Computer Networks

Unit 2

* Link Layer - Services and Addressing

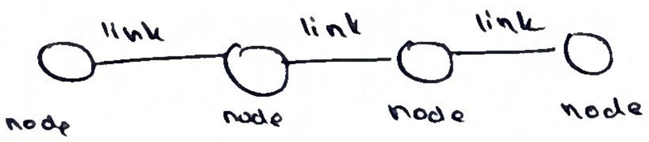
The internet is a combination of networks glued together by connecting devices (routers or switches). If a packet is to travel from a host to another host, it needs to pass through these layers

* 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

→ LANs and WANs are connected by routers.

→ The end hosts are called nodes and the network in between is called links



* Services of the Data-link Layer

→ provides services to the network layer, receives services from the physical layer.

→ responsible for delivering a datagram to the next node in the path.

→ data link layer of the sending-node encapsulates the datagram received from the network in a frame, and the data link layer of the receiving node needs to decapsulate the datagram from the frame.

Framing - encapsulation of a datagram in a frame (A packet at the data link layer is called a frame)

Flow control - sending data link layer = producer

receiving data link layer = consumer.

Two options : (i) receiving data link layer may drop the frames if its buffer is full

(ii) the receiving data-link layer may send feedback to the sending data link-layer to ask it to slow or stop

Error Control. - The frame in a data-link layer needs to be changed to bits, transformed into electromagnetic signals & transmitted through the transmission media & vice versa at the receiving node.

→ Electromagnetic signals are susceptible to error, a frame is also susceptible

→ Need error detection & correction

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 congestion control - though some WANs do.

* Categories of Links

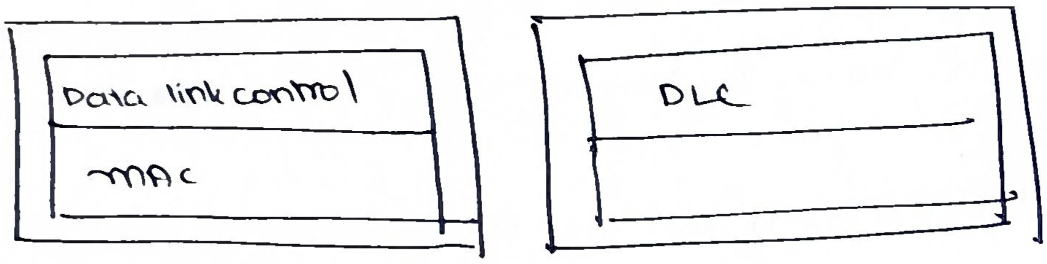
A. point-to-point link - link is dedicated between 2 devices

B. broadcast link - link is shared between several pairs of devices

* Two Sublayers

A. Data link control (DLC) - deals w/ both P2P and broadcast links

B Media access control - only issues specific to the broadcast links



Broadcast P2P

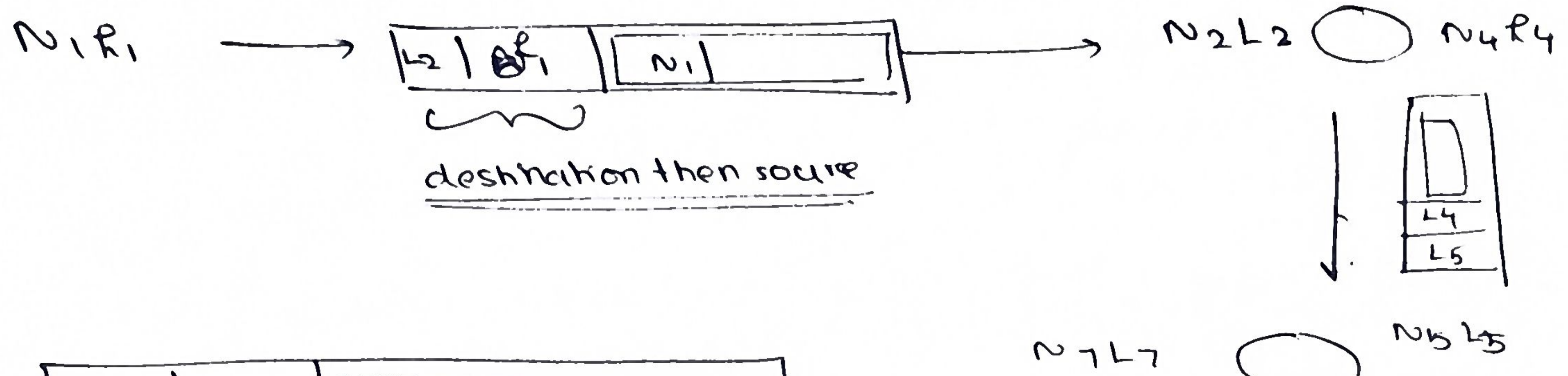
* Link-Layer Addressing

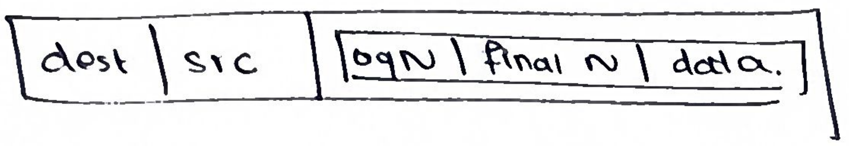
→ The source and destination IP define the 2 ends, but cannot define which links the packet should pass through

→ The link-layer addresses of 2 nodes are called
link - address
physical address
MAC address.

→ It is encapsulated in a frame and the 2 data link address (IP & link-layer) addresses are added to the frame header.

→ These two addresses are changed every time the frame moves from one link to another.





* Additional Questions

A. If the IP address of a router does not appear anywhere in the datagram, why does it have to be assigned?

→ In some protocols, routers may act as the sender or receiver of a datagram

B. Why do we need more than one IP address in a router, one for each interface?

→ An interface is a connection of a router to a link.

→ An IP address defines a point on the Internet at which a device is connected.

→ A router with n interfaces is connected to the Internet at n points.

C. How are the source and destination IP addresses determined?

→ The host should know its own IP address, which becomes the source IP.

→ The application layer uses DNS to find the destination packet's address

D. How are the source and destination link-layer addresses determined for each link?

→ Each hop (router or host) should know its own link layer address.

→ The destination link-layer address is determined by the Address Resolution Protocol.

E. What is the size of link-layer addresses?

→ depends on the protocol used by the link

→ different data link protocols may be used in different links

Three Types of Addresses

A. Unicast Address

→ Each host or interface is assigned a unicast address.

→ Unicasting means one-to-one communication.

→ A frame with a unicast address destination is destined only for one entity in a link

Representation in LAN, Ethernet

are 48 bits (6 bytes), represented as 12 hex digits

Ex

A2 : 34 : 45 : 11 : 92 : F1

↓

LSB of the first byte should be 0.

B. Multicast Address

→ one-to-many communication

→ the jurisdiction is local (inside the link)

Representation - same as unicast, but LSB of first byte

should be 1

A3 : 34 : 45 : 11 : a2 : F1

c. Broadcast Link-Layer Address

→ one-to-all communication

→ all bits are 1s

eg. FF : FF : FF : FF : FF : FF

* Address Resolution Protocols (ARP)

→ Anytime a node has an IP datagram to send to another node in a link, it has the IP address of the receiving node.

→ However, merely the IP address of the next node is not helpful in moving a frame through a link - the link layer address is needed.

→ This is when the Address Resolution Protocol is used.

→ The ARP is an auxiliary protocol defined in the network layer,

→ It maps an IP address to a logical-link address.

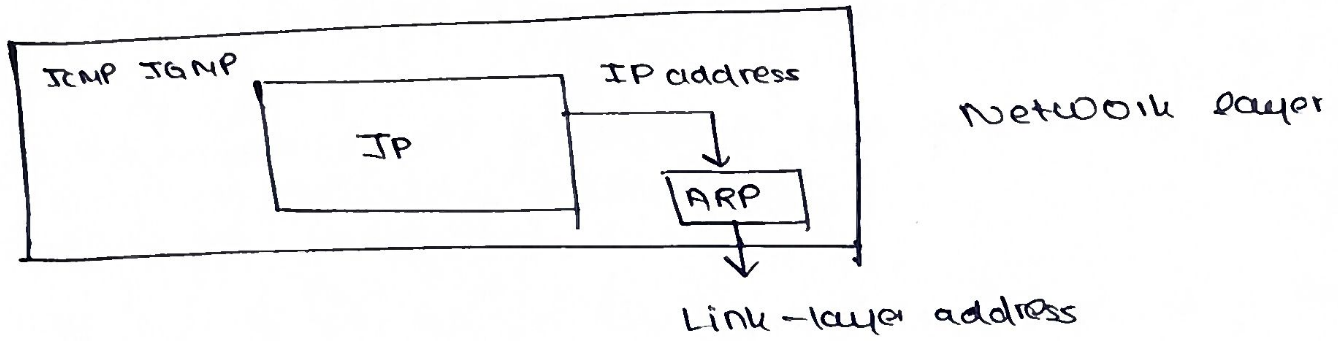
→ Anytime a host or a router needs to find the link-layer address of another host or router, it sends an ARP packet request.

→ The packet includes the link-layer and IP address of the sender and the IP address of the receiver

→ Every host or router on the network receives and processes the ARP request, but only the intended recipient recognizes its IP address and sends an ARP response packet.

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

* Position of ARP in TCP/IP protocol suite



* ARP Packet

0	8	16	31
hardware type		protocol type	
h/w length	protocol length	operation request : 1, reply : 2	
source hardware address			
source protocol address			
destination h/w address (empty in request)			
destination protocol address			

Hardware = LAN or WAN protocol

Protocol : network-layer protocol.

* Caching

→ If A can broadcast a frame to find the link layer address of system, why can't system A send the datagram itself via a broadcast frame?

→ This process includes : 1 broadcast frame (ARP req)
1 unicast frame (ARP response)
1 unicast frame - send datagram.

Answer : Issues w/ efficiency

A may have more than one datagram to send B.

Assume: there are 20 systems, including A & B, A needs to send 10 datagram

w/o ARP - A needs to send 10 broadcast frames

- each of the other systems needs to receive, decapsulate remove. the datagram, and pass to network layer to see if the datagram belongs to them

- This means processing and discarding 180 broadcast frames

w/ ARP - send one broadcast frame

- processing and discarding only 18 frames

* Link Layer - Flow Control Protocols and HDLC

* DLC Services

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

Framing

→ The postal system practices a type of framing. The act of inserting a letter into an envelope separates one piece of information from another, the envelope is the delimiter

→ Similarly, frame in the data-link layer separates a message from source to destination, by adding a sender and destination address

Fixed-size Framing → There is no need for defining the boundaries of the frames, the size itself can be used as a delimiter eg. ATM WAN

Variable-size framing → need to define the end of one frame and the beginning of the next.

2 ways : (i) character-oriented framing (byte-oriented)

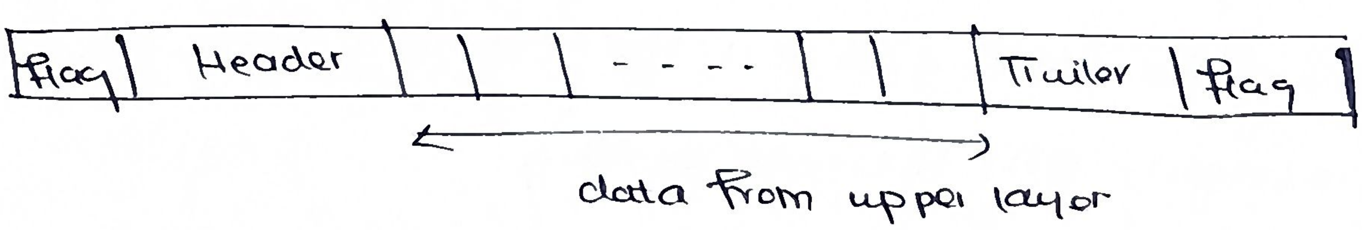
(ii) bit-oriented approach

A. Character-Oriented Framing

→ The data to be carried are 8-bit characters from a coding system such as ASCII.

→ The header has the source and destination addresses, control information and the trailer, which has error detection & redundant bits.

→ To separate one frame from the next, an 8 bit flag is added at the beginning and end of a frame.



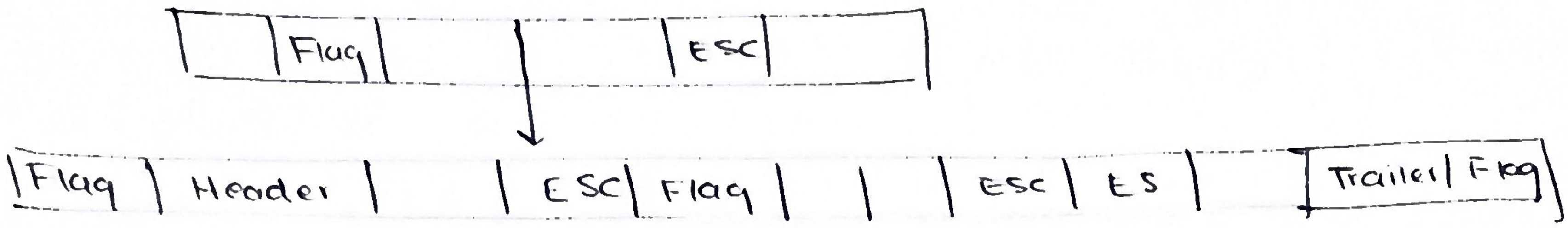
Byte-stuffing

→ A special byte called the escape character (Esc) is added to the data section of the frame when there is a character with the same pattern as the flag

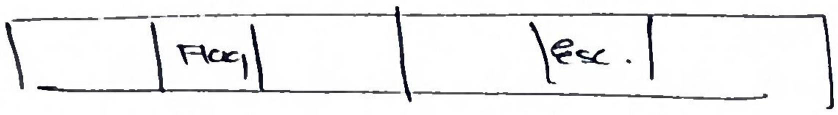
→ Esc has a predefined bit pattern

Example

Data from upper layer



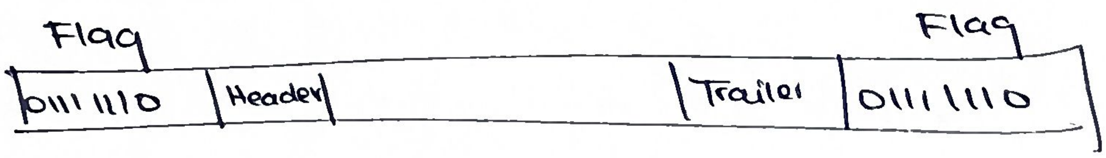
unstuffed



b. Bit - Oriented Framing

→ The data section of a frame is a sequence of bits to be interpreted by the upper layer.

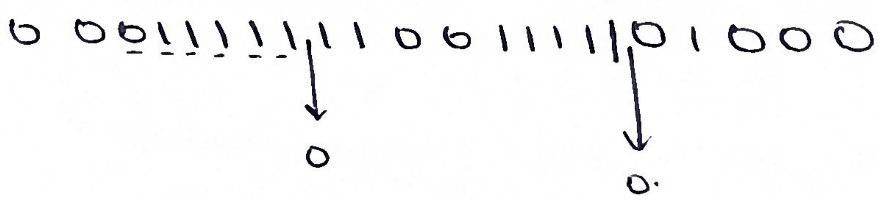
→ The delimiter to separate one frame from the other is 0111110



Bit Stuffing

→ The process of adding one extra 0 whenever 5 consecutive 1s follow a zero in the data, so that the receiver does not mistake the pattern 0111110 as a flag

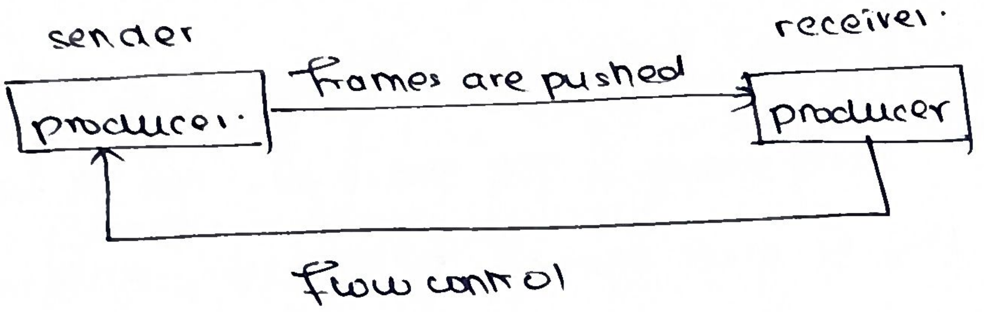
Example



* Flow and Error Control

→ Flow and error control are collectively known as data link control.

Flow control → refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgement



→ implement flow control with buffers

Error Control → based on automatic repeat request, which is the retransmission of data

method1 → discard frame
method2 → Ack sent for the accepted frame alone.

Combination of Flow and Error Controls

→ acknowledgement that is sent for flow control can also be used for error control to tell the sender the packet has arrived uncorrupted

→ The lack of acknowledgement means there is a problem with the sent frame.

* DLC Protocols

Connectionless vs. connection-oriented

Connectionless

(i) Frames sent w/o any relationship between the frames, each frame is independent

(ii) Frames not numbered.

(iii) eg. data-link protocols for LANs

Connection-oriented

(i) a logical connection should be established between the 2 nodes (setup phase)

(ii) transfer phase, and teardown phase

(iii) Frames are numbered and sent in order. If they are not in order, the receiver needs to wait untill all frames belonging to the same set are received and then deliver them in order.

(iv) eg. in some P2P protocols, wireless LANs and some WANs.

* Data Link Layer Protocols

Protocols

- For noiseless channels
  - (i) simplest
  - (ii) stop and wait
- For noisy channels
  - (i) stop and wait ARQ
  - (ii) GO - Back - N - ARQ
  - (iii) Selective repeat ARQ

* Representation of DLL Protocols with FSMs

→ The behavior of a data-link-layer protocol can be shown as a finite state machine (FSM).

→ An FSM is thought of as a machine with a finite no. of states.

→ The machine is always in one of the states until an event occurs.

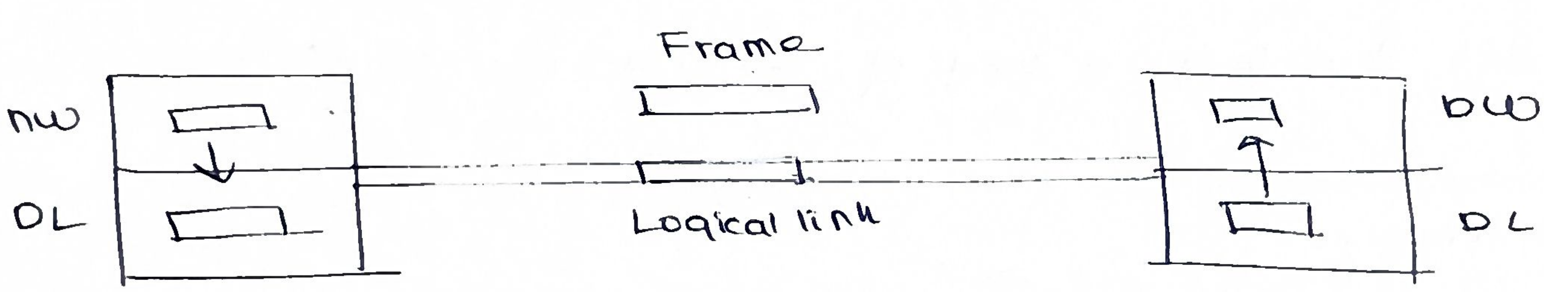
→ Each event is associated with 2 reactions - defining the list of actions to be performed and determining the next state.

* DLL Protocols with FSM Diagrams

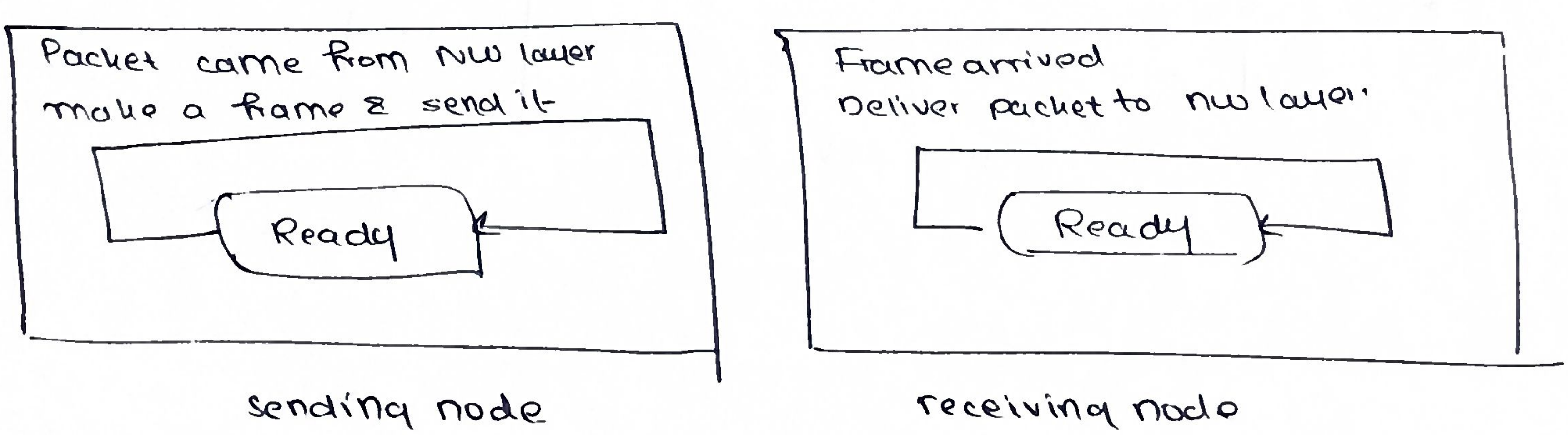
A. Simple Protocol

→ neither flow nor error control

→ receiver can never be overwhelmed w/ incoming frames.



FSM



B. Stop and Wait Protocol

→ uses both flow and error control

→ sender sends one frame at a time and waits for an acknowledgement, before sending the next one.

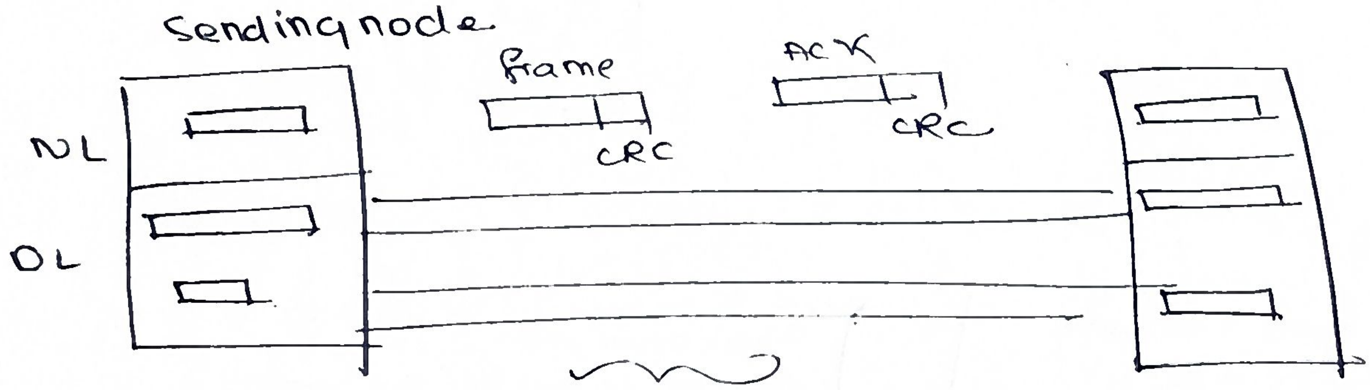
→ To detect CRC, add a CRC to each data frame. If the CRC is incorrect, the frame is corrupted and silently discarded.

→ Every time the sender sends a frame, it starts a timer. If an acknowledgement arrives before the timer expires, the timer is stopped and the sender sends the next frame

→ If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted.

→ The sender thus keeps a copy of the frame until its ack. arrives.

Sending node



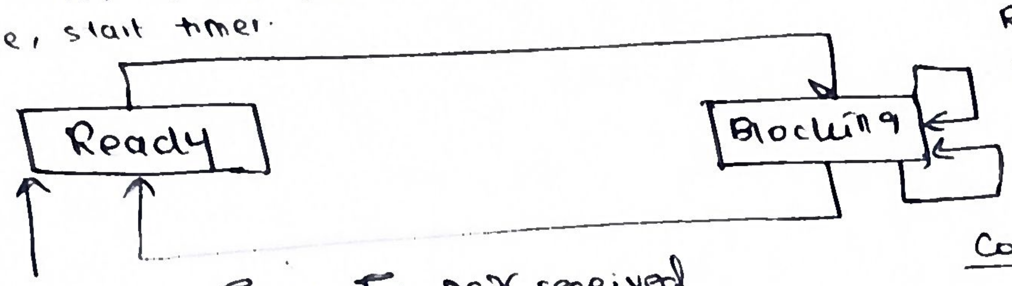
logical link (duplex)

FSM

Sending Node

Packet from NL
make a frame, save a copy,
send frame, start timer.

Time-out
Resend the saved frame
Restart the timer



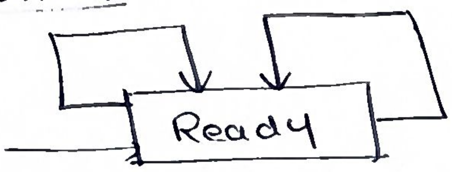
Start

Error-free ACK received
Stop the timer
Discard the saved frame

Corrupted ACK arrived
Discard ACK

Receiving Node

Corrupted frame arrived
Discard the frame



start

Error-free frame arrived
extract and deliver the packet
to the network layer

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

Ready State – waits for packet from NL
creates a frame
makes a copy
starts timer
sends frame
then moves to blocking state

Blocking State – 3 events can occur
(i) timeout → resend saved copy
(ii) corrupted ACK → discard
(iii) error free ACK → sender stops timer, discard copy, move to the ready start.

Receiver States → The receiver is already in the ready state.

Two events may occur:

(i) error free frame ⇒ deliver to NL, send ACK

(ii) corrupted frame ⇒ discard

* Piggybacking?

→ Data in one direction is piggybacked with the acknowledgement in the other direction.

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

* HDLC

→ High-level data link control (HDLC) is a bit-oriented protocol for communication over point to point & multipoint links.

Configurations and Transfer Modes

(i) Normal response mode – station config. is unbalanced

→ one primary station & multiple secondary stations

→ A primary station can send commands, a secondary station can only respond.

(ii) Asynchronous balanced mode – configuration is balanced

→ link is point to point

→ Each station can function as primary and secondary.

Framing?

HDLC defines 3 kinds of frames:

(i) information frames (I - frames)

Flag	Address	Control	User info	FCS	Flag

(ii) supervisory frames (S - frames)

Flag	Address	Control	FCS	Flag

(iii) unnumbered frames (U - frames)

Flag	Address	Control	mgmt info	FCS	Flag

Fields

A. Flag - pattern 01111110 - identifies the beginning and ending of a frame

B. Address Field - contains address of secondary station

C. Control Field - one or two bytes used for flow and error control

D. Info. field - contains user's data from the network or mgmt. info

E. FCS field - HDLC error detection field.

Control field formats

0				P/F			
N(S)					N(R)		

I

1	1			P/F			
Code					Code		

1	0			P/F			
Code					N(R)		

S

00 → receive ready
01 → receive not ready
10 → reject NAQ
11 → selective reject

* MAC - Random Access

→ When nodes / stations 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 a shared link. All of these protocols belong to a sublayer in the data link layer called media access control (MAC).

→ They are categorized as :-

Multiple - access protocols

Random access protocols	Controlled access protocols	Channelization protocols
(i) ALOHA	(i) Reservation	(i) FDMA
(ii) CSMA	(ii) Polling	(ii) TDMA
(iii) CSMA/CD	(iii) Token passing	(iii) CDMA.
(iv) CSMA / CA		

* Random Access / Contention Methods

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

→ No station permits or does not permit another station to send

→ Station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send

→ There is no scheduled time ⇒ random transmission

→ Stations compete with one another → contention

1) Pure ALOHA

→ Each station sends a frame whenever it has a frame to send

→ However, since there is only one channel to share, there is the possibility of collision between frames.

→ The pure ALOHA protocol relies on acknowledgements from the receiver. When a station sends a frame, it expects the receiver to send an ack. It waits for a specific time-out period.

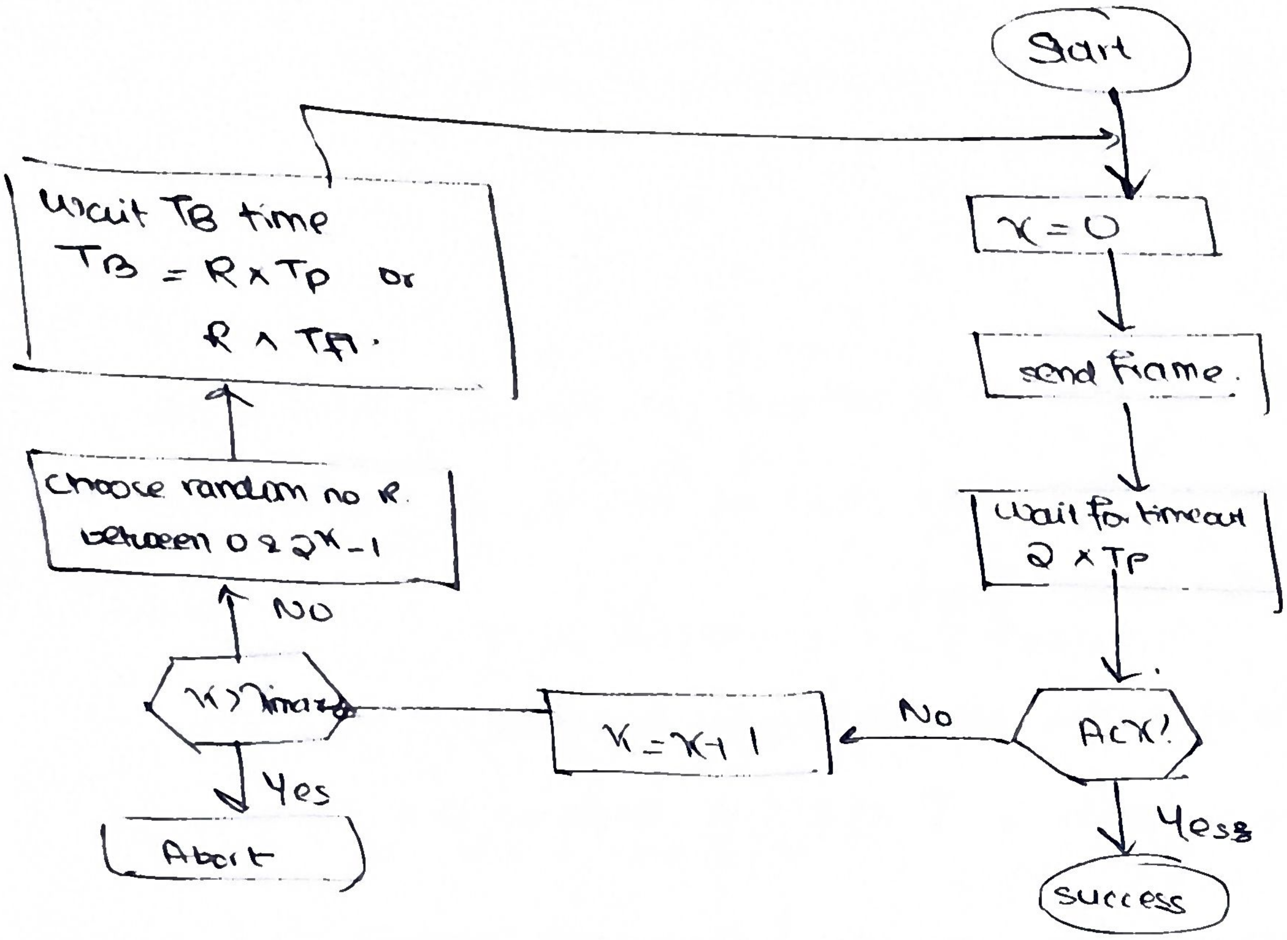
→ A collision involves two or more stations. If all those stations try to resend their frames again after timeout, the frames will collide again

→ Assign a random time before resending. called as backoff time = TB

K = no. of attempts $\quad K_{max} = 15$

T_p = maximum propagation time

T_{fr} = avg. transmission time for a frame



Vulnerable Time – length of time in which there is a possibility of collision.

$= 2 \times T_p$

Throughput : Let G = avg. no. of frames generated by the system during one frame transmission time

avg. no. of successfully transmitted frames

$$S = G \times e^{-2G}$$

$$S_{max} = 0.184 \quad \text{when} \quad G = 1/2$$

Numericals on PURE ALOHA

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

Find T_p and T_B for diff. values of x.

Solution: $T_p = (600 \times 10^3) / (3 \times 10^8)$

$= 2\ ms$

For $K = 1$ $\quad 0\ 2^k - 1 \Rightarrow \{0, 1\}$

$\rightarrow T_B = 0 \times 2ms = 0$

or $1 \times 2ms = 1$

Example 2 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?

$$T_{fr} = \frac{200 bits}{200 kbps} = 1ms$$

$$\text{Vulnerable Time} = 2 \times T_{fr} = 2ms$$

→ This means that no station should send later than 1ms or 1ms after transmission.

Example 3 A pure ALOHA network transmits 200-bit frames on a shared channel of 200kbps. What is the throughput if the system produces:

a. 1000 frames per second

b. 500 frames per second

c. 250 frames per second

frames	second
1000	1
	10^{-3}

Ans (a) 1000 frames per second

= 1 frame per ms

$\Rightarrow G = 1$

$S = G \times e^{-2G}$

$S = 0.135$

Throughput $= 0.135 \times 1000$

$= 135$

$\Rightarrow$ 135 out of 1000 frames will survive

b. 500 frames per second

frame	sec
500	1
x	10^{-3}

$x = 500 \times 10^{-3} = 0.5$ frames

$G = 0.15$

$S = G \times e^{-2G} = 500 \times 0.184 = 92$

92 out of 1000 frames will survive

frame sec

250 1

10^{-3}

(B) Slotted 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.

→ Because 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.

→ There is still the possibility of collision if two stations try to send at the beginning of the same time slot.

Here, vulnerable time $= T_{fr}$

Throughput : $S = G \times e^{-G}$

$S_{max} = 0.368$ when $G = 1$

(C) CSMA = Carrier Sense Multiple Access

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

→ CSMA requires that each station first listen to the medium, based on the principle of 'sense before transmit' or 'listen before talk'

→ The possibility of collision still exists because of propagation delay. i.e a station may sense the medium & find it idle, only because the first bit sent by another station has not yet been received.

Vulnerable time = T_p = propagation time.

* Persistence Methods

→ determines what a station should do if the channel is busy / idle.

→ of 3 types

① 1-Persistent

→ after the station finds the line idle, it sends its frame immediately

→ This method has the highest chances of collision because 2 or more stations may find the line idle & send their frames immediately

→ eg. Ethernet

② Non-persistent

→ If idle - send frame

→ If not, wait a random amount of time & sense line again

→ reduces chances of collision

→ reduces efficiency, as channel may be idle even when there are frames to send.

③ p-Persistent

→ used if the channel has time slots with a slot duration >= the max. propagation time

→ 1. with probability p, the station sends its frame

2. with probability $q = 1 - p$, the station waits for the

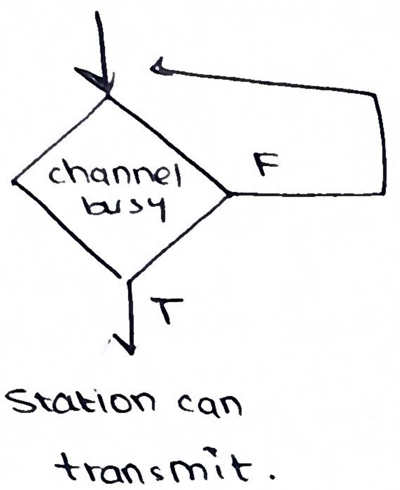
beginning of the next time slot & checks again

a. If idle, go to step

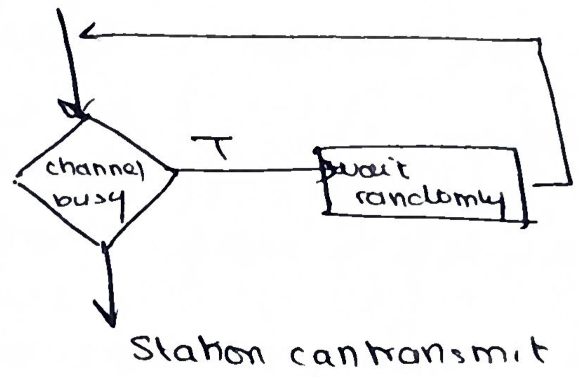
b. If busy, act as through a collision has occurred &

use the back off procedure.

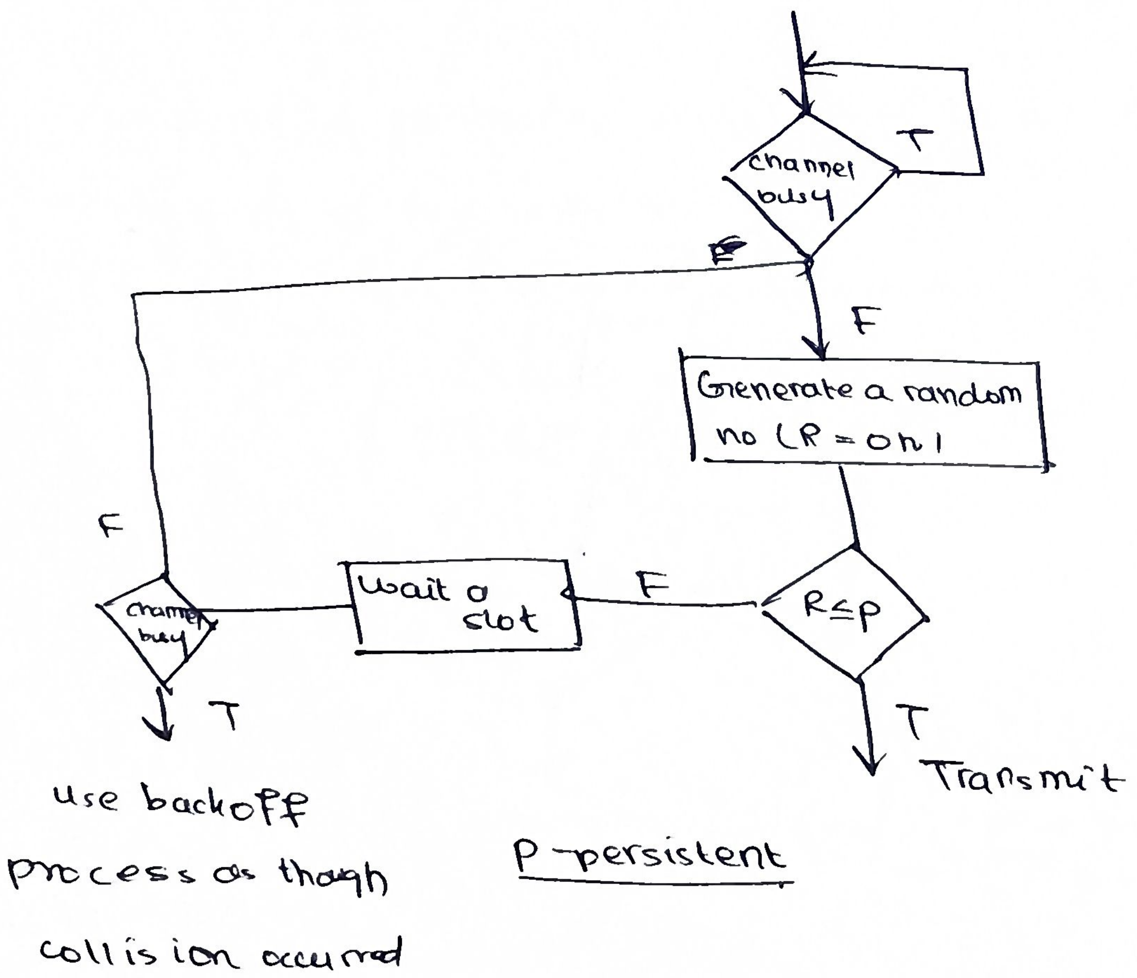
Flow - Diagrams



1-peristent



Non-persistent



p-persistent

(D) CSMA/CD

→ In Carrier sense multiple access with collision detection, there is an algo to handle collision

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

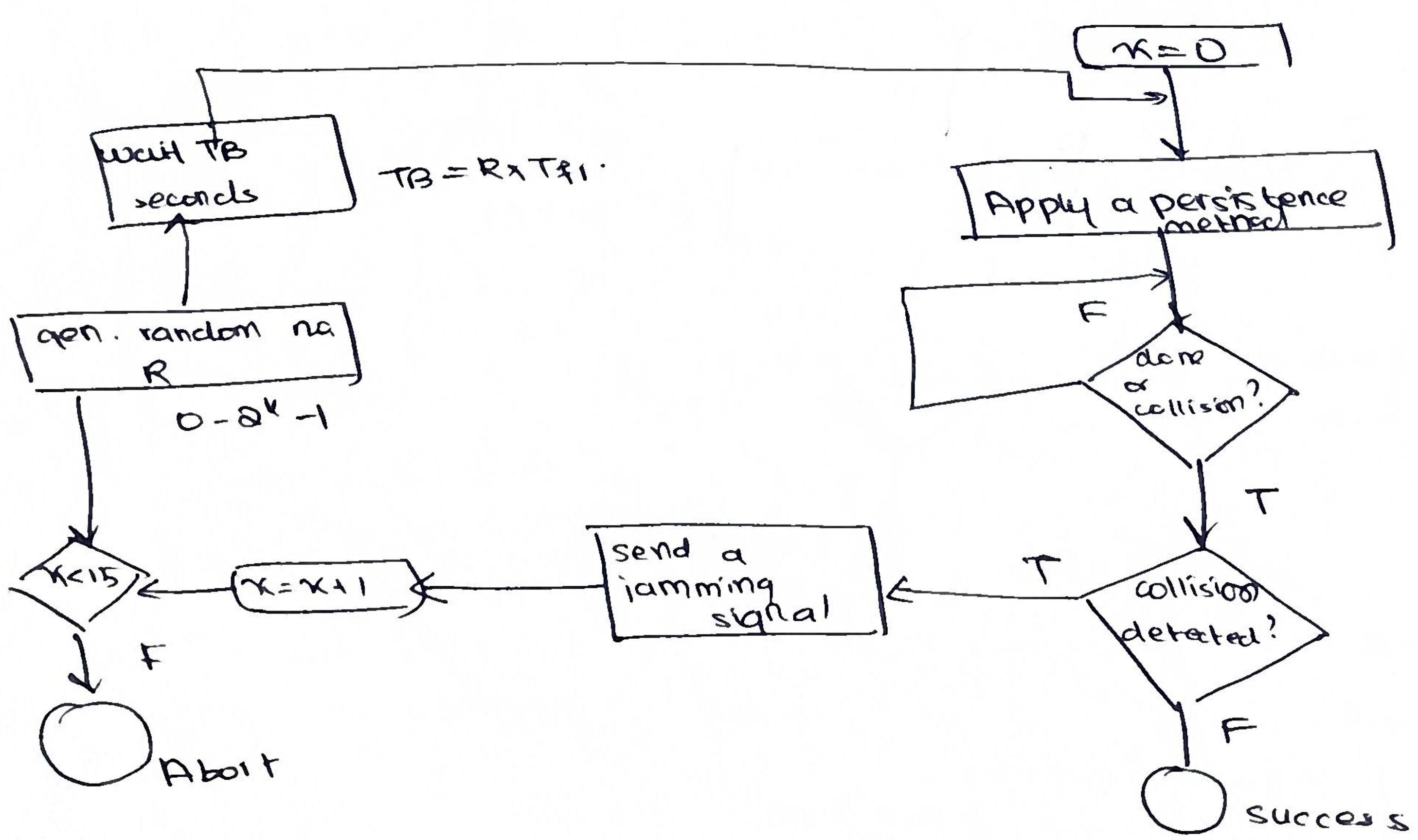
→ If so, the station is finished. If there is a collision, the frame is sent again

→ For CSMA/CD to work, there is a restriction on the frame size.

→ Before sending the last bit of the frame, the sending station must detect a collision, and if any, must abort. This is because the station, does not keep a copy of the frame

→ $T_{fr} = 2 \times T_p$

Flow Diagram



Example A network using CSMA/CD has a bandwidth (ϑ) of 10 Mbps. If the max. propagation time is 25.6 μs, what is the min. frame size?

$T_{fr} = 2 \times T_p = 51.2\,\mu s$

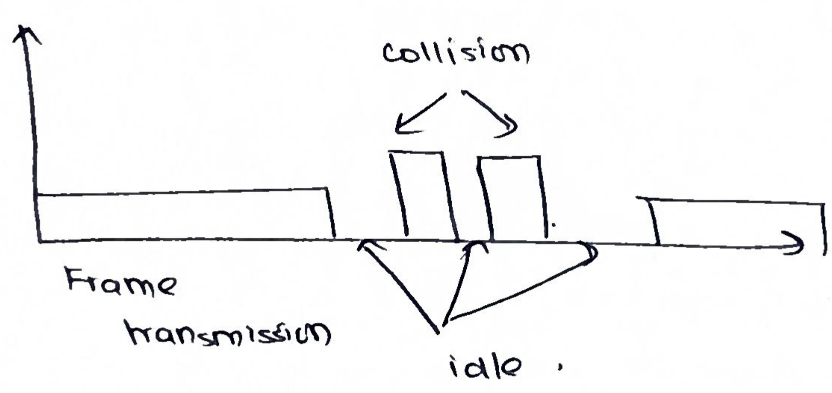
min frame size $= 10\text{ Mbps} \times 51.2\,\mu s$

$= 512 \text{ bits} = 64 \text{ bytes}$

* Difference between ALOHA & CSMA/CD

1. addition of the persistence process
2. In CSMA/CD transmission & collision detection are continuous processes.
3. Sending a jamming signal to make sure that all other stations are aware of the collision.

* Energy Levels



* Throughput

→ depends on persistence value

1-persistent = 50% when G = 1

non-persistent = upto 90% when 3 < G < 8

(E) CSMA/CA

↳ collision avoidence

→ Collisions are avoided with IFS, contention window &

acknowledgements

IFS = interframe space

→ defer transmission even when channel is idle

→ wait for a period of time called IFS

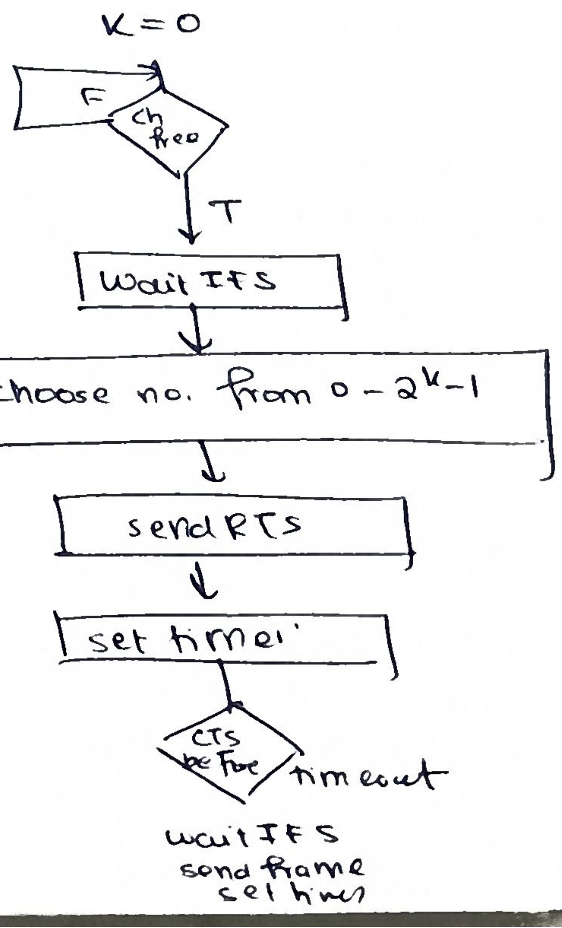
Contention window → an amt. of time divided into slots

→ a station that is ready to send chooses a random no. of slots as its wait time

→ slots depend on binary exp. backoff strategy

Acknowledgement → receive +ve ack to guarantee that receiver has received frame

Flow diagram



RTS - request to send

CTs - clear to send

* Network Allocation Vector (NAV)

→ when a station sends an RTs frame, include the duration of time it needs to occupy the channel

→ Stations affected by this transmission - create a NAV - shows how much time should pass before they can check for idleness.

* Collision during Handshaking

→ when CTs & RTS control frames are in transition - called the handshake period.

→ 2 or more stations may try to send RTs frames at the same time & may collide

* Hidden Station Problem

2 stations are in the range of a common point, but are unable to detect each other's presence

Solve using RTs and CTS

* Multiple Access - Controlled & Channelization Methods

Controlled Access

→ The stations consult one another to find which station has the right to send.

→ A station cannot send unless it has been authorized by other stations

Types: (i) Reservation
(ii) Polling
(iii) Token Passing

A. Reservation - station needs to make a reservation before sending data. Time is divided into intervals. In each interval, there are diff. reservation slots

B. Polling - One device is designated as primary station, other devices = secondary stations

→ All data exchanges must be made through primary device

→ The primary device ~~follows~~ controls link, others follow its instructions.

→ primary device is always the initiator

→ drawback - if 1° fails, the system goes down

→ Collision avoided using the poll & select functions

poll: 1° device solicits transmissions from 2°

select: when 1° has something to send

c. Token Passing

→ stations in a network are organized in a logical ring.

→ For each station, there is a prodecessor and sucessor.

→ 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.

→ station must wait to receive token from predecessor

* Channelization

→ a multiple access method in which the available bandwidth of a link is shared between time, frequency or code between diff stations

Unit 2- Contd.

* **Chanelization** → also called channel partitioning, is a multiple access method in which the available bandwidth of a link is shared in time, frequency or through code.

→ There are 3 channelization protocols : (i) FDMA
(ii) TDMA
(iii) CDMA

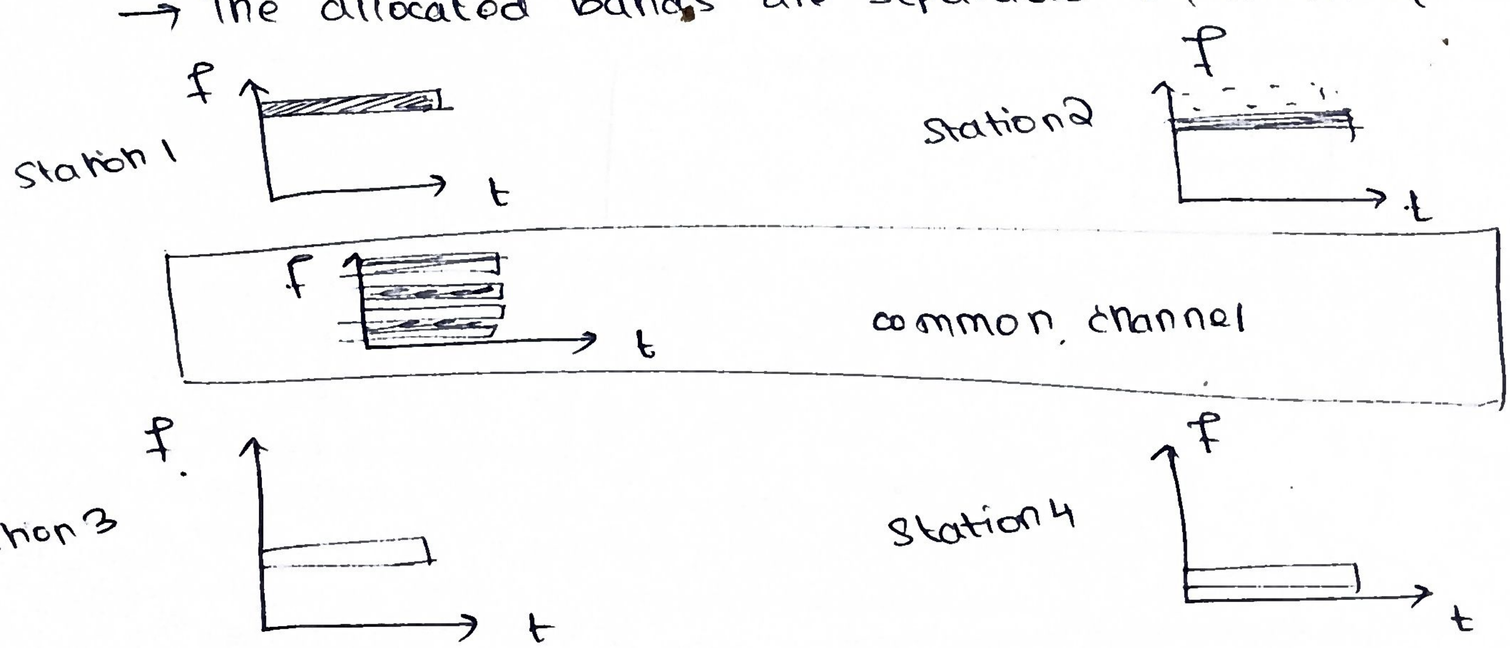
① **FDMA** → Frequency - division multiple access

→ the available bandwidth is divided into frequency bands

→ each station is allocated a band to send its data.

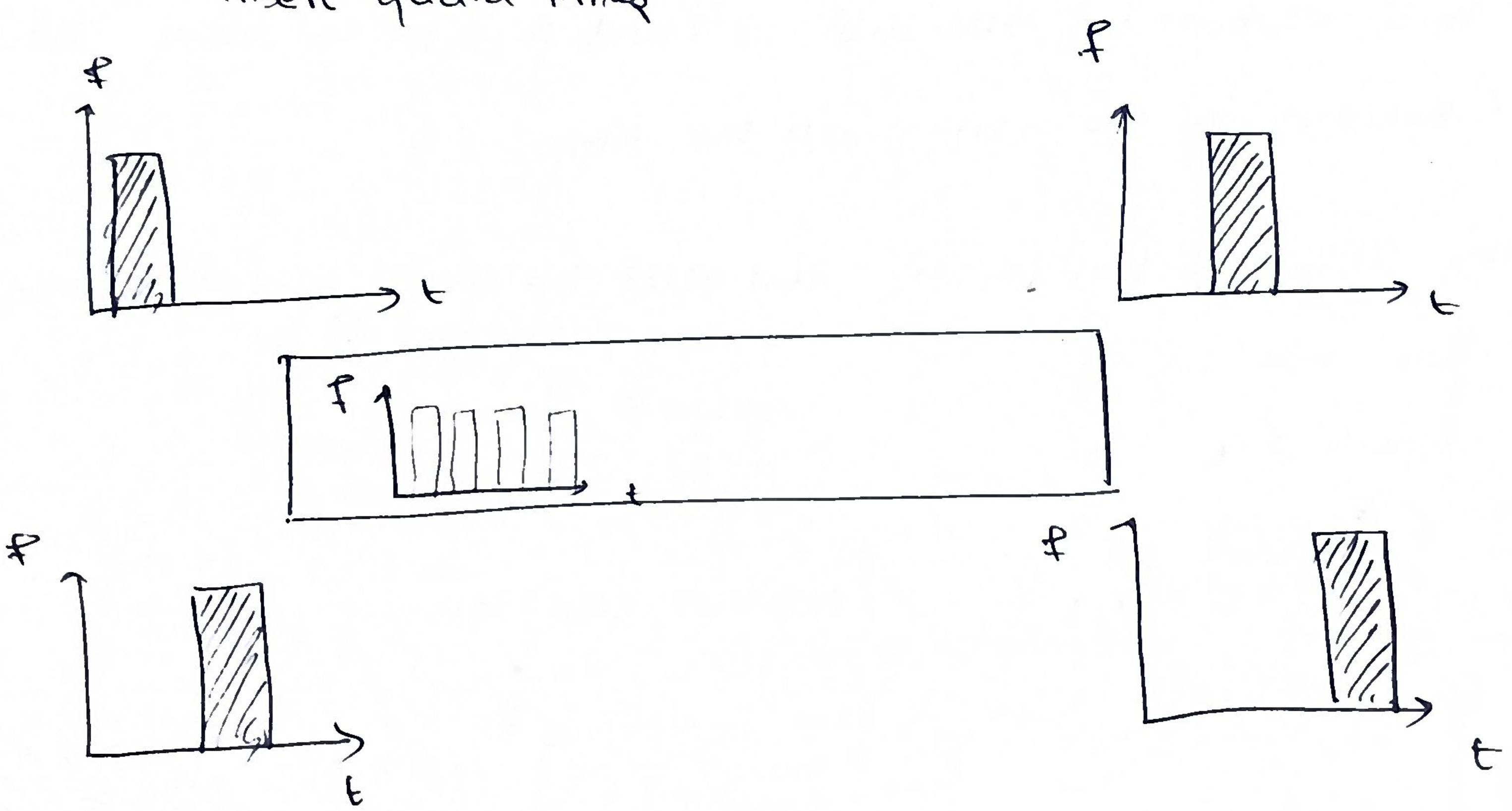
→ each station is allocated a band to send its data - and it belongs to the station all the time.

→ The allocated bands are separated by small guard bands



(2) TDMA - Time Division Multiple Access

- Stations share bandwidth of the channel in time
- each station is allocated a time slot during which it can send data.
- each station transmits its data in its designated time slot
- the main problem with TDMA lies in achieving synchronization between different stations
- each station needs to know the beginning of its slot and the location of its slot.
- may be difficult because of propagation delays - to compensate, insert guard times



(3) CDMA - code division multiple access

- one channel carries all transmissions simultaneously
- CDMA means communication w/ different codes.

Assume that there are 4 stations 1, 2, 3, 4. The data from station 1 is d_1, from station 2 is d_2, and so on.

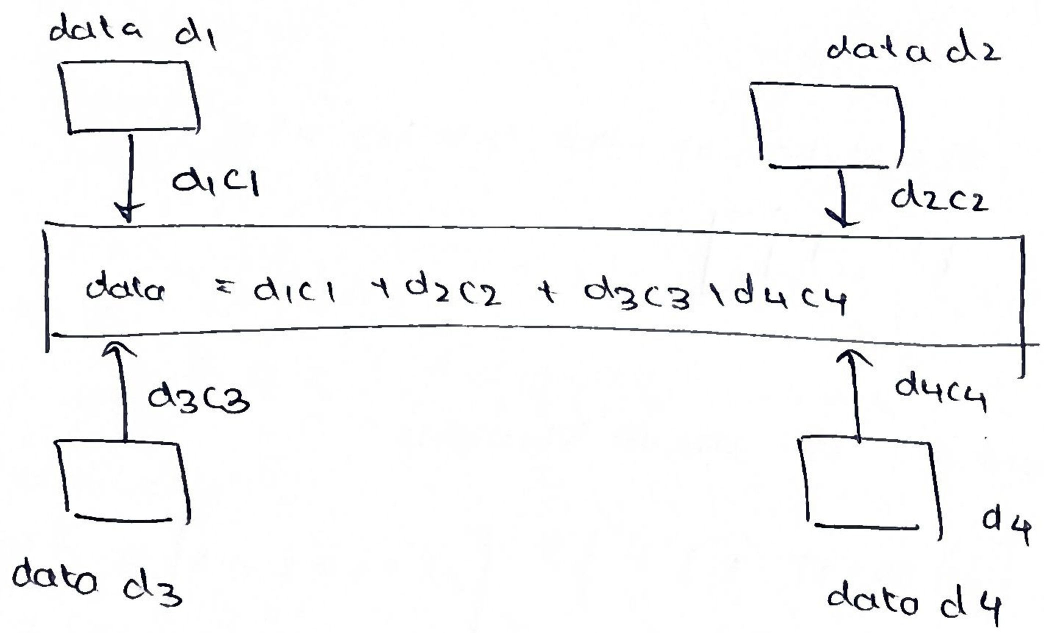
- The codes assigned to the first station is c_1, the second station is c_2 and so on.

- The assumed codes have the following attributes:

  (i) if we multiply each code by another - we get 0

  (ii) If we multiply each code by itself - we get 4, i.e the no. of stations

- CDMA is based on coding theory. Each station is assigned a code, which is a sequence of numbers called chips. - those are called orthogonal sequences



Data representation is as follows:

send	0	bit	$\Rightarrow -1$
send	1	bit	$\Rightarrow +1$
idle			$\Rightarrow 0$

Generate chip sequences using a $\boxed{\text{Walsh table}}$

$$w_1 = [+1] \qquad w_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix} \qquad w_4 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$$

Example : There are 4 stations.

Stations 1 and 2 are sending a 0 bit

Station ~~channel~~ 1 is sending a 1 bit

Station 3 is silent

Find the bit transmitted when:

(i) station 3 wants to listen to station 2

(ii) station 3 wants to listen to station 4

Ans Step 1: Generate the data at the sender site

$[-1 \quad -1 \quad 0 \quad +1]$

Step 2: Find data bit ~~chip sequences~~ of all 4 stations

sum

Station 1 $[-1 \ -1 \ 0 \ +1] \ [+1 \ +1 \ +1 \ +1] \quad [-1 \ -1 \ \pm 1 \ -1] = \underline{\underline{-4}}$ d_1c_1

Station 2 $[-1 \ -1 \ 0 \ +1] \ [+1 \ -1 \ +1 \ -1] = -1 +1 -1 +1 = \underline{\underline{0}}$ d_2c_2

$[+0 \ 0 \ 0 \ -0]$

Station 3 $[-1 \ -1 \ 0 \ +1] \ [+1 \ +1 \ -1 \ -1] = \underline{\underline{0}}$ d_3c_3

$[+1 \ \mp 1 \ -1 \ +1]$

Station 4 $[-1 \ -1 \ 0 \ +1] \ [+1 \ -1 \ -1 \ +1] = \underline{\underline{0}}$ d_4c_4

$\boxed{\sum d_i c_i = -4}$

Step3 Find resultant sequence.

$$\begin{bmatrix} -1 & -1 & -1 & -1 \end{bmatrix}$$

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

$$\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix} \quad +$$

$$\begin{bmatrix} +1 & -1 & -1 & +1 \end{bmatrix} \qquad -2+1$$

$$\begin{bmatrix} -1 & -1 & -3 & +1 \end{bmatrix}$$

Step4 : station 3 wants to listen to station 2

$= \begin{bmatrix} -1 & -1 & -3 & +1 \end{bmatrix} \times C_2$

$= \begin{bmatrix} -1 & -1 & -3 & +1 \end{bmatrix} \times \begin{bmatrix} +1 & -1 & +1 & -1 \end{bmatrix}$

$= -1 + 1 - 3 - 1$

$= -4$

data bit $= -4/4 = 1$

station 3 wants to listen to station 4

$\begin{bmatrix} -1 & -1 & -3 & +1 \end{bmatrix} \begin{bmatrix} +1 & -1 & -1 & +1 \end{bmatrix}$

$= -1 + 1 + 3 + 1$

$= 4$

data bit $= 4/4 = 1$ //

* Wired Lans - Ethernet

IEEE Project 802 - to set standards to enable intercommunication among equipment from a variety of manufacturers.

- It does not seek to replace any part of the OSI / TCP/IP protocol suite. - rather it is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

- The IEEE has subdivided the data-link layer into 2 sublayers: Logical link control (LLC) and media access control (MAC).

$\underbrace{\text{Logical link control (LLC)}}$ handles : flow control, error control, framing duties

$\underbrace{\text{media access control (MAC)}}$ handles: random access, controlled access, channelization

* Types of Ethernet

1. Standard Ethernet — 10Mbps
2. Fast Ethernet — 100 Mbps
3. Gigabit Ethernet — 1 Gbps
4. 10 Gigabit Ethernet — 10 Gbps

(1) Standard Ethernet

→ data rate of 10 Mbps

→ provides a connectionless service - each frame sent is independent of the other - no connection establishment / termination phases.

- sender can overwhelm w/ frames, or frames may drop
- can also get corrupted

Ethernet Frame

preamble	S/D	Destination address	Source address	Type	Data and padding	CRC

Addressing · with an NIC

- uses a 48 bit hexadecimal notation

sending addresses

eg. 47 : 20 : 1B : 8E : 08 : EE

binary 01000111 00100000 00011011 00101110 00001000

sent as 11101110

11100010 00000100 11011000 01101000 00010000

Access Methods - use CDMA/CD 01110111

Efficiency - $\left(\frac{1}{1+6.4 \times a}\right)$

Encoding and Decoding? - convert to a digital signal using the Manhattan scheme

- decode to data at receiver, after interpreting signal as Manchester

② Fast Ethernet

goals :

(i) upgrade data rate to 100Mbps

(ii) make it compatible with Standard Internet

(iii) keep the same 48 - bit address

(iv) Keep the same frame format.

→ includes a feature called autonegotiation. It has the following capabilities :

(i) allow incompatible devices to connect with one another

(ii) to allow one device to have multiple capabilities

(iii) to allow a station to check a hub's capabilities

③ Gigabit Ethernet

goals :

(i) upgrade data rate to 1Gbps

(ii) make it compatible w/ Standard or Fast Ethernet

(iii) use the same 48 - bit address

(iv) use the same frame format

(v) Keep the same min & max frame lengths

(vi) support autonegotiation defined in Fast Ethernet

④ 10 Gigabit Ethernet

- use of Ethernet for metropolitan areas -

- extend the technology, data rate & coverage distance that it can be used in LANs & MANs.

goals : (i) upgrade data rate to 10 Gbps

(ii) keep same frame size and format

(iii) allow interconnection of LANs, MANs and WAN

→ This data rate is possible only with fibre-optic technology

* Wireless LANs

* Architectural Comparison between wired & wireless LANs

A. Medium

wired - use wires to connect hosts

wireless - medium is air

B. Hosts

wired - host is always connected to its network with a fixed link layer address related to its NIC

wireless - host is not physically connected to the network.

C. Isolated LANs

wired - connect hosts with a link layer switch

wireless - adhoc network - hosts that communicate freely w/ one another.

D. Connection to other Networks

wired - connect to another network using a router

wireless - connect via access point

L. Moving between environments

→ To move from wired to wireless network - change the NIC cards,

→ The link layer address changes, but the network - layer addresses (IP addresses) remains the same.

* Characteristics of Wireless Networks

1. Attenuation - strength of em signals decreases with ~~distance~~ distance.

2. Interference - receiver may receive signals not only from the intended sender, but also from others if they are using the same frequency band.

3. Multipath Propagation - may receive more than one signal from the same sender because em waves are reflected back from obstacles like walls, the ground or objects

4. Error - more susceptible to errors - measure with SNR.

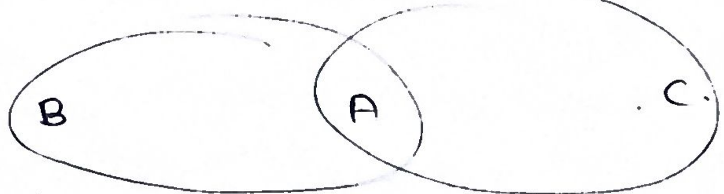
* Access Control - standard Ethernet uses CSMA/CD. however, this does not work in wireless media for 3 reasons

(1) Wireless networks are not duplex - cannot send & receive a signal at the same time - to detect collisions

(2) Hidden Station Problem

B & A both send

collision occurs at A



(3) Distance between stations is very large.

* IEEE 802.11 Project

→ specifications for wireless LAN - also called wireless Ethernet.

Architecture - defines 2 kinds of service

(i) Basic Service Set (BSS)

(ii) Extended Service set (ESS)

A. $\boxed{\text{BSS}}$

→ made up of stationary or mobile wireless stations and an optimal central base station called the access point

→ if the BSS does not have an AP- it is called an adhoc architecture,

with an AP- it is called an infrastructure BSS.

B. $\boxed{\text{ESS}}$

→ made up of 2 or more BSSs with APs.

→ The BSSs are connected through a distribution system

→ When BSSs are connected, stations within reach of one another can communicate without an AP, but between a station in a BSS and the outside BSS occurs via the AP.

Station Types - 3 types

(i) no-transition mobility - stationary or within BSS

(ii) BSS - transition mobility - move from one BSS to another, but the movement is constrained within the ESS

(iii) ESS - transition mobility - move from one ESS to another