24/12/2020 Computer Networks and Security: CO1

Computer Network: A set of communication elements connected by communication links.

→ A device which is capable of sending or recieving the data generated by other nodes on the network like computer, printer.. etc.

What is network?

set of devices connected and they are knows as nodes.

→ Set of devices (nodes) connected by media link is net work.

→ Set of communication elements connected by communication link is computer network (or) Group of computer connected each other with wire (or) wireless (or) internet is also known as computer network.

What is bridge?

It is a device that joins similar topologyies and are used to divide network segments.

disadvantage:

They cannot network different networks

Hub:

A Hub connects from multiple connects wires coming from different networks

Switch:

A switch is a multiport bridge with a buffer and design that increases network efficiency.

What do you mean by a router?

It connects multiple networks types and determines the best path for sending.

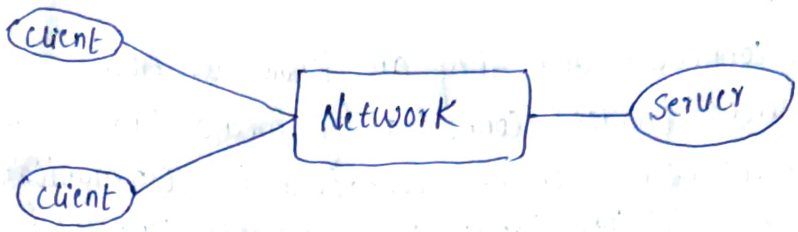
Computer Networks: They are four uses.

1. Bussiness Applications
2. Home Application
3. mobile users
4. Social issues.

1. Business Application of Network:

a) Resource sharing (hardware, software, information.)
b) Providing communication medium (e-mail, video conferencing)
c) Doing business electronically (B2B, B2C, e-commence)

- A network with two clients and one server



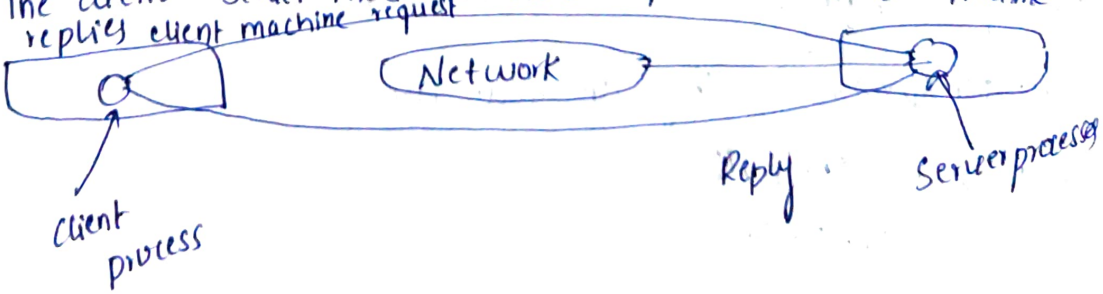
Goals of Network for Computer:

- Resource sharing: equipment, programs, data.
- high reliability
  - replicated data
  - hardware
- Saving money
- mainframe: 10 times faster, but 1000times more expensive than it
- client - server model
- Scalability:
  - mainframe: replace a larger one
  - client - server model: add more servers
- communication medium for seperated employees

Business Application of Networks (2)

a) Two processes are involved:
b) A communication network is needed

- the client-server model involves request and server machine replies client machine request



Home Network Applications

- Some forms of e-commerce

Tag	Full name	Ex
B2C	Business-to-Consumer	ordering books online
B2B	Business-to-Business	Car manufacturer ordering tyres from supplier
G2C	gov-to-Consumer	gov. distributing tax forms electronically
C2C	consumer-to-consumer	Auctioning second-hand products online
P2P	peer-to-peer	File sharing

Mobile Network users:

- Combinations of wireless networks and mobile computing

wireless	mobile	Application
No	No	Desktop computers in offices
No	Yes	A Notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	portable office; PDA for store inventory mobile-commerce

→ PDA stands for personal digital assistant (PDA)

Home Network Application (2)

- In peer-to-peer system there are no fixed clients and servers.

Home Network Applications:

1. Access to remote information (shopping, financial)
2. person-to-person Communication (email, news groups),
3. Interactive entertainment (VOD, TVS)
4. Electronic commerce.

Network Hardware:

Network hardware is based on two types.

1. Transmission technology
2. Scalability

1. Transmission technology: They are two types.

a. Broad cast

b. Point-to-point.

a) Broad cast: It has a singal communication channel that is shared by all the machines on the network.

→ A single message send will reach the all the machines.

b) point-to-point: It prouides a deedicated link between the source and the destination.

Classification of Inter Connected processors bysccale:

Interprocessor distance	processor located in-same	EX
1m	Square meter	personal area network
10m	Room	local area
100m	Building	
1km	campus	
10km	city	metro polian area
100km	country	wide area
1000km	Countinent	
10,000 km	Plantent	the Intanet

Characteristics of Network:

personal area network

local area network

metropolitan area network

wide area network

The Internet.

Social issues.

1. communication Breakdown
2. Defamation character
3. Identity theft
4. Cyber butlying
5. Ganing Addiction
6. privacy
7. Healty and fitness
8. Education
9. terrorism & C
10. Sercality.

Local Area Networks:

They are used to connect personal computers and work stations in a company (or) an organization to share the resources.

→ The lands are distinguished by

a) privated -owned
b) Small size
c) transmission technology
d) topology

Metropolitan Area Networks :- (MAN)

- A metropolitan area Network based on cable TV

Wide Area Network (WANs)

- WANs are point-to-point networks.
- WANs consists of two distance components transmission lines (copper, fiber, microware) and switches (electronics, optics)
- Relation between hosts on LANs and the Subnet.

Subnet (WAN'S):

→ Subnet (WAN's) is consists of two components:

- transimission lines (circuits, channels, trunks)
- more bits between machines.

→ Switching elements:-

- Connect transmission lines
- Router: also called packet switching nodes, intermediate System and data switching exchanges
- operate in store-and-forward, & Packet-switched mode.

Wide Area Networks (2):

- A Stream of packets from Sender to receiver. (virtual-Circuit)
- Routing decisions are made locally
- How a makes the decision is called the routing algorithm

Wireless Networks:

- Categories of wireless networks
- System interconnection
  (short-range radia, e.g. Bluetooth)
- Wireless LANs
  (802.11a, 802.11b, 802.11g)
- Wireless WANs
  (802.16, Cellular telephones satellites)
- wireless sensor network

Network Topology:

It refers to the way in which a network is layed out physica

Types of Network topologies:

1. Mesh
2. Star
3. Bus
4. Ring

Mesh Topology: Every device has a dedicated point-to-point l to every other device

→ Every node 'n' must be connected "n-1" nodes
→ n*(n-1) links are there in mesh topology

Ex: 5*(5-
5*4
=20

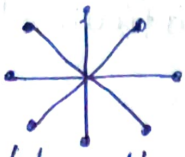
Advantages of Mesh Topology:

→ Gsantied the dedicated link
→ Robust
→ privacy & Security
→ Easy fault Identification & isolation.

Disadvantages:

→ high Cabling
→ difficult to install
→ expensive

2. Star Topology:
→ Each device has a dedicated point-to-point link only to a central controller



→ No direct connection b/w the devices
→ if one device wants to send data to other it sends the data to the controller then data forwarded to the device.

Advantages:
1. less Expensive
2. easy installation and reconfiguration
3. Robust
4. easy fault identification and isolation.

disadvantages:
1. network dependency on single device
2. High cabling for wires.

3. Ring Topology: Each device has a dedicated point-to-point connection with only two devices on either side of it.

Advantages:
1. easy to install
2. Add or delete a node is easy
3. fault isolation is simple.

Disadvantages:
If there is a break in the ring then the total network is fails

4. Bus Topology:
→ one long cable acts as a back done to link all the devices

Advantages:
1. easy installation
2. less cabling

Disadvantages:

1. Difficult to reconnect (or) difficult to add a new device
2. faults detendtion is less

Home Network categories:

- Computers (desktop PC, PDA, shared peripherals)
- Entertainment (TV, DVD, VCR, camera, stereo, MP3)
- Telecomm (telephone, cell phone)
- Applicances (microware, clock)
- Telemetry (utility meter)

Internet works:

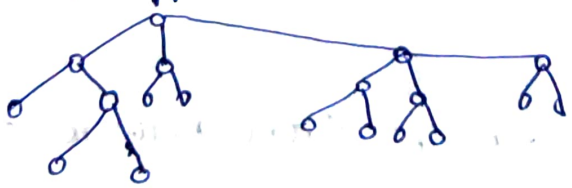
- Internet work connect networks with different hardware and software.
- A Collection of interconnected networks is called an internetwork (or) Internet.
- Internet is one specific internet
- gateways are used to make the connection and to provide the necessary translation (protocol convertion).

Network Software:

Hybrid topology:

Combination of all topology

Tree topology:



→ Fundomentally different properties

1. Devices have to be easy to install
2. the network and device have to be foolproof in operation
3. Low price i.e essential
4. the network needs sufficient capacity
5. network interface.

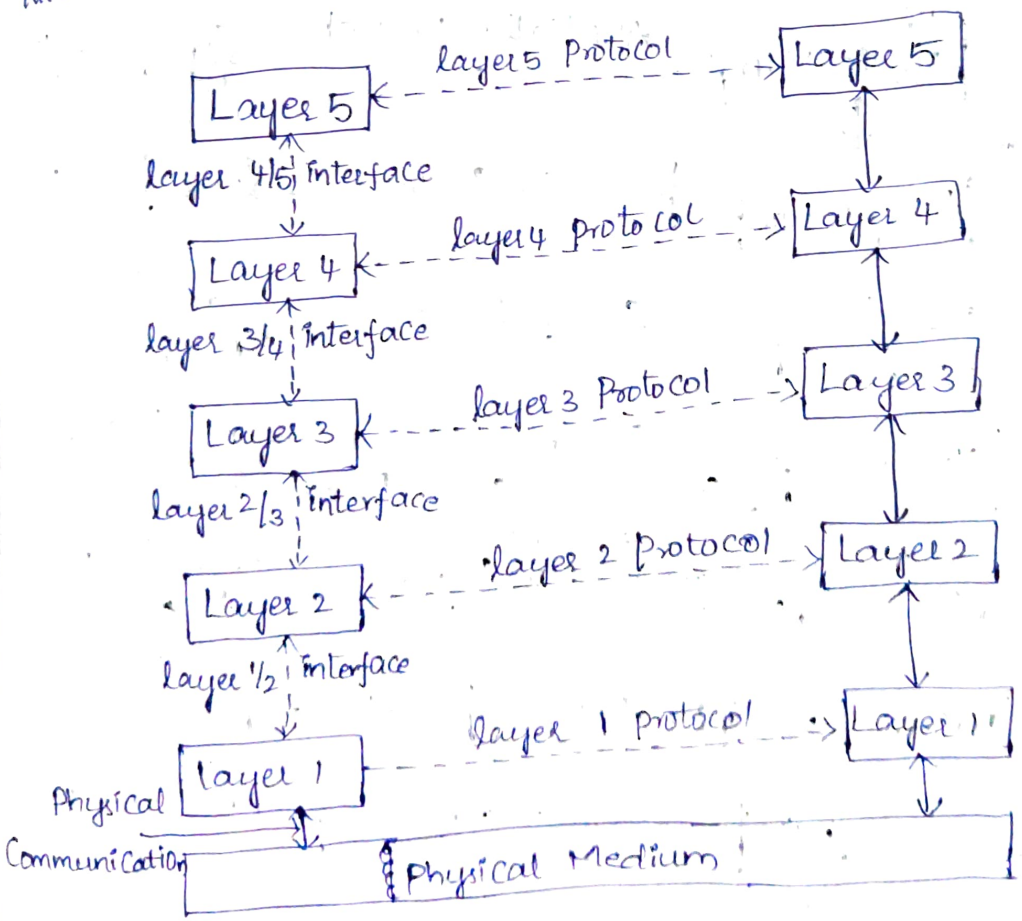
Internetworks
→ It connect network with different hardware, software
→ Collection of interconnected network, called internet.

Network Software:
→ protocol hierarcy
→ Design issues for the
→ connect oriented and connectionless services.
→ Service prinitives
→ Relation swip of service to protocols

protocol hierorchies:
- Series of layers
- Lower layer provides Service to higher layers

protocol:
Agreement between communication parties on how communication proceed.

peers:
Network Architecture: A Set of layers and protocols



Session 5 & 6

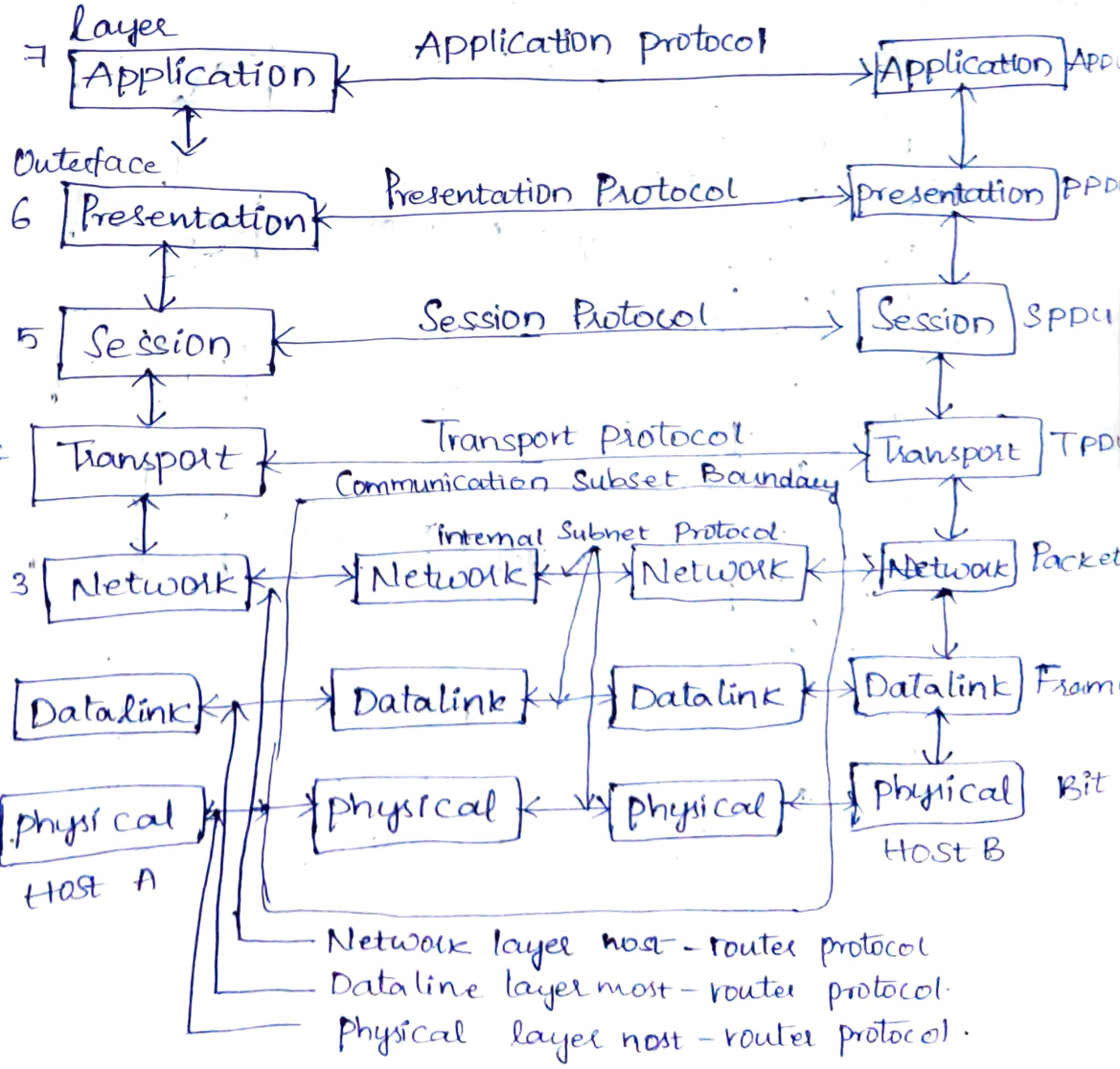
31/12/2020

Reference models:

* The OSI (Open System Inter Connection ISO)
* The TCP/IP Reference model
* A comparison of OSI and TCP/IP
* A Critique of the osi model and protocols.
* A Critique of the TCP/IP Reference model.

Design principles Of the OSS reference Model :-

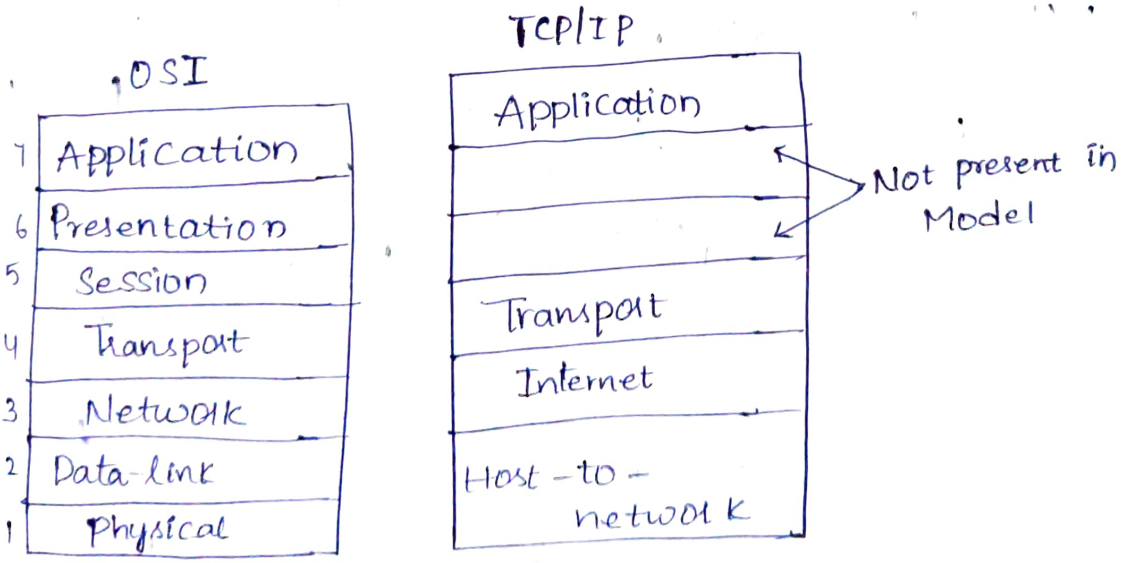
* A layer should be Created where a different abstraction is needed.
* Each layer should perform a well designed function.
* The function of each layer can be chosen to minimize the information flow accross the interface.
* The no. of layers should be not too large or not too small.



Functions of 7 Layers:-

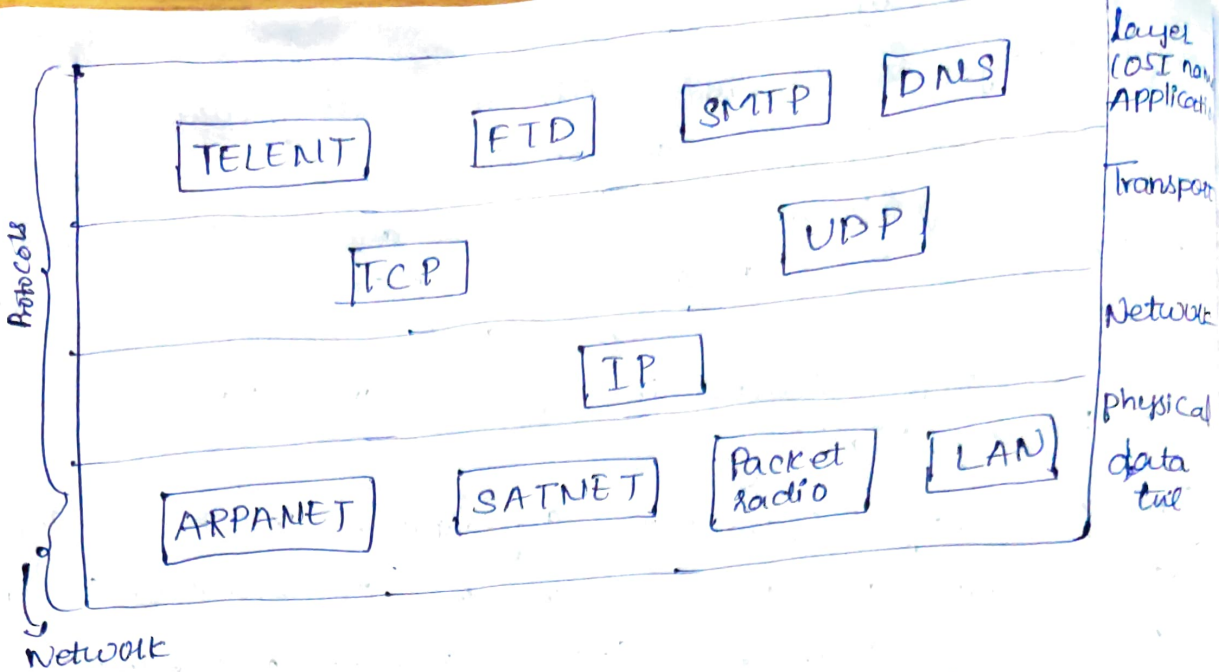
1. physical layer is Concerned with Transmitting raw bit streams Over a communication channel.
2. Data link layer performs flow control and also transformed a raw transmission into a line appears error free, error control and uses physical address.
3. Network layer controls the operation of subnet.
   Eg:- Routing, Masking.
4. Transport layer controls the Segmentation, flow-control and error-Control and determines the type of Services (TCP, UDP)
5. Session layer stablishes Sessions, manage, & Terminate Connection.
   Ex:- login, logout.
6. presentation layer Concerned with translation, data Compression, Encryption.
7. Application layer Contains Variety of Commonly used Protocol process (HTTP, e-mail)

Ip - Internet protocol.



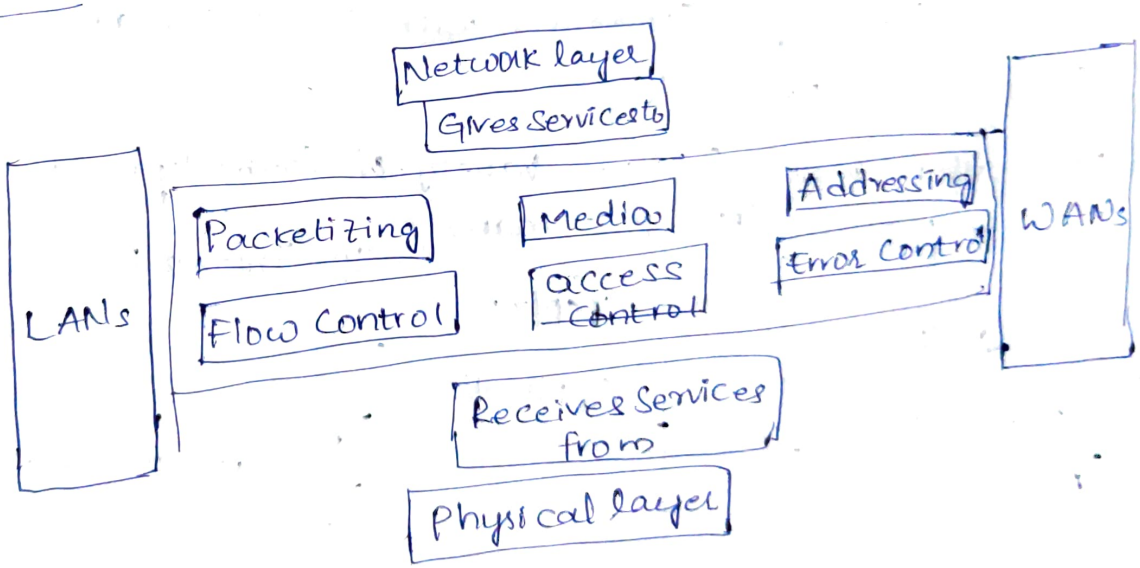
→ An TcpIp Model 4 layer are available

* protocol and network Rule TcpIp model initiall.



7-1-21

Position of datalink layer:-



Responsibilities of physical layer:-

1. physical characteristics and of interfaces and medium
2. Representation of bits.
3. Data Rate - No. of bits transmitted per second
4. line Configuration - Connection of devices
5. physical topology

6. Transmission Mode - Simplex
7. Synchronization of bits.

2) Data - Link layer:-

→ it goes with error detection and correction.

Responsibilities of data link layer:-

1. Framing - Access Control
2. physical Addressing
3. Flow control
4. Error control
5. Access control.

3) Network layer:-

Responsibilities of Network Layer:-

1. Logical Addressing
2. Routing

Data link layer Design issues:-

1. providing a well defined service interface to the network layer.
2. Dealing with transmission errors.
3. Regulating the flow of data so that slow receivers are not swapped by fast senders.

Services provided to the Network layer:-

* Unacknowledged Connectionless service
* Acknowledged connectionless service
* Acknowledged connection oriented service

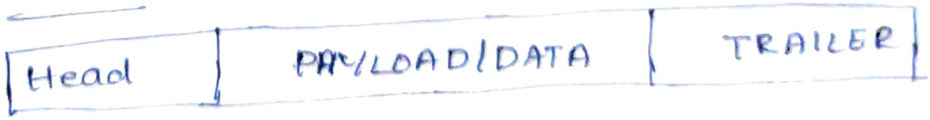
ERROR CONTROL:- Sender must be acknowledged Postive, negative.

FLOW CONTROL:- Systematic tramission of frames to the receiver feedback based, rate based

Framing:-

* DLL packs the bits into frames, so that each frame is distinguishable from another.
* Frames seperate a message from one source to a destination, by adding a sender address and a destination address.
* Message is divided in to smaller units.

FRAME FORMAT:-



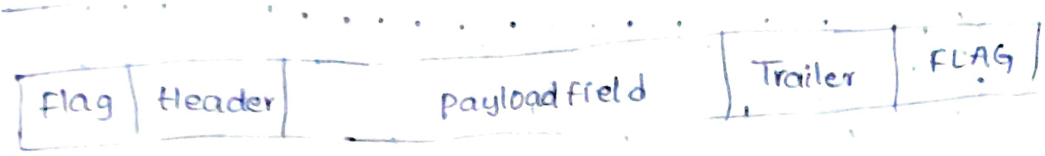
Framing Methods:-

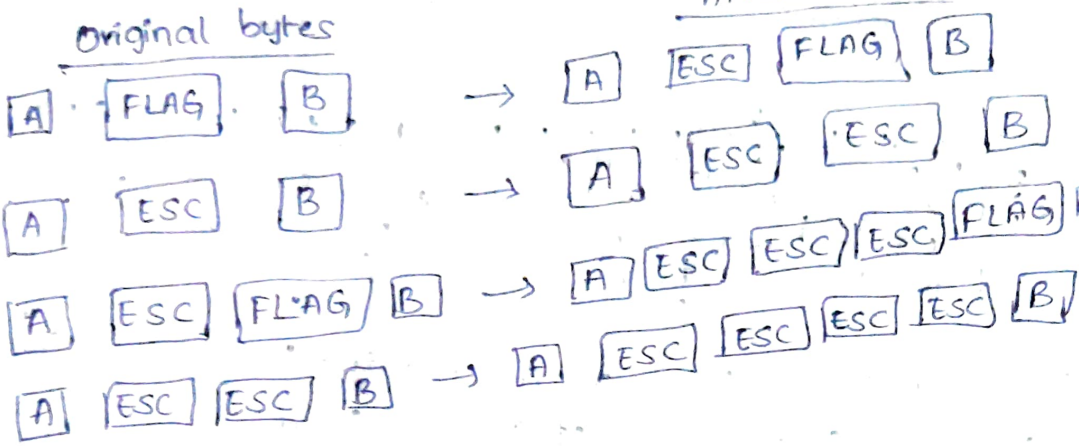
→ A good design must make it easy for a receiver to find the start of new frames:

* character count
* Flag bytes with byte stuffing

* Flag bits with bit stuffing

Byte Stuffing:-

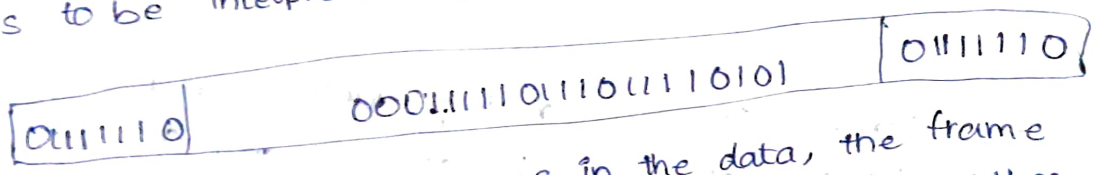




→ A frame delimited by flag bytes.

Bit Stuffing:-

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



* If the flag pattern appears in the data, the frame cannot be distinguished between one to another.
* So it is overcome by stuffing a bit 0 after 5 consecutive 1's.

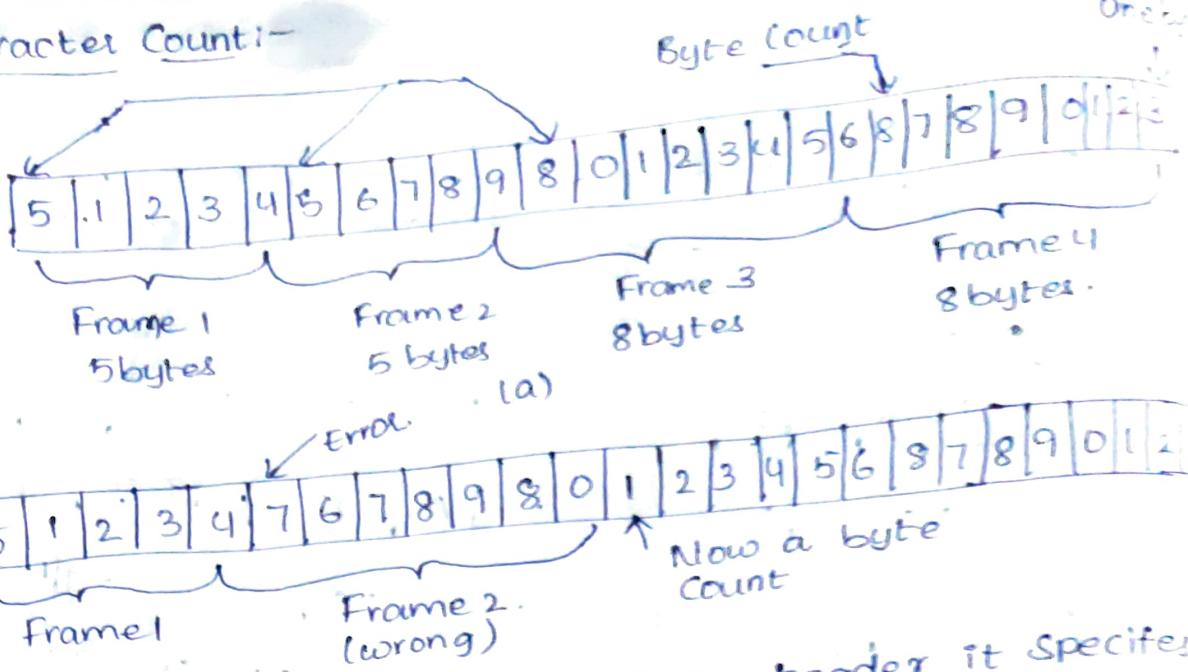
Ex:- (a) 0110111111111111111110010

(b) 0110111111011111101111101001010

Stuffed bits

(c) 0110111111111111111110010

Character Count:-



→ This method uses a field in the header it specifies no. of characters in the field

Error Detection and Correction:-

1. Types of Errors
2.
3.

→ Data can be corrupted during transmission. For reliable communication, error must be detected and corrected.

→ Error detection and correction are implemented either at the data link layer or the transport layer of the OSI Model.

Type of Errors:-

1. Single Bit Error:- is when only one bit in the data unit has changed

Ex:- (ASCII STX - ASCII LF)

2. Multiple - Bit Error:- is when two (or) more non consecutive bits in the data unit have changed

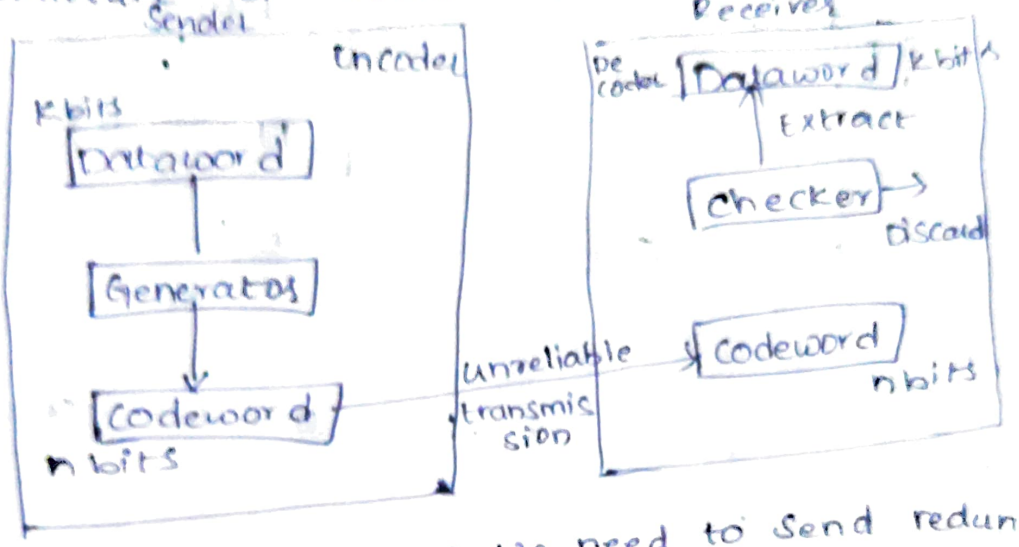
Ex:- ASCII B - ASCII LF

→ Means that 2 (or) more consecutive bits in the data unit have changed.

Detection:

* Error detection uses the concept of redundancy, which means adding extra bits for detecting errors at the detection.

The structure of encoder and decoder:-



→ To detect or correct errors, we need to send redundant bits.

Block coding:-

→ In block coding we divide our message into blocks each of k bits called datawards.

Error detection

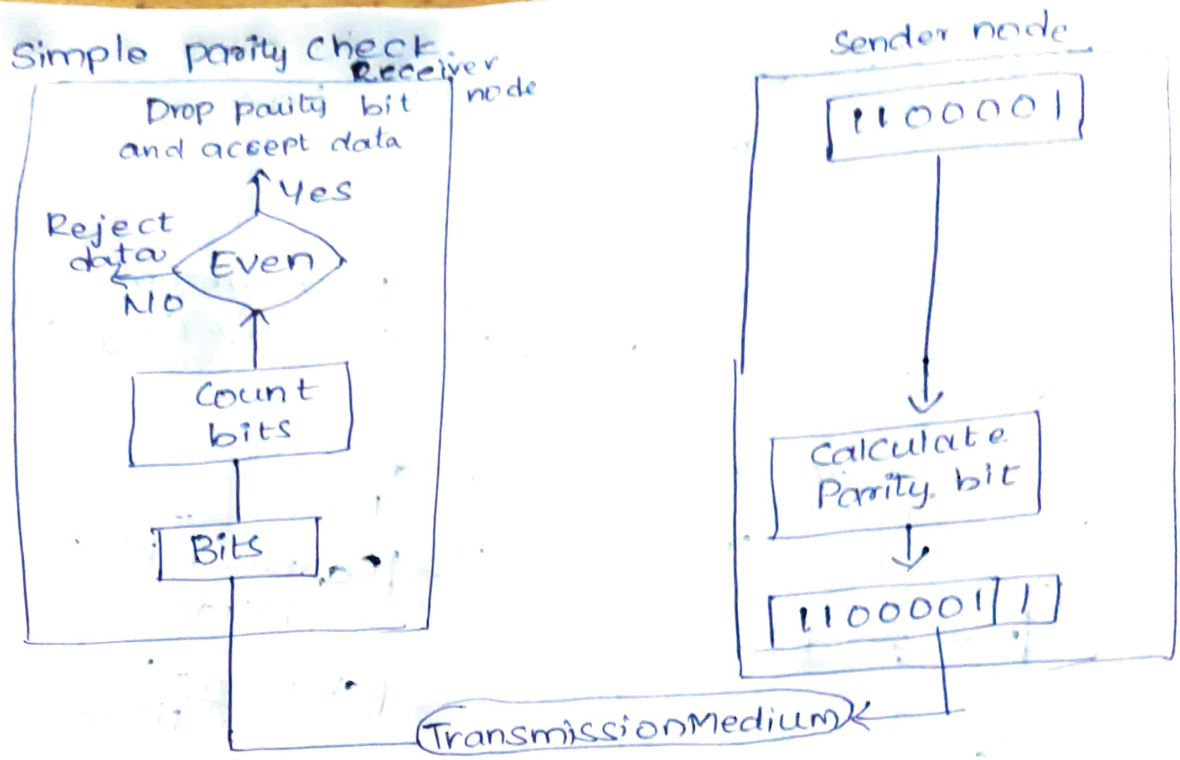
Error detection methods are:-

1. Parity check
2. Cyclic redundancy check
3. Checksum

1. parity check:-

→ A parity check bit is added to every data unit so that the total number of 1s (including the parity bit) becomes even for even-parity check (or) odd parity check.

→ Simple parity check.



Cyclic codes:-

→ if a codeword is cyclically rotated, then the result is another codeword.

Ex:- Codeword 1 - 1011000
Codeword 2 - 0110001

Cyclic Redundancy check (CRC):-

→ we can create cyclic codes to correct errors.

→ Suppose dataword is of the length k and code word is of n length, then n-k 0's are to be added to the dataword.

→ If data word is of 'k' length and generator (n-k+1) has been given then first find n and then n-k 0's are to be added to the dataword (redundant bits)

Ex:- Consider the message M = 1001 and do the cyclic Redundancy check for the above message using the following divisor 1011. Also check for errors on the received data using CRC

Sol:- Given Dividend = 1001 (K = 4) and Divisor = 1011 (n-K+1)

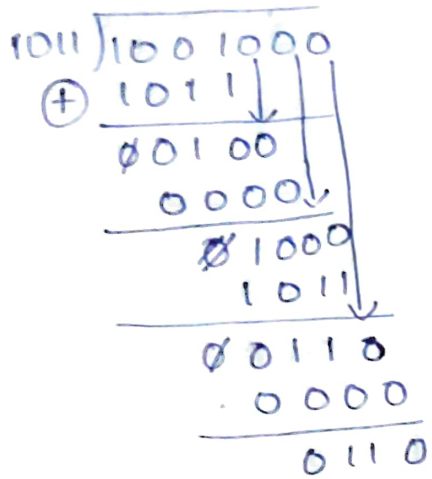
Given n-k+1 = 4, first we need to find n an

then calculate redundant bits

$$n-k+1 = 4$$
$$n-4+1 = 4$$
$$n = 7$$

if $n=7$ then no. of redundant bits $= n-k = 7-4 = 3$

So we need to add three 0's to the data word.



21/1/21

(Ex-4:- $M(x) = x^3+1$ and $G(x) = x^3+x+1$

Sol:- Given data)x

Detection

→ Check Sum:- used by the higher layer protocols.

→ is based on the Concept of redundancy.

Ex:- Original data : 10101001 00111001

```
10101001
00111001
--------
11100010   Sum
00011101   checksum
```

10101001 00111001 00011101

Ex - Received data : 10101001 00111001 00011101

```
 10101001
 00111001
 00011101
+--------
 11111111  ← Sum
 00000000  ← Complement
```

Ex2:- Original data is 10110011 10101011 01011010 11010101. perform checksum to detect error.

Sol:-

```
  10110011
  10101011
 ---------
① 01011110
      →1
 ---------
  01011111
  01011010
 ---------
  10101001
  11010101
 ---------
  10001110
      1
 ---------
```

→ Checksum = 01110001

Error Correction:-

Error Correction can be handled in two ways.

→ when an error is discovered, the receiver can have the Sender retransmit the entire data unit.

→ a receiver can use an error-correcting code, which automatically corrects certain errors.

→ If the total no. of bits in a transmittable unit is m+r, then r must be able to indicate atleast m+r+1 diff states.

$$2^r \geq m+r+1$$

Ex:- For value of m is 7 (ASCII), the smallest r value that can satisfy this equation is 4

Sol:- $2^4 \geq 7+4+1$

r=0 $2^0 \geq 7+0+1$ → $1 \geq 8$ ✗

r_1 = $2^1 \geq 7+1+1$ → $2 \geq 9$ ✗

r=2 $2^2 \geq 7+2+1$ → $4 \geq 10$ ✗

$r^3\ 2^3 \geq 7+3+1$

$8 \geq 11$

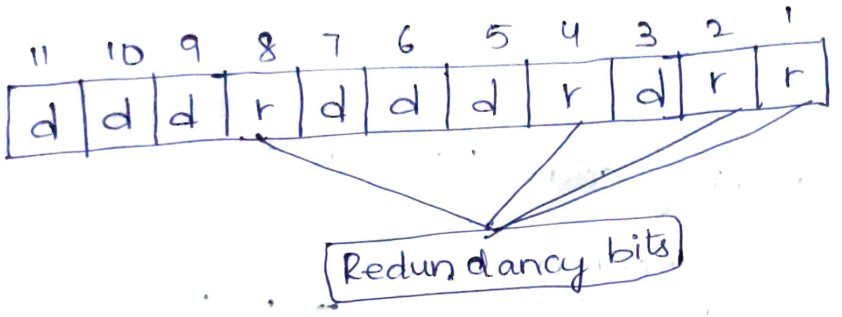
$r=4 \quad 2^4 \geq 7+4+1$

$16 \geq 12 \checkmark$

Hamming Code :-

→ developed by R.W. Hamming.

→ positions of redundancy bits in Hamming code.



→ each r bit is the vertical Redundancy Check (VRC) bit for XOR combination of data bits.

r_1 = bits 1, 3, 5, 7, 9, 11

r_2 = bits 2, 3, 6, 7, 10, 11

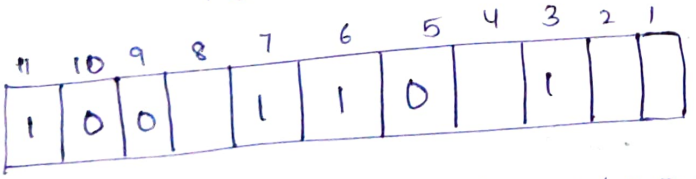
r_4 = bits 4, 5, 6, 7.

r_8 = bits 8, 9, 10, 11

LSB

0001 - 1
0010 - 2
0011 - 3
0100 - 4
0101 - 5
0110 - 6
0111 - 7
1000 - 8
1001 - 9
1010 - 10
1011 - 11
1100 - 12
1101 - 13
1110 - 14
1111 - 15

1001101

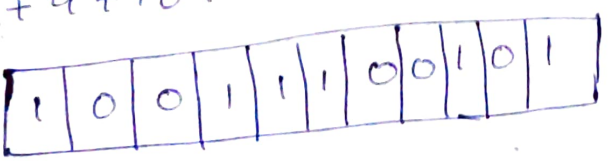


$r_1 = 1+3+5+7+9+11 = 1+0+1+0+1 = 1$

$r_2 = 2+3+6+7+10+11 = 1+1+1+0+1 = 0$

$r_4 = 4+5+6+7 = 0+1+1 = 0$

$r_8 = 8+9+10+11 = 0+0+1 = 1$



Receiver Side:-

$r_1 = 1+0+0+0+1+1 = 1$

$r_2 = 1+0+0+1+1+0 = 1$

$r_4 = 0+1+0+0 = 1$

$r_8 = 1+0+0+1 = 0$

$0\ 1\ 1\ 1 = 7 \rightarrow$ The bit in position 7 is in error.

Ex:- perform Hamming code 1011001

Sol:-

1011001

11	10	9	8	7	6	5	4	3	2	1
1	0	1		1	0	0		1		

$r_1 = 1+3+5+7+9+11 = 1+0+1+1+1$

$= 0$

$r_2 = 2+3+6+7+10+11 = 1+0+1+0+1$

$= 1$

$r_4 = 4+5+6+7 = 0+0+1$

$= 1$

$r_8 = 8+9+10+11 = 1+0+1$

$= 0$

11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	1	0	0	1	1	1	0

∴ The data after performing hamming code is

10101001110

→ Multiple-Bit Error Correction:-

→ The hamming code can be modified to correct a single error and detect double errors by adding a parity bit as the MSB, which is the XOR of all other bits.

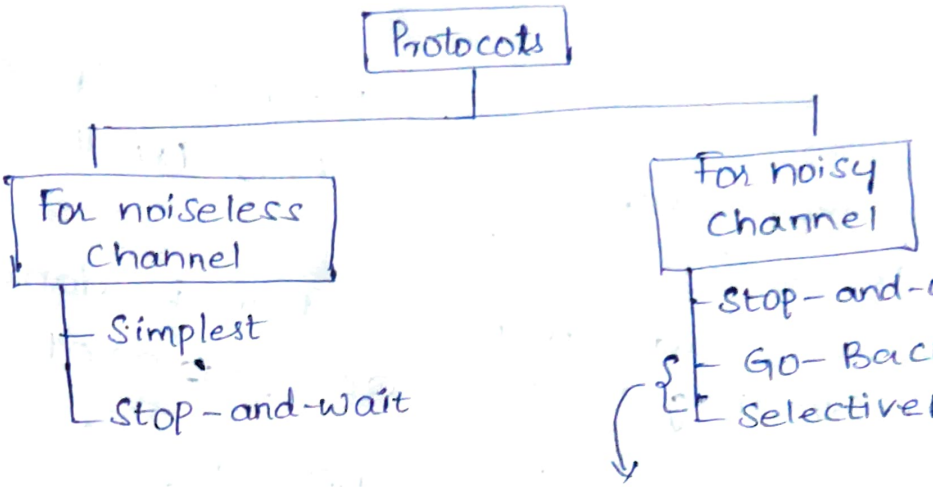
Ex:- If we consider the codeword 10011100101 (previous ex) after adding p = XOR(1,0,0,1,1,0,1) = 0, the new codeword to be sent will be 0.

At the receiver's end, error detection is done as shown in the following table - 10011100101.

C	P	conclusion
C = 0	0	NO error
C = 0	1	Error has occured in the p bit. So the data bits can be sent to the upper layers after removing all check bits
C ≠ 0	1	Single bit error occured that can be corrected by reversing the bit value at the bit position given by value of C
C ≠ 0	0	Double error detected that cannot be corrected.

Protocols :-

→ They are two types :-



Sliding window protocol :-
allows the Sender to send multiple frames before needing the acknowledgements.

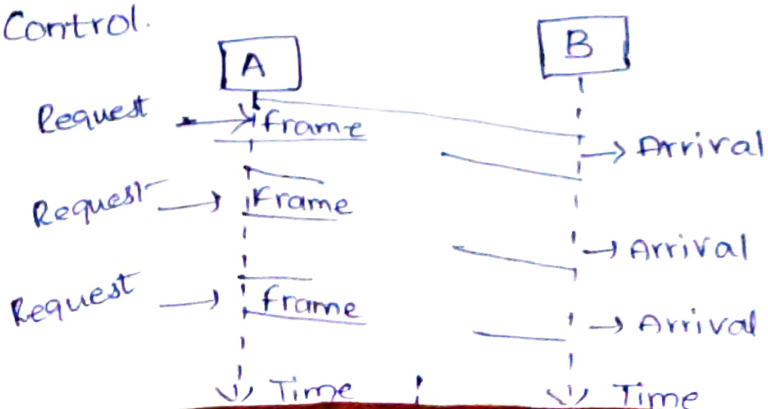
Noiseless Channels :-

→ An ideal channel in which no frames are lost, duplicated, or corrupted.

→ They are two types
1. Simplest protocol
2. Stop-and-wait protocol.

1. Simplest protocol :-

→ The design of the simplest protocol with no flow (or) error Control.



→ Algorithm for Sender data in Simplest protocol:

```
While(true)                    // Repeat forever
{
WaitForEvent();                // Sleep until an event occurs
if(Event(RequestToSend))       // There is a packet to send
{
  GetData();
  MakeFrame();
  SendFrame();                 // Send the frame
  }
}
```

→ Algorithm for Receiver data in Simplest protocol

```
while(true)                    // Repeat forever
{
WaitForEvent();                // Sleep until an event occurs.
if(Event(ArrivalNotification))  // Data frame arrived.
{
  ReceiveFrame();
  ExtractData();
  DeliverData();               // Deliver data to network layer
  }
}
```

2) Stop-and-wait protocol:-

→ The Stop-and-wait protocol is bi-directional.

→ Algorithm for Sender data:-

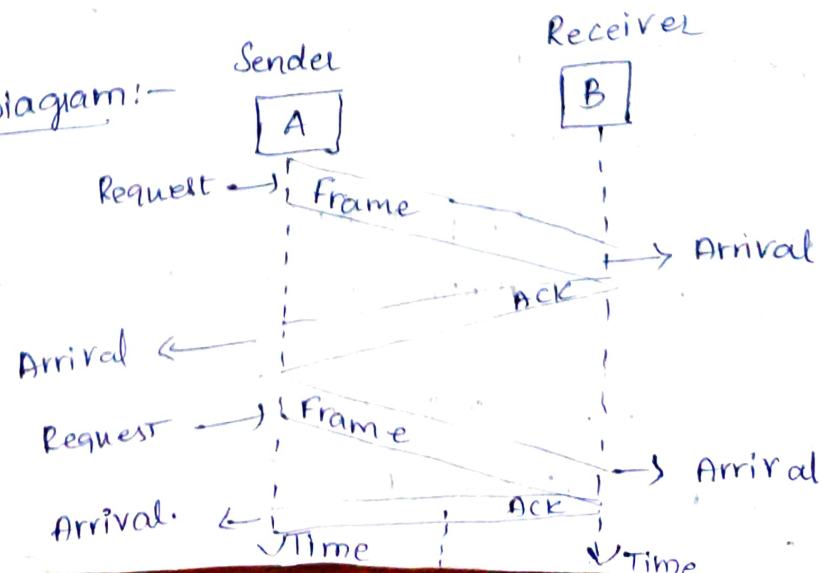
```
while(true)                    // Repeat forever
CanSend = true                 // Allow the first frame to go
{
WaitForEvent();                // Sleep until an event occurs
if (Event (RequestToSend) AND CanSend)
```

```
    GetData();
    MakeFrame();
    SendFrame();                    // Send the data frame
    CanSend = false                 // Cannot Send until ACK
                                       arrives.
}

WaitForEvent();                     // Sleep until an event
                                       occurs.
if (Event(ArrivalNotification)      // An ACK has arrived
  {
   ReceiveFrame();                  // Receive the ACK frame
   CanSend = true;
  }
}
```

→ Algorithm for Receiver form :-

```
While(true)                         // Repeat forever
{
WaitForEvent();                     // Sleep until an event occurs

if (Event(Arrival Notification))    // Data frame arrives
 {
  ReceiveFrame();
  ExtractData();
  Deliver(data);                    // Delives data to network layer
  SendFrame();                      // Send an ACK frame
 }
}
```

Flow Diagram :-



2) Noisy Channel :-

→ They are 3 types :-

1. Stop-and-Wait ARQ
2. Go-Back-N ARQ
3. Selective Repeat ARQ.

1. Stop and Wait ARQ :-

→ Error Correction in Stop-and-wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires.

→ In Stop-and-wait ARQ, we use sequence numbers to number the frames.

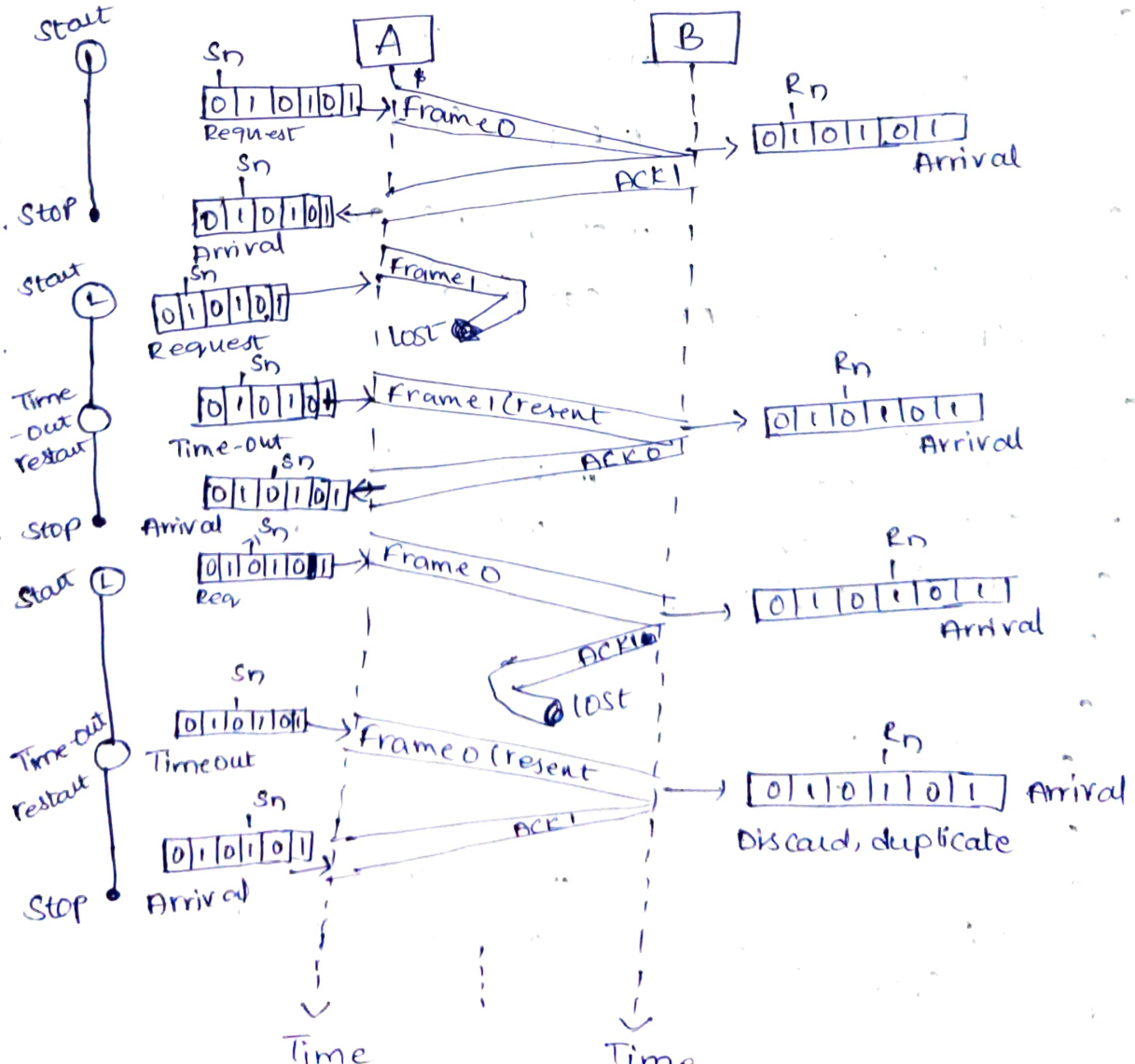
→ The sequence numbers are based on modulo-2 arithmetic

→ Algorithm for Receiver side :-

```
Sn = 0;                          // Frame 0 should be sent first
CanSend = true;                  // Allow the 1st request to go
while (true)                     // Repeat forever.
{
WaitForEvent();                  // Sleep until an event occurs
if (Event(RequestToSend) AND CanSend)
{
 GetData();
 MakeFrame(Sn);                  // The SeqNO is Sn
 StoreFrame(Sn);                 // Keep copy
 SendFrame(Sn);
 StartTimer();
 Sn = Sn + 1;
 CanSend = false;
 }
 WaitForEvent();                 // Sleep until an event occurs
 If (Event(ArrivalNotification)  // An ACK has arrived
 {
```

```
If (Event (ArrivalNotification)          //Arrival
  ReceiveFrame(ackNO);                   // Receive the ACK frame
  IF(not Corrupted AND ackNO == Sn)      // Valid ACK.
    {
     StopTimer( );
     PurgeFrame(Sn - 1);                 // COPY is not needed
     CanSend = true;
    }
  }
if (Event (TimeOut)                      // The timer expired
  {
  StartTimer( );
  ResendFrame (Sn-1);                    // Resend a Copy
  }                                         Check.
}
```

Flow Diagram:-



28-1-21

Go-Back-N- Automatic Repeat Request :-

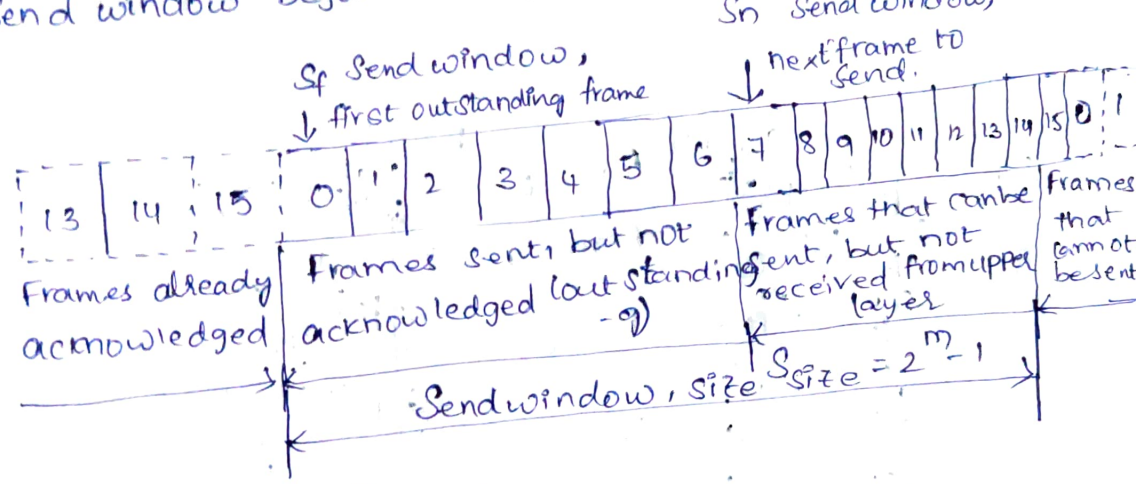
→ In this protocol we can send several frames before receiving acknowledgments.

→ We keep a copy of these frames until the acknowledgments arrive.

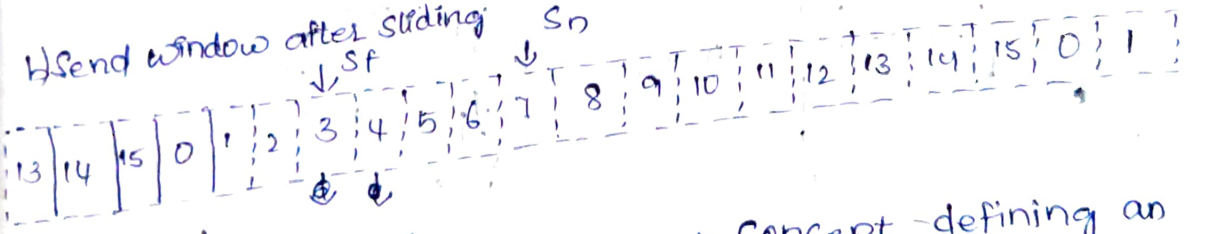
Sliding window protocols :-

→ In the Go-Back-N protocols, the sequence numbers are modulo 2^m, where m is the size of the sequence number field in bits.

a) Send window before sliding

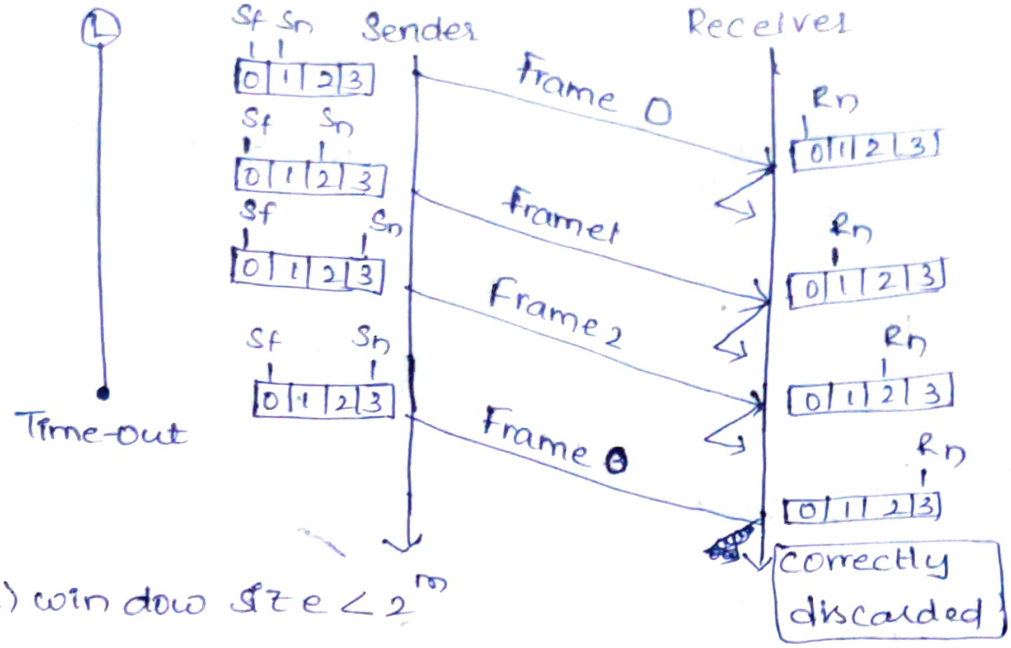


b) Send window after sliding

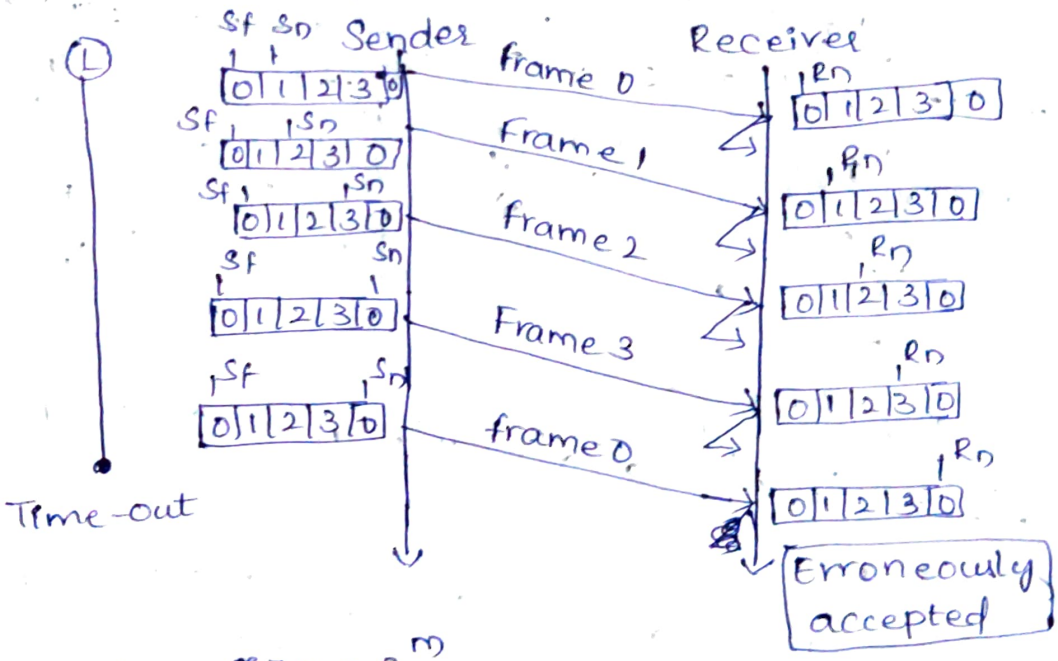


∴ The Send window is an abstract concept - defining an imaginary box of size $2^m - 1$ with three variables: Sf, Sn, and Ssize

Window size for Go-Back-N ARQ



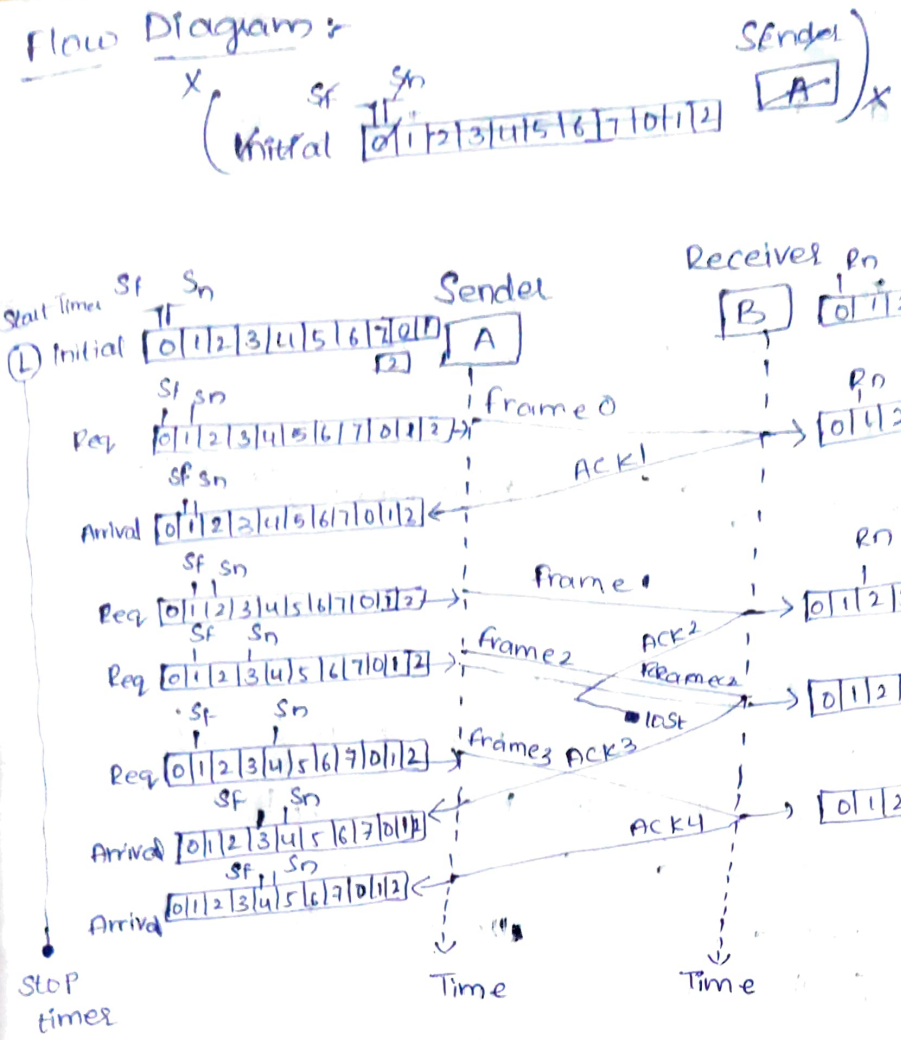
a) window size $< 2^m$



b) window size = 2^m

∴ In Go-Back-N ARQ, the size of the Send window must be less than 2^m; the size of the receiver window is always 1.

Flow Diagram:-



Selective Repeat ARQ:-

→ The disadvantage of GO-Back-N is that the receiver side is maintained with only one window, which makes the Protocol inefficient for noisy link.

→ So this Selective Repeat ARQ is used to stop resending N-frames and forward only the damaged frame.

Multiple access links, protocols.

→ They are two types of links

- point-to-point
  - → point-to-point link blw Ethernet switch/host
  - → ppp for dial-up access
- broadcast (shared wire or medium)
  - → old-fashioned ethernet
  - → upstream HFC in cable-based access network
  - → 802.11 wireless LAN, 4G/4G, Satellite

Channel Allocation problem:

- Allocating a single broadcast channel among competing users
- The channel might be a portion of the wireless spectrum in a geographic region, or a single wire or optical fiber to which multiple nodes are connected.

Static channel allocation:-

→ Traditionally Frequency Division Multiplexing (FDM) was used.

→ Disadvantage:-

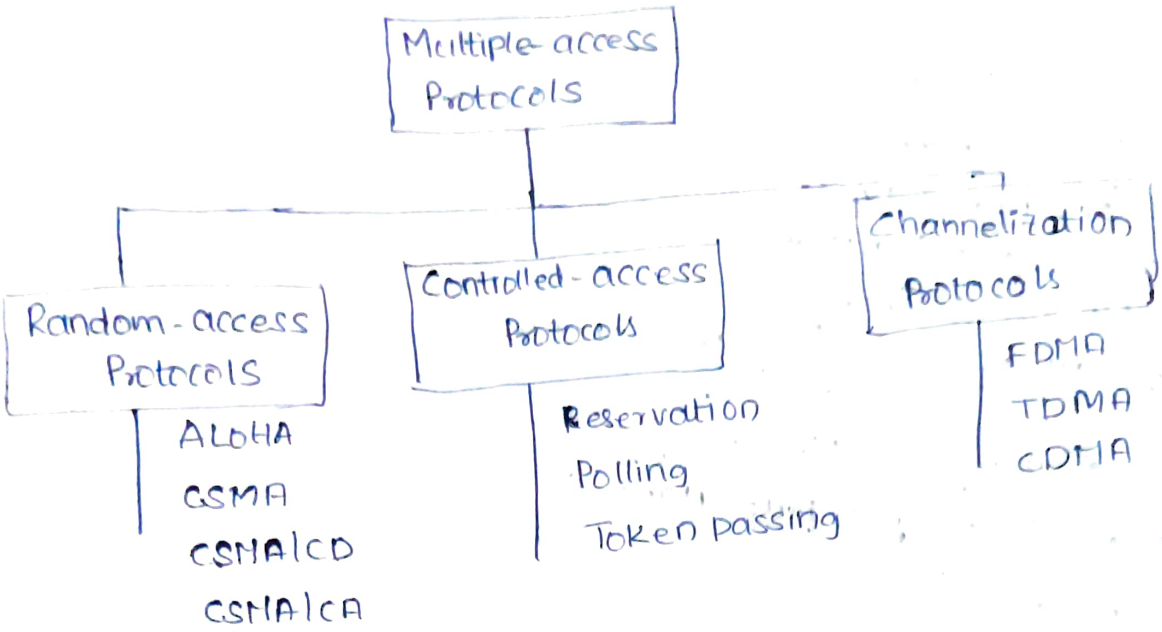
* Not efficient for large or more users
* Random division of the channel into N-regions, but if the users (n) are less than the regions (N), then the spectrum will be wasted and vice-versa.
* If a user is not a channel allocated then it becomes unused, even for those who require
* Hence static FDM is inefficient.

Dynamic channel allocation:-

Key Assumptions:-

1. Station model: Model

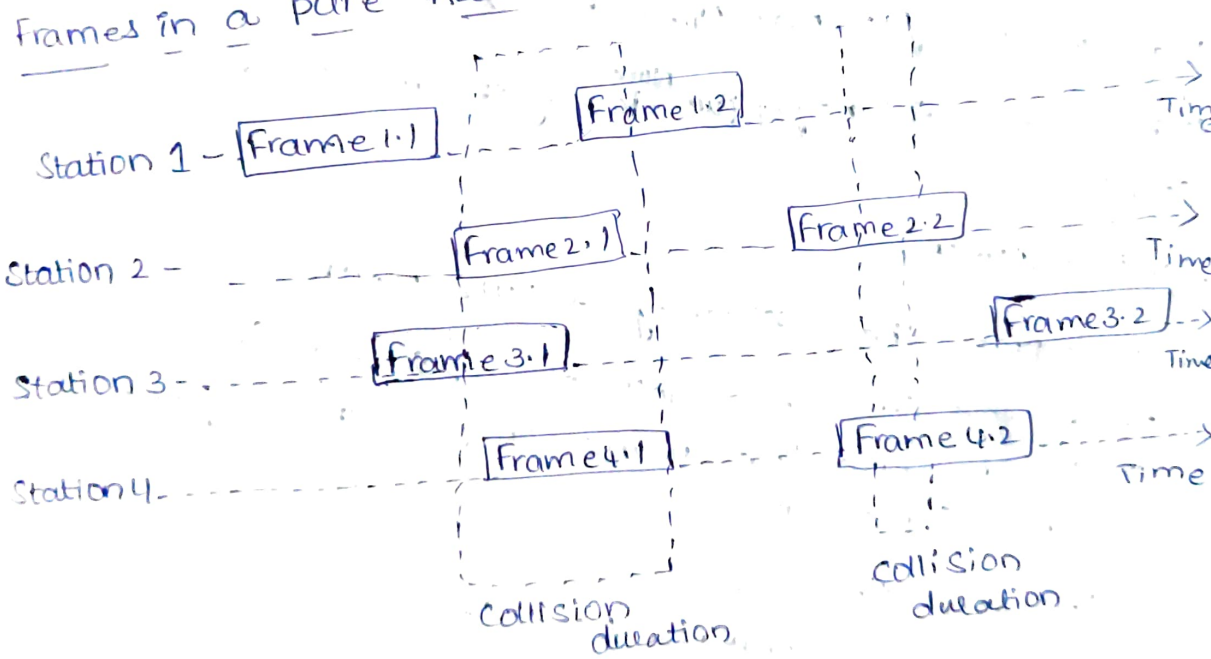
Multiple access protocols:-



Random access protocols:-

ALOHA:- They are two types 1. Original ALOHA, Pure ALOHA

Frames in a pure ALOHA Network:-



→ This is a simple, but elegant protocol

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

→ Since there is only one channel to share, there is the possibility of collision b/w frames from diff stations.

4 2-21

Assumptions Considered in pure ALOHA:-

* Station Model
* Single channel
* Continuous time
* Collision Assumption
* No Carrier Sensing

Max Efficiency of pure ALOHA:-

Substituting $G = 1/2$, we get

Max efficiency of pure Aloha

$= 1/2 \times e^{-2 \times 1/2}$

$= 1/2 e$

$= 0.184$

$= 18.4\%$

Max efficiency of pure Aloha (η) = 18.4%

* The max efficiency of pure Aloha is very less due to large no. of collisions

Slotted ALOHA:-

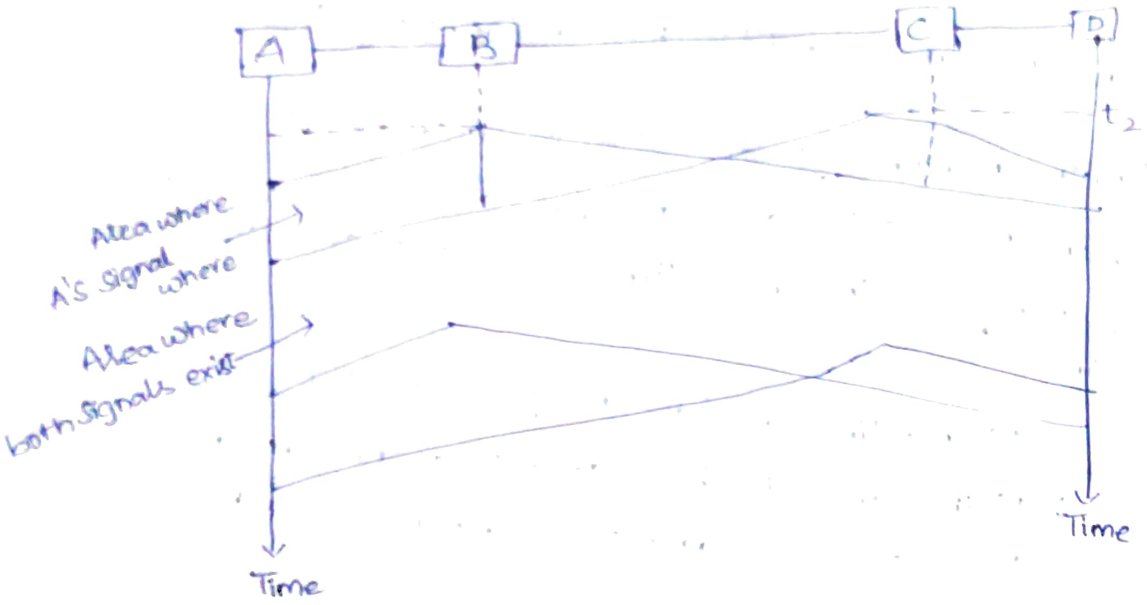
→ To improve the efficiency of pure ALOHA

→ Divide the time into slots, of T_{fr}'s and force the station to send the frame only at the beginning of the time slot.

→ vulnerable time = T_{fr}

CSMA (Carrier-Sense Multiple Access):-

→ 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 before sending.

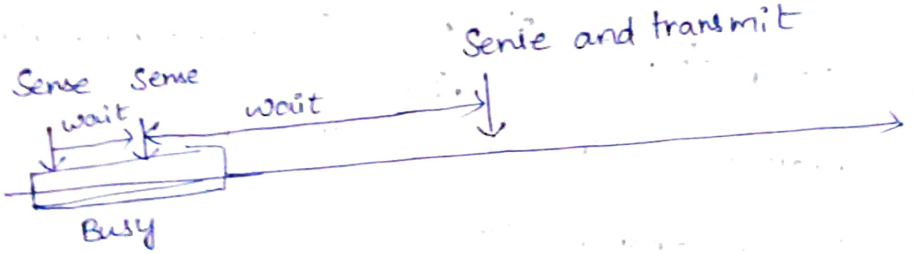


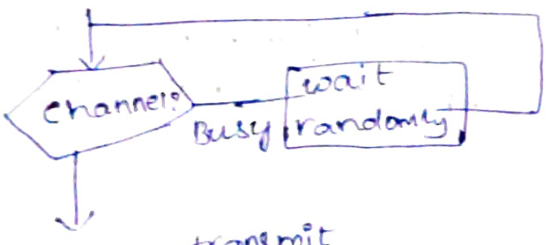
→ CSMA Vulnerable Time = T_p

1-Persistent:-

Nonpersistent Method:-

→ In this method, a station that has a frame to send senses the line. If the line is idle, it sends immediately.





P- Persistent :-

→ In this method, after the station finds the line idle

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 set 1.
   b) If the line is busy, it acts as through a collision has occured and uses the backoff procedure.

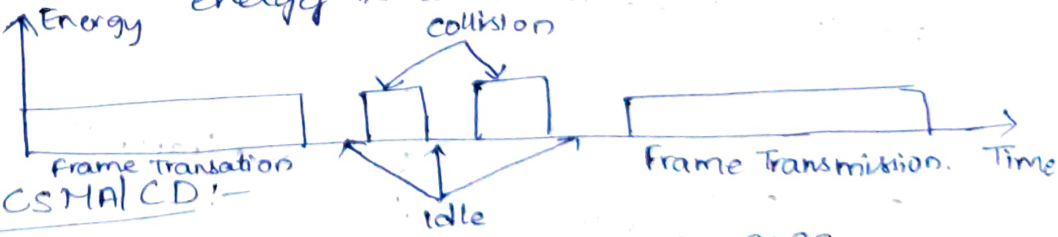
CSMA/CD :-

→ The Csma method does not specify the procedure following a collision. CSMA/CD provides the algorithm to handle the collision.

Energy level :-

→ There are 3 types :-

1. Zero level → is the channel is idle.
2. Normal level → is a station has successfully captured the channel and is sending its frame.
3. Abnormal level → there is a collision and the level of the energy is twice the normal level.



CSMA (VS) CSMA/CD :-

1) is the addition of the persistence process.
2) is the frame transmission.
3) is the sending of a short jamming signal that enforces the collision in case other stations have not yet sensed the collision.

Throughput :-

→ is CSMA/CD is greater than that of pure or slotted ALOHA. The max throughput occurs at a diff value of G and is based on the persistance method and the value of P in the persistance.

→ They are various Random Access protocols.

- → CSMA
- → CSMA/CD
- → CSMA/CA.

CSMA/CA :-

* If the station needs to be able to receive while transmitting to detect a collision.
* when there is no collision, the station receives one signal : its own signal.
* when there is a collision, the station receives two signals : its own signal transmitted by a second station.
* To distinguish blw the above 2 signals, the received signals in these two cases must be significatly diff. In other words, the

*

Interface Space [IFS] :-

→ Collisions are avoided by deferring transmission even if the channel is found idle.

Contention window :-

→ Contention window channel is free, they wait a random amount of time before they start sending.

Collision

11-2-21

Network Layer:-

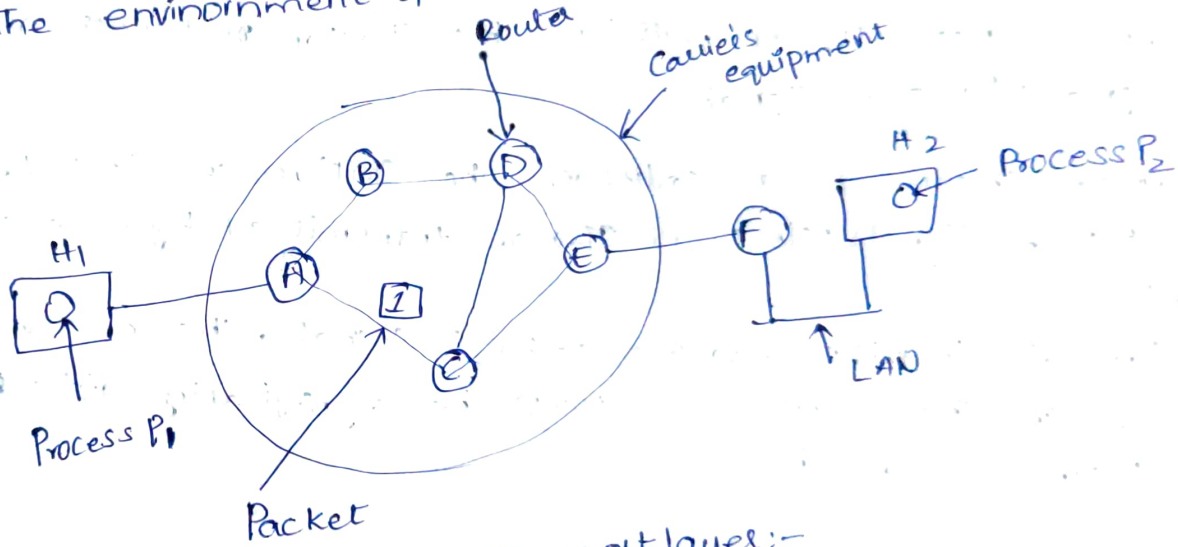
Design Issues:-

→ Store-and-Forward packet switching
→ Services provided to the Transport layer
→ Implementation of Connectionless Service
→ Implementation of Connection-Oriented Service
→ Compaison of Virtual-circuit and datagram Subnets

* Main Task of the Network layer is to move packets from the source host to the destination host.

1. Store-and-Forward packet switching:-

* The environment of the network layer protocols.



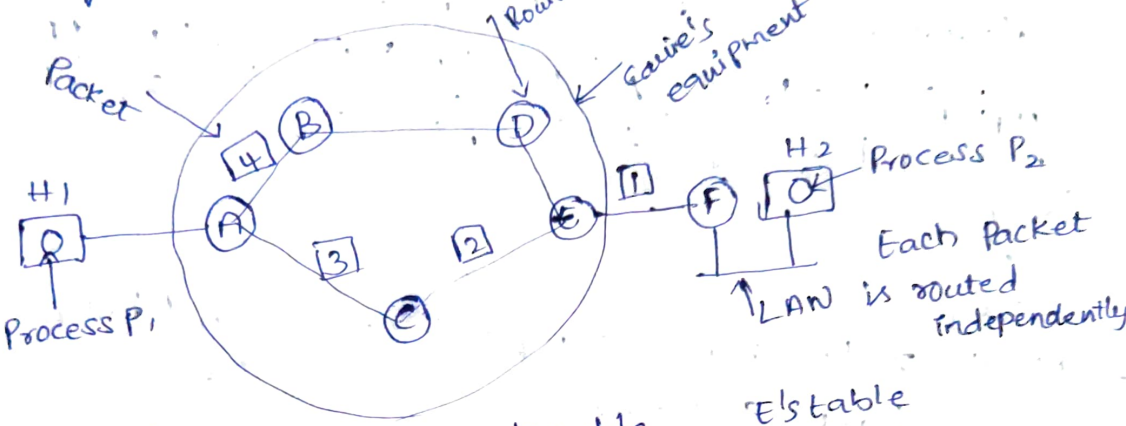
2. Services provided to the Transport layer:-

* The network layer provides services to the transport layer at the network layer / transport layer interface.

1. The services should be independent of the router technology.
2. The transport layer should be shielded from the no, type, and topology of the routers present.
3. The network addresses made available to the transport layer should use a uniform numbering plan even accross LAN's and WANS

3. Implementation of Connectionless Service:-

→ Packets are injected into the subnet individually and routed independently
→ No advance setup is required.
→ In this context, the packets are frequently called datagrams and the network is called a datagram network.
→ The algorithm that manages the tables and makes the routing decisions is called the routing algorithm.



A's table

Dest.	initially line	later line
A	-	-
B	B	B
C	C	C
D	B	B
E	C	B
F	C	B

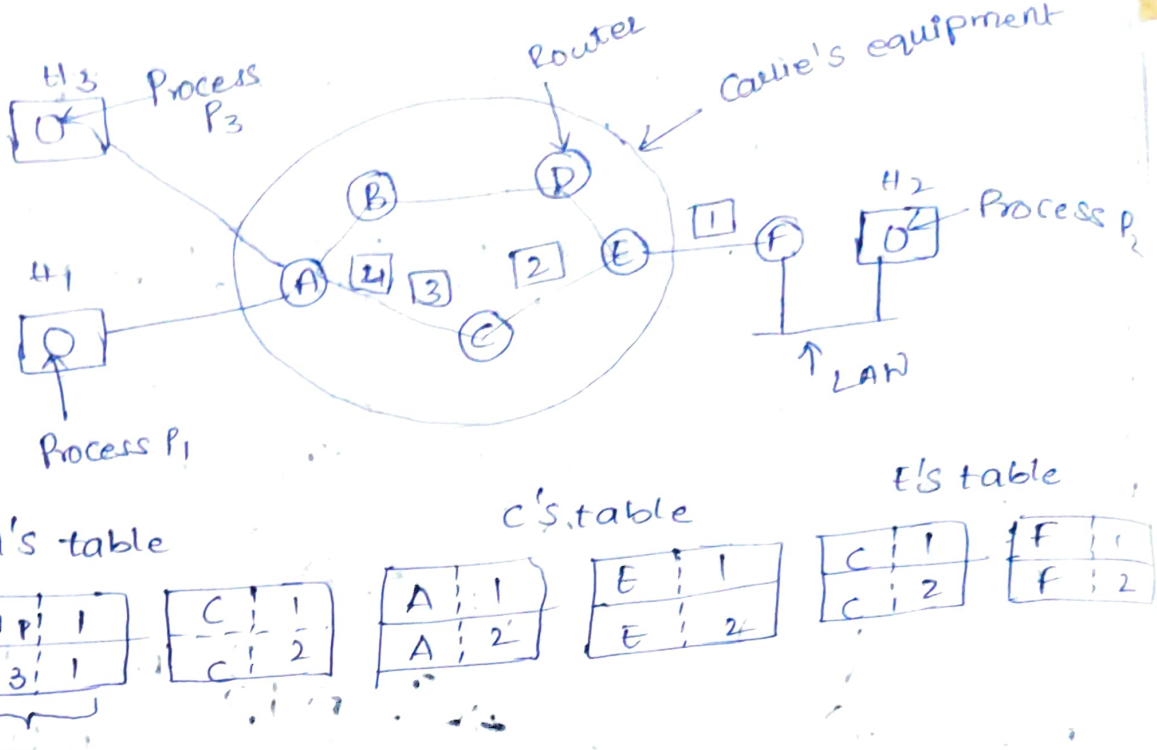
C's table

Dest.	line
A	A
B	A
C	-
D	D
E	E
F	E

E's table

Dest.	line
A	C
B	D
C	C
D	D
E	-
F	F

4.
→ Virtual circuit network is required.
→ Instead of choosing a new route every time, a route from source to destination is chosen as a part of the connection set up and stored in tables of the routers.
→ When the connection is released, the virtual circuit is also terminated.
→ All packets carries an identifier indicating the virtual circuit it belongs to.



~~Ability~~.

→ Ability of the routes to replace Connection Identifiers is Called Label Switching.

5.

Issue	Datagram Subnet	Virtual-circuit Subnet
Circuit setup	Not needed.	Required
Addressing	Each packet contains the full Source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table Space per connection
Routing	Each packet is routed independently	Route Chosen when VC is setup; all packets follow it
Effect of router failures	None, except for Packets lost during the Crash	All VC's that passed through the failed routes are terminated.
Quality of Service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Routing Algorithms:-

→ The main func of the network layer is routing packets from the source machine to the destination machine

→ Session Routing:-

→ If the Subnets uses virtual circuits internally, then routing decisions are made only when a new virtual circuit is being set up.

→ when a router receives a packet, it handles using two Process:

1. looking up the outgoing line to use for it in the routing table - Forwarding
2. responsible for filling in and updating the routing table.

→ Routing algorithms for both datagrams and virtual circuits should satisfy:

1. Correctness
2. Simplicity
3. Robustness
4. Stability
5. Faisness
6. ~~opti~~ optimality

Flooding:-

→ Requires no network information like topology, load condition, cost of diff. paths.

→ Every incoming packet to a node is sent out on every outgoing like expec' except the one it arrived on.

→ Characteristics:-

* All possible routes blw Source and destination is tried. A Packet will always get through if path exists.
* As all routes are tired, there will be atleast one route which is the shortest.
* All nodes directly or Indirectly Connected are visited.

Limitations:-

→ Flooding generates vast number of duplicate packets.
→ Suitable damping mechanism must be used.

Hop:-

→ A hop is a computer networking term that refers to the no. of routers that a packet (a portion of data) passes through from its source to its destination.

Hop-Count:-

→ A hop counter may be contained in the packet header which is decremented at each hop with the packet being discarded when the counter becomes zero
→ The sender initializes the hop counter. If no estimate is known, it is set to the full diameter of the subnet
→ keep track of the packets which are responsible for flooding using a sequence no. Avoid sending them out a second time.

→ Selective Flooding:- Routers do not send every incoming Packet out on every time line, only on those lines that go in approximetely in the direction of the destination.

→ Advantages of Flooding:-

* Highly Robust, emergency or immediate messages can be sent (eg military applications)
* Set up route in virtual circuit
* Flooding always chooses the shortest path
* Broadcast messages to the nodes.

Shortest path Routing:-

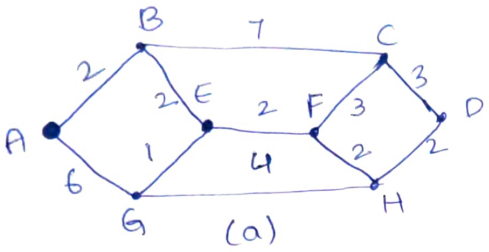
* A graph for the subnet is built with each node of the graph representing a router and each arc of the graph representing communication line.
* The algorithm finds a shortest path from a node to all other nodes in the network.

* Dijkstra's algorithm is used for solving the problem
* Steps followed:

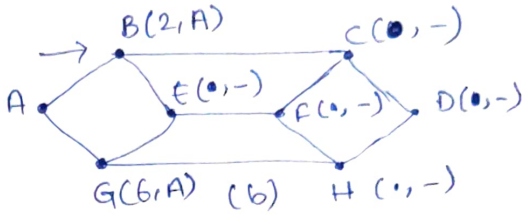
→ Dijkstra's algorithm starts by assigning some initial values for the distance from node S to every one other node in the network.

→ At each step, the shortest distance from node S to another node is determined.

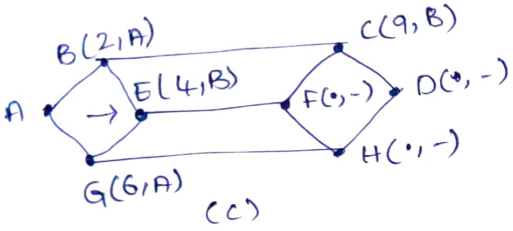
Ex:-



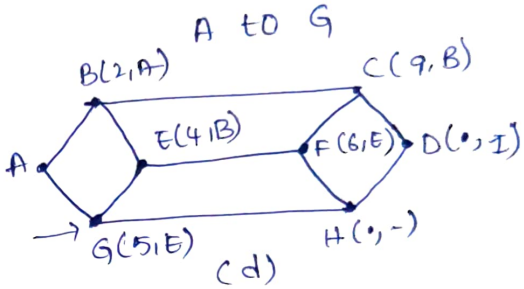
A to B



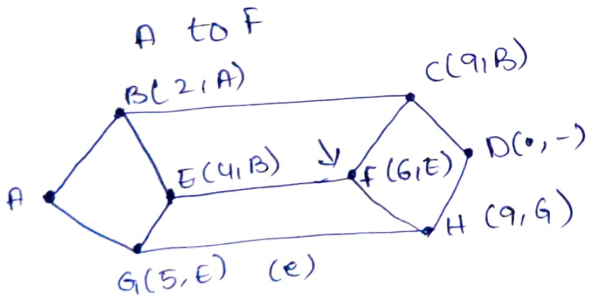
A to E



A to G



A to F



A to H