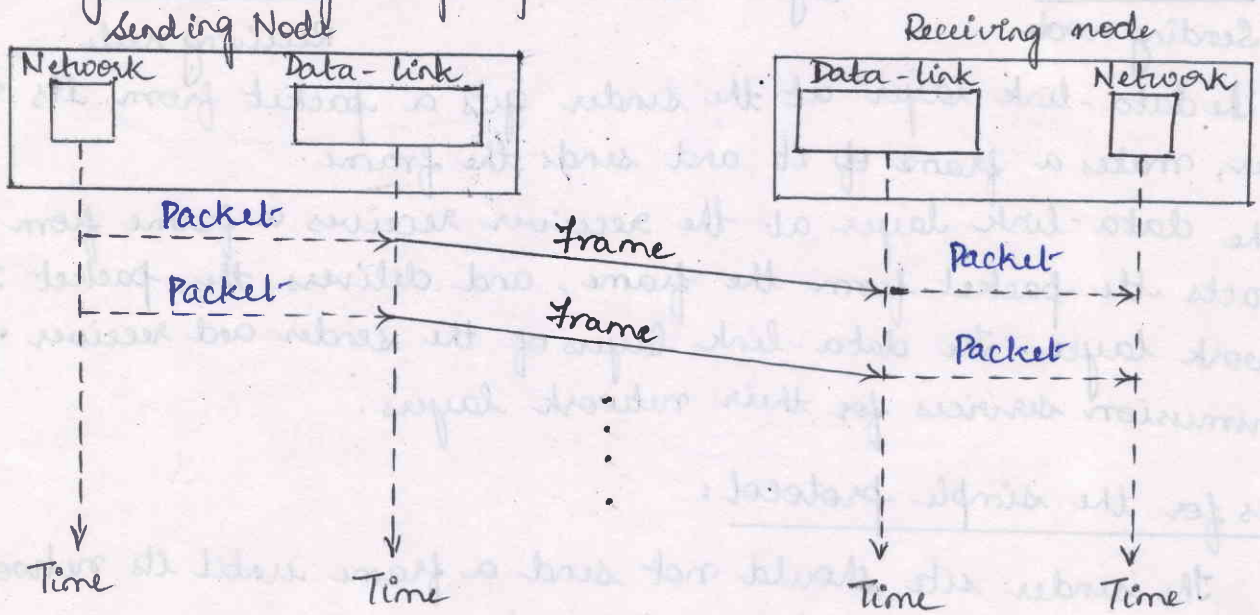
The receiving machine remains in the ready state until a frame arrives from the sending machine.

When this event occurs, the receiving machine decapsulates the message out of the frame and delivers it to the process at the network layer.

Figure shows the FSM of simple protocol.



Flow diagram using simple protocol;



(P.T.O)

Stop and Wait Protocol :

(i) Stop and wait protocol uses both flow and error control. In this protocol, the sender sends one frame at a time and waits for an acknowledgement before sending the next one.

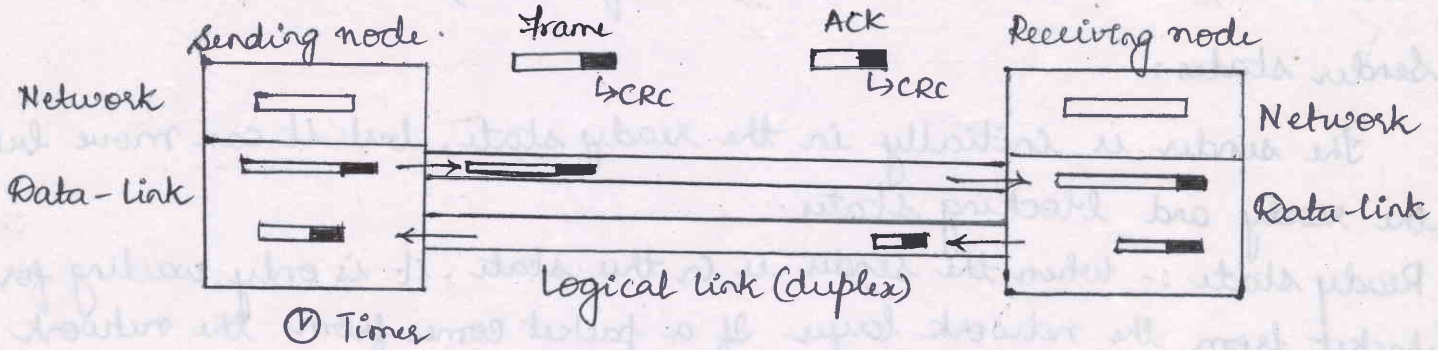
(ii) To detect corrupted frames, we need to add CRC to each data frame. When a frame arrives at the receiver site, it is checked. If its CRC is incorrect, the frame is corrupted and silently discarded.

(iii) The silence of the receiver is a signal for the sender that a frame was either corrupted or lost.

(iv) Every time the sender sends a frame, it starts a timer. If an acknowledgement arrives before the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted.

(v) This means the sender needs to keep a copy of the frame until its acknowledgement arrives. When the corresponding acknowledgement arrives, the sender discards the copy and sends the next frame if it is ready.

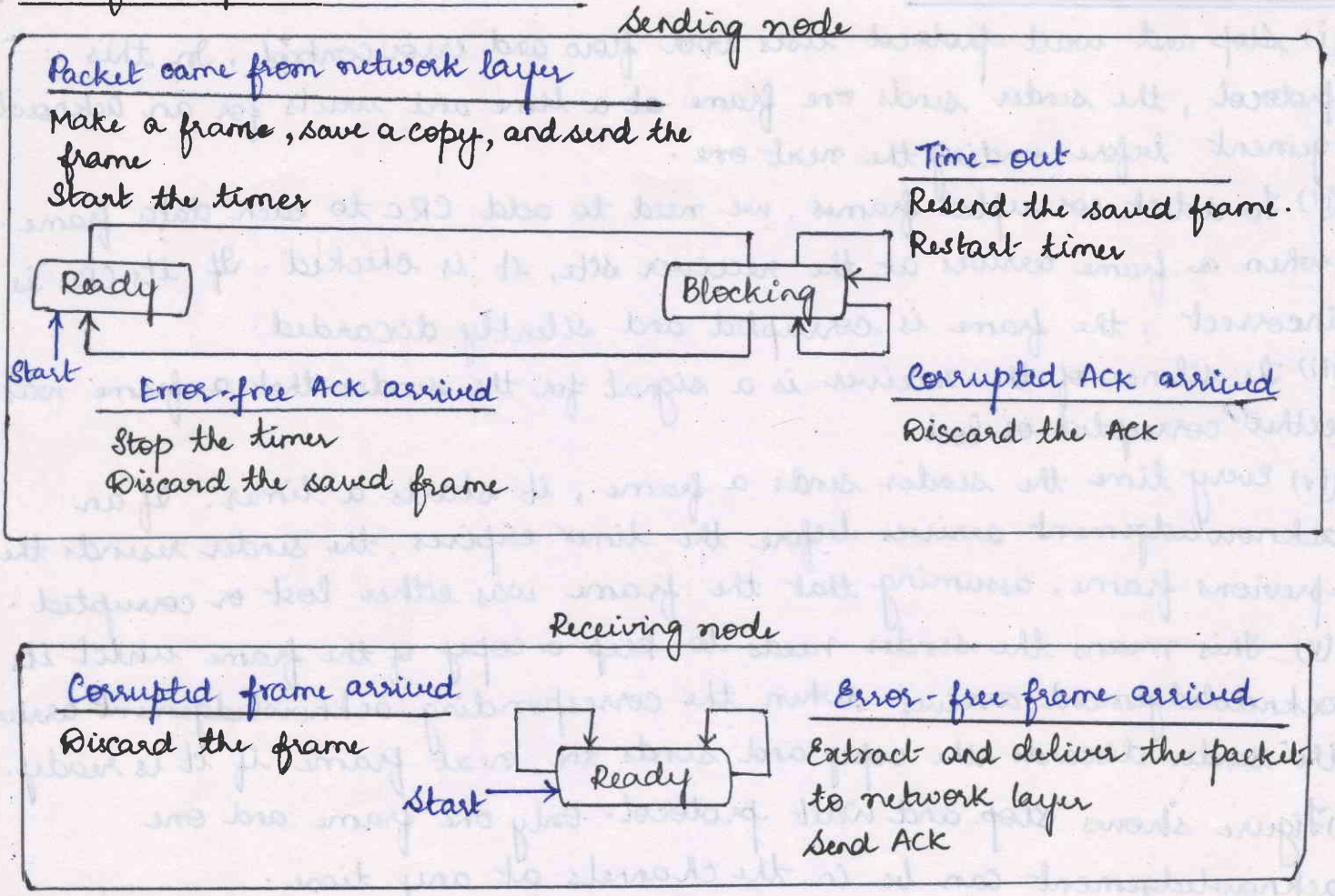
(vi) Figure shows Stop and Wait protocol. Only one frame and one acknowledgement can be in the channels at any time.



The FSM for primitive Stop and wait protocol is shown;

(P.T.O.)

FSM for Stop and Wait Protocol:



The sender and receiver states are as follows;

Sender states:

The sender is initially in the ready state, but it can move between the ready and blocking states.

Ready state :- When the sender is in this state, it is only waiting for a packet from the network layer. If a packet comes from the network layer, the sender creates a frame, sends a copy of the frame, starts the only timer and sends the frame. The sender then moves to the blocking state.

Blocking state :- When the sender in this state, three events can occur.

(i) If a time-out occurs, the sender resends the saved copy of the frame and restarts the timer

(ii) If a corrupted ACK arrives, it is discarded.

(iii) If an error-free ACK arrives, the sender stops the timer and discards

the saved copy of the frame. It then moves to the ready state

Receiver States:

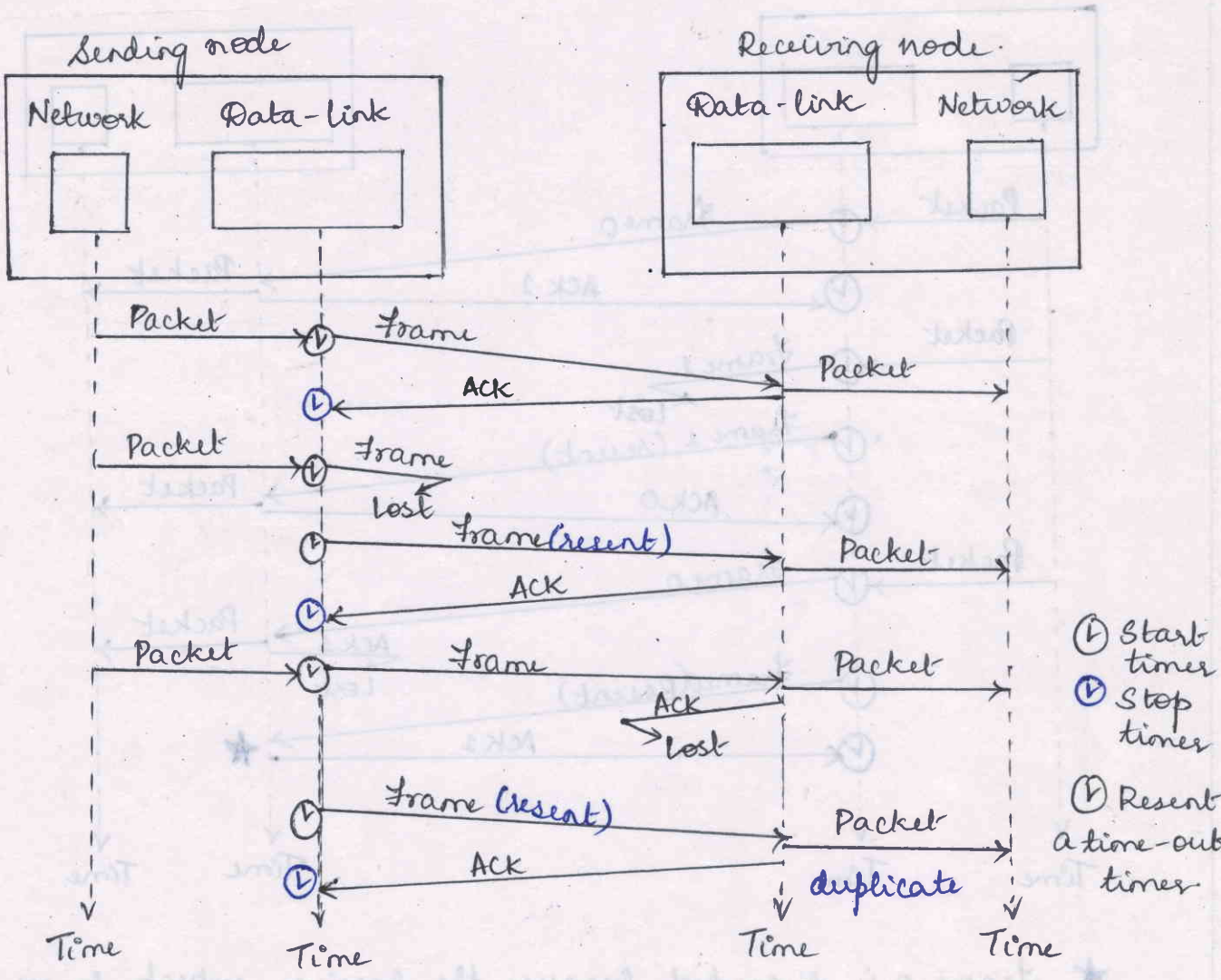
The receiver is always in the ready state. Two events may occur.

(i) If an error-free frame arrives, the message in the frame is delivered to the network layer and an ACK is sent.

(ii) If a corrupted frame arrives, the frame is discarded.

Ex:- The figure shows an example. The first frame is sent and acknowledged. The second frame is sent, but lost. After time-out, it is resent. The third frame is sent and acknowledged, but the acknowledgement is lost. The frame is resent.

The problem with this scheme is, at the network layer in receiver site receives two copies of the third packet, which is not right.

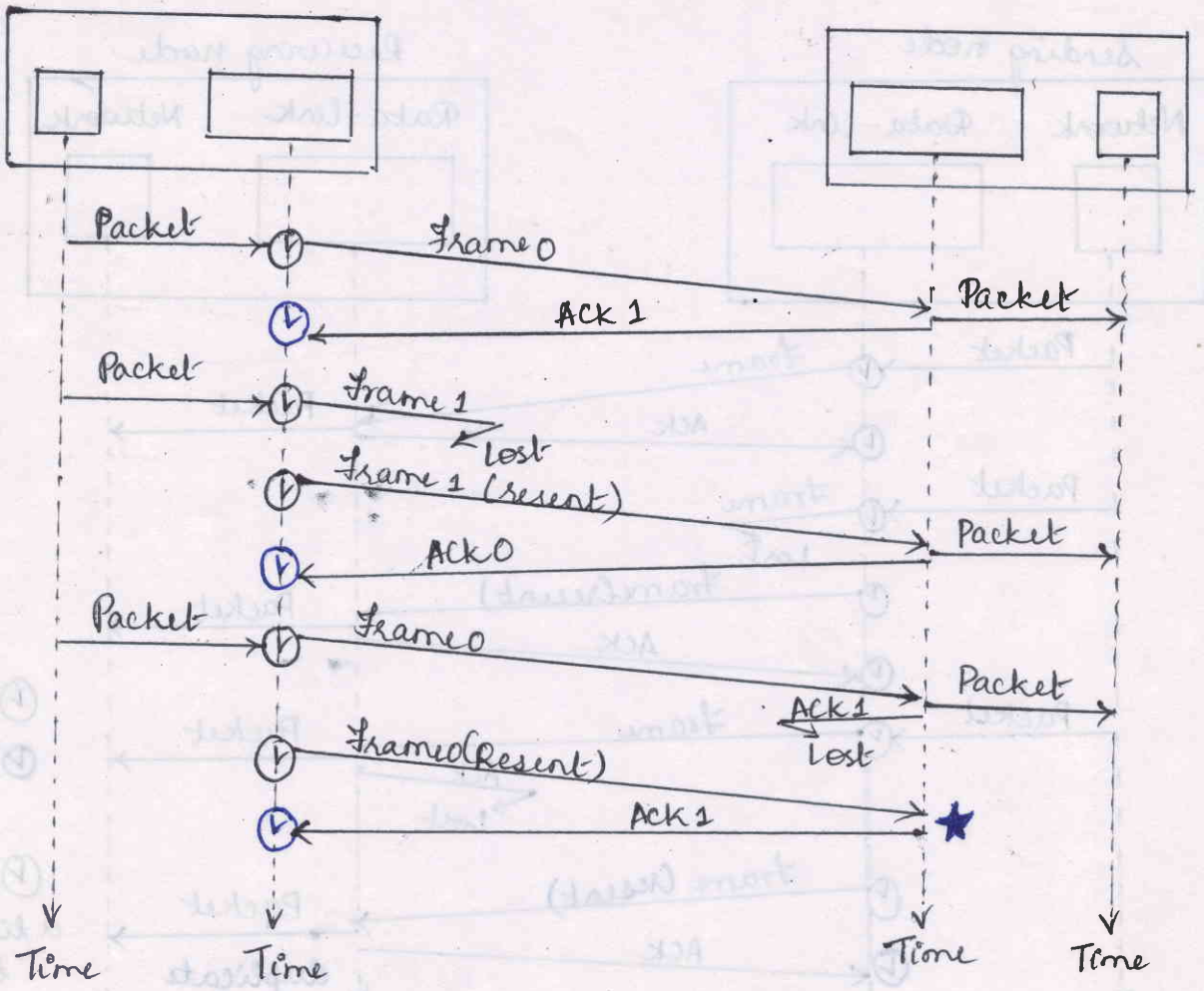


Sequence and Acknowledgement Numbers :-

The problem from earlier example needs to be addressed and corrected. Duplicate packets, as much as corrupted packets, needs to be avoided. To correct this problem, we need to add sequence numbers to the data frames and acknowledgement numbers to the Ack frames. Numbering is very simple, sequence numbers are 0, 1, 0, 1, 0, 1 .....; acknowledgement numbers can be 1, 0, 1, 0, 1 .....;

The sequence numbers start with 0, the acknowledgement numbers start with 1. An acknowledgement number always defines the sequence number of the next frame to receive.

FMS with sequence and acknowledgement numbers:



★ Frame 0 is discarded because the receiver expects frame 1

Piggybacking :-

The previous protocols are designed for unidirectional communication, in which data is flowing only in one direction although the acknowledgement may travel in other direction.

To make communication more efficient, the data in one direction is piggybacked with the acknowledgement in the other direction.

When a node A is sending data to node B, Node A also acknowledges the data received from node B.

Piggybacking makes communication at the data-link layer more complicated.

Module: 2

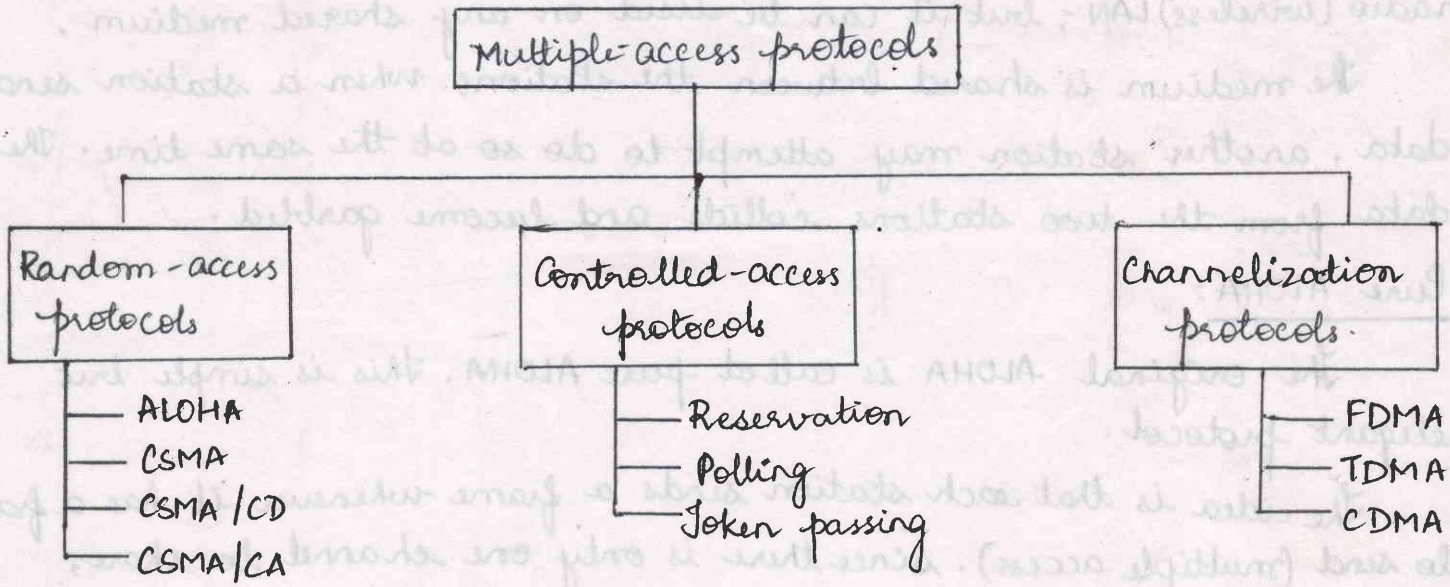
Media Access Control: Random Access: ALOHA, CSMA, CSMA/CD, CSMA/CA. Controlled Access: Reservation, Polling, Token Passing.

Wired LANs: Ethernet: Ethernet Protocol: IEEE802, Ethernet Evolution, Standard Ethernet: Characteristics, Addressing, Access Method, Efficiency, Implementation, Fast Ethernet: Access Method, Physical Layer, Gigabit Ethernet: MAC Sublayer, Physical Layer, 10 Gigabit Ethernet. **L1, L2**

MEDIA ACCESS CONTROL:

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.

Many protocols have been devised to handle access to shared link. All of these protocols belong to a sublayer in the data-link layer called media access control (MAC).



RANDOM ACCESS:-

In random-access or contention methods, no station is superior to another station and none is assigned control over another. 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).

The two features of this methods are;

(i) There is no scheduled time for a station to transmit. Transmission is random among the stations. Hence it is called random access.

(ii) No rules specify which station should send next. Stations compete with one another to access the medium. Hence it is also called contention methods.

In random-access method, each station has the right to the medium without being controlled by any other station. If more than one station tries to send, there is an access conflict - collision, and the frames will be either destroyed or modified. To resolve this each station follows a procedure.

ALOHA:

ALOHA is an earliest random access method. It is designed for a radio (wireless) LAN, but it can be used on any shared medium.

The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

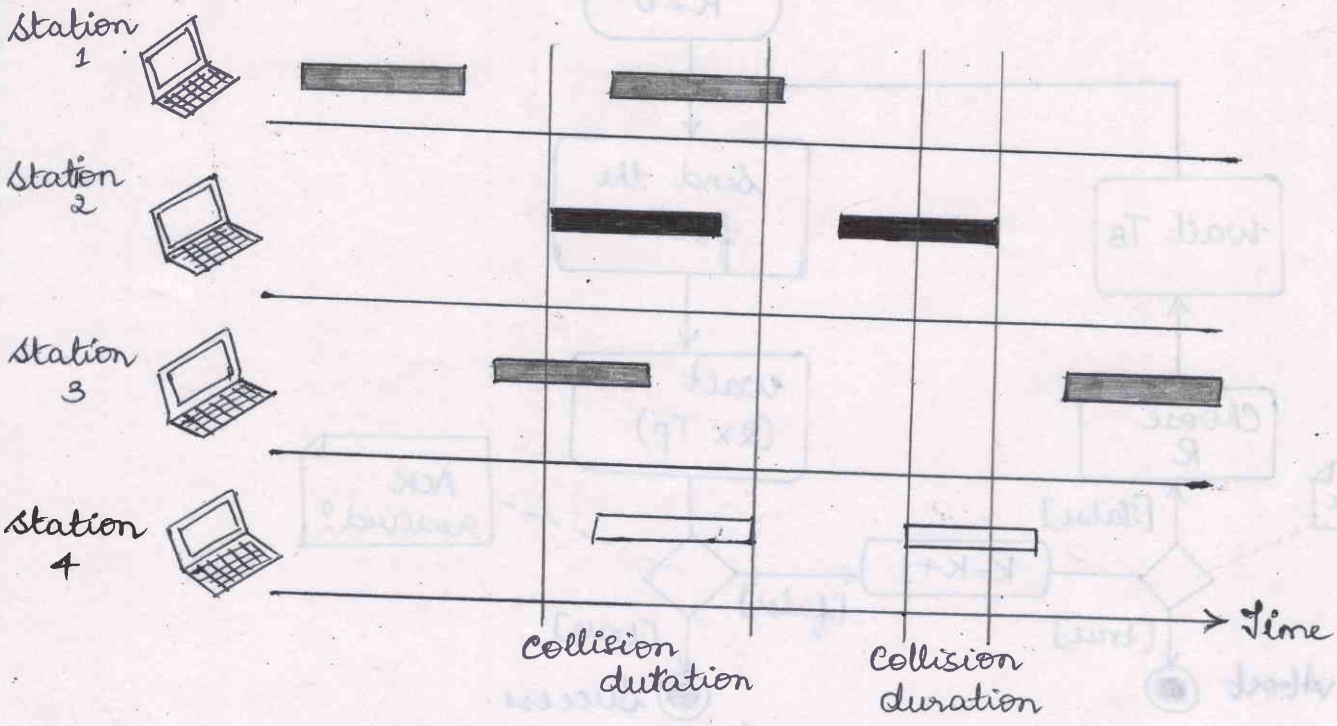
Pure ALOHA:

The original ALOHA is called pure ALOHA. This is simple but elegant protocol.

The idea is that each station sends a frame whenever it has a frame to send (multiple access). Since there is only one channel to share, there is the possibility of collision between frames from different stations. The figure shows the example of frame collisions in pure ALOHA.

There are four stations that contend with one another for access to the shared channel. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention

for a shared medium. The figure also shows that only two frames survive; one frame from station 1 and one from station 3. Even if one bit of a frame coexists on the channel with one bit from another frame, there is a collition and both will be destroyed. So the frames which are destroyed during collision should be resent.



FRAMES IN A PURE ALOHA NETWORK.

The pure ALOHA protocol relies on acknowledgements from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgement.

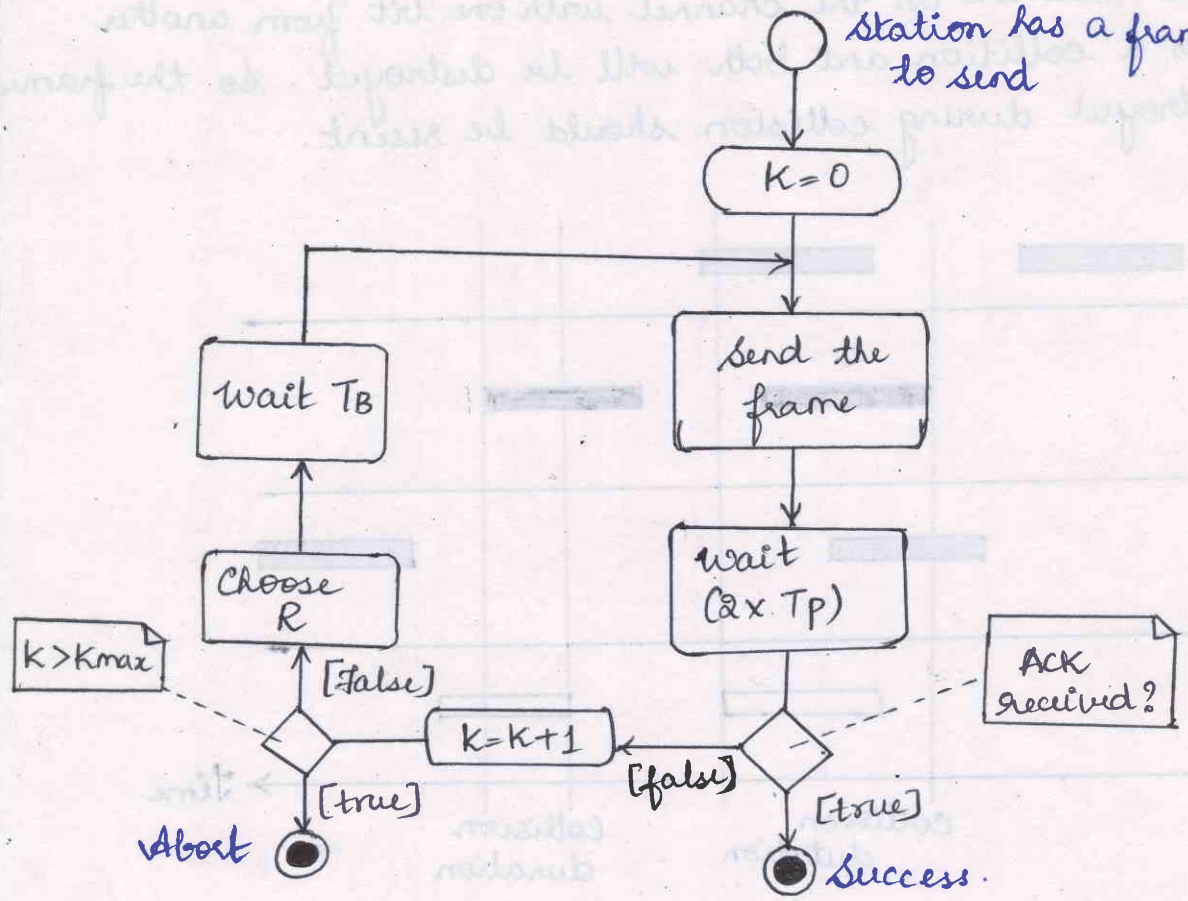
If the acknowledgement does not arrive after a time-out period, the station assumes that the frame (acknowledgement) has been destroyed and resends the frame.

A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again.

Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid further collisions. The time is called the backoff time 'TB'.

Pure ALOHA has another method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission

attempts Kmax, a station must give up and try later. The figure shows the procedure for pure ALOHA based on the strategy.



where; K = Number of attempts
Tp = Maximum propogation time.
Tfr = Average transmission time.
TB = Backoff time = R x Tp or R x Tfr.
R = Random number = 0 to $2^K - 1$

The time-out period is equal to maxium possible round-trip propogation delay, which is twice the amount of time required to send a frame between the two most widely separated stations (2 x Tp).

The backoff time TB is a random value that normally depends on K (the number of attempted unsuccessful transmissions). The formula for TB depends on the implementation. The most common is binary exponential backoff. In this method, for each retransmission, a multiplier R = 0 to $2^K - 1$ is randomly choosen and multiplied by Tp (maximum propogation time) or Tfr (the average time required to send out a frame) to find TB. The range of random numbers increases after each collision; value of Kmax = 15

Ex:-

1) The stations on a wireless ALOHA network are a maximum of 600 km apart. If we assume that the signal propogate at 3×10^8 m/s.

we can find $T_p = (600 \times 10^3) / (3 \times 10^8) = 2$ ms.

For $k = 2$; the range of R is $\{0, 1, 2, 3\}$

$\therefore T_B$ can be $= R \times T_p$.

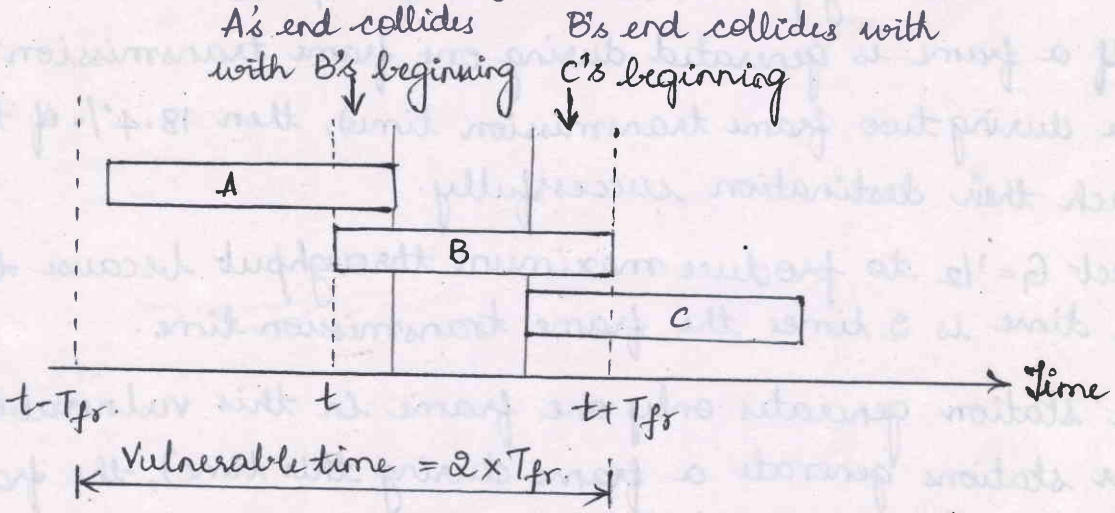
$\therefore T_B = 0, 2, 4$ and 6 ms. based on outcome of random variable.

$R = 0$ to $2^k - 1$.
$(R = 0$ to $4)$ at $k = 2$.
$R = 2^2 - 1 = 4$

Vulnerable time :-

To find the vulnerable time, the length of time in which there is a possibility of collision.

We assume that the stations send fixed length frames with each frame taking T_{fr} seconds to send. Figure shows the vulnerable time of station B



Station B starts to send a frame at time t. If station A has started to send its frame after $(t - T_{fr})$. This leads to a collision between the frames from station B and station A. If station C starts to send a frame before time $(t + T_{fr})$, there is a collision between frames of station B and station C

From the figure, the vulnerable time during which a collision may occur in pure ALOHA is 2 times the frame transmission time.

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

Ex:- A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?.

Average frame transmission time T_{fr} = 200 bits / 200kbps = 1ms.

Vulnerable time is = $2 \times T_{fr}$ = 2 x 1ms = 2ms.

This means no station should send later than 1ms before this station starts transmission and no station should start sending during the period (1ms) that this station is sending.

Throughput :-

The average number of frames generated by the system during one frame transmission time is G.

Then it can be proven that the average number of successfully transmitted frames for pure ALOHA is $S = G \times e^{-2G}$.

The maximum throughput S_{max} is 0.184 for G = 1/2

If one-half a frame is generated during one frame transmission time (one frame during two frame transmission times), then 18.4% of these frames reach their destination successfully.

We expect G = 1/2 to produce maximum throughput because the vulnerable time is 2 times the frame transmission time.

∴ If a station generates only one frame in this vulnerable time (and no other stations generate a frame during this time), the frame will reach its destination successfully.

The throughput for pure ALOHA is $S = G \times e^{-2G}$

The maximum throughput $S_{max} = 1/(2e) = 0.184$ when $G = (1/2)$

Ex:- A pure ALOHA network transmits 200-bits frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

(a) 1000 frames / second.

(b) 500 frames / second

(c) 250 frames / second.

The frame transmission time is $T_{fr} = 200/200\text{kbps} = 1\text{ms}$.

(a) If system creates 1000 frames/second; or 1 frame per millisecond
Then $G = 1$.

$$\text{Throughput} \Rightarrow S = G \times e^{-2G} = 1 \times e^{-2}$$
$$S = 0.135 \text{ or } 13.5\%.$$

This means that the throughput is $1000 \times 0.135 = 135$ frames
Only 135 frames out of 1000 will survive.

(b) If system creates 500 frames per second; or 1/2 frame per millisecond, then $G = 1/2$

$$\text{Then } S = G \times e^{-2G} = 0.184 \ (18.4\%)$$

This means that the throughput is $500 \times 0.184 = 92$ frames
Only 92 frames out of 500 will probably survive.
(This is the maximum throughput case, percentagewise).

(c) If the system creates 250 frames per second; or 1/4 frame per millisecond; then $G = 1/4$.

$$S = G \times e^{-2G} = 0.152 \ (15.2\%).$$

The throughput is $250 \times 0.152 = 38$ frames
Only 38 frames out of 250 will survive.

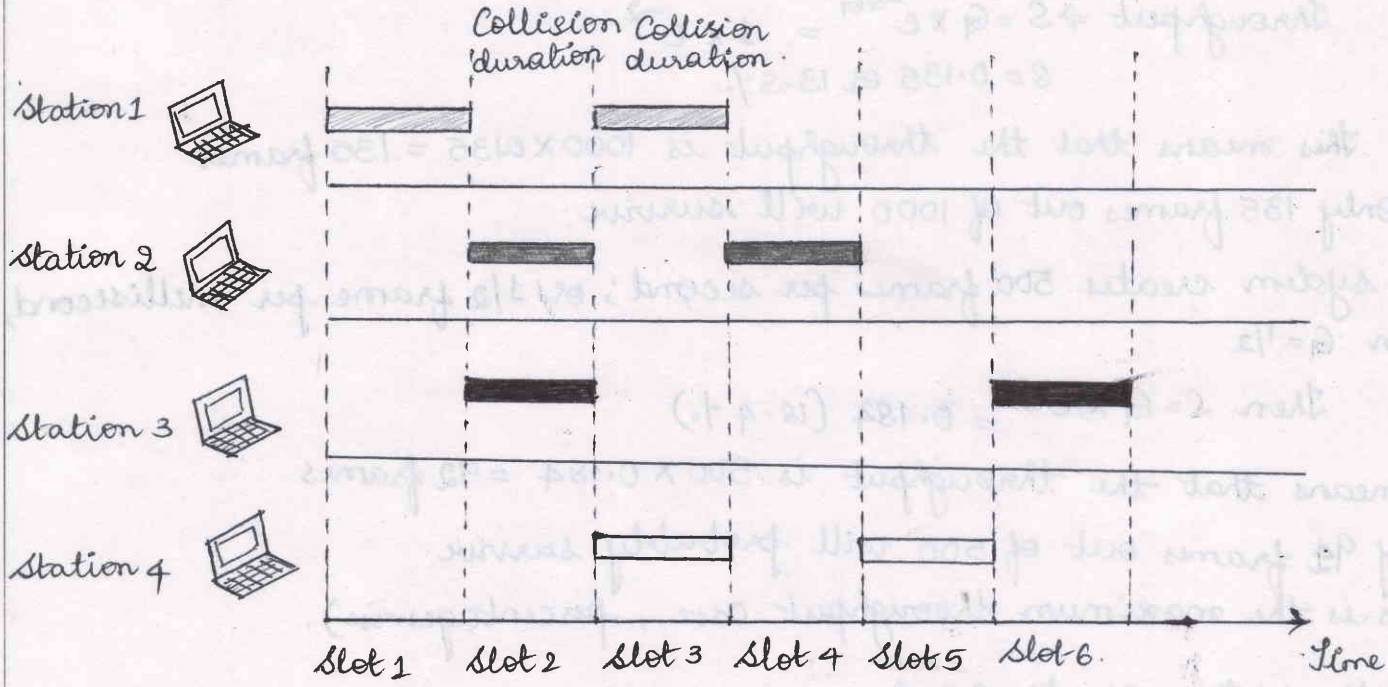
Slotted ALOHA :-

Pure ALOHA has a vulnerable time of $2 \times T_{fr}$. This is because there is no rule that defines when a station can send. A station may send soon after another station has started or just before another station has finished.

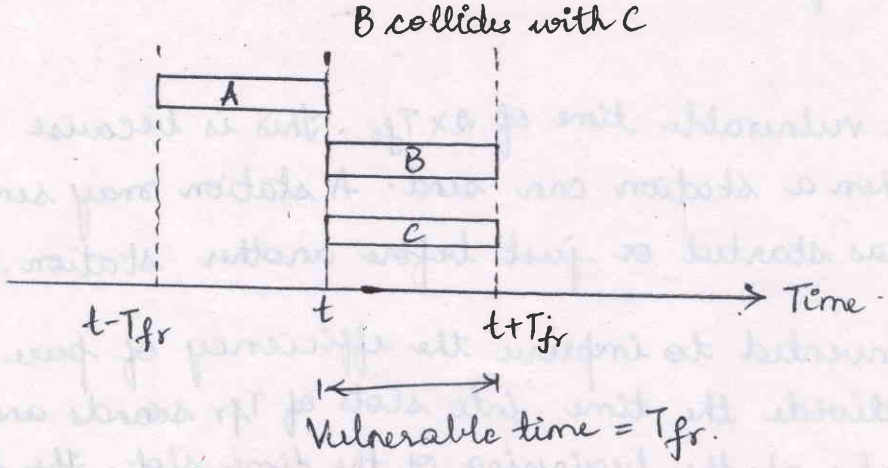
Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA we divide the time into slots of T_{fr} seconds and force the station to send only at the beginning of the time slot. The figure shows an example of frame collisions in slotted ALOHA.

(P.T.O)

Since a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot.



The station which started at the beginning of this slot has already finished sending its frame. 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 reduced to one-half, equal to T_{fr}.



Slotted ALOHA vulnerable time = T_{fr}

Throughput :-

The average number of successful transmissions for slotted ALOHA is $S = G \times e^{-G}$. The maximum throughput S_{max} is 0.368, when $G = 1$. If one frame is generated during one frame transmission time, then 36.8% of these frame reach their destination successfully.

$G = 1$ produces maximum throughput because the vulnerable time is equal to the frame transmission time.

If a station generates only one frame in this vulnerable time (and no other station generates a frame during this time), the frame will reach its destination successfully.

> The throughput of slotted ALOHA is $S = G \times e^{-G}$
> The maximum throughput $S_{max} = 0.368$ when $G = 1$

Ex:- A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200 kbps bandwidth. Find the throughput if the system (all stations together) produces

(a) 1000 frames/sec (b) 500 frames/sec (c) 250 frames/sec

The frame transmission time is 200/200kbps = 1 ms.

(a) $G = 1$ ∵ 1000 frames/sec = 1 frame/msec.

Throughput is given by;

$$S = G \times e^{-G} = 0.368 \ (36.8\%).$$

Throughput = $1000 \times 0.368 = 368$ frames.

Only 368 out of 1000 frames survive.

(b) 500 frames/sec = 1/2 frame/ms.

$$S = G \times e^{-G} = 0.303 \ (30.3\%).$$

Throughput = $500 \times 0.303 = 151$ frames.

Only 151 out of 500 frames survive.

(c) 250 frames/sec = 1/4 frame/ms ∴ $S = G \times e^{-G} = 0.195 \ (19.5\%)$

Throughput = $250 \times 0.195 = 49$ frames.

Only 49 out of 250 frames survive.

Carrier Sense Multiple Access [CSMA] :-

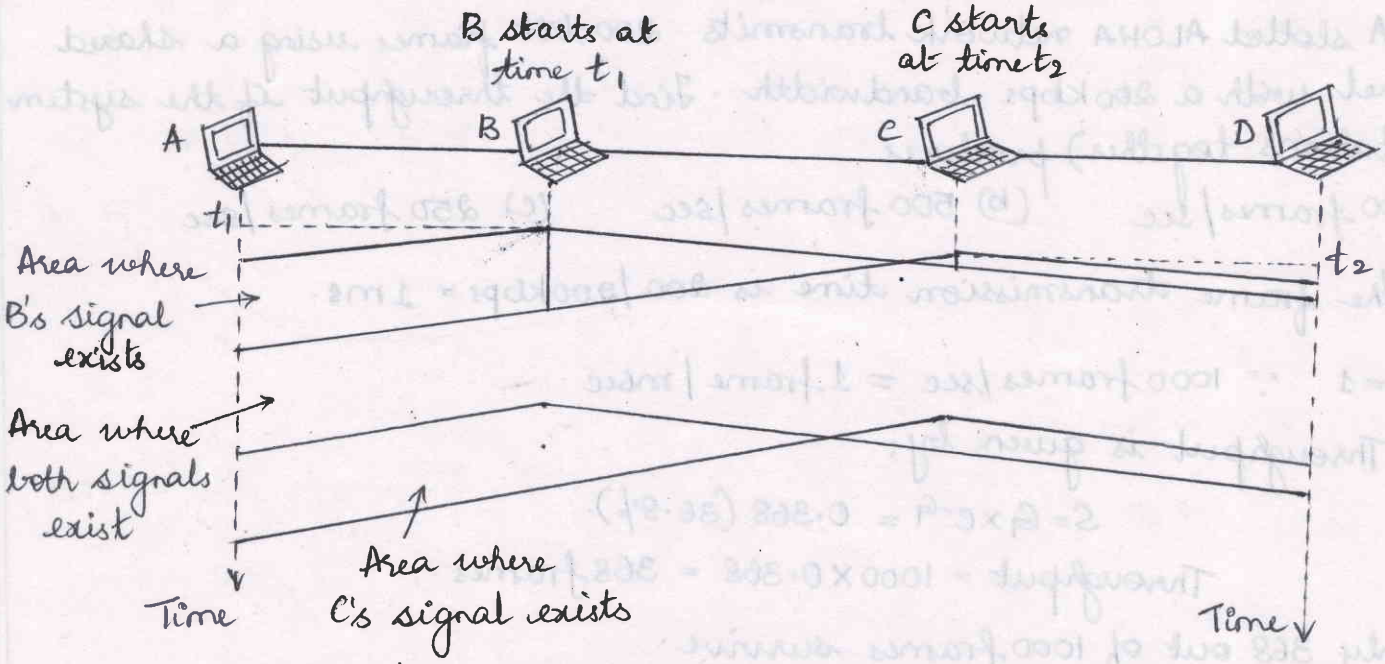
To minimize the chance of collision and to increase the performance the CSMA method was developed.

The chance of collision can be reduced if a station senses the medium before trying to use it.

Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.

CSMA is based on the principle "sense before transmit" or "listen before talk".

CSMA can reduce the possibility of collision, but it cannot eliminate it. The reason for this is shown in the figure; a space and time model of a CSMA network. Stations are connected to a shared channel.



SPACE/TIME MODEL OF A COLLISION IN CSMA.

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

A station may sense the medium and find it idle, only because the first bit sent by another station has not yet received.

At time t_1, station B senses the medium and finds it idle, so it sends a frame.

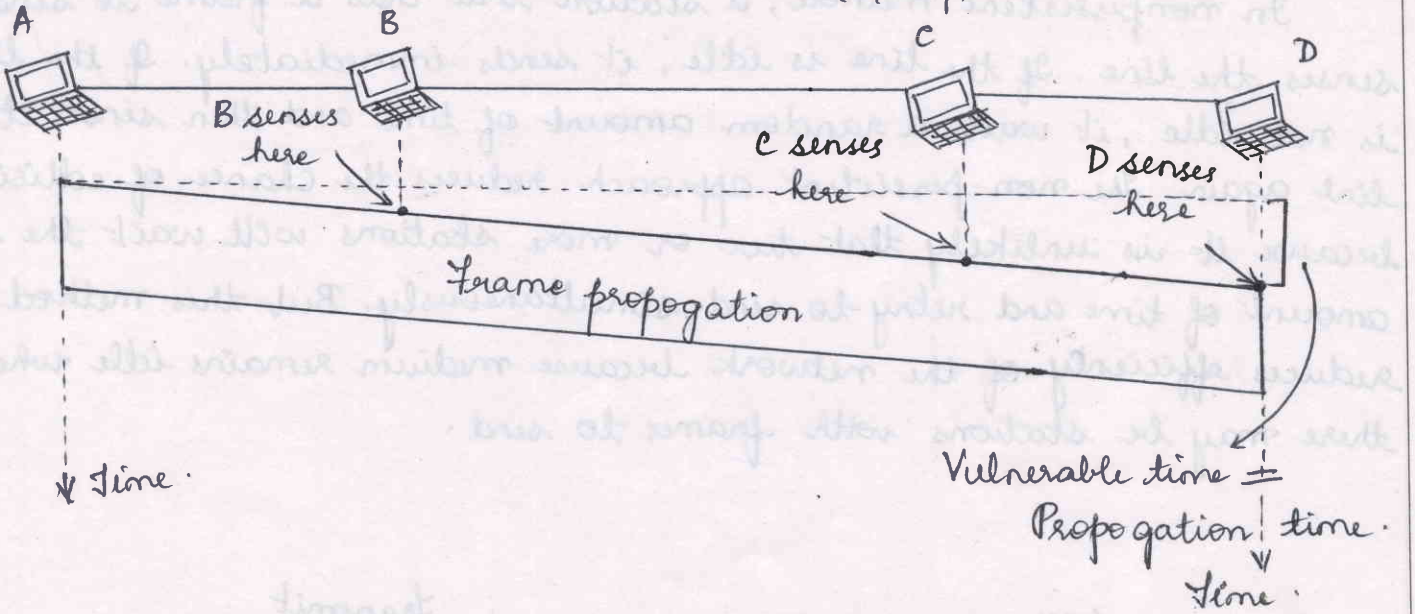
At time ($t_2 > t_1$), station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame. The two frames collide and are destroyed.

Vulnerable time:

The vulnerable time for CSMA is the propogation time (T_p). This is the time needed for a signal to propogate 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, it results in collision. But if the first bit of the frame reaches the end of the medium, every station would have heard the bit and will refrain from sending.

The figure shows the worst case; station A sends a frame at time t_1, which ~~results~~ reaches the station D at time ($t_1 + T_p$).



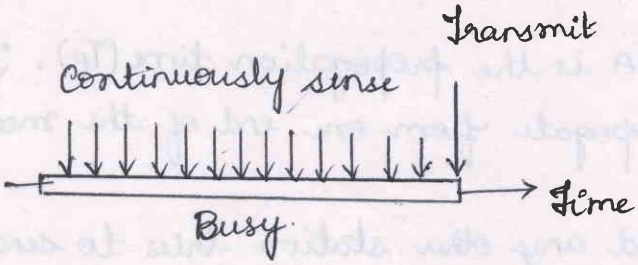
Persistence Methods:

If a ~~station~~ channel is busy or idle, what a station needs to do is devised using three methods;

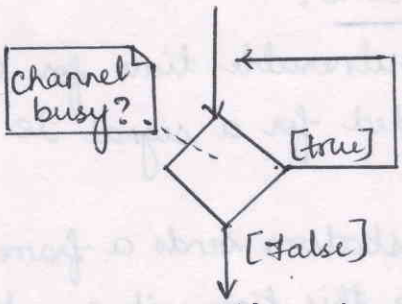
(i) 1-persistent method.
(ii) Non-persistent method.
(iii) p-persistent method.

(i) 1-Persistent Method:-

The 1-persistent method is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.



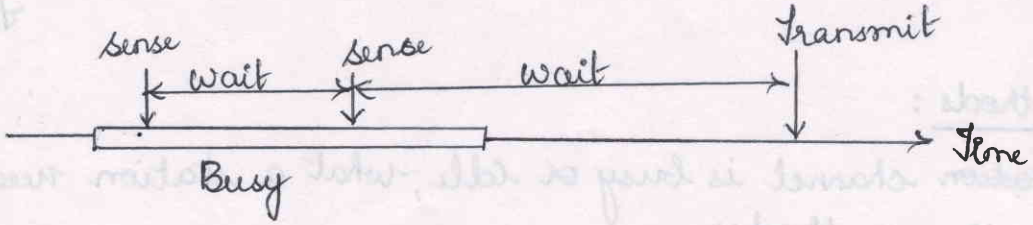
BEHAVIOR OF 1-PERSISTENT METHOD.



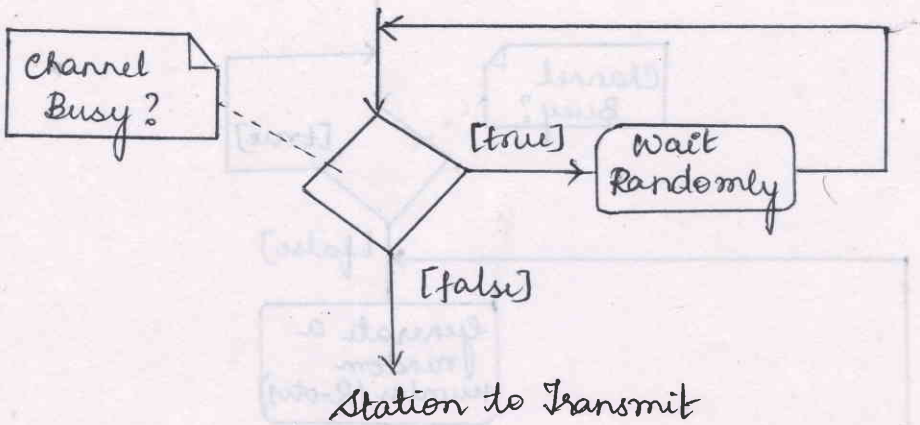
FLOW DIAGRAM.

(ii) Nonpersistant Method :-

In nonpersistent 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. The non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. But this method reduces efficiency of the network because medium remains idle when there may be stations with frames to send.



BEHAVIOR OF NONPERSISTENT METHOD.



FLOW DIAGRAM.

(iii) p-Persistent Method :-

The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propogation time. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency.

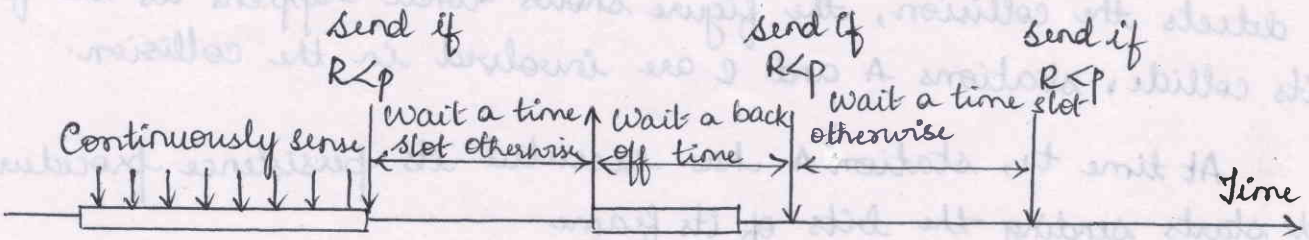
In this method, after the station finds the line idle it follows these steps;

(1) With probability p, the station sends its frame.

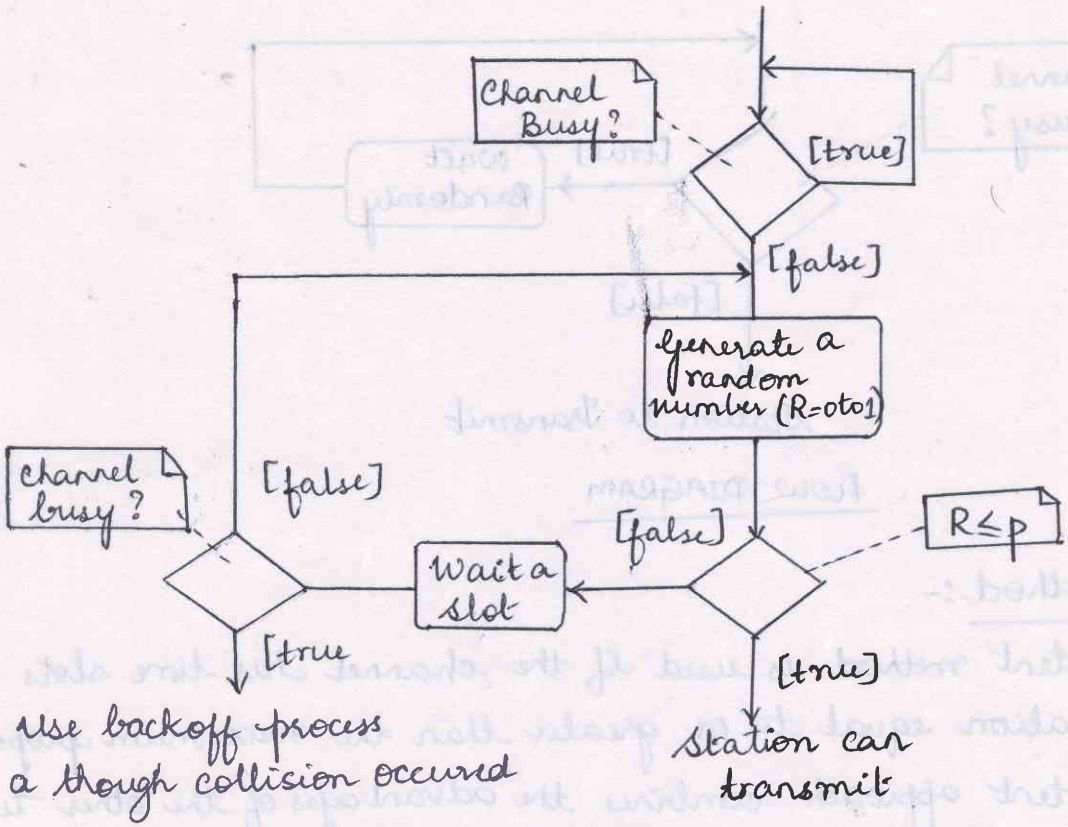
(2) With probability $q = 1-p$; the station waits for the beginning of the next time slot and checks the line again

(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 back-off procedure.



p-PERSISTENT METHOD.



FLOW DIAGRAM

CSMA/CD : Carrier Sense Multiple access with collision detection :-

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, there is a collision, the frame is sent again.

Each station ~~Continuous~~ continues to send bits in the frame until it detects the collision, the figure shows what happens as the first bits collide, stations A and C are involved in the collision.

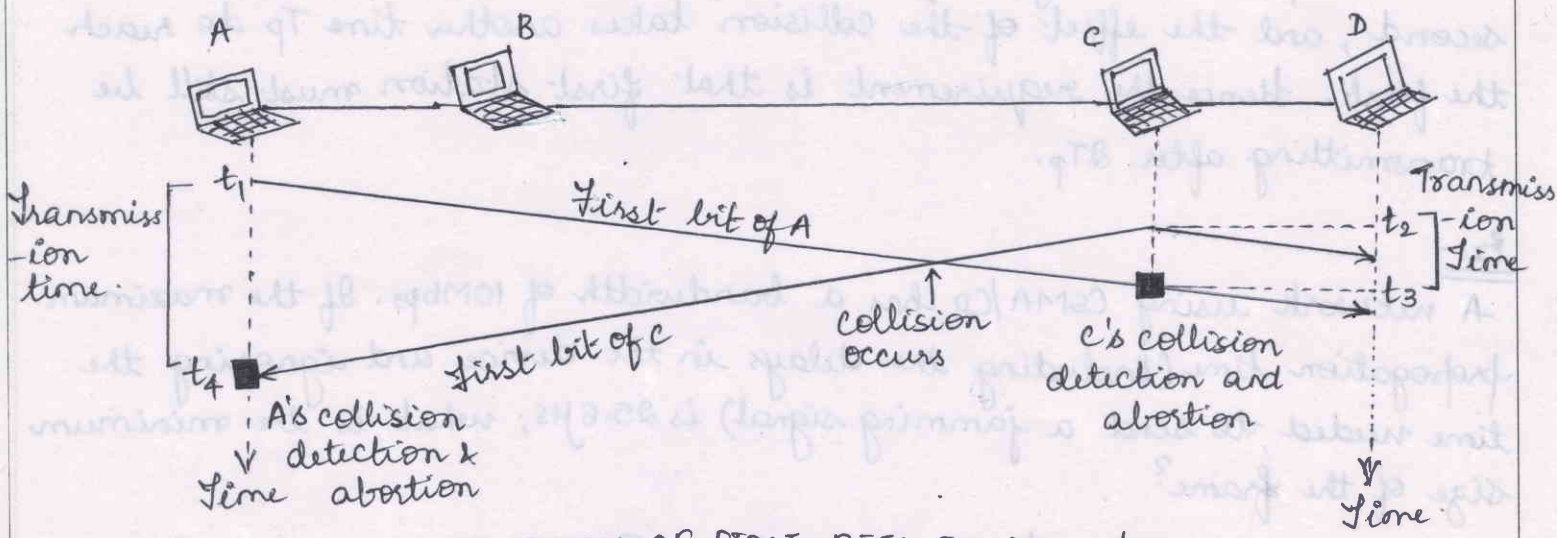
At time t_1, station A has executed its persistence procedure and starts sending the bits of its frame.

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 propogate both to the left and to the right.

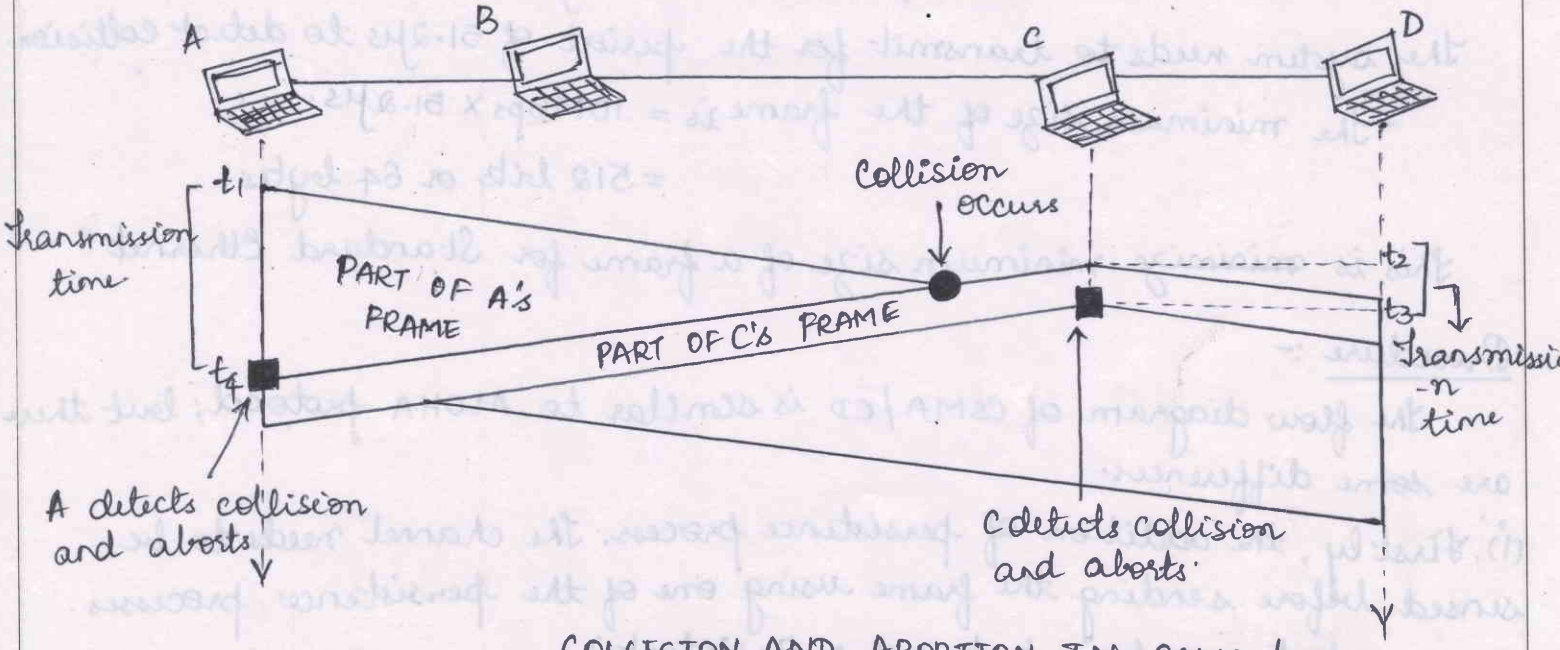
The collision occurs sometime after time t_2. Station C detects a collision at time t_3 when it receives the first bit of A's frame.

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.

From figure, A transmits for the duration $t_4 - t_1$; C transmits for the duration $t_3 - t_2$



COLLISION OF FIRST BITS IN CSMA/CD



COLLISION AND ABORTION IN CSMA/CD.

Minimum Frame size:-

For CSMA/CD to work, a restriction on the frame size is mandatory. Before sending the last bit of the frame, the sending station should detect

a collision, if any, and abort the transmission.

Once the entire frame is sent, the station does not keep any copy of the frame and does not monitor the line for collision detection.

Thus the frame transmission time T_{fr} must be atleast two times the maximum propogation time T_p.

Consider if two stations involved in a collision are maximum distance apart, the signal from the first takes time T_p to reach the second, and the effect of the collision takes another time T_p to reach the first. Hence the requirement is that first station must still be transmitting after $2T_p$.

Ex:-

A network using CSMA/CD has a bandwidth of 10Mbps. If the maximum propogation time (including the delays in the devices and ignoring the time needed to send a jamming signal) is 25.6μs; what is the minimum size of the frame?

Minimum frame transmission time = $T_{fr} = 2 \times T_p$.

$T_{fr} = 2 \times 25.6 = 51.2\mu s$.

The system needs to transmit for the period of 51.2μs to detect collision.

The minimum size of the frame is = 10Mbps × 51.2μs.

= 512 bits or 64 bytes.

This is ~~minimize~~ minimum size of a frame for Standard Ethernet.

Procedure :-

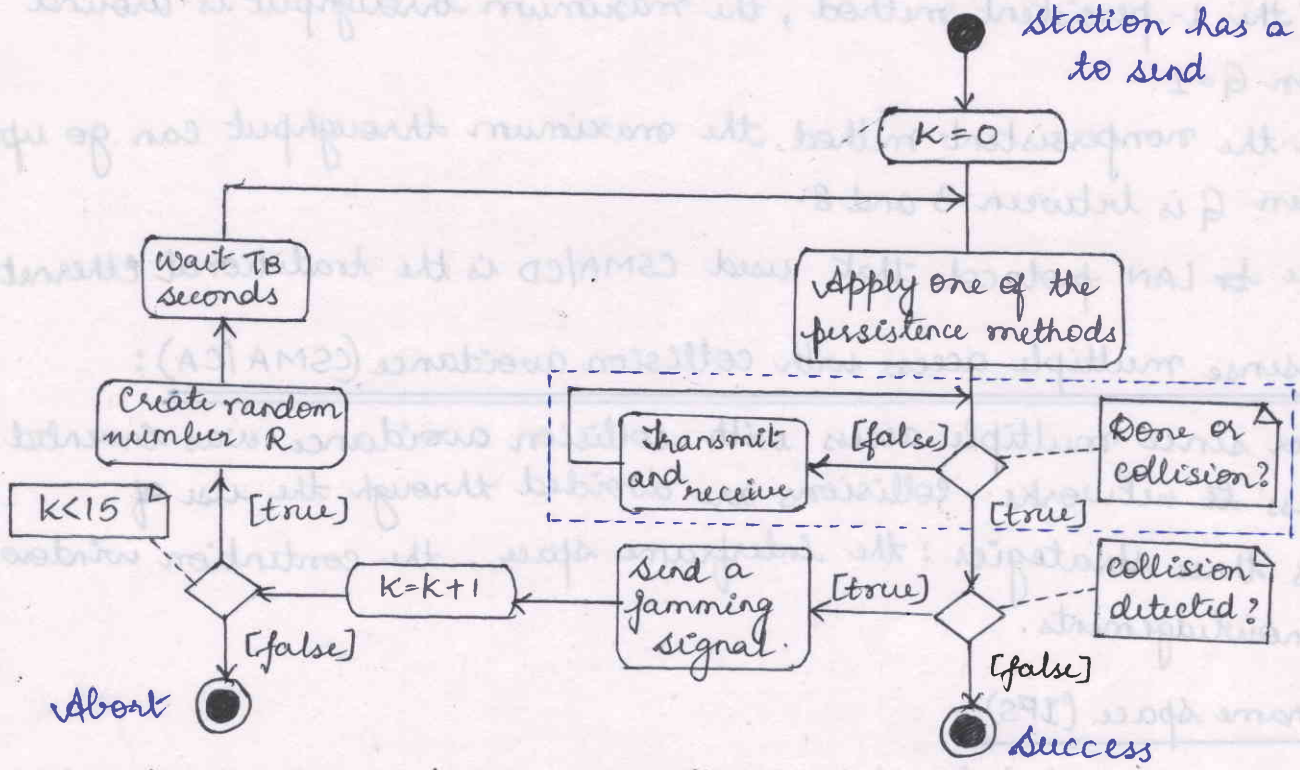
The flow diagram of CSMA/CD is similar to ALOHA protocol; but there are some differences.

(i) Firstly, the addition of persistence process. The channel needs to be sensed before sending the frame using one of the persistence processes. (1-persistent, nonpersistent and p-Persistent).

(ii) Secondly, the frame transmission. In ALOHA, the entire frame is transmitted and then wait for acknowledgement. In CSMA/CD, transmission and collision detection are continuous process. The station transmits and

receives continuously and simultaneously. It is constantly monitored in order to detect either of the conditions: transmission is finished or a collision is detected. Either event stops transmission.

(iii) Finally, the sending of a short 'jamming signal' to make sure that all other stations become aware of the collision.



T_{fr} → Frame average transmission time.

K → Number of attempts.

R → Random number = 0 to $2^K - 1$

T_B → Backoff time = $R \times T_{fr}$.

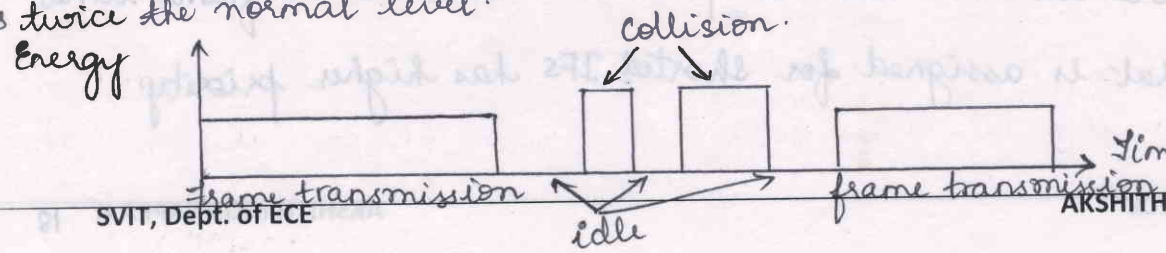
~~ter~~ Energy level :-

The level of energy in a channel can have three values: zero, normal and abnormal.

(i) At the zero level, the channel is idle.

(ii) At the normal level, a station has successfully captured the channel and is sending its frame.

(iii) At the abnormal level, there is a collision and the level of the energy is twice the normal level.



Throughput :-

The throughput of CSMA/CD is greater than that of pure or slotted ALOHA. The maximum throughput occurs at a different value of G and is based on the persistence method and the value of p in the p-persistent approach.

For the 1-persistent method, the maximum throughput is around 50% when G=1.

For the nonpersistent method, the maximum throughput can go upto 90% when G is between 3 and 8.

One of the LAN protocols that used CSMA/CD is the traditional Ethernet.

Carrier sense multiple access with collision avoidance (CSMA/CA):

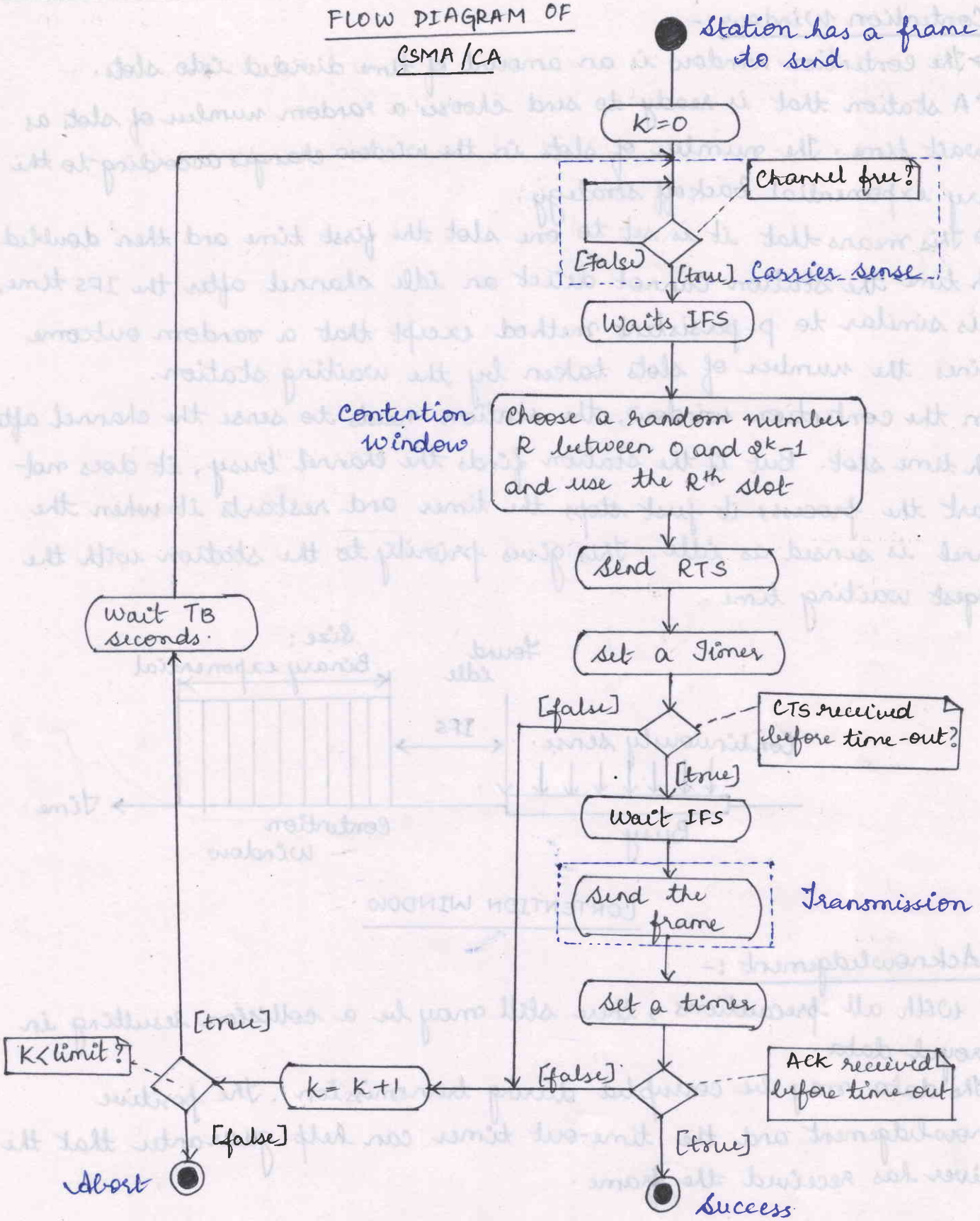
Carrier sense multiple access with collision avoidance was invented for wireless networks. Collisions are avoided through the use of CSMA/CA's three strategies : the interframe space, the contention window and acknowledgements.

(i) Interframe space (IFS):-

→ Collisions are avoided by defering transmission even if the channel is found idle.
→ When an idle channel is found, the station does not send immediately. It waits for a period of time called interframe space or IFS.
→ Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting.
→ The distant station's signal has not reached this station. The IFS time allows the front of the transmitted signal by the distant station to reach this station.
→ After waiting an IFS time, if the channel is still idle, the station can send, but if it still needs to wait a time equal to contention window.
The IFS variable can be used to prioritize stations or frame times

Ex:- Station that is assigned for shorter IFS has higher priority.

FLOW DIAGRAM OF CSMA/CA



Where; k → Number of attempts
T_B → Backoff time
IFS → Interframe Space
RTS → Request to send
CTS → Clear to send.

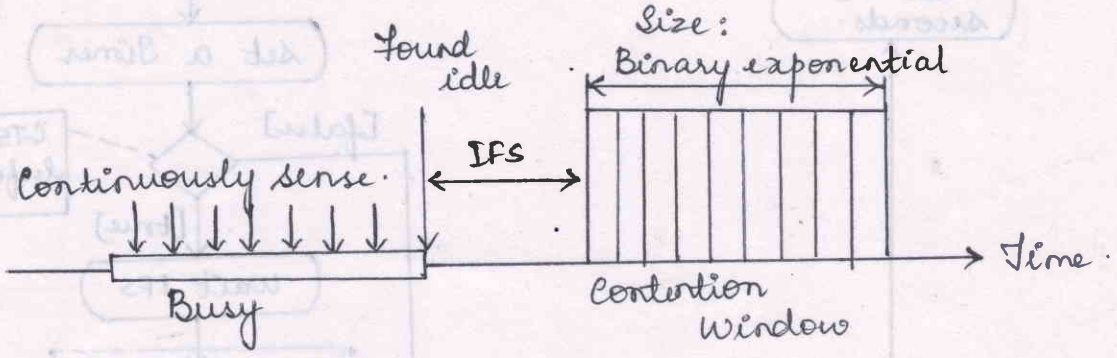
(ii) Contention Window :-

→ The contention window is an amount of time divided into slots.

→ A station that is ready to send chooses a random number of slots as its wait time. The number 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 doubled each time the station cannot detect an idle channel after the IFS time. It is similar to p-persistent method except that a random outcome defines the number of slots taken by the waiting station.

→ In the contention window, the station needs to sense the channel after each time slot. But 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.



CONTENTION WINDOW.

(iii) Acknowledgement :-

With all precautions, there still may be a collision resulting in destroyed data.

The data may be corrupted during transmission. The positive acknowledgement and the time-out timer can help guarantee that the receiver has received the frame.

Frame Exchange Time Line:

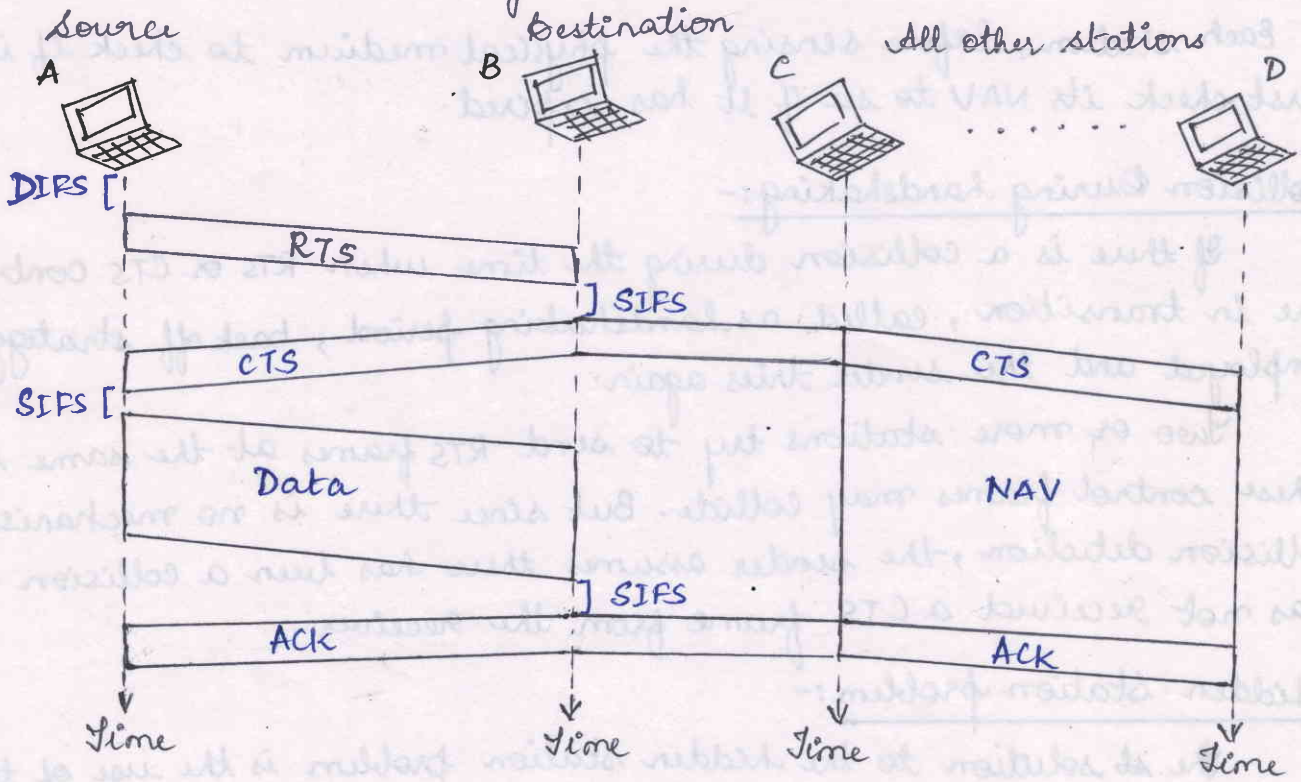
The figure shows the exchange of data and control frames in time.

(1) Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.

① The channel uses a persistence strategy with backoff until the channel is idle.

② After the station is found to be idle, the station waits for a period of time called the DCF interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

(ii) After receiving the RTS and waiting a period of time called short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates that destination station is ready to receive data.



CSMA/CA and NAV

(iii) The source station sends data after waiting an amount of time equal to SIFS.

(iv) The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been arrived. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination. The lack of collision in CSMA/CD is kind of indication to the source that data has arrived.

(P.T.O)

Network Allocation Vector:-

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 starts their NAV.

Each station, before sensing the physical medium to check if its idle, first check its NAV to see if it has expired.

Collision During handshaking:-

If there is a collision during the time when RTS or CTS control frames are in transition, called as handshaking period, back off strategy is employed and the sender tries again.

Two or more stations try to send RTS frames at the same time. These control frames may collide. But since 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.

Hidden-Station problem:-

The sb solution to the hidden station problem is the use of the handshake frames (RTS and CTS)

The figure shows that RTS message from B reaches A, but not C. Since both B and C are within the range of A, the CTS message, which contains the duration of data transmission 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.

WIRED LAN'S : ETHERNET:

ETHERNET PROTOCOL:-

Every LAN except Ethernet has disappeared from the market place because Ethernet was able to update itself to meet the needs of the time. Ethernet protocol was designed so that it could evolve with the demand for higher transmission rates.

IEEE 802 :-

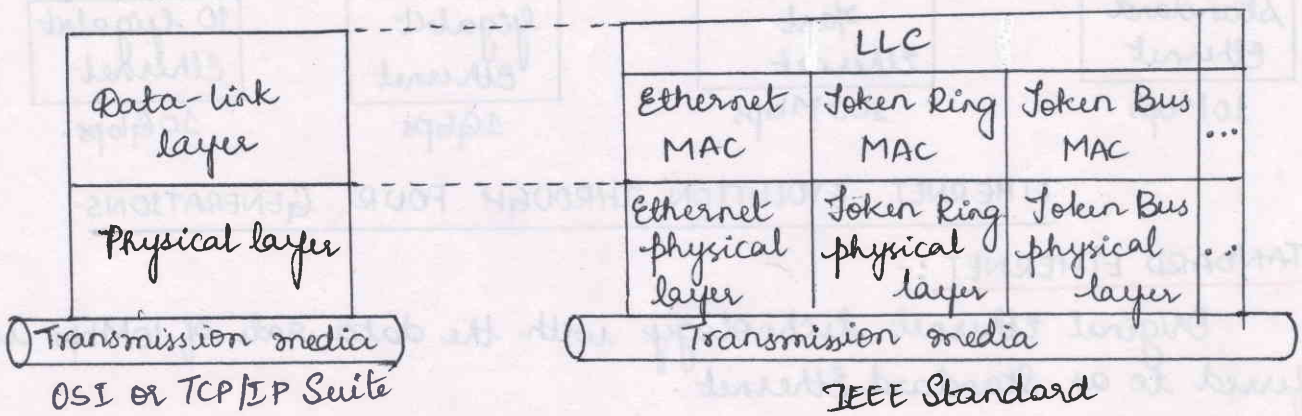
In 1985, the Computer Society of the IEEE started a project, called 'Project 802', to set standards to enable intercommunication among equipment from a variety of manufacturers.

Project 802 does not seek to replace any part of OSI model or TCP/IP protocol suite. Instead, it is a way of specifying functions of the physical layer and the data-link layer of major LAN protocols.

The relationship of the 802 Standard to the TCP/IP protocol suite is shown in the figure. The IEEE has sub-divided the data-link layer into two sublayers :-

(i) Logical link control (LLC)
(ii) Media access control (MAC).

IEEE STANDARD FOR LANs.



Logical Link Control (LLC):-

(i) In IEEE Project 802, flow control, error control and part of the framing duties are collected into one sublayer called the logical link control (LLC).
(ii) Framing is handled in both the LLC sublayer and the MAC sublayer.

(iii) The LLC provides a single link layer control protocol for all IEEE LANs. Thus LLC can provide interconnectivity between different LANs because it makes the MAC sublayer transparent.

Media Access Control (MAC):-

(i) IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN.

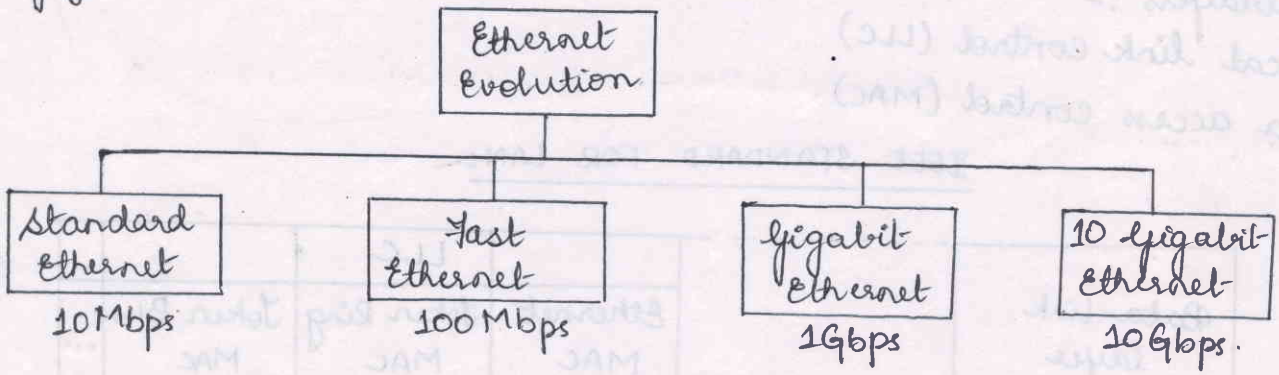
Ex:- It defines CSMA/CD as the media access method for Ethernet LANs and defines the token-passing method for Token ring and token bus LANs.

Ethernet Evolution:-

The Ethernet LAN was developed in 1970s by Robert Metcalfe and David Boggs.

It has gone through four generations:-

Standard Ethernet (10Mbps)
Fast Ethernet (100Mbps)
Gigabit Ethernet (1Gbps)
10 Gigabit Ethernet (10Gbps).



ETHERNET EVOLUTION THROUGH FOUR GENERATIONS.

STANDARD ETHERNET:-

Original Ethernet technology with the data rate of 10Mbps is referred to as Standard Ethernet.

Characteristics:-

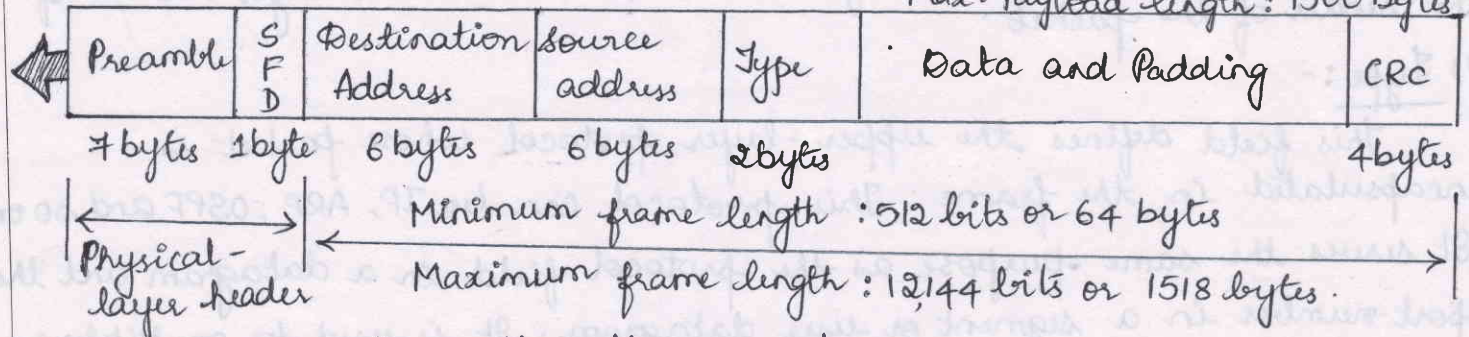
① Connectionless and Unreliable Service:-

(i) Ethernet provides a connectionless service, i.e., each frame sent is independent of the previous or next frame.

(ii) It has no connection establishment or connection termination phases.
(iii) The sender sends the frame whenever it is ready, the receiver may or may not be ready for it.
(iv) The sender may overwhelm the receiver with frames, which may result in dropping frames. If a frame drops, the sender will not know about it. Since IP, which is using the service of Ethernet, is also connectionless, it will not know about it either.
(v) If the transport layer is also connectionless protocol, such as UDP, the frame is lost and salvation may only come from application layer.
(vi) 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 CRC-32, the receiver drops the frame silently.

(2) Frame Format :-

The Ethernet frame contains seven fields; Min. payload length : 46 bytes
Max. Payload length : 1500 bytes



Preamble: 56 bits of alternating 1s and 0s.
SFD : Start frame delimiter, flag (10101011)

(i) Preamble :-

This field contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its clocks if its out of synchronization.

The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not part of the frame.

(ii) Start frame delimiter (SFD):-

This field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or 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.

This field is actually a flag that defines the beginning of the frame. Ethernet frame is a variable length frame, so it needs a flag to define the beginning of the frame. The SFD is also added at the physical layer.

(iii) Destination address (DA):-

This field is six bytes (48 bits) and contains link-layer address of the destination station or stations to receive the packet.

When the receiver sees its own link-layer address, or a multicast address for a group that the receiver is a member of, or a broadcast address, it decapsulates the data from the frame and passes the data to the upper-layer protocol defined by the value of the type field.

(iv) Source Address (SA):-

This field is also six bytes and contains the link-layer address of the sender of the packet.

(v) Type:-

This field defines the upper-layer protocol whose packet is encapsulated in the frame. This protocol can be IP, ARP, OSPF and so on. It serves the same purpose as the protocol field in a datagram and the port number in a segment or user datagram. It is used for multiplexing and demultiplexing.

(vi) Data:-

This field carries data encapsulated from the upper-layer protocols. It is minimum of 46 and a maximum of 1500 bytes.

If the data coming from the upper layer 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 0s.

A padded data frame is delivered to upper layer protocol as it is. It is the responsibility of the upper layers to remove, or in case of the sender, to add padding.

(vii) 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. If the receiver calculates the CRC and finds that it is not zero (corruption in transmission), it discards the frame.

(3) Frame Length :-

(i) Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame.

(ii) The minimum length restriction is required for the correction operation of CSMA/CD. An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is a header and the trailer.

(iii) If we count 18 bytes of header and trailer (6 bytes of SA, 6 bytes of DA, 2 bytes of length/type and 4 bytes of CRC), then minimum length of data from upper layer is 64 - 18 = 46 bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.

(iv) The maximum length of a frame (without preamble and SFD) is 1518 bytes. If we subtract 18 bytes of header and trailer, the max. length of the payload is 1500 bytes

(v) The maximum length restriction is due to two factors; (a) Memory was expensive when Ethernet was designed; max. length restriction helped to reduce the size of the buffer. (b) The max. length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

Minimum frame length : 64 bytes	Minimum data length : 46 bytes
Maximum frame length : 1518 bytes	Maximum data length : 1500 bytes

Addressing :-

Each station on an Ethernet network (such as a PC, workstation or printer) has its own Network interface card (NIC). The NIC fits inside the station with a link-layer address.

The Ethernet address is 6 bytes (48 bits), written in hexadecimal notation, with a colon between the bytes.

Ex:- Ethernet MAC address;

4A:30:10:21:10:1A

(i) Transmission of Address bits:

The way the addresses are sent out outline is different from the way they are written in hexadecimal notation.

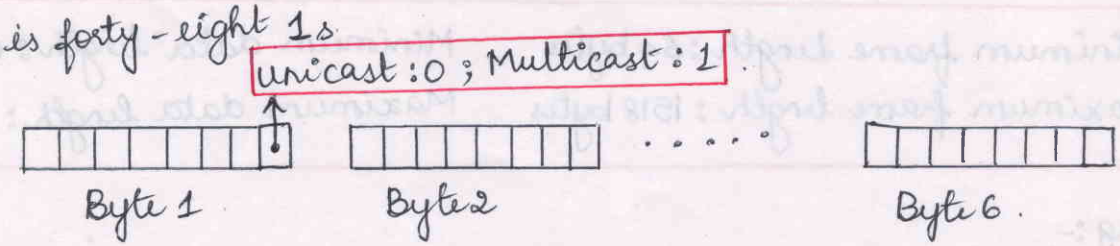
The transmission is left to right, byte by byte; for each byte the least significant bit is sent first and most significant bit is sent last. The bit that defines an address as unicast or multicast arrives first at the receiver. This helps the receiver to immediately know if the packet is unicast or multicast.

Ex:- Show how the address 47:20:1B:2E:08:EE is sent out outline.

Hexadecimal	47	20	1B	2E	08	EE
Binary	01000111	00100000	00011011	00101110	00001000	11101110
Transmitted ←	11100010	00000100	11011000	01110100	00010000	01110111

(ii) Unicast, Multicast and Broadcast Addresses:

A source address is always a unicast address — the frame comes from only one station. The destination address can be unicast, multicast or broadcast. The figure shows how to distinguish a unicast address from a multicast address. If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise it is multicast. The broadcast address is a special case of multicast address: the recipients are all the stations on the LAN. A broadcast destination address is forty-eight 1s.



UNICAST & MULTICAST ADDRESSES

Ex:- (a) 4A:30:10:21:10:1A → Unicast Address because A in binary 1010 (even)
(b) 47:20:1B:2E:08:EE → Multicast Address because 7 in binary 0111 (odd)
(c) FF:FF:FF:FF:FF:FF → Broadcast Address; all digits are F's

(iii) Distinguish between Unicast, Multicast and Broadcast Transmission :-

Standard Ethernet uses a coaxial cable (bus topology) or a set of twisted-pair cables with a hub (star topology).

The transmission in the standard Ethernet is always broadcast. In the bus topology, when station A sends a frame to station B, all station will receive it.

In the star topology, when station A sends a frame to station B, the hub will receive it. Since hub is passive element, it does not check the destination address of the frame; it regenerates the bits and sends them to all stations except A. (Refer to figure in page 11 : module 1).

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

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

(c) In a broadcast transmission, all stations (except the sender) will receive the frame and all stations (except the sender) keep and handle it.

Access Method :-

Since the network that uses the Standard Ethernet protocol is a broadcast network, an access method should be used to control the access to sharing medium. The standard Ethernet chose CSMA/CA with 1-persistent method. Let us use a scenario to see how this works;

(a) Assume station A (figure in page 11 : module 1) has a frame to send to station D.

(i) Station A should first check whether any other station is sending (carrier sense). Station A measures the level of energy on the medium (for a short period of time, normally less than 100μs).

(ii) If there is no signal energy on the medium, it means that no station is sending (or the signal has not reached station A).

(iii) Station A interprets this situation as idle medium. It starts sending its frame.

(iv) But if the signal energy level is not zero, it means that the medium until it becomes idle for 100μs. It then starts sending the frame.

(v) Station A needs to keep a copy of the frame in its buffer until it is sure that there is no collision.

(b) The medium sensing does not stop after station A has started sending the frame. Station A needs to send and receive continuously. Two cases may occur;

(1) Station A has sent 512 bits and no collision is sensed, the station then is sure that the frame will go through and stops sensing the mediu

(ii) Consider the transmission rate of the Ethernet as 10Mbps, it takes the station 512/10Mbps = 51.2μs to send out 512 bits.

(iii) With the speed of propogation in a cable(2×10^8 m), the first bit coul have gone 10,240 m (one way) or only 5120 m (round trip), have collided with a bit from the last station on the cable, and have gone back.

(iv) If a collision were to occur, it should occur by the time the sender has sent out 512 bits. and the first bit has made a round trip of 5120 m

(v) If collision occurs in the middle of the cable, station A hears the collision and aborts transmission.

(vi) The assumption is that the length of the cable is 5120m. The desig of standard Ethernet has put a restriction of 2500m as we need to consider the delays encountered in the journey.

(vii) The problem occurs when another station starts sending before the first bit of station A has reached it.

(viii) The other stations mistakenly think that the line is free because the first bit has not reached it.

(2) Station A has sensed a collision before sending 512 bits. This means one of the previous bits has collided with a bit sent by another station

(ii) In this case both stations should refrain from sending and keep the frame in their buffer for resending when the line becomes availab

(iii) To inform other stations that there is a collision in the network, the station sends a 48-bit jam signal. The jam signal is to create ~~eng~~ enough signal to alert other stations about the collision.

(iv) After sending the jamming signal, the station needs to increment the value of k (no. of attempts). If after increment k=15, it is show

that the network is too busy, the station needs to abort its effort and try again.

(v) If $k<15$, the station can wait a backoff time (TB) and restart the process. The station creates a random number between 0 to 2^k-1, which means each time the collision occurs, the range of random numbers increases exponentially.

(vi) So after each collision, the probability increases that the backoff time becomes longer. This is due to the fact that if the collision happens even after the third or fourth attempt, it means that the network is really busy; a longer back off time is needed.

Efficiency of Standard Ethernet :-

The efficiency of the Ethernet is defined as the ratio of the time used by a station to send data to the time to the medium is occupied by this station. The practical efficiency of standard Ethernet is measured

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

where a= is the number of frames that can fit on the medium.

It is calculated by;

$$a = \frac{\text{(propogation delay)}}{\text{(transmission delay)}}$$

Transmission delay is the time it takes a frame of average size to be sent out and the propogation delay is the time it takes to reach the end of the medium.

As the value of a decreases, the efficiency increases. This means that if the length of the media is shorter or the frame size longer, the efficiency increases.

In the ideal case, $a=0$ and the efficiency is 1.

Implementation :-

The standard ~~Im~~ Ethernet have four implementations that are ~~used~~ popularly.

(P.T.O)

MODULE: 3

Wireless LANs: Introduction: Architectural Comparison, Characteristics, IEEE 802.11: Architecture, MAC Sublayer, Addressing Mechanism, Physical Layer, Bluetooth: Architecture, Layers.
Connecting Devices: Hubs, Switches, **Virtual LANs:** Membership, Configuration, Communication between Switches and Routers, Advantages.
Network Layer: Introduction, Network Layer services: Packetizing, Routing and Forwarding, Other services, Packet Switching: Datagram Approach, Virtual Circuit Approach, IPV4 Addresses: Address Space, Classful Addressing, Classless Addressing, DHCP, Network Address Resolution, Forwarding of IP Packets: Based on destination Address and Label. **L1, L2**

WIRELESS LAN'S :

INTRODUCTION :-

Wireless communication is one of the fastest-growing technologies. The connecting devices without the use of cables is increasing.

Architectural Comparison :-

Medium :-

The first difference between a wired and wireless LAN's is the medium.

(i) In a wired LAN, wires are used to connect hosts. In a switched LAN, with a link-layer switch, the communication between the hosts is point-to-point and full-duplex (bidirectional)

(ii) In a wireless LAN, the medium is air, the signal is generally broadcast. When hosts in a wireless LAN communicate with each other, they are sharing the same medium (multiple access).

(iii) In rare cases, point-to-point communication between two wireless LAN host is created by using a very limited bandwidth and two-bidirectional antennas.

Hosts :-

(i) In a wired LAN, a host is always connected to its network at a point with a fixed link-layer address related to its network interface card (NIC)

(ii) In a wireless LAN, a host is not physically connected to the network

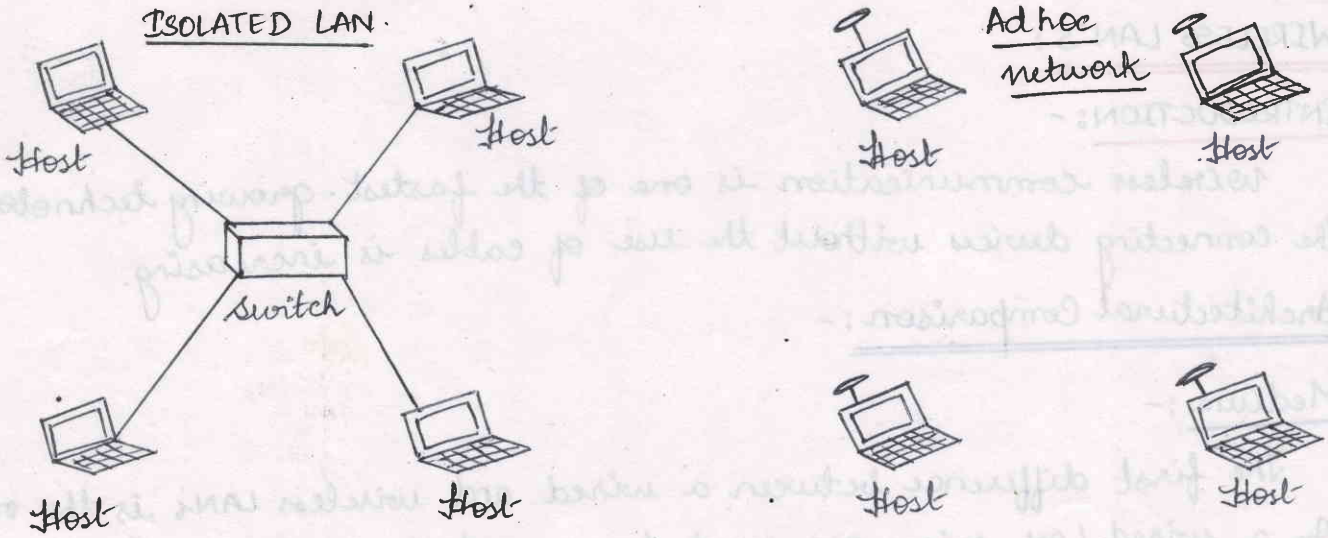
it can move freely and can use the services provided by the network. Mobility in a wired network and wireless network are totally different.

Isolated LANs:

(i) A wired isolated LAN is a set of hosts connected via a link-layer switch.

(ii) A wireless isolated LAN, called an ad hoc network in wireless LAN terminology, it is a set of hosts that communicate freely with each other.

The figure shows two isolated LANs, one wired and the other wireless.

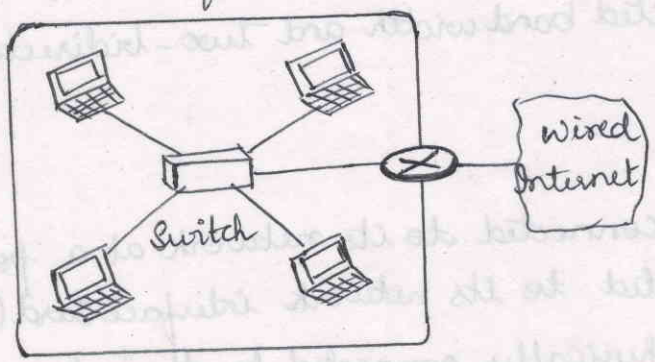


Connection to Other Networks:

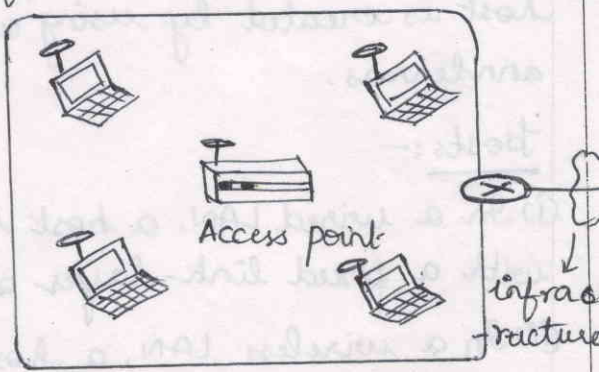
(i) A wired LAN can be connected to another network or an internetwork such as an Internet using a router.

(ii) A wireless LAN may be connected to a wired infrastructure network, to a wireless infrastructure network, or to another wireless LAN.

Connection of a wireless LAN to a wired infrastructure network is shown.



WIRED LAN.



INFRASTRUCTURE NETWORK

(iii) The wireless LAN is referred to as an infrastructure network, and the connection to the wired infrastructure, such as the Internet is done via device called the 'Access point' (AP).

An access point is gluing two different environments together; one wired and one wireless. Communication between the AP and the wireless host occurs in a wireless environment; communication between the AP and the infrastructure occurs in wired environment.

Moving between Environments:

(i) A wired LAN or a wireless LAN operates only in the lower two layers of the TCP/IP protocol suite.

(ii) If we have a wired LAN in a building that is connected via a router or a modem to the Internet, all we need inorder to move from the wired environment to a wireless environment is to change the network interface cards designed for wired environments to the ones designed for wireless environments and replace the link-layer switch with an access point.

(iii) The link-layer addresses ~~(IP addresses)~~ will change (because of changing NICs), but the network layer addresses (IP addresses) will remain the same.

Characteristics:-

There are several characteristics of wireless LANs that either do not apply to wired LANs or the existence of which is neglibible and can be ignored.

Attenuation:-

The strength of electromagnetic signals decreases rapidly because the signal disperses in all directions, only a small portion of it reaches the receiver.

This situation becomes worse with mobile senders that operate on batteries and normally have small power supplies.

Interference:-

Another issue is that a receiver may receive signals not only from the intended sender, but also from other senders if they are using same frequency band.

Multipath Propogation :-

A receiver may receive more than one signal from the same sender because electromagnetic waves can be reflected back from obstacles such as walls, the ground, or objects. The result is that the receiver receives some signals at different phases (because they travel different paths). This makes the signal less recognizable.

Error :-

With the above characteristics, errors and error detection are more serious issues in a wireless networks.

If the error level is thought as the measurement of signal-to-noise ratio (SNR), we can understand why error detection and correction and retransmissie are more important in wireless network.

If SNR is high, it means that the signal is stronger than noise (unwanted signal), we may be able to convert the signal to actual data.

When SNR is low, the signal is corrupted by the noise and data cannot be recovered.

IEEE 802.11 Project :-

IEEE has defined the specification for a wireless LAN called IEEE 802.11, which covers the physical and data-link layers. It is also called as 'wireless Ethernet'.

In some ~~con~~ countries, the peblic uses the term 'WiFi' (short for wireless fidelity) as a synonyn for wireless LAN.

WiFi, is a wireless LAN that is certified by the WiFi Alliance, a global, nonprofit industry association of more than 300 member companies devoted to promoting growth of wireless LANs.

Architecture :-

The standard defines two kinds of services : the basic service set (BSS) and extented service set (ESS).