CN

Hardware

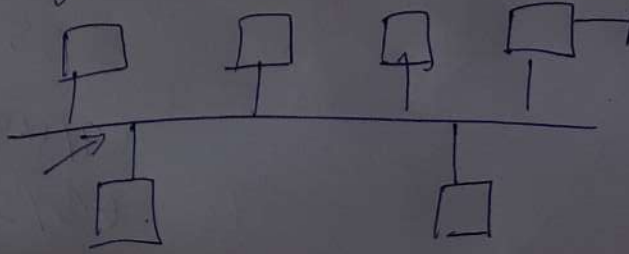
Network Topology

Objective: Describe the backbone structure that form the foundation for most LAN.

Physical Topology: Physical layout of nodes on n/w

a) BUS topology

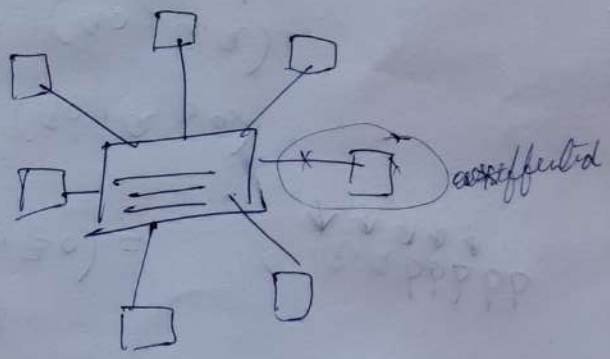
* On this config, every computer shares n/w total bus capacities
* By adding more computers, will reduce the access speed on n/w
* Devices share responsibility for getting data from one pt to another



* All computers are connected to a long cable called bus.
* In this topology, any computer can send data over the bus at any time.
* Terminator stops signals after reaching end of wire. (to avoid signal bounce).
* peer to peer n/w.

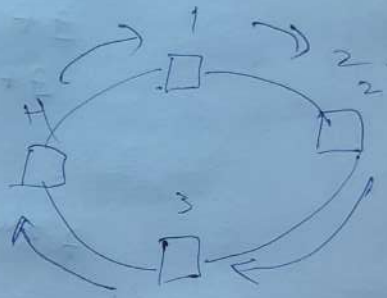
Star topology.

* Every node in on n/w is connected through a central device like hub, switch, router.



Ring Topology

* Used for LAN, WAN in which each system has 2 neighbours for communication

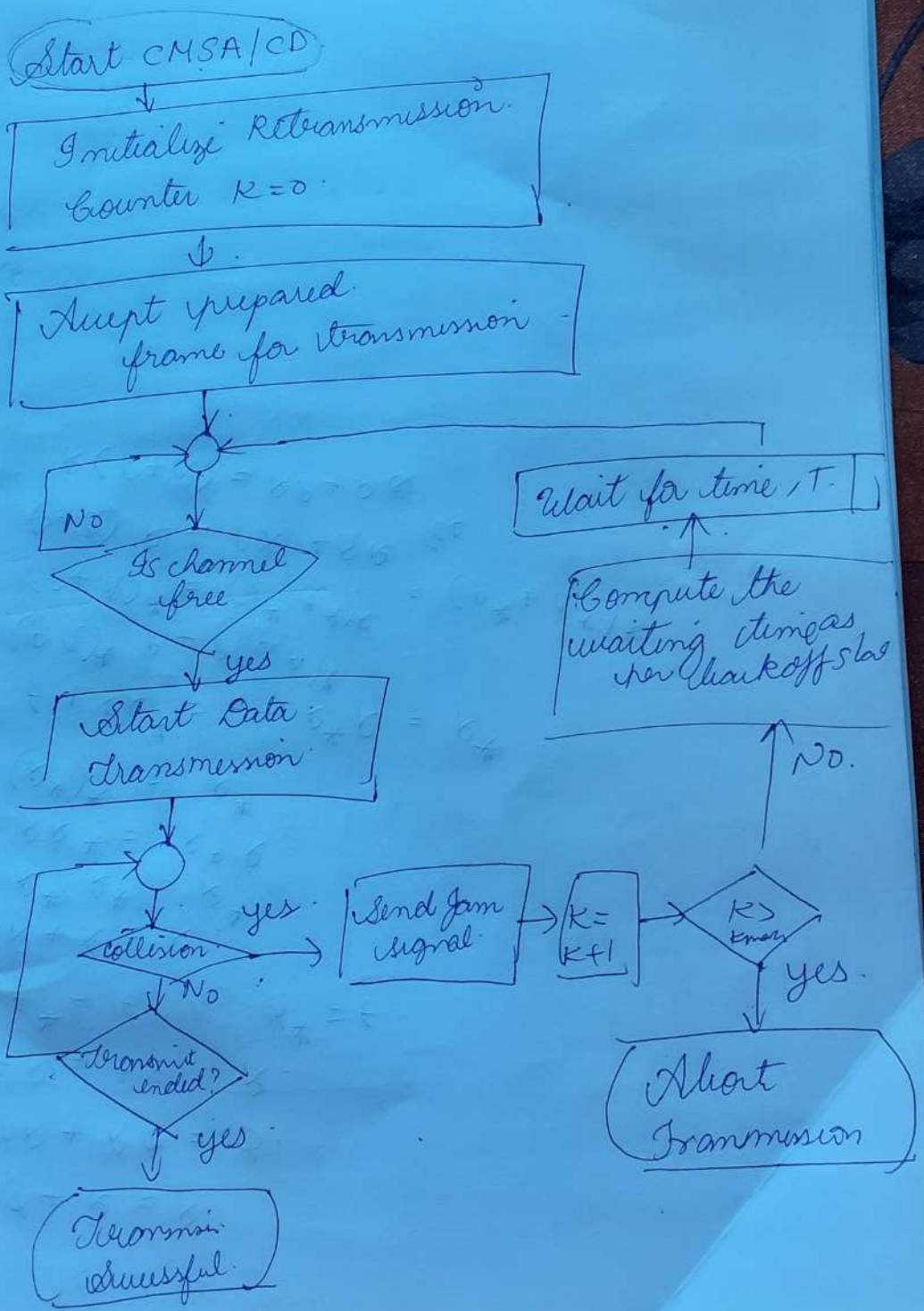


* One direction

CSMA/CD

Theory:- In this a station monitors the medium offers it sends the frame to see if the transition was successful if so, the station is finished more, else if there is a collision the frame is sent again

Flow diagram


Start CMSA/CD
Initialize Retransmission Counter K=0
Accept prepared frame for transmission
No
Is channel free
yes
Start Data transmission
collision
yes
Send Jam signal
K= K+1
K> Kmax
yes
Abort Transmission
No.
Compute the waiting time as per backoff algo
Wait for time, T.
No
Transmit ended?
yes
Transmission successful

DNS

* Domain Name System
* Directory service that provides mapping b/w name of host on the network & numerical address
* DNS is a service that translates the domain name into IP address
* This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering IP address
* Eg:- FTP site at EduSoft had an IP of 132.147.165.50, most people would reach out to this site by specifying ftp.EduSoft.com
* Domain name is more flexible than IP address
* DNS is TCP/IP protocol
* Domain name space is divided into generic domains, country domains, inverse domain

Generic:

biz - business, com - commercial, edu - educational, gov - govt, info - information service providers, mil - military groups, org - non profit organisat

Country

In - India, uk - UK,

Inverse

* The inverse domain is used for mapping an address to a name.
* When the server has received a request from the client, The server has files only of authorized clients
* To determine whether the client is authorized or not, it sends a query to the DNS server, & ask for mapping an address to name

Application Layer protocols

used by users
eg :- email

which help & support the protocols
eg :- DNS

DNS Working

* Works on client server model
* translates DN into IP address
* eg :- domain name www.shreya.com
  ⇓
  198.105.137.55

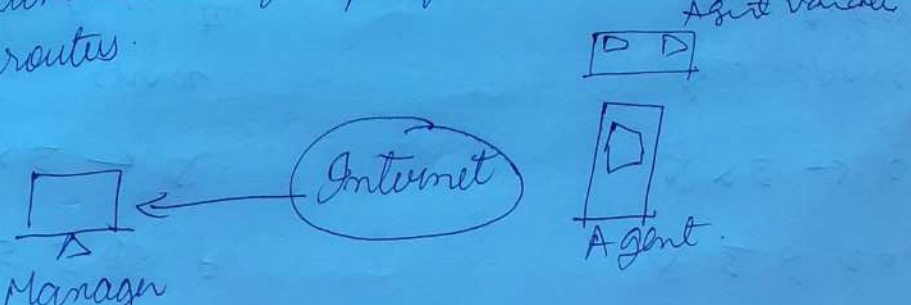
SMTP

* Simple Mail Transport Protocol.
* Internet standard for e-mail transmissio
* SMTP connections are secured with SSL
* In SMTP, the messages are stored & then forwarded to the destination

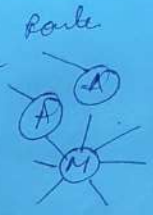
* SMTP uses a port no of 25 of TCP
* The concept of SN

SNMP

* SNMP means Simple Network Management Protocol defined by IETF
* It is used to manage the network
* It is an internet standard protocol that monitors devices in IP networks
* SNMP is supported by most of network devices such as hub, switch, router, bridge, modem & printer
* The concept of SNMP is based on manager & agent
* The manager is like a host that controls a group of agents, such as routers



Components



① Manager :- Centralized system to monitor n/w

② Agent :- It is a software program that is located in the network
* It collects real-time info from the device & passes this info to SNMP manager

~~(3)~~

Management Components

① SMI :-
* Structure of Management Info :-
* It is a network management comp.
* It defines rules for naming object & object type.

② MIB.
* Management Information Base :-
* Second comp of network managent.
* Virtual Info storage where management is stored

SNMP basic Operation

- Get Req ↓ retrieve one or more values. [M→A]
- Get next Req ↓ next value [M→A]
- Set Request ↓ setting value [M→A]
- Trap ↓ send acknowledgement messages [A→M]
- Get Bulk Request ↓ retrieve large data [M→A]

HTTP

* Hypertext transfer protocol
* Transfer data
* Good efficiency
* Similar to FTP
  - coz - transfers file from 1 host to other
  - but - HTTP better coz only 1 connection
* Similar to SMTP:
  - coz - Client server.
  - but HTTP better coz SNTP - stored & forwarded
    HTTP - delivered immediately

HTTP features

① Connectionless :

* client sends req, wait for res.
* server gets req, process the req, sends res after which client disconnects connection.

② Media Independent

* data can be sent as long as both CS know how to handle data content
* Requirement : Content type in MIME header

③ Stateless :

CS know each other only during current req

URL :

Method :// Host : port / Path

http:// www. ____ .com / path

E-Mail

* Transmission of messages on Internet.
* most common communication
* Info stored in one PC is sent through net to an individual
* It uses multiple protocols within TCP/IP.
* Uses SMTP to send msgs.
* IMP or POP to retrieve msgs.
* Login, email, Pswd,
* Webmail servers automatically configure mail.
* Manual config for - Outlook, Apple Mail.
* Email msg — 3 components — Msg envelop.
  — Msg header
  — Msg body.
* Org Email supports plain text — Modern, html, CSS.
* Send all kinds with msgs.
* 1971, Ray Tomlinson, sent to himself — QWERTYUIOP, transmitted — ARPANET
* MAILBOX — MIT, first email system
* Advantages — cost effective, access from anywhere. Better communication, speed of simplicity, mass sends.

Streaming

* Early websites — text, img.
* Today — HD movies, audio calls
* Streaming is continuous transmission of audio or video files from server to client.
* AV broken into data packets

WWW

* collection of websites
* stored in web servers.
* connected to local comp thru Internet.
* Websites contain
* Users can access from any part of the world.
* BBoj web → HTML —connected by links→ Hyperlinks —accessed by→ HTTP
* WWW → like huge e-book whose pages r stored on multiple servers.
* Book — one page to other;
  WWW — hyperlinks to more.
* Need a browser, to access web.

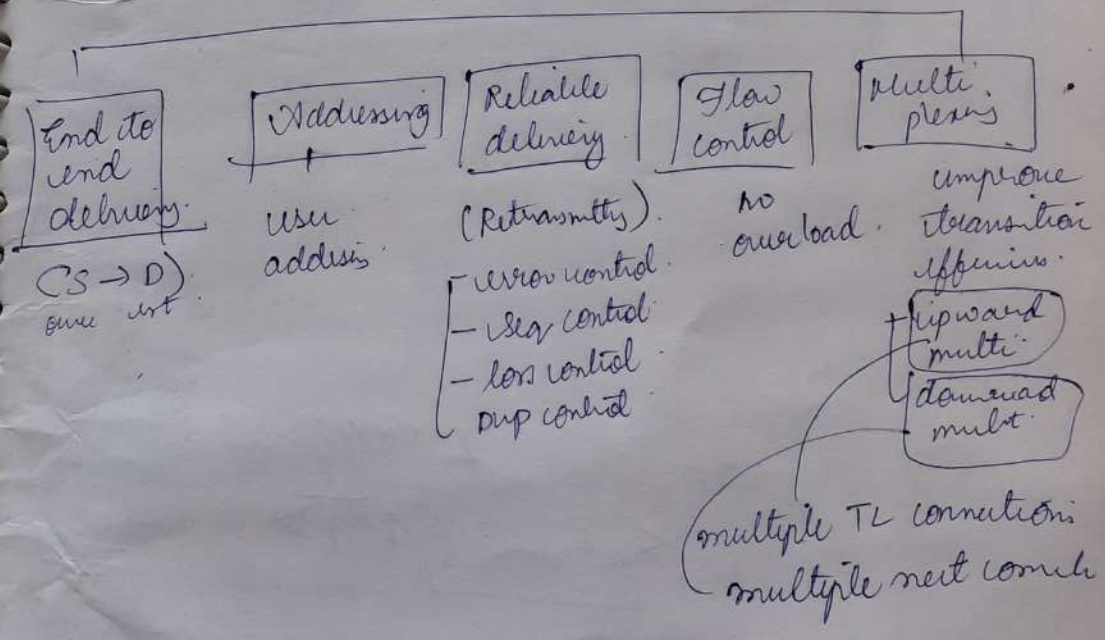
UNIT-4

Transport Layer

Services provided by TL

* similar to DLL.
* but TL provides services across an internetwork made up of many networks
* Controls all the lower layers

TL Services



Elements of TP

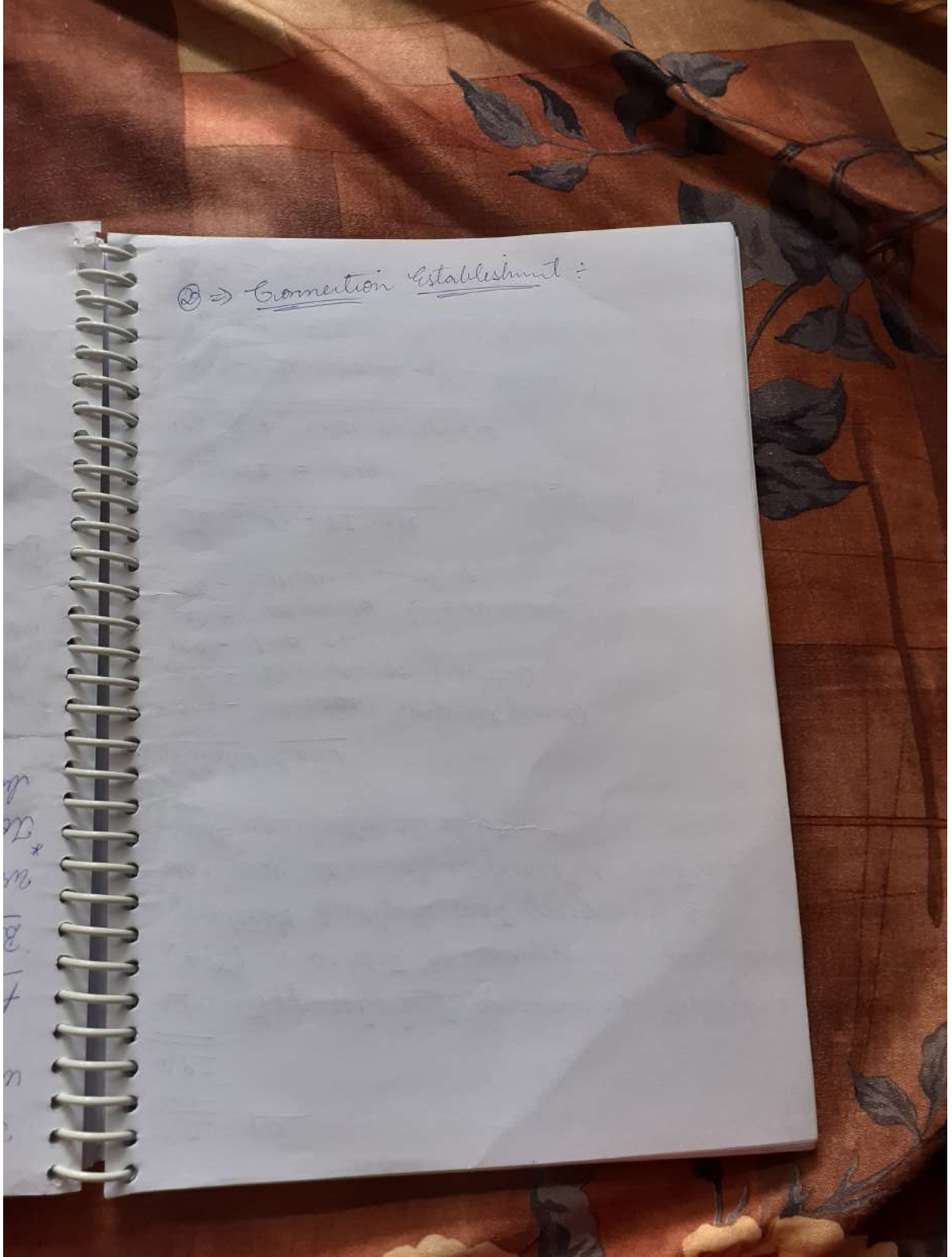
1. Addressing
2. Connection establishment
3. Connection Release
4. Error control, flow control
5. Multiplexing

(1) ⇒

* When an application process wishes to set up a connection to remote application process, it must satisfy which one to connect to
* The method normally used is to define transport address
* In internet, these endpoints are called ports

3 Ports

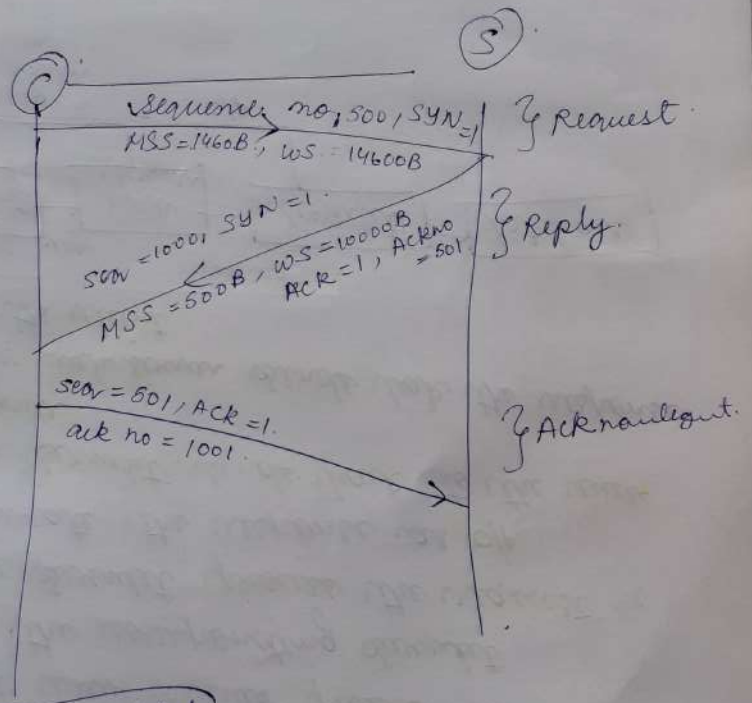
* TSAP: Transport Service Access point to mean a specific endpoint in transport layer
* IP addrss are examples of NSAP


② ⇒ Connection Establishment :

Connection Management

Connection establishment

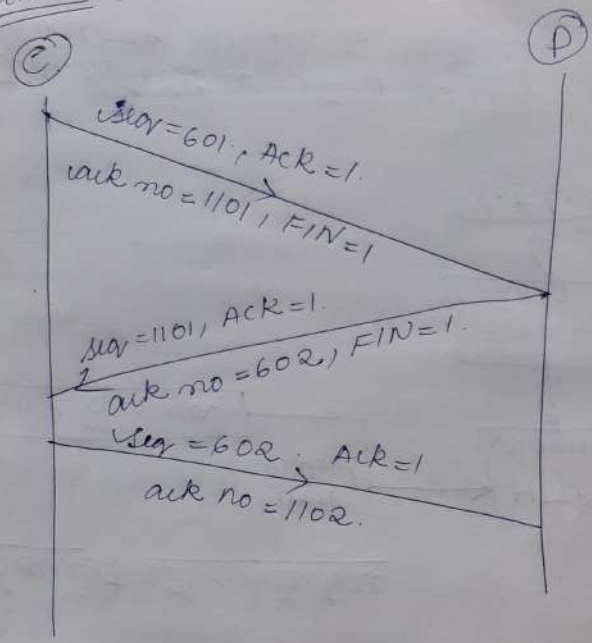
Connection Termination



3 way handshake

Request, Reply Acknowledgment

Termination.



SYN	ACK	
1	0	→ I
1	1	→ II
1	0	X.
0		

~~Ack~~ r

Ack is always 1.

UNIT-3

Network Layer Design Issues

*(1) Store & forward packet switching
*(2) Services provided to Transport layer
*(3) Implimentation of connectionless service
*(4) Implimentation of connection oriented service
*(5) Routing
*(6) Congestion Control

(1)* The node which has packet to send, delivers it to the nearest node i.e router.
* The packet is stored in the router until it has fully arrived & its checksum is verified for error detection.
* Once this is done, the packet is transmitted to the next router.
* The same process is continued un

each router until the packet reaches destination

(2) Services provided to Transport Layer
Goals to keep in mind:

* Offering services must not depend on router stuff
* The transport layer needs to be protected from the no of Topology available

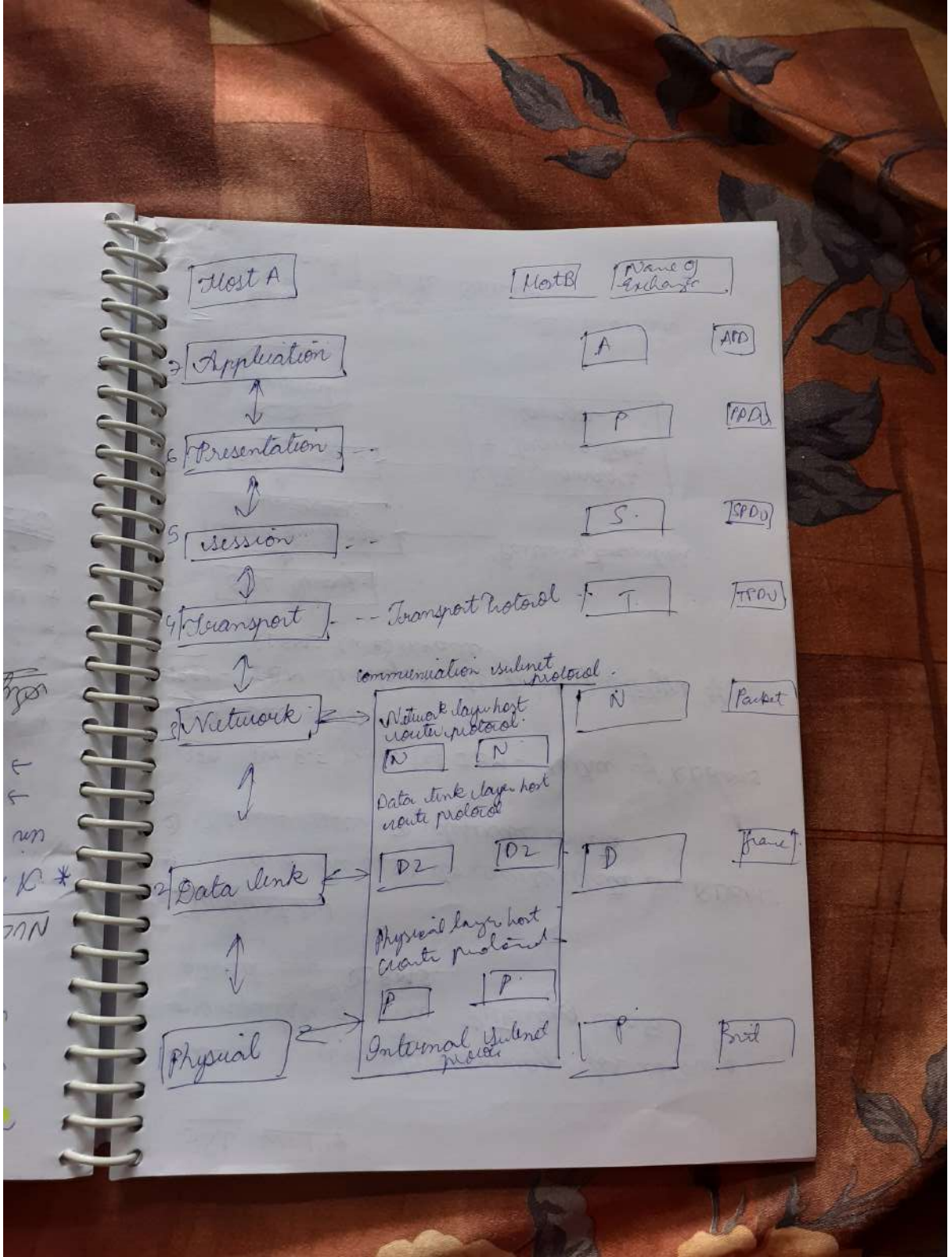
OSI Reference Model

In, CN, RM gives conceptual framework that standardizes comm b/w 2 heterogenous networks

2pop - OSI / TCP/IP

OSI

* Open System Interconnection
* dev by ISO.
* gives layered Networking framework
* conceptualizes :-
* 7 interconnected layers.
* Each lay - self contained - each perform tasks independently.


Host A
Host B
Name of exchange
Application
Presentation
session
Transport
Transport protocol
Network
communication subnet protocol
Network layer host route protocol
N
N
Data link layer host route protocol
D2
D2
Data link
Physical layer host route protocol
P
P
Internal subnet protocol
Physical
A
P
S
T
N
D
P
APDU
PPDU
SPDU
TPDU
Packet
Frame
Bit

PL

- Physical Medium — bits are transmitted
- lowest layer.
- establishes, maintain deactivate physical conn.

DLL

* Error free transfer of Dataframes.
* Reliable & efficient. com. b/w 2 devices.
* 2 sub layers.
  1. logical link
  2. Media acc.

NL

* Layer 3.
* Manages a) device addressing,
  b) tracks location

Determines best path to move data from S-D.

Factors ÷ network cond.
priority of service.

Routers Network traffic protocols are called.

NL protocols

Eg ÷ IP & IPV6.

Transport

— 4.
— no duplication of data.
— main res : transfers data completely.
— 2 main protocols
  * TCP, UDP

Session

— 5
— establish, maintain & synchronize interaction b/w comm dev

Presentation

— 6
— contents concerned with :
  Syntax & Semantics of info exchange b/w 2 sys.
— PL also called Syntax layer

App layer.

* 7
* Window for users & app processes.
* Provides n/w to end users.

TCP/IP (NIDTA)

* Dev by DSI
* 5 layers
* ~~ACINPLPL~~
* Its a hierarchical protocol

① Network Layer
* lowest
* combo of PL & DLL
* Protocols : ethernet, Token ring, FDDI, X.25, frame relay

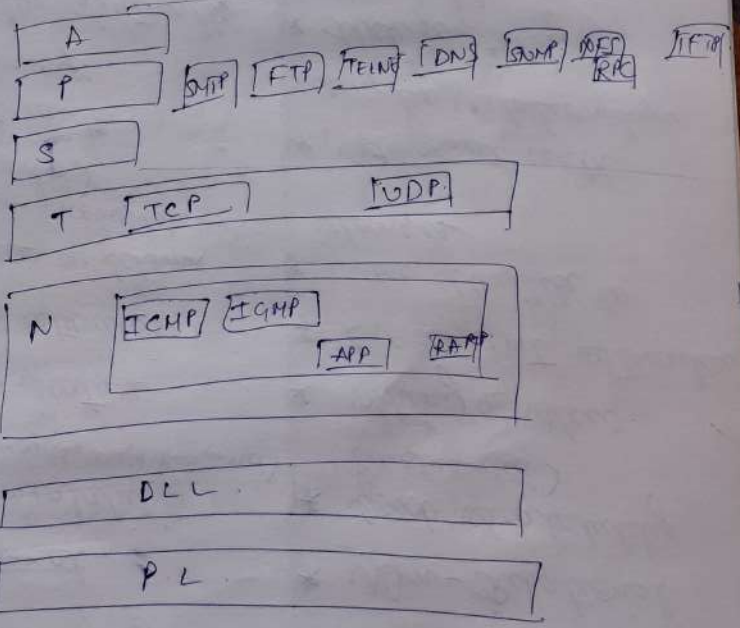
② Internet layer
* 2nd
* known as network layer

③ DLL
* Identifies the protocol packet, here TCP/IP.
* provides : error control.
flow

④ TL
* ~~Options~~ TC is responsible for reliability flow control & connection data which is being sent over the network

(5) Application

* topmost
* user interacts with communication
* Responsible for high level protocol services eg: ftp.



CRC

* Cyclic Redundancy Check.
* Error detection.

Steps

* 0's is appended to Data unit.
* n no is less than no of digits in predivisor no known as division unit n+1 bits
* Secondly :- the newly extended data is divided by a divisor — process — binary division.
— Remainder generated — CRC Remainder
* Thirdly :- the CRC Remainder replaces the appended 0's at the end of org data
— This newly gen is sent to the receiver.
* Receiver receives the data followed by CRC remainder.
* Receiver treats the whole as single unit.
* Then decides that it is divided by the same divisor

Error detection Methods

VRC | CRC | Checksum | ¢RC

CRC

CRC generation at sender side

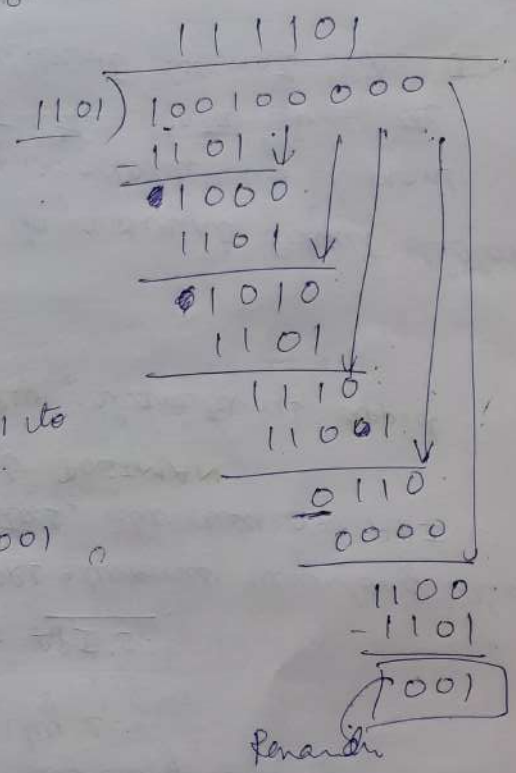
1. find the lt of divisor L
2. Append L-1 'zeros' to Long msg
3. perform binary operation
4. Remainder division = CRC

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Note: CRC must be L-1 bits.

eg. 1101

100100



L = 4, L-1 = 3

So 3 zeros are appended to msg

appending 001 to the orig msg

i.e 100100001

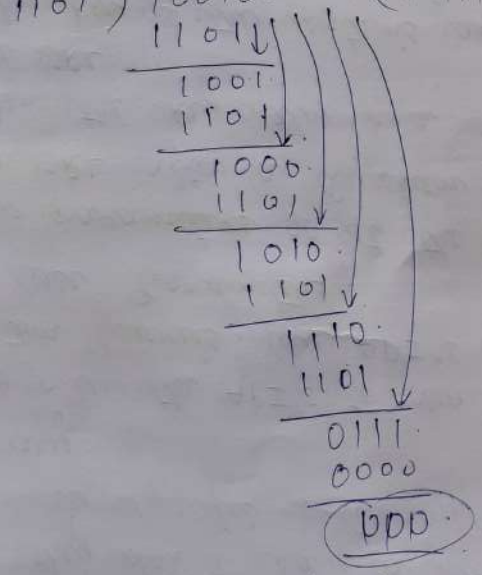
At receiver side.

CRC = 001

Data Transmitted = 1001 00 001

Let the same data be received by receiver without transmission error.

divisor is same



If all are 0's the receiver understands that that is no error

Protocols

Noiseless channels

- Simplest
- Stop & wait

Noisy channels

- Stop & wait ARQ
- Go Back N ARQ
- Selective Repeat ARQ

Stop & wait

* PDL protocol over noiseless channels
* Used for transmission of frames.
* provides unidirectional, with flow control without error control facility.
* One frame $\xrightarrow{\text{tran}}$ sender waits for ack by transmits next frame.
* flow control ✓ error control ✗

PRIMITIVES.

Sender

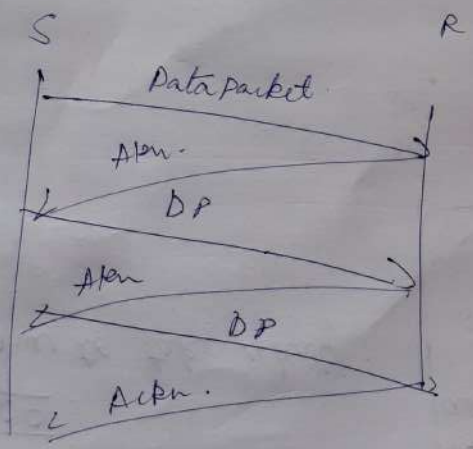
Rule 1: Send one packet at a time.

Rule 2: Send next pckt only after receiving akn for the previous.

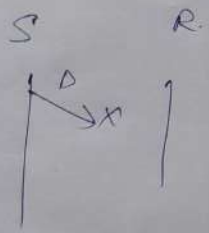
Receiver

Rule 1: Receive the consumed data packet.

Rule 2: After consuming the packet, Ack needs to be sent.



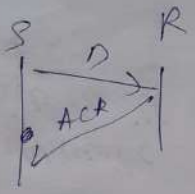
Problems



Problems due to lost data

* Sender waits for ack for ages.
* Recvr waits for data.

Prob due to ~~ack~~ delayed ack/data

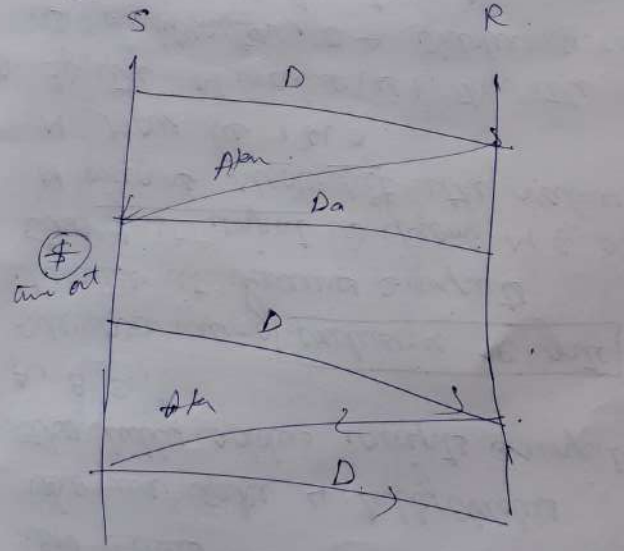


* After timeout on Sendr.

Sliding Window Protocol

Up-Back ARQ ce utilizeaza Repeat ARQ is called sliding window protocol.

STOP ce WAIT ARQ

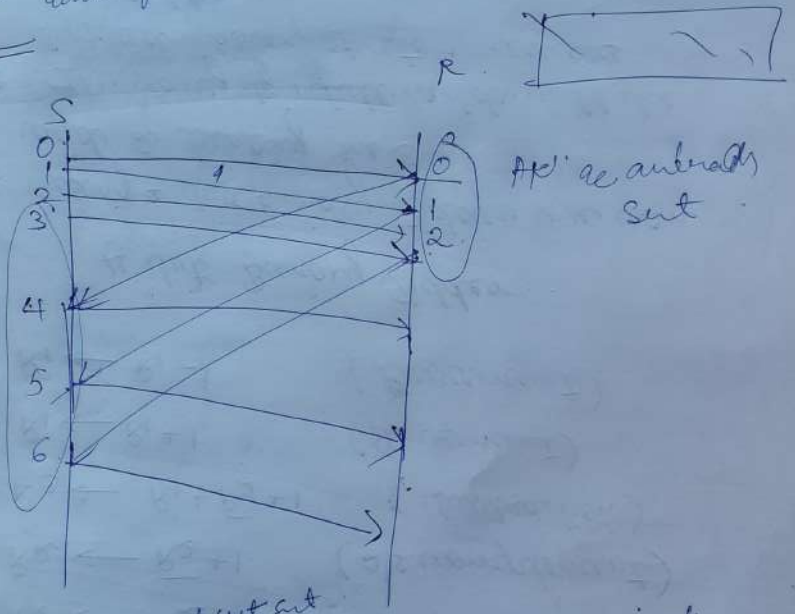


DRAWBACKS

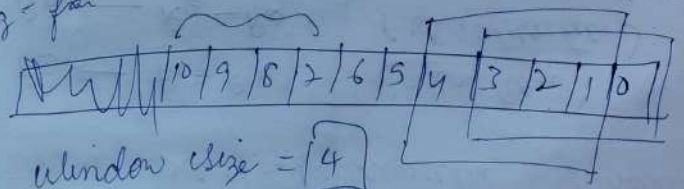
only one frame pothuda
Poor utilization of BW.
Poor performance

SWP

* Sending multiple frames.
* No of frames to be sent is based on window size.
* Each frame is numbered called seq no.



Eg:- frames



0 is akn.
4 is sent

window size = 4

Go Back N ARQ

Nw sender window size

If n=3
2 frames can be sent

Automatic Repeat ARQ
Retransmission

* Concept : protocol pipelining
* Sender sends multiple frames by using the ack for first frame
* no of seq no's
* no of frames = window
* If ack of frame is not received it is relevant

Window size = 4 = (2^2)

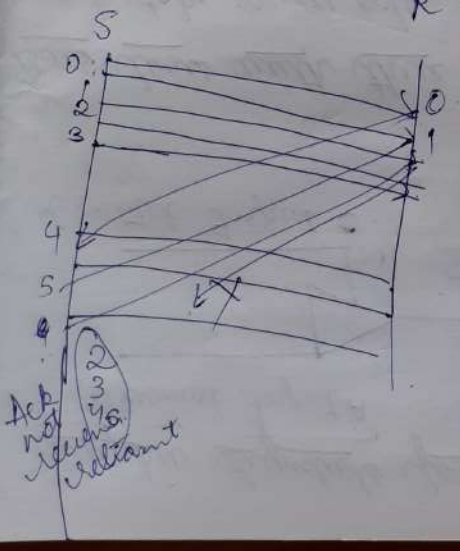
0123

0123 0123 01 . . . .

| 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

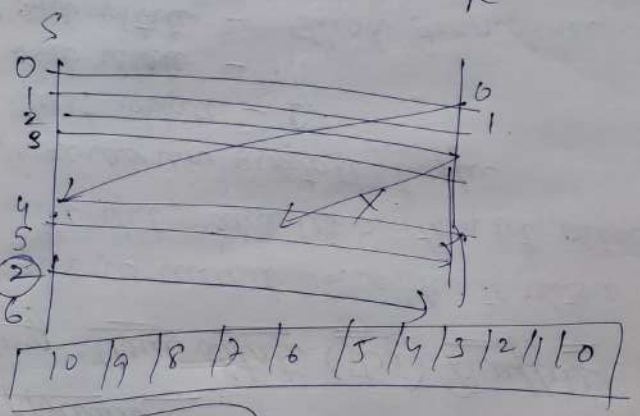
W = 4

| 3 | 2 | 1 | 0 |



Selective Repeat

* Only lost frame are retransmitted
* Receiver - ve ackn



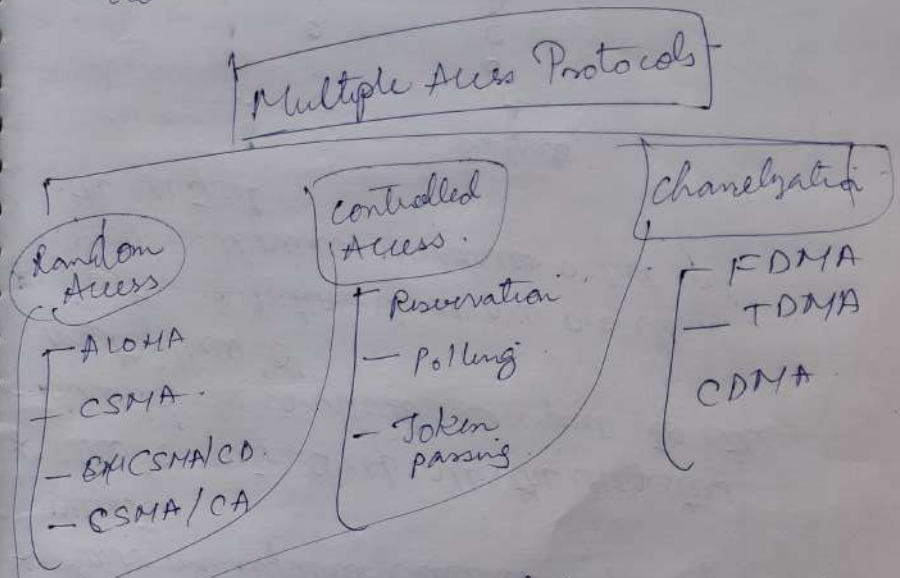
10	9	8	7	6	5	4	3	2	1	0

$w = 4$

Multiple Access Protocols

collision.

* It is used if it is not in the side in common



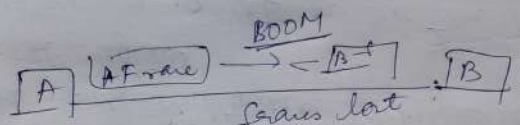
→ Any station can send at any time.

→ Medium will be controlled by station Authority

→ Multiple access Method bandwidth share.

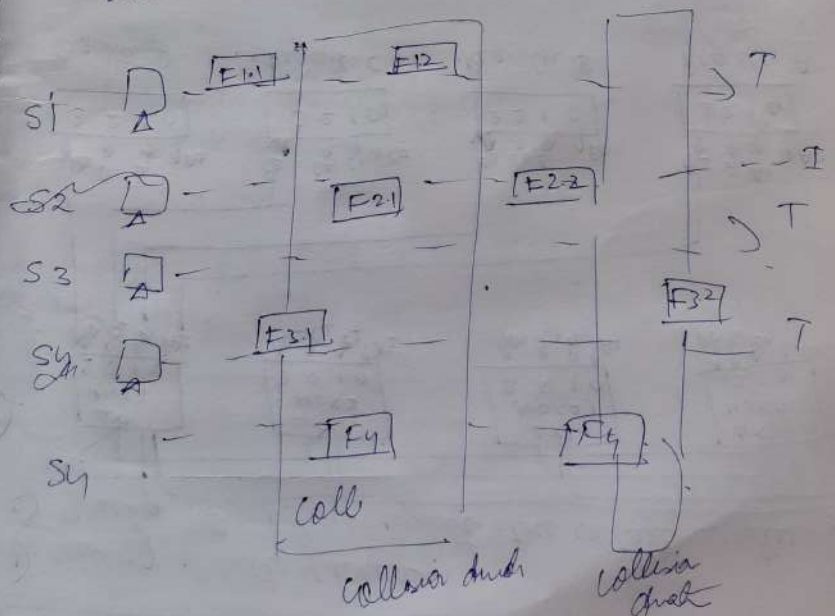
ALOHA

* RA Protocol
* WLAN & Shared Medium
* collision avoidance



2 types

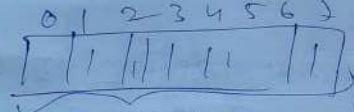
Pure Aloha
Slotted Aloha



collision free Protocols

1. Bit Map
2. Binary Count Down
3. Limited Contention
4. Adaptive tree Walk

(1) * Operates in MAC layer
* N slots
1 Total stations - same medium
* slot 1 is to send others wait



Sets Bit value to 1
done by slot no's

Wireless LAN's

very flexible.
Adhoc n/w do not need plans
no wiring difficulties
more robust.

Disadv

Low Bandwidth
National restrictions

Design

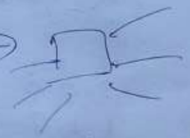
global
Low power for battery use
Robust to Tech.

Adv

flexible
Plans
design
solutions
cost
Ease of use.

Switching

→ Computer Network.

→ 

→ PDZ do proost

→ home config X.

→ forwards packets based on MAC adress

→ Duplex mode.

→ Switches is very busy (Bandwidth)
    (collision)

Hierarchial Routing Protocols

Benefits.

Reduction in the use of Routing

- Better Scalability

Multi clustering - to enhance resource allocation & management.

At every level A leader is elected.

Each cluster one leader

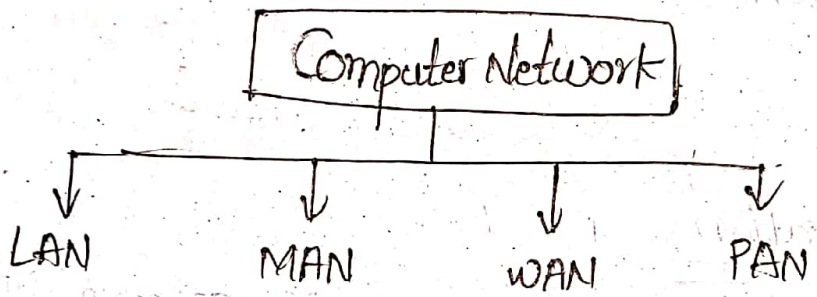
path b/w 2 cluster heads consisting multiple links called virtual link

2. Explain types of Computer Networks?

⇒ A Computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data and application.

⇒ A Computer can be categorized by their size.

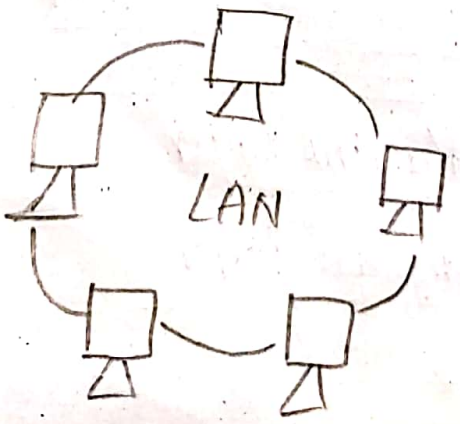
⇒ A Computer network is mainly of 4 types.



① LAN [Local Area Network]:

⇒ Local area network is a group of computers connected to each other in a small area such as building, office.

⇒ LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable etc.

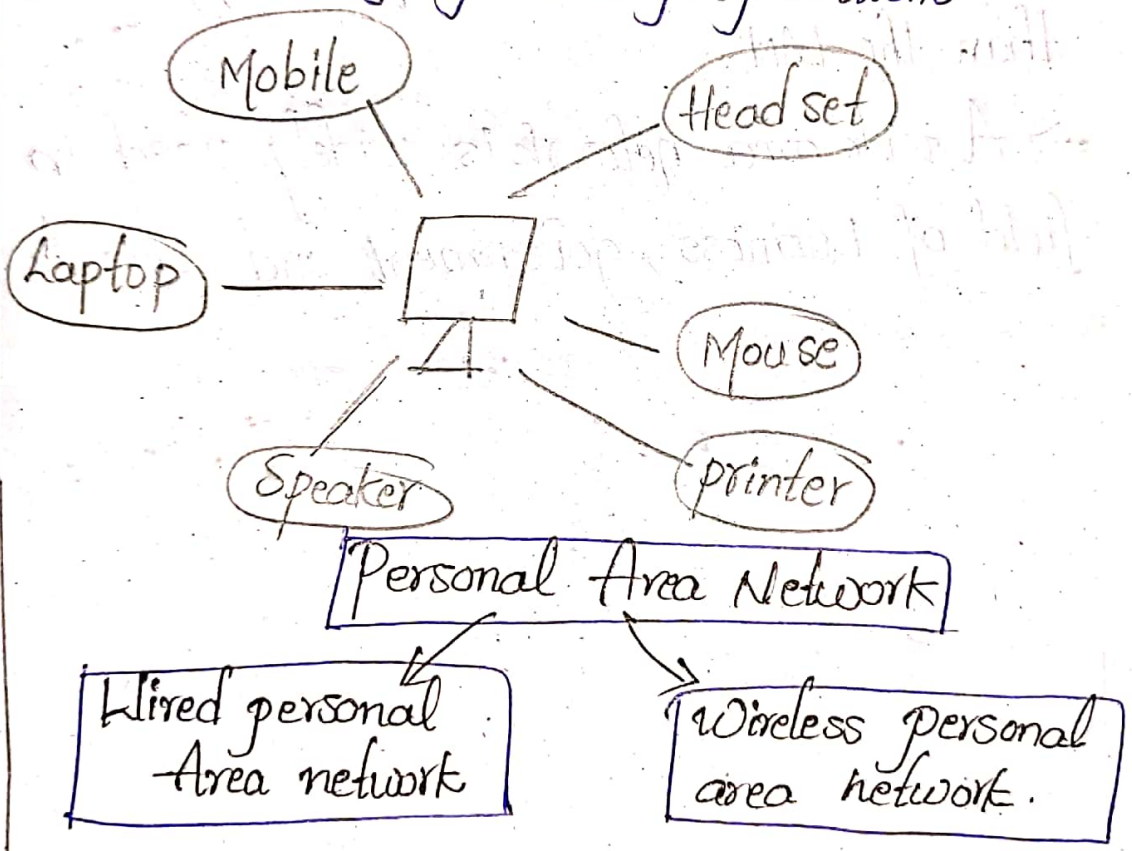


(ii) PAN (Personal Area Network):

⇒ personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.

⇒ Personal area network covers an area of 30-feet.

⇒ Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.



(iii) MAN (Metropolitan Area Network):

⇒ A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to perform a larger network.

⇒ It has a higher range than local area network

⇒ The most widely and protocols in MAN are RS-232, frame Relay, ATM, ISDN, OC-3, ADSL etc.

(N) WAN (Wide Area Network):

⇒ A wide area network (WAN) is a network that extends over a large geographical area such as States or Countries.

⇒ A wide area network is quite bigger network than the LAN.

⇒ A wide area network is widely used in the field of Business, government and education.

UNIT-1

Assignment-1

1. Explain Reference models in Computer networks?

In Computer networks, reference models give a conceptual framework that Standardizes Communication between heterogenous networks.

⇒ The two popular reference models are:

* OSI Model
* TCP/IP protocol Suite

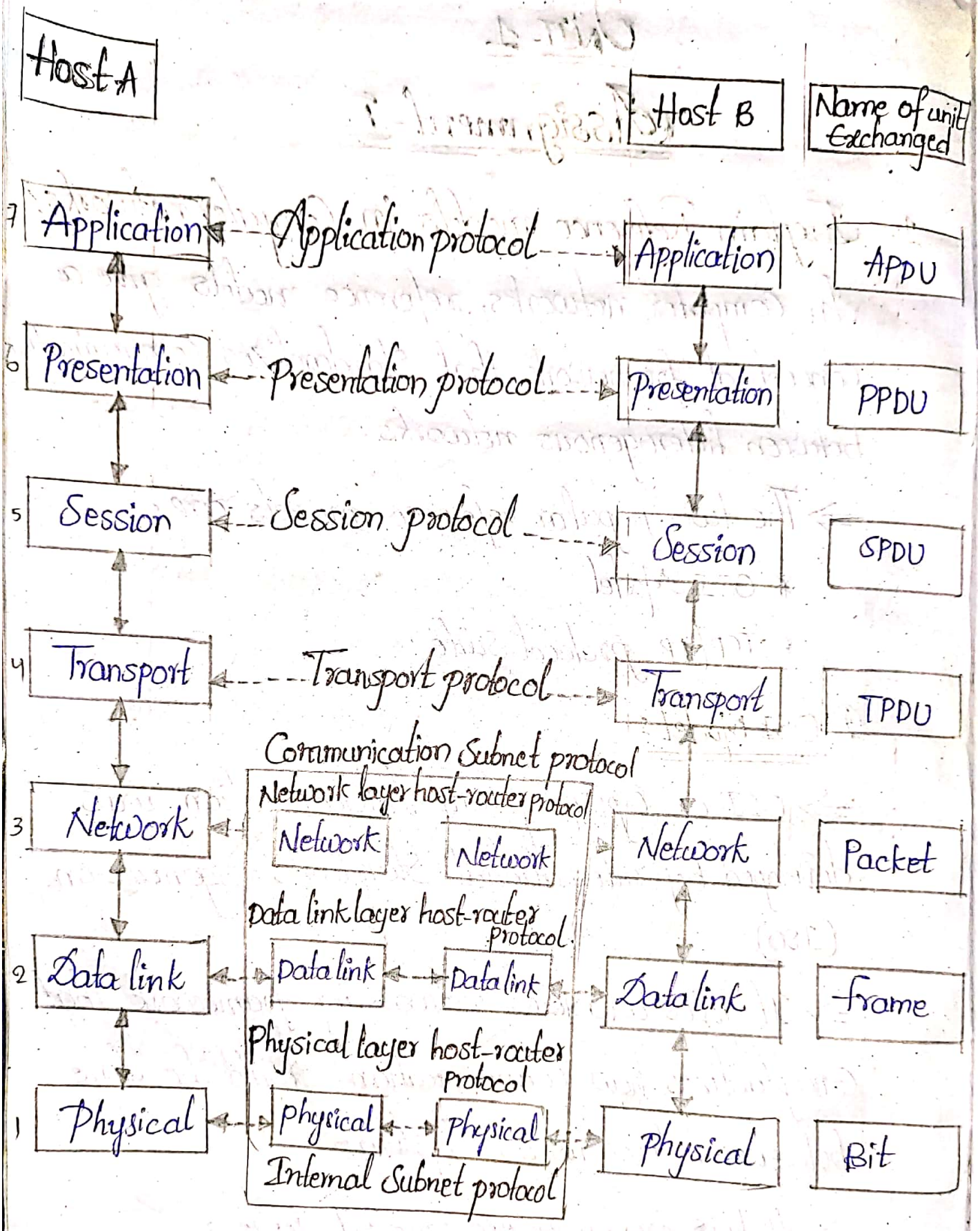
1) OSI Model:

⇒ OSI or Open System Interconnection was developed by international Standards Organization (ISO).

⇒ It gives a layered networking framework that Conceptualizes how Communication should be done between heterogeneous Systems.

⇒ It has Seven interconnected layers.

⇒ Each layer is self-Contained, So that task assigned to each layer can be performed independently



⇒ OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.

⇒ The Seven layers of the OSI Model are a

- physical layer
- Data link layer
- Network layer
- Transport layer
- Session layer
- presentation layer
- Application layer.

① Physical Layer:

⇒ It provides a physical medium through which bits are transmitted.

⇒ It is the lowest layer of the OSI model.

⇒ It establishes, maintains and deactivates the physical connections.

② Data-Link Layer:

⇒ This layer is responsible for the error-free transfer of data frames.

⇒ It provides a reliable and efficient communication between two or more devices.

⇒ It Contains two Sub-layers:

(i) Logical link control layer

(ii) Media access Control layer.

③ Network layer:

⇒ It is a layer 3 that manages devices addressing tracks the location of devices on the network.

⇒ It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.

⇒ The protocols used to route the network traffic are known as Network layer protocols.

* Examples of protocols are IP and IPV6.

④ Transport layer :

⇒ The transport layer is a layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.

⇒ The main responsibility of the transport layer is to transfer the data completely.

⇒ The two protocols used in this layer are :

* Transmission Control protocol
* User Datagram protocol.

⑤ Session layer :

⇒ It is a layer 5 in the OSI model

⇒ The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

⑥ presentation layer:

⇒ A presentation layer is mainly concerned with the syntax and Semantics of the information exchanged between the two systems.

⇒ The presentation layer is also known as the Syntax layer.

⑦ Application layer:

⇒ An application layer serves as a window for users and application processes to access network service.

⇒ This layer provides the network services to the end users.

*TCP/IP Model:

⇒ The TCP/IP model was developed prior to the OSI model.

⇒ The TCP/IP model consists of five layers: the application layer, transport layer, network issue, data link layer and physical layer.

⇒ TCP/IP is a hierarchial protocol made up of interactive modules, and each of them provides specific functionality.

(i) Network Access Layer:

⇒ A network layer is the lowest layer of the TCP/IP model.

⇒ A network layer is the combination of the physical layer and Data link layer defined in the OSI reference model.

⇒ The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

(ii) Internet layer:

⇒ An internet layer is the second layer of the TCP/IP model.

⇒ An internet layer is the known as the network layer.

(iii) Data-link layer:

⇒ The data-link layer identifies the network protocol type of the packet, in this instance TCP/IP.

⇒ The data-link layer also provides error control and framing.

(iv) Transport layer:

The transport layer is responsible for the reliability flow control and correction of data which is being

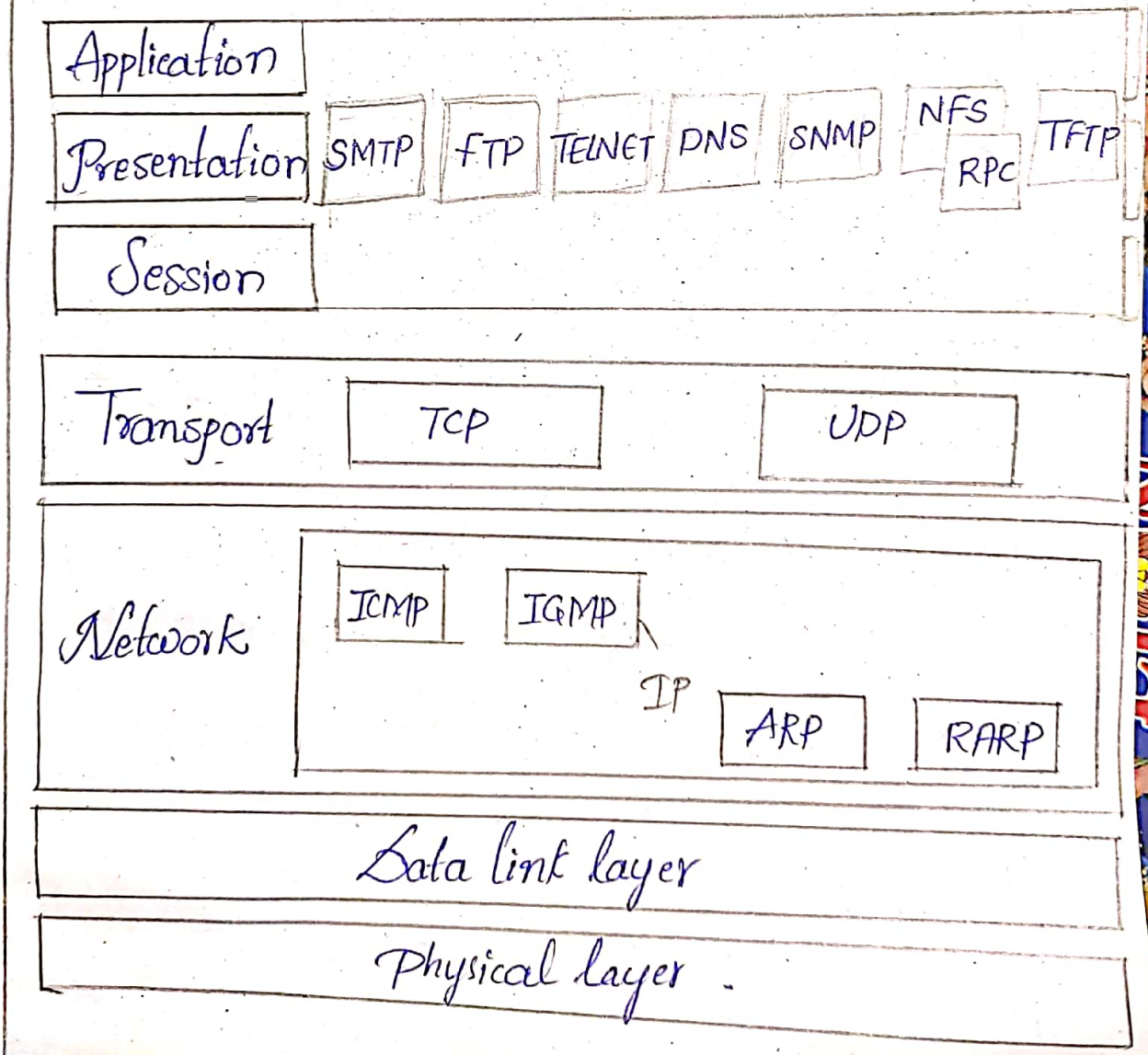
Sent over the network.

⑤ Application layer:

⇒ An application layer is the topmost layer is the TCP/IP model.

⇒ It is responsible for handling high-level protocols, issues of representation.

⇒ This layer allows the user to interact with the application.



CN ASSIGNMENT

Write about CRC?

CRC – Cyclic redundancy check

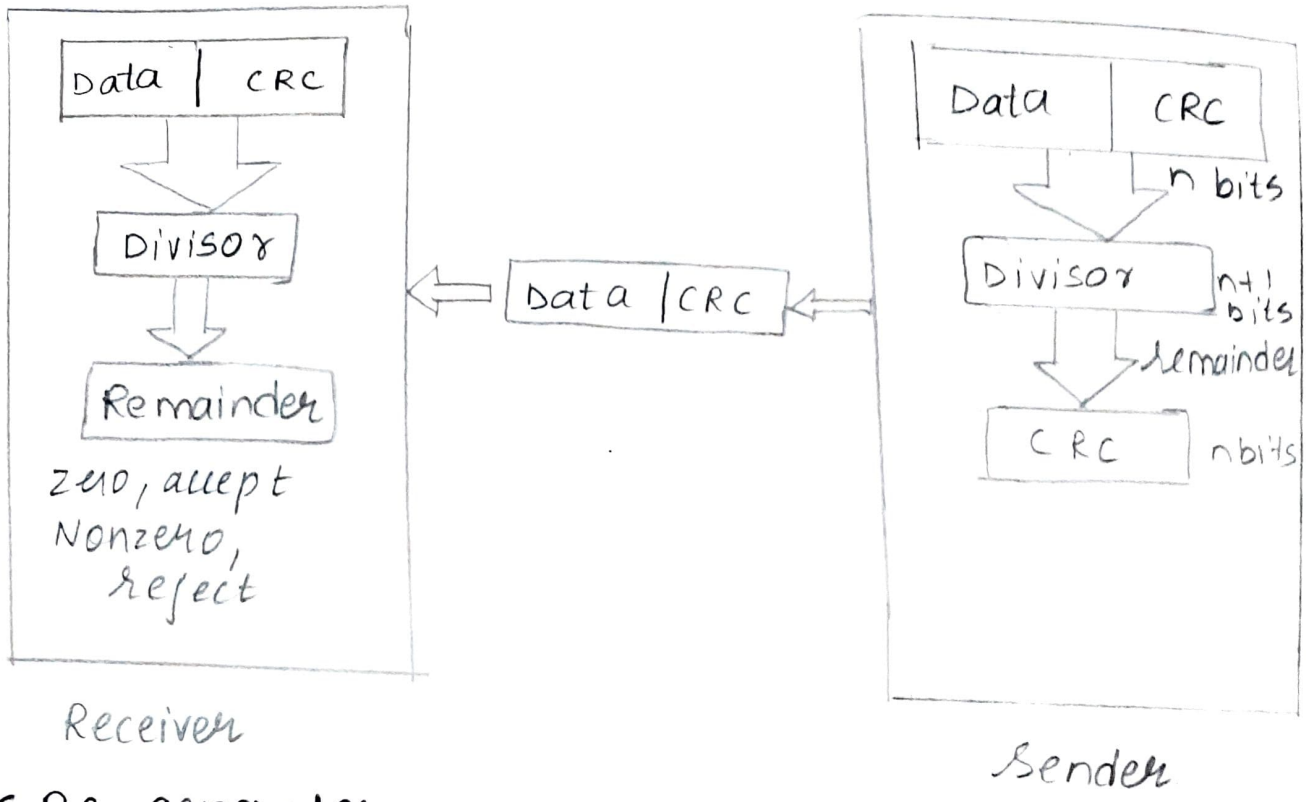
CRC is a redundancy error technique used to determine the erro

Following are the steps used in CRC for error detention

In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division with n+1 bits.

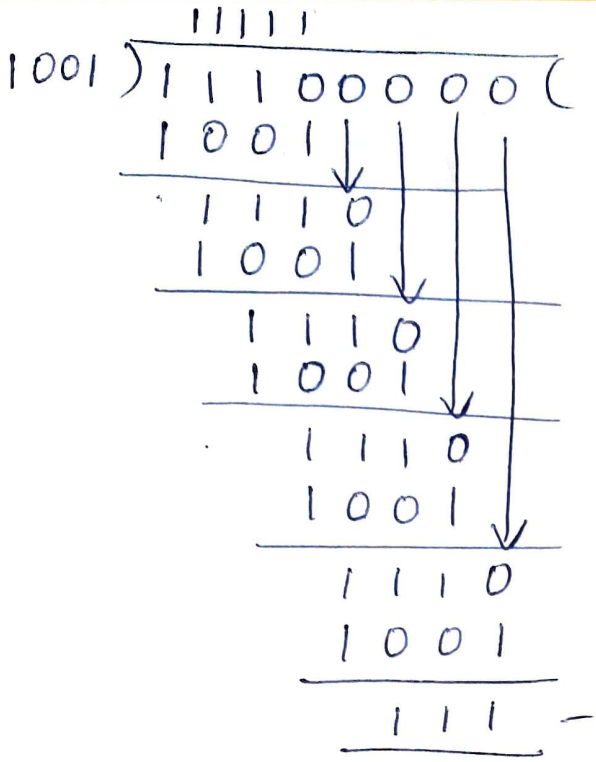
Secondly, the newely extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.

- Thirdly, the CRC remainder replaces the appended 0s at the end of the ouiginal data. This newly generated unit is sent to the receiver.
- The receiver receives the data followed by the CRC remainder. The receiver will toeat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.
- If the resultant of the division is zero which means that it has no error, and the data is accepted.
- If the resultant of this division is not zero which means that the data consists of an error Therefore the data is discarded.
- Let's understand this concept through an example.



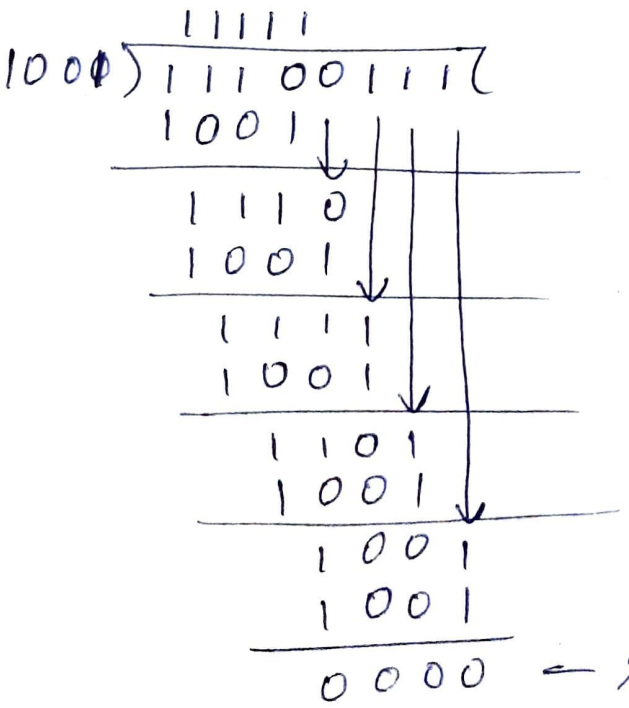
CRC generator

- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network



CRC checker

- The functionality of the CRC checker is similar to the CRC generator
- When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division
- A string is divided by the same divisor
- In this case, CRC checker generates the remainder of zero. therfore the data is accepted.



2) Write about wait and stop protocol and sliding window protocol?

- Here stop and wait means, whatever the data that sender wants to send, he sends the data to the receiver.
- After sending the data, he stops and waits until he receives the acknowledgement from the receiver.
- The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.
- It is a data link layer protocol which is used for transmitting the data over the noiseless channels
- It provides unidirectional data transmission which means that either sending or receiving of data will take place at a time.
- It provides flow control mechanism but does not provide any error control mechanism.
- The idea behind the usage of the frame is that when the sender sends the frame then he waits for the acknowledgement before sending the next frame.

Primitives of stop and wait protocol

Sender side

Rule 1: Sender sends one data packet at a time

Rule 2:- sender sends the next packet only when it receives the acknowledgement of the previous packets.

The idea of stop and wait protocol in the sender's side is very simple, i.e send one packet at a time and do not sent another packet before receiving the acknowledgement.

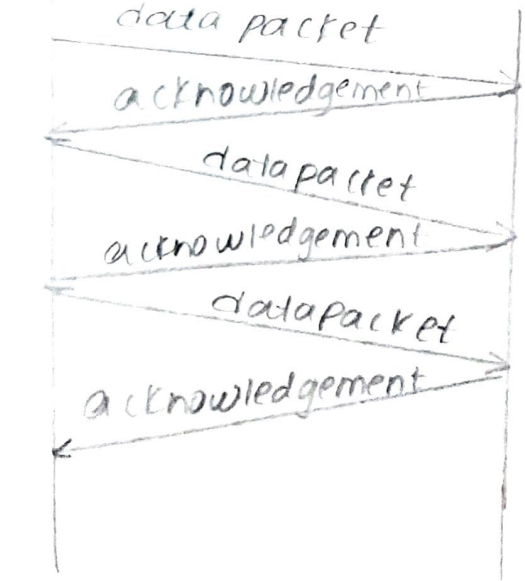
Receiver side.

Rule 1: Receive and then consume the data packet.

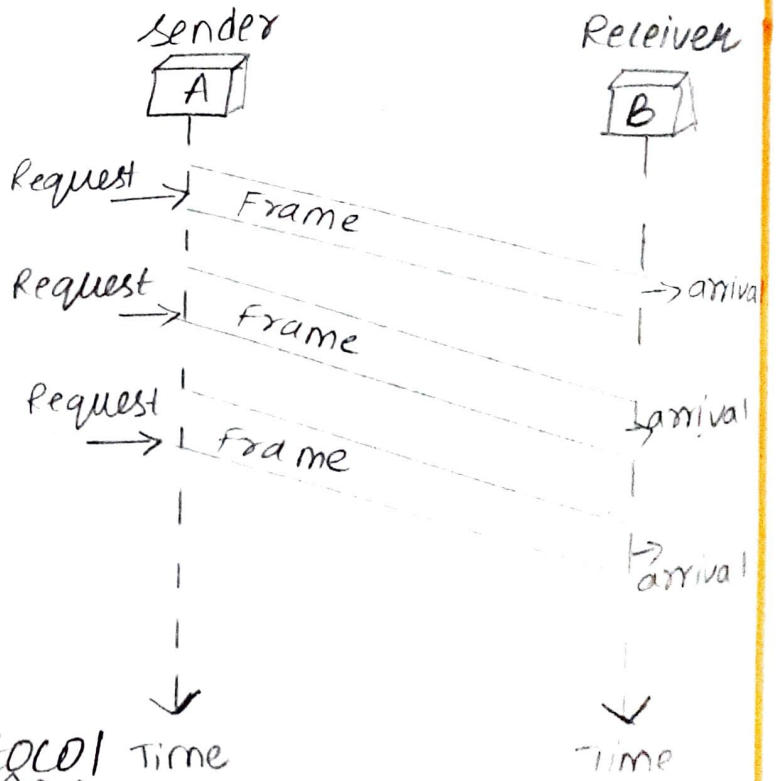
Rule 2: when the data packet is consumed, receiver sends the acknowledgement to the sender.

Therefore, the idea of stop and wait protocol in the receiver's side is also very simple. i.e consume the packet, and once the packet is consumed, the acknowledgement is sent. This is known as a flow control mechanism.

Stop and Wait Protocol



Noiseless protocol.



Sliding ~~Pro~~ window Protocol

It is a technique for sending multiple frames at a time. It controls the data packets b/w the two devices where reliable and

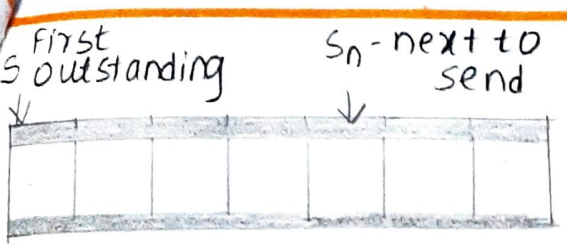
gradual delivery of data frames is needed. It is also used in TCP.

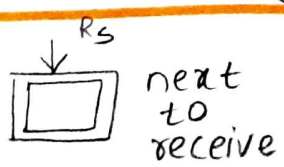
- In this technique, each frame has sent from the sequence numbers are used to find the missing data in the receiver end.
- The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

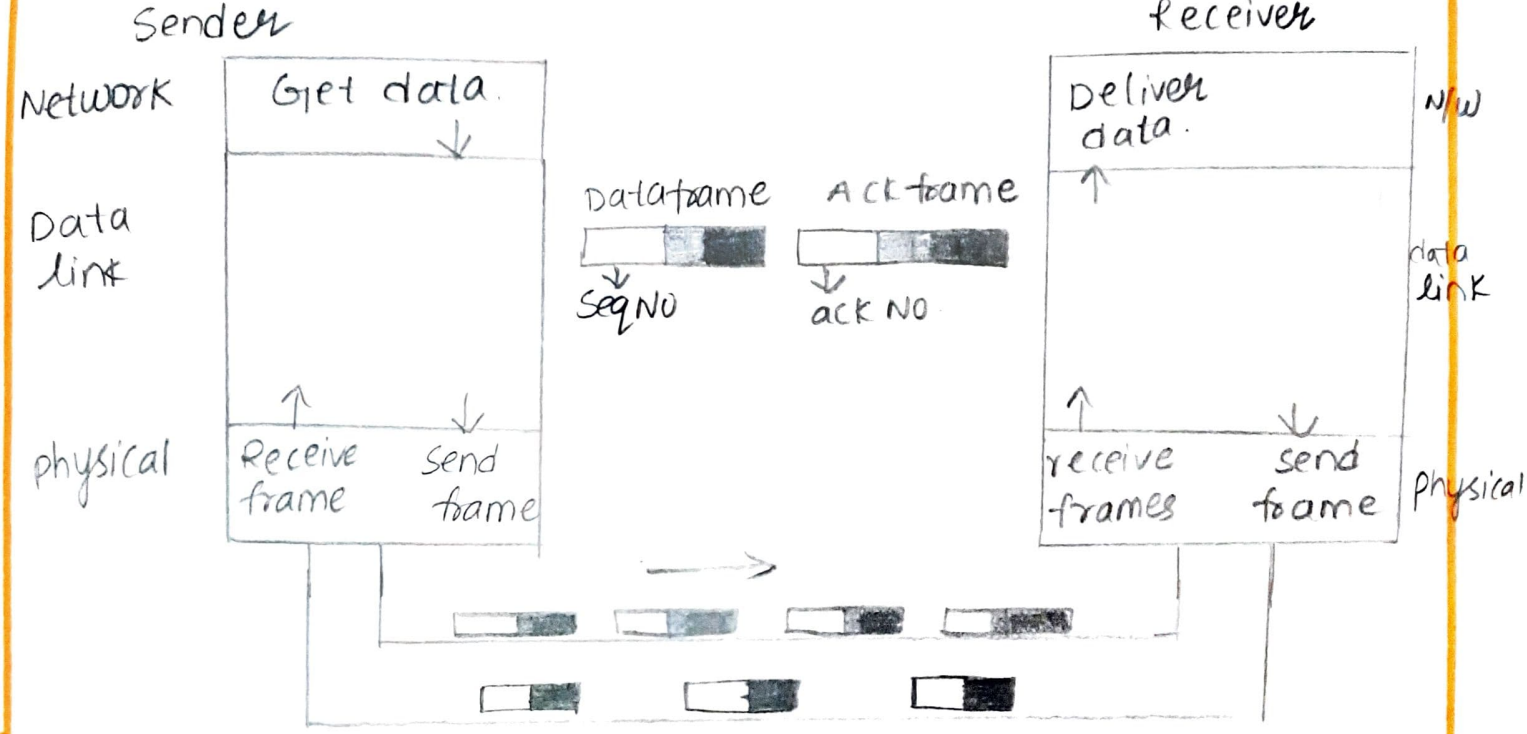
Types

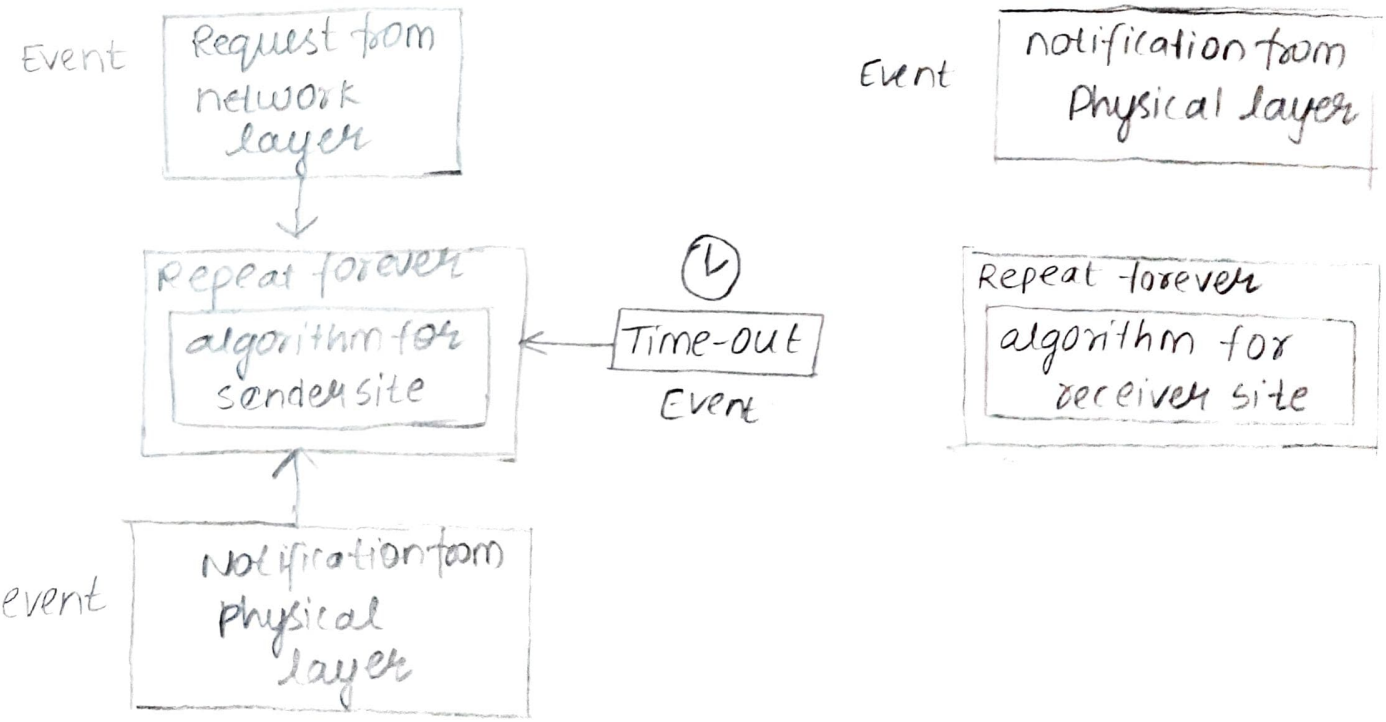
1) Go Back N ARQ (Automatic Repeat request)

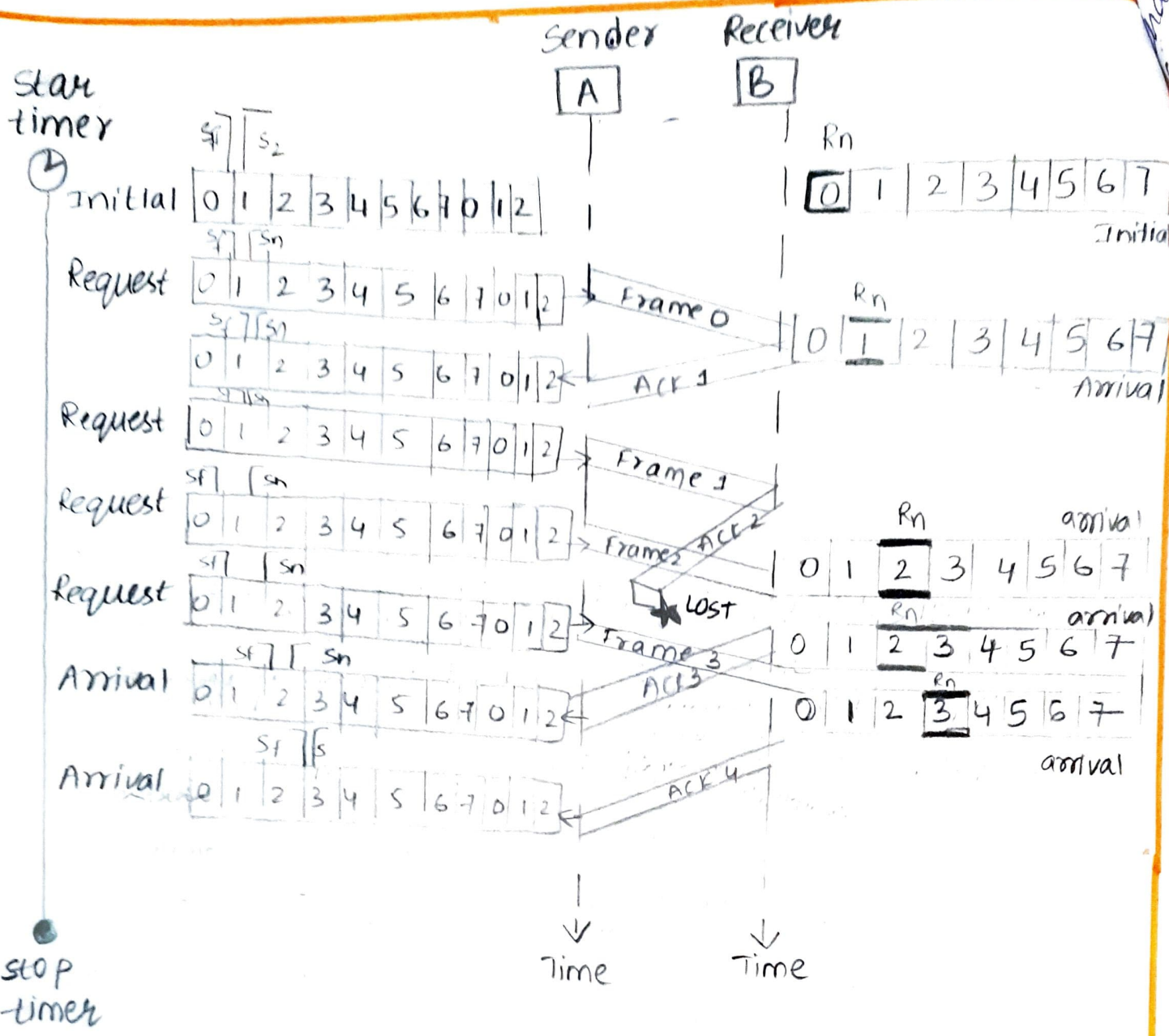
- It is a data link layer protocol that uses a sliding window method.
- In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.
- The size of the sender window is N in this protocol Forexample:- Go Back 8, the size of the sender window, will be 8. The receiver window size is always 1.
- If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. when the timer expires the sender sends the correct frame again. The design of the Go Back N-ARQ protocol is shown below.


First
S outstanding
Sn - next to
send


Rs
next
to
receive


Sender
Receiver
Network
Get data
Deliver
data
N/W
Data
link
Data frame
ACK frame
Seq NO
ack NO
data
link
physical
Receive
frame
send
frame
receive
frames
send
frame
Physical

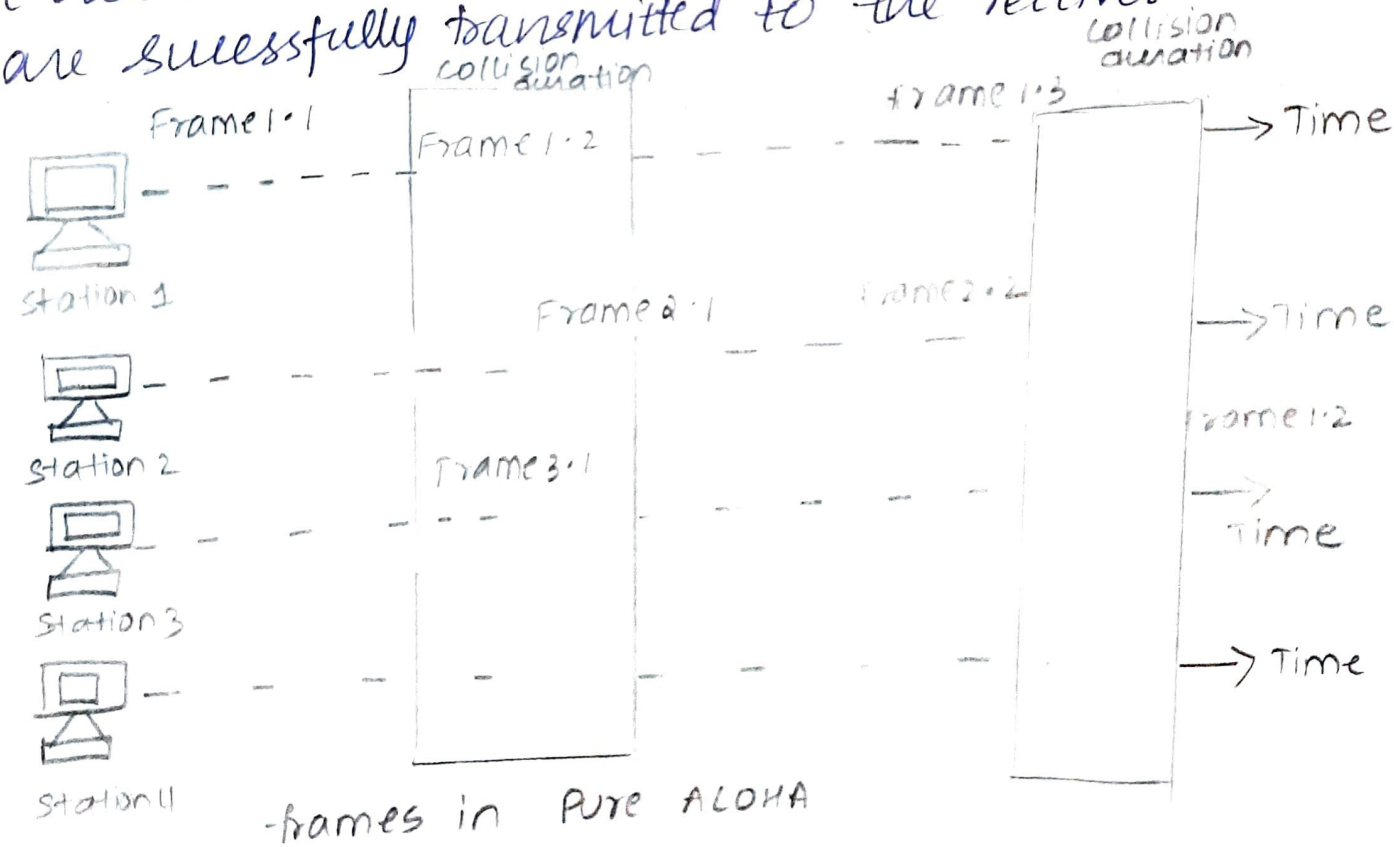

Event
Request from
network
layer
Event
notification from
Physical layer
Repeat forever
algorithm for
sender site
Time-out
Event
Repeat forever
algorithm for
receiver site
event
Notification from
Physical
layer



Selective Repeat ARQ

- It is a data link protocol that uses a sliding window method.
- The Go-back N ARQ protocol works well if it has fewer errors.
- But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again we can use the selective repeat protocol.
- In this protocol, the size of the sender window is always equal to the size of the receiver window.

frames of collision may occur, and the data frame can be lost. When a station transmits the data frame to a channel is free or not, there will be a possibility of the collision of data frames. station expects the acknowledgement from the receiver and if the acknowledgement of the frame is received at the specified time, then it will be OK otherwise the station assumes that the frame is received at the specified time, then it will be OK; otherwise the station assumes that the frame is destroyed. Then station waits for a random amount of time, and after that it retransmits the frame until all the data are sucessfully transmitted to the receiver



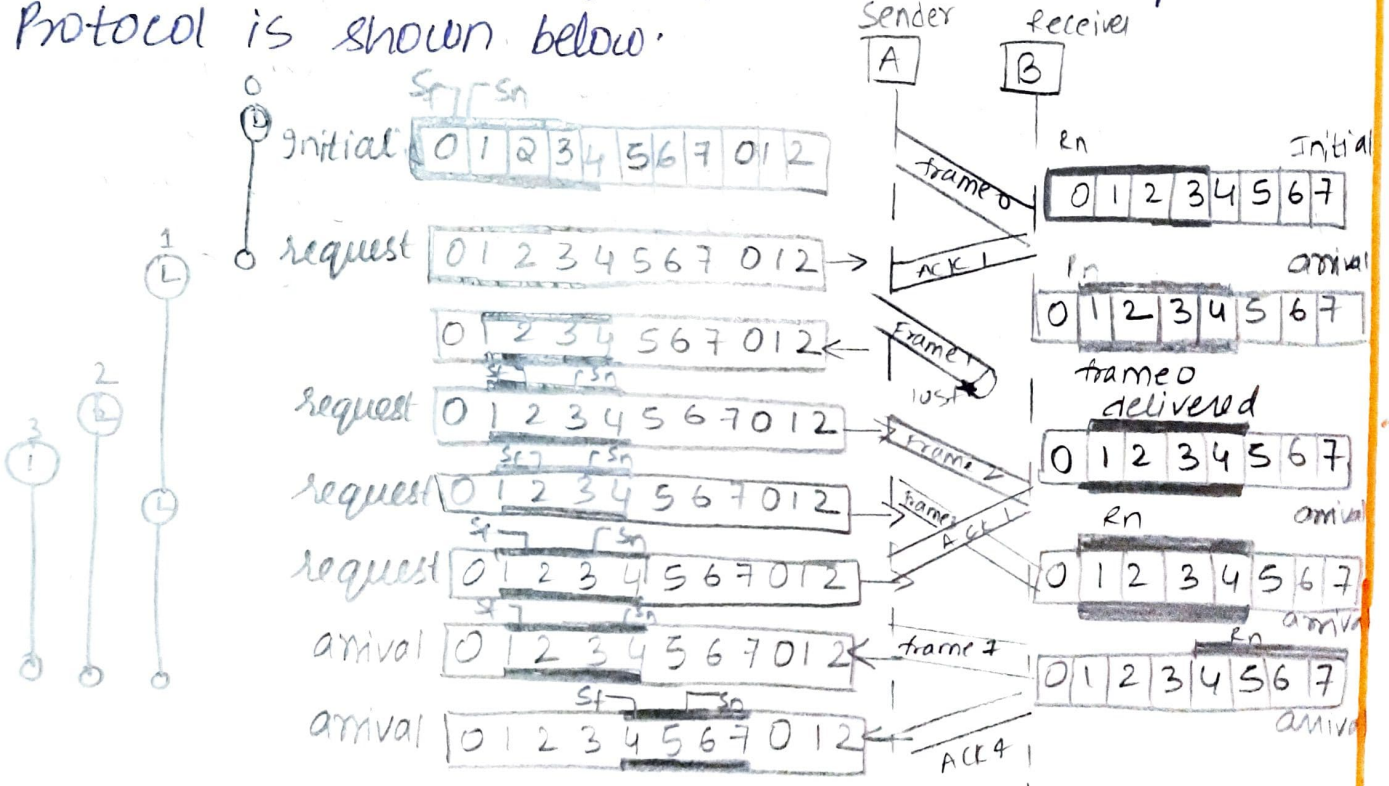
frames in PURE ALOHA

Slotted Aloha

There is a high possibility of frame hitting in Pure aloha, so slotted aloha is designed to overcome it. Unlike pure aloha slotted aloha does not allow the transmission of data whenever

- The size of the sliding window is always greater than 1
- If the receiver a corrupt frame, it does not directly discard it.
- It sends a negative acknowledgement.

There is no waiting for any time out to send that frame. The design of the selective repeat protocol is shown below.



Q3 Write about the multiple access protocol?

1 Aloha :- It is designed for wireless LAN but can also be used in a shared medium to transmit data

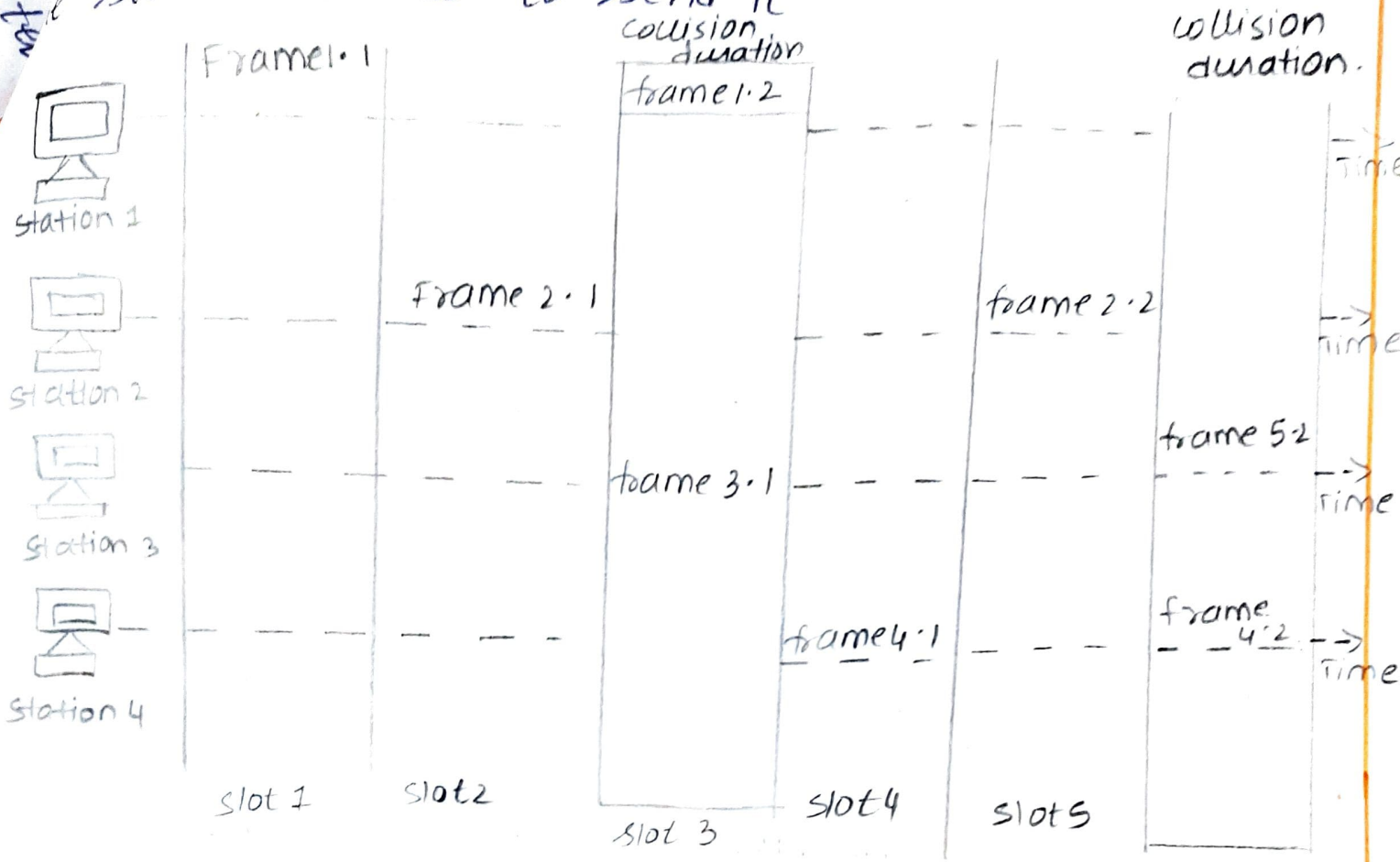
In aloha, any station can transmit data to a channel at any time. It does not require any carrier sensing

Pure aloha

It is used when data is available for sending over a channel at stations. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the

greater

station wants to send it



Frames in slotted ALOHA

In slotted Aloha, the shared channel is divided into a fixed time interval called slots. so that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. If the station is failed to send the data, it has to wait until the next slot.

However, there is still a possibility of a collision because suppose if two stations try to send a frame at the beginning of the time slot.

CSMA carrier sense multiple access ensures fewer collisions as the station is required to first sense the medium before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay.

CSMA access modes -

- 1 persistent :- The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally as soon as the channel gets idle.
- Non-persistent :- The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time and transmits when found idle
- P-persistent :- The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted then it waits for some time and checks the medium again, now if it is found idle then it sends with probability.
- O-persistent :- superiority of nodes is decided before hand and transmission occurs in that order. If the medium is idle, node waits for its time slots to send data.