INTRODUCTION TO COMPUTER NETWORKS

NETWORK : A network is a set of devices (often reffered as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or recieving data generated by other nodes on the network

"Computer Network" means a collection of autonomous computers interconnected (i.e able to exchange information)

USES :-

1. BUSINESS APPLICATION
   (resource sharing) (client server model) (communication medium) (desktop sharing) (e-commerce)
2. HOME APPLICATION
   (peer-peer communication) (e-commerce) (entertainment)
3. MOBILE USERS
   (Messaging) (GPS) (NFC) (Smart phones)

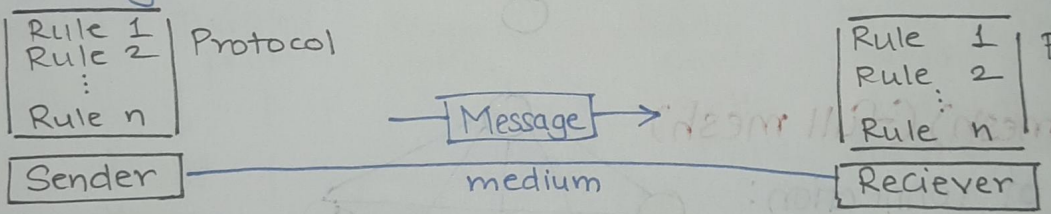
SOCIAL ISSUES

PHISHING : attacker masquerades as a trusted entity to steal user credentials. personal information. by opening a email or message

BOTNET : performs distributed denial of service (DDoS) to steal data, send spam. allows attacker access of device and communication.

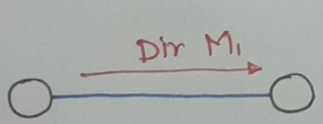
EFFECTIVENESS of communication depends on:
1. Delivery 2. Accuracy 3. Timeliness 4. Jitter

DATA COMMUNICATION SYSTEM
1. Message 2. Sender 3. Reciever 4. Medium 5. Protocol



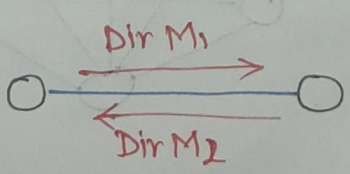
DATA FLOW

SIMPLEX



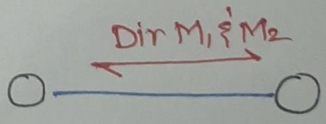
one way communication

HALF DUPLEX



two way but one at a time

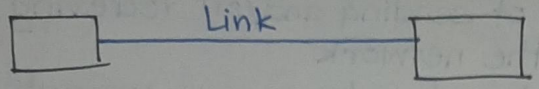
FULL DUPLEX



two way and simultaneous

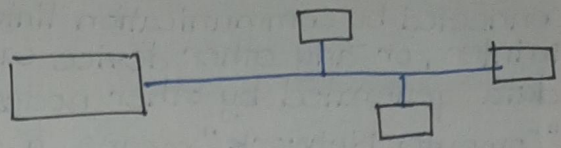
TYPES OF CONNECTION

POINT to POINT



dedicated link between 2 devices

MULTIPOINT

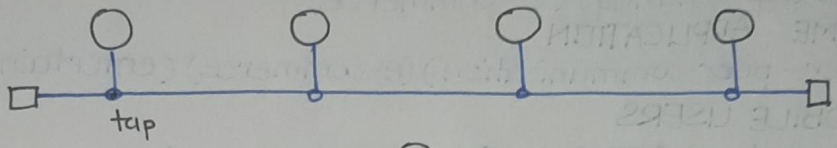


Multiple device share a same link.

PHYSICAL TOPOLOGY.

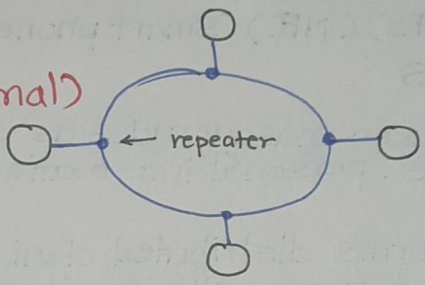
BUS :

(line topology)



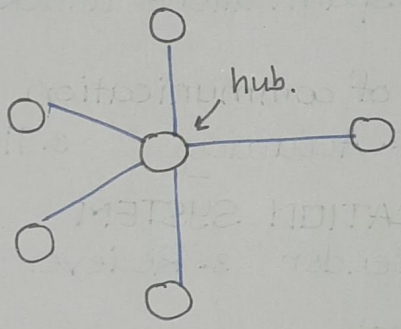
RING :

(unidirectional) (bidirectional)



STAR :

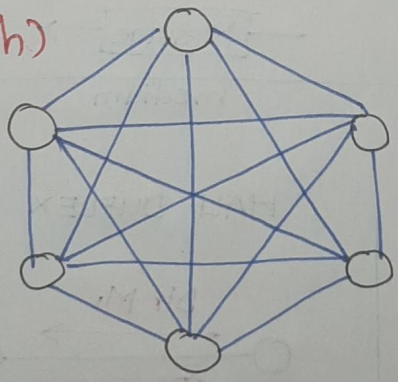
most common network setup



MESH

(partial mesh) (-full mesh)

number of connection:
if n device $n(n-1)/2$



HYBRID

mix of all above topologies.

TYPES OF NETWORK (based on size)

LAN: Group of interconnected computers within a small area
example: room, building, campus
Coaxil cable normally used, minimum noise, 10 to 100 mbps data transfer rate

MAN: extends over a larger area. Joins multiple LAN's
ranges from 5km to 50 km radius
owned by organization or individual
Data transfer rate lower ~~tan~~ than LAN

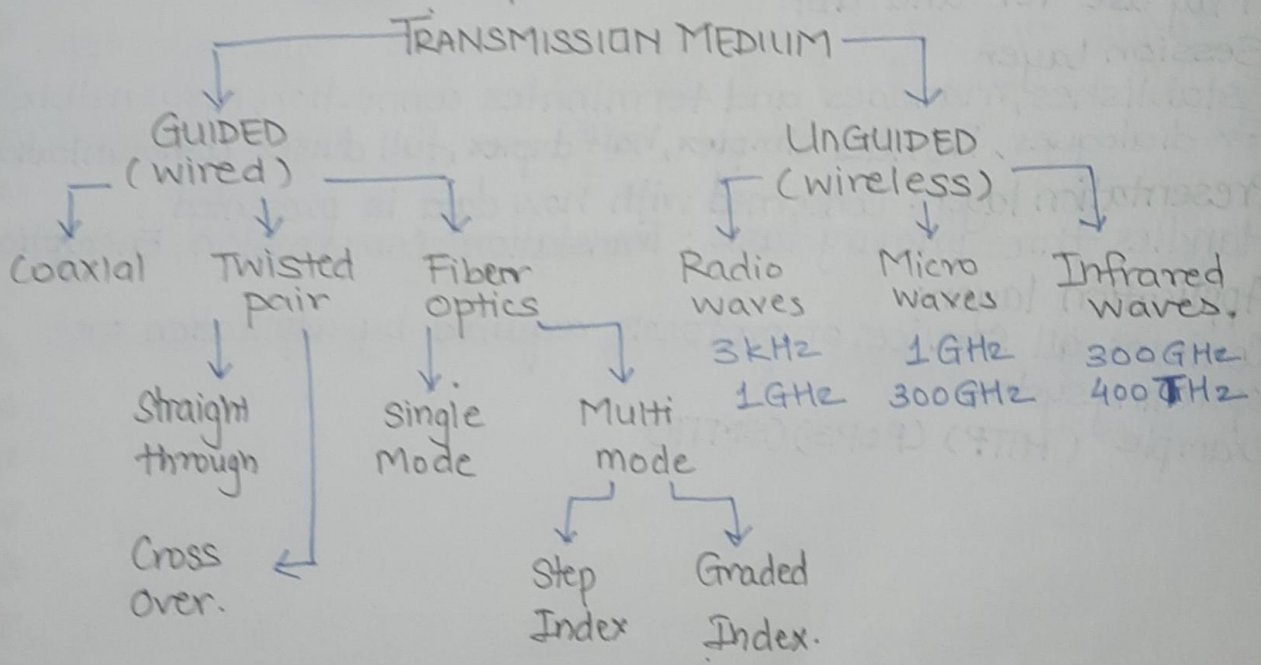
WAN: country or worldwide network. contains multiple MAN's and LAN's. uses satellites and microwave relays
Data transfer rate depends upon the ISP provider and varies

Other types

WLAN (wireless LAN): A LAN used for high frequency radio waves for communication. short range with high speed data transmission.

PAN (Personal area network) used for personal use

SAN (Storage area network) used to connect data storages with servers by fibre optics.



OSI (open systems Interconnection)

created by ISO, general framework and reference model
not a standard that MUST be followed
All layer work together to move data around.

Application	Presentation	session	Transport	Network	Datalink	Physical
DATA in each layer:	DATA		Segment	Packet	Frame	Bits.

Physical layer: physically moving data, converting data from higher levels to bits. used to transmit data.
cables, frequencies etc defined example: Hub

Data link layer: organize bits into frames to provide hop-hop delivery. requires MAC address

NETWORK layer: responsible for moving packet within network. require IP address
example: router

Transport layer: Takes data from higer OSI layer and ~~bre~~ breaks them into segments for lower layer to transmit and does reverse white recieving (also does sequencing)
May use TCP and UDP

Session layer
Establishes, manages and terminates connection, responsible for dialogues, Provides simplex, half duplex, full duplex communication

Presentation layer: Concerned with how data is presented
Handles three primary task: Translation, Compression, Encryption

Application layer:
Contains all services or protocols required by application or operating system.
example (HTTP) (POP3) (SMTP)

TCP/IP MODEL

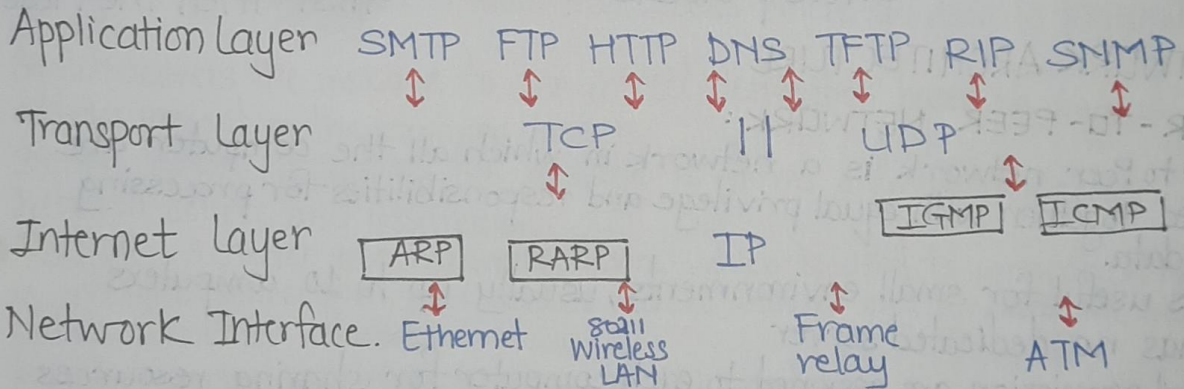
A protocol suite is a large number of related protocol that work together to allow networked computers to communicate.

Application layer: FTP (File transfer protocol)
Telnet (Remote terminal protocol), SMTP (Simple Mail transfer Protocol)
HTTP (Hyper-Text transport protocol)

TRansport layer: TCP : connection oriented protocol
allows virtual connection (virtual circuit)
UDP: divides chunk of data into segments also reassembles data into original chunk.
reordering and data resend

Internet layer: deals with packets and connects independant networks to transport packets accross network boundaries.
has IP & ICMP (Internet control Message Protocol) used for error reporting.

Network Interface (Host to network layer)
combines physical and data link layer from OSI model
At this layer data is transported between adjacent LAN's & WAN's or nodes within same LAN

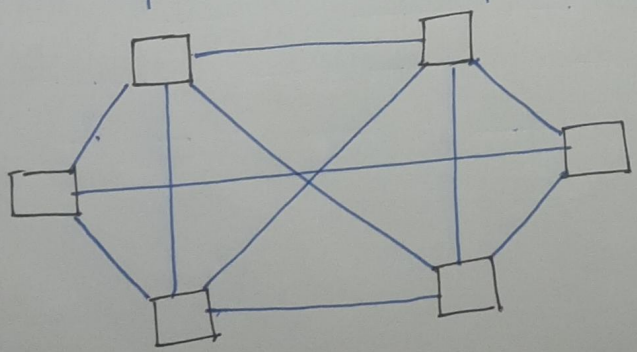


	OSI MODEL	TCP/IP MODEL
Layers.	7 layers	4 layers.
arrangement	strict, vertical	loose, horizontal
Support (Network layer)	connectionless & connection oriented communication	only connectionless communication.
Support (Transport layer)	only connection oriented communication	connectionless & connection oriented communication.
Distinction	clear between service, Interface & protocol	not clear between service, Interface & protocol.
Transparency.	Protocols are hidden & can be replaced relatively easily	Protocols not hidden & cant be replaced easily.
	(Replacing IP by substantial different protocol is virtually Impossible)	
Discovery.	OSI was designed before protocols	The protocol came first then the Model

NETWORK ARCHITECTURE

PEER-TO-PEER NETWORK:

Peer to Peer network is a network in which all the computer are linked together with equal privilege and responsibilities for processing the data.
It is useful for small environments, usually up to 10 computers
It has no dedicated server
Special permission are assigned to each computer for sharing resources but this can lead to problem if the computer with the resource is down



CLIENT-SERVER NETWORK

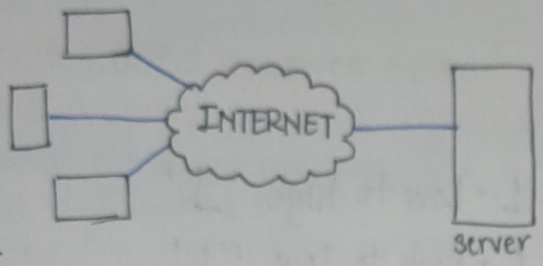
Client/Server network is a network model designed for the end user called clients, to access the resources such as song, video etc. from central computer knownas server

The central controller is known as a server while all other computers in the network are called clients.

A server performs all the major operations such as security and network management.

A server is responsible for managing all the resources such as files, directory, printer etc.

All the clients communicate with each other through the server



COMPONENTS

- SWITCH : a hardware device that connects multiple device on a computer network. A switch contains more advanced features than hub.
The switch contains updated table that decides where the data is transmitted or not.
Switch delivers the message to the correct destination based on physical address present in the incoming message
Switch doesnt broadcast the message it forms a direct connection between source and destination.
- ROUTER : A router is a hardware device which is used to connect LAN with an internet connection. It is used to recieve analyze and forward the incoming packets to another network.
A router works in Network layer of OSI model.
A router forwards the packet based on the information available in the router table
It determines best path from the available ~~in the routing table~~ path for the transmission of the packet.
- BRIDGE : A bridge is a network device that connects multiple subnetwork to create single network.
It provides interconnection with other computer networks that use the same protocol
Through Bridge multiple LAN can be connected to form MAN or extended LAN

- GATEWAY : A gateway is a computer on a network that provides the interface between two applications on a network that use different protocols. They are used to provide a connection to the internet. A gateway in a network converts information from one protocol to another and then transfers it over the web.
- ACCESS POINT : An access point (AP) is a term used for a network device that bridges wired and wireless network
Consumer AP's are often called "wireless routers" as they typically also serve as both internet routers and firewalls
Commercial AP's tend towards minimal network routing facilities & rarely have firewalls.

LINE CODING SCHEMES

1.] MANCHESTER ENCODING

1 - high to low '⌐'
0 - Low to high '¬'

G.E. THOMAS

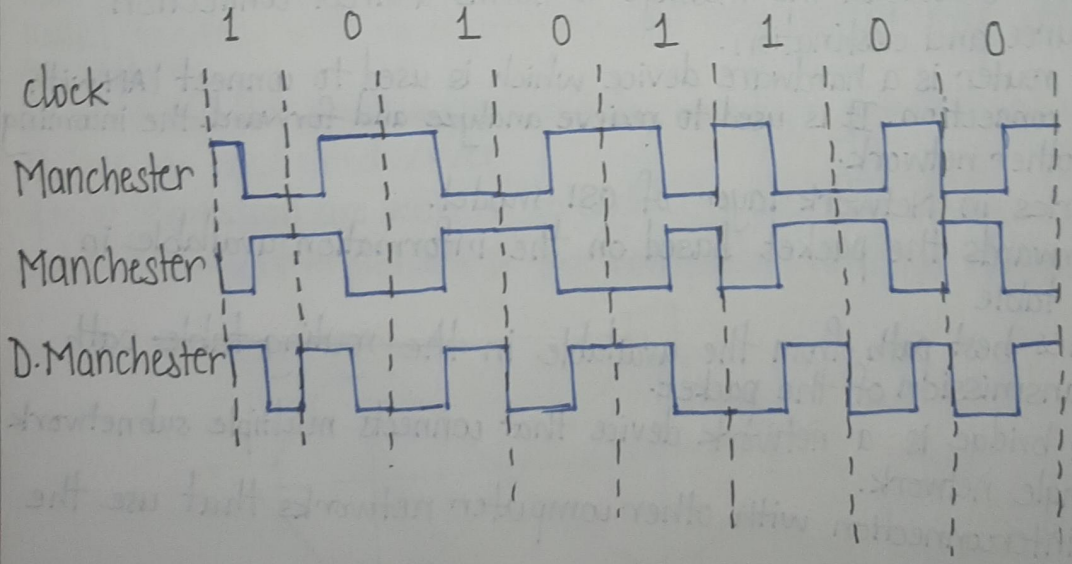
1 - Low to high '¬'
0 - high to low '⌐'

IEEE

2.] DIFFERENTIAL MANCHESTER ENCODING

1- '⌐' '¬'
0- '⊓' '⊔'

ENCODE THE FOLLOWING



FHSS (Frequency hop spread spectrum)

It is a method of transmitting radio signals by rapidly changing the carrier frequency among many frequencies occupying a large spectral band. The changes are controlled by code known to both transmitter and reciever. FHSS is used to avoid interference, to prevent eavesdropping, and to enable code distribution multiple access (CDMA) communication.

The frequency band is divided into smaller sub-bands. Signals rapidly change ("hop") their carrier frequencies among the centre frequencies of these sub bands in a determined orders. Interference at a specific frequency will affect the signal only during a short interval.

DSSS (Direct sequence spread spectrum)

It is a spread spectrum modulation technique primarily used to reduce overall signal interference. The Direct sequence modulation makes the transmitted signal wider in bandwidth than the information bandwidth. After the despreading or removal of the direct sequence modulation in the reciever, The information bandwidth is restored while the ~~unn~~ unintentional and intentional interference is substantially reduced.

UNIT 2

DATA LINK LAYER

FUNCTIONS

1. Providing service to the network Layer :
   - Unacknowledged connectionless service : Appropriate for low error rate & real-time traffic example Ethernet
   - Acknowledged connectionless service : Useful in unreliable channels.
   - Acknowledged connection oriented service : Guarentee frames are recieved exactly once and in the right order. Appropriate over long, ~~use~~ unreliable links such as a satellite channel or a long-distance telephone ~~service~~ circuit.
2. Framing : frames are streams of bits recieved from the network layer into managing data units. This division of stream of bits is done by Data Link Layer.
3. Physical Addressing : The data link layer adds a header to the frame in order to define physical address of the sender or reciever of the frame if the frame are to be distributed to different system on the network
4. Flow Control : A recieving node can recieve the frames at a faster rate than it can process the frame. Without flow control. The reciever's buffer can overflow and frames can get lost. To overcome this problem. The Data link layer uses flow control to prevent the sender node from overwhelming the reciever node. Thus prevents traffic jam at recieving side.
5. Error Control : It is achieved by adding a trailer at the end of the frame Duplication of frames is also prevented by this mechanism Data link layer adds this mechanism.
   - Error Detection : Errors can be introduced by signal attenuation and noise Data link layer protocol provides a mechanism to detect one or more error This is done by adding error detection bits in the end which are then checked by reciever.
   - Error Correction : It works similar to detection but here the reciever also determines where the error has occurred.
6. Access Control : Protocol of this layer determine which device has control over the link at any given time. When two or more devices are connected to same link.
7. Reliable delivery : Data link layer provides a reliable delivery service i.e transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmission and acknowledgement A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally link at which an error occurs rather than forcing to retransmit the data.

FRAMING

1. Character count :
uses a field in header to specify the number of character in the frame
When the data link layer at the destination sees the character count
- It knows how many character follow and hence where the end is
- resynchronization error after a error.

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

Frame 1 char - 5 | Frame 2 char - 5 | Frame 3 char - 8 | Frame 4 char - 8

2. Flag byte with byte stuffing
It resolves resynchronization error by having each frame start with a special character & end with them too
In older versions different byte were used but in recent years FLAG byte is being used for starting & ending.

FLAG header Payload Field trailer FLAG

A Flag 5 1 2 3 4 Flag B A Flag 5 6 7 8 9 Flag B

It may happen that Flag byte pattern may occur in data thus the Data link layer puts a special Esc byte before the Flag.

A ESC Flag 5 1 2 3 4 Flag ESC B

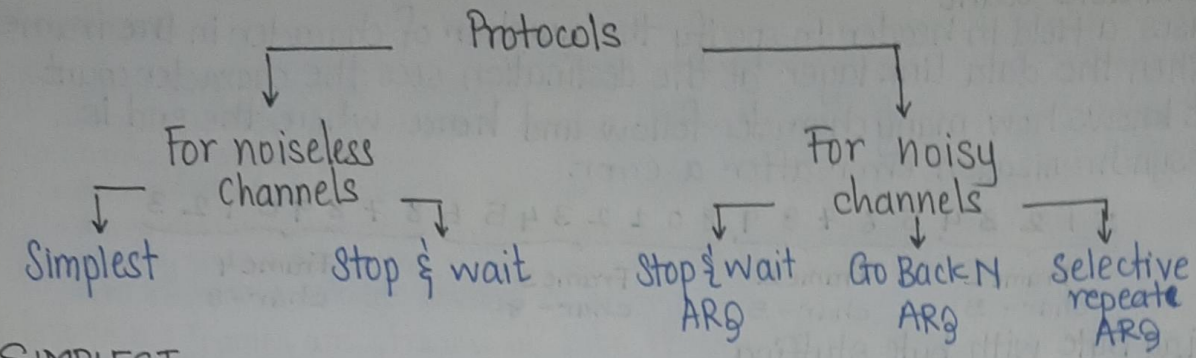
Thus the reciever data link layer removes escape byte before transferring to network layer.
If a Escape byte occured in data then it checks for doubled thus single Escape bytes are ignored.
disadvantage: closely tied with 8-bit character thus cant be used for UNICODE which is 16-bit.

3. Flag with bit stuffing
It allows arbitary number of bits and allows character code with arbitary number of bits per character
Each frame begins and ends with special bit pattern
whenever the sender encounters 5 consecutive 1's they stuff a 0 bit just like esc bit.
when recieverer recieves the message it destuffs the frames before passing it on to network layer.

0 11 0 11111 0 0110 11111 0 00101101111110

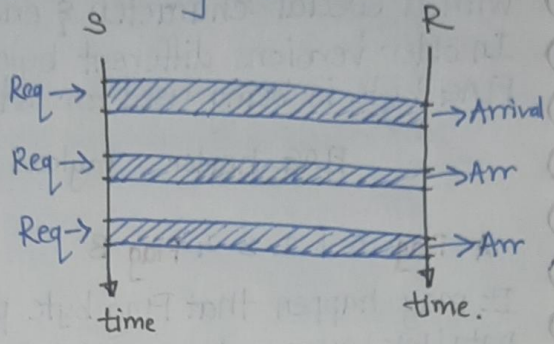
stuffed bits.

FLOW CONTROL STRATEGIES



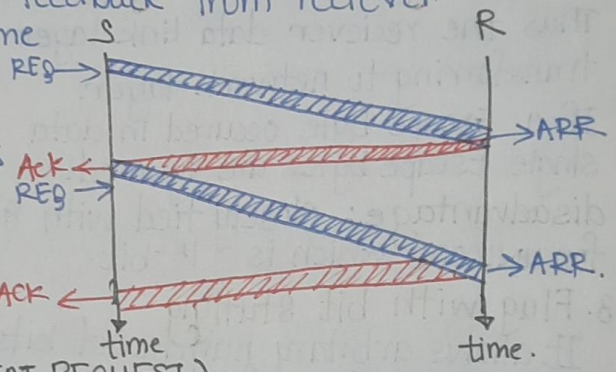
SIMPLEST

sender sends sequence of frames without thinking about buffer.
Data transmission in one direction
Both sender & reciever always ready
Processing time can be ignored
Infinite buffer space available
Communication channel never damages or looses frames.
It doesnt handle flow control or error correction.



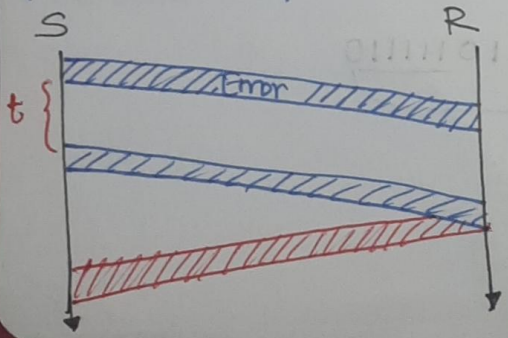
STOP AND WAIT

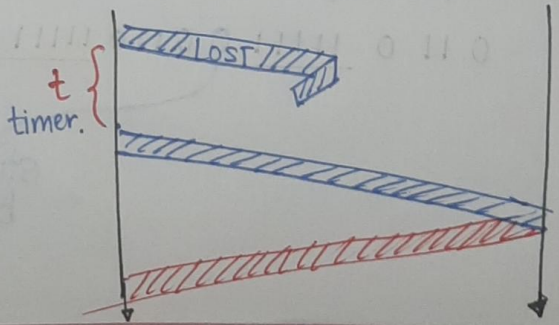
sender sends aframe and waits for feedback from reciever when Ack arrives it sends next frame
As we add ack to the protocol
This adds flow control to protocol
If Ack goes missing the protocol waits infinitely.



STOP & WAIT ARQ (AUTOMATIC REPEAT REQUEST)

To detect and correct corrupted frames . we need to add redundant bits to our data frame . When the frame arrives at the reciever side It is checked. If corrupted no ACK is sent thus after time interval It resends the frame. This repeats until ACK recieved.
Thus we encorporated error detection in the protocol.





GO-BACK-N ARQ (AUTOMATIC REPEAT REQUEST)

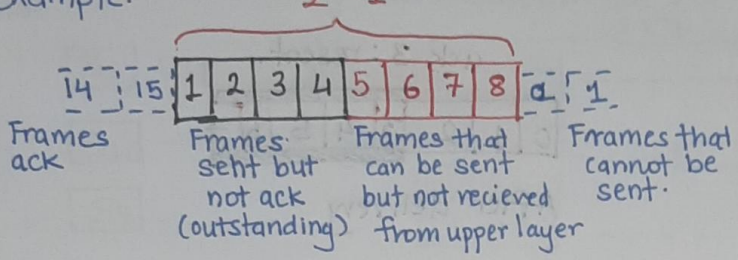
To improve the efficiency of transmission (filling the pipe). multiple frames must be in transmission while waiting for acknowledgement. In other words we need to let more than one frame be outstanding to keep the channel busy ~~with~~ while the sender is waiting for acknowledgement.

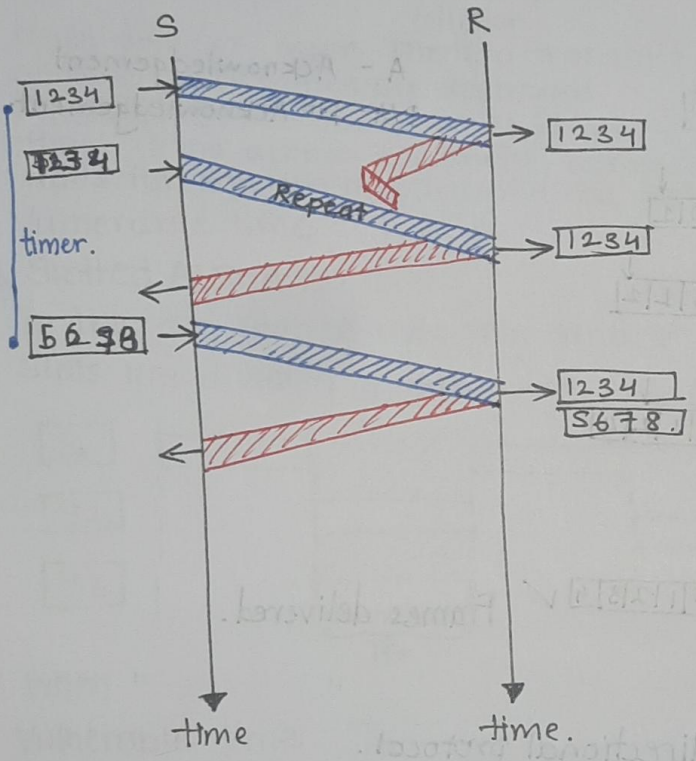
The first is called GO BACK N Automatic Repeat. In this protocol we can send several frames before recieving ~~a~~ acknowledgement. we keep a copy of these frames until acknowledgement arrives.

Number of modulo 2^m, where m is size of the sequence number field in bits.

The sequence number ranges from 0 to $2^m - 1$

Example.



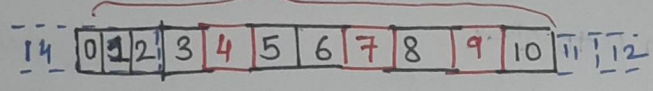


SELECTIVE REPEAT AUTOMATIC REPEAT REQUEST

In Go Back N ARQ the reciever tracks only one variable, and there is no need to buffer out of order frames; they are simply discarded. However, this protocol is highly inefficient for noisy link.
In a noisy link the frame has higher chance of damage which means resending of multiple frames. This uses bandwidth and slows transmission.

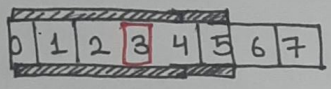
size of sender & reciever window should be at most one half of 2^m

Sender window: $2^m - 1$



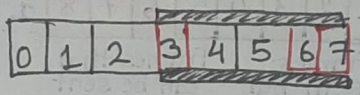
- no ack
- ack recieved.
- cant be sent.

Delivery of Data.

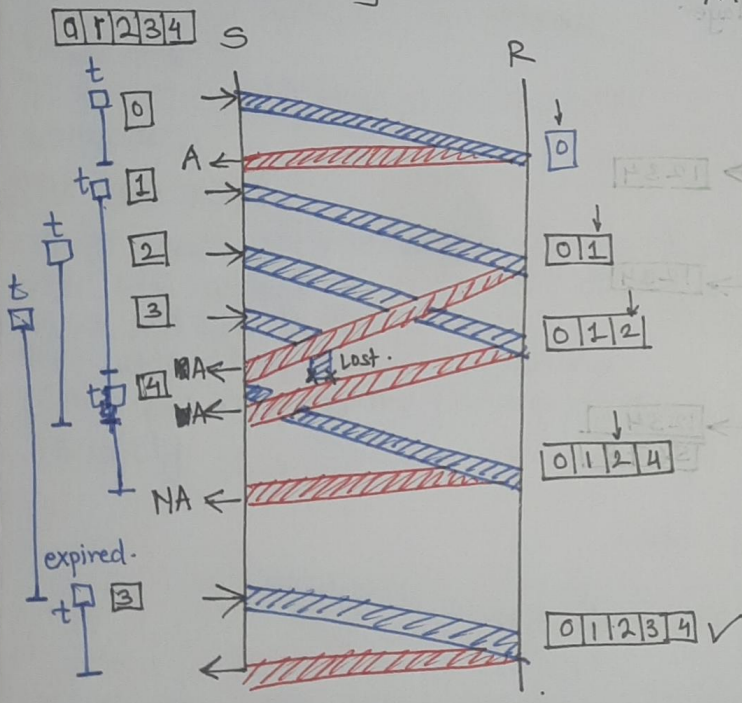


Before delivery

ack 3 : resent.



After delivery



A - Acknowledgement
NA - No Acknowledgement.

Frames delivered.

PIGGY BACKING

Used to improve efficiency of bidirectional protocol.
When frame ~~carring~~ carrying data from A to B it can also carry control info about arrived or lost frames from B and vice versa.

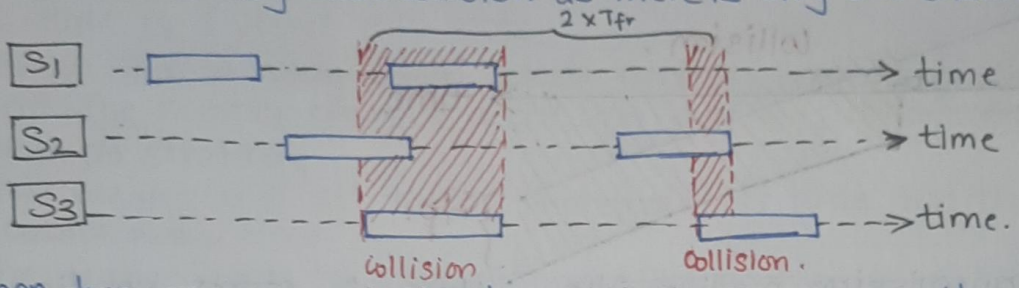
RANDOM ACCESS PROTOCOLS (Contention methods)

In these no station is superior to other thus no one is assigned control over other.

1. There is no scheduled time for station to transmit
   Transmission is random between stations
2. No rule specify which station will send next.
   Station compete with one another to access the medium.

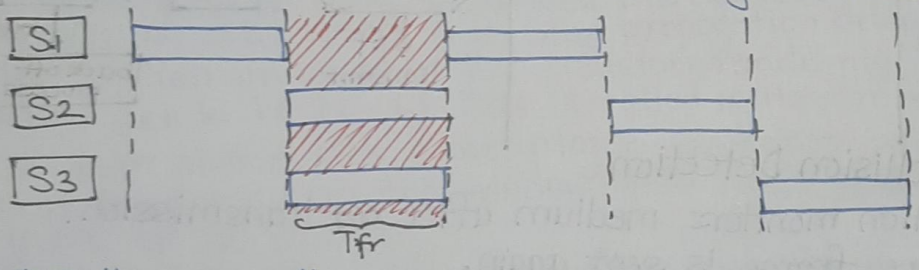
ALOHA

1. Pure ALOHA:
   Simple but elegant protocol
   each station sends when it has a frame to send
   However this may cause collision as there is only one channel to share



when two or more station transmit simultaneously it causes collision and frames are destroyed.
the station sends frame, waits for acknowledgement, waits for specific time. if no acknowledgement, assumes the frame is destroyed, waits for random amount of time and resends
Vulnerable time : $2 \times T_{fr}$

2. Slotted ALOHA:
   In this the station may only send at beginning of slot.
   Slots are division of time with Tfr (length of frame)

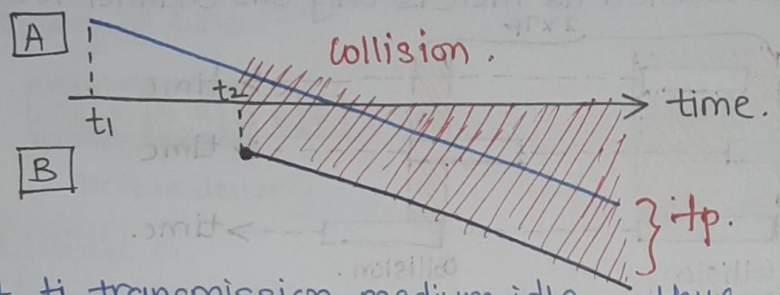


When " "
Vulnerable time : Tfr

CARRIER SENSE MULTIPLE ACCESS (CSMA)

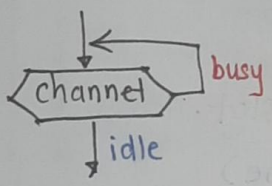
To minimize the chance of collision and increase performance.
It requires each station to first listen to the medium (or check state of medium) before sending.
Based on principle "sense before transmit" or "listen before talk"
It reduces the possibility but doesnt eliminate collisions.
For example. if A & C start sending simultaneously
• Propogation delay causes fake idle states.

Vulnerable time : T_p (propogation time).

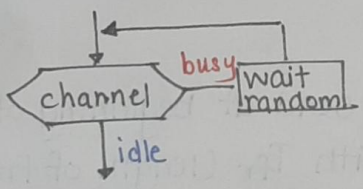


At t_1 transmission medium idle. thus A starts sending
At t_2 transmission medium idle due to propogation delay.
thus collision occurs.

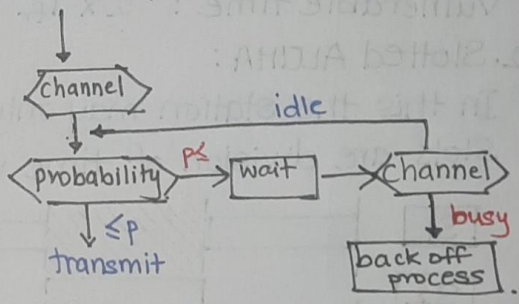
1. Persistent.



2. Non Persistent

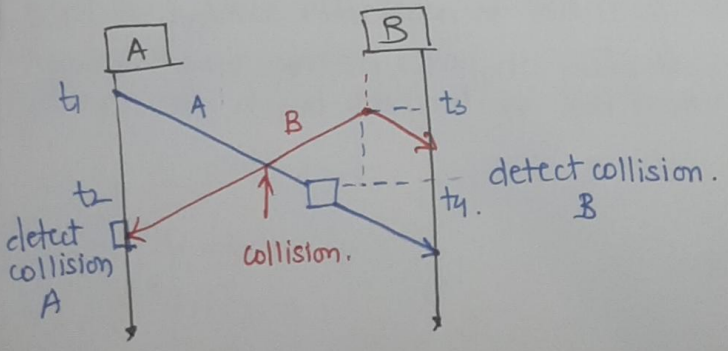


3. p - persistent



CSMA with collision Detection

In this the station monitors medium after ~~con~~ transmission.
if collision occurs frame is sent again.



CARRIER SENSE MULTIPLE ACCESS with COLLISION AVOIDANCE

we need to avoid collisions on wireless networks because they cannot be detected. CSMA/CA uses 3 strategies

- Inter frame space
- contention window
- acknowledgment

IFS:

when a channel is found idle it doesnt send immediately
It waits for a period of time called inter frame space IFS
IFS also varies thus IFS shorter has higher priority.
After waiting if channel is idle it waits for contention time.

CONTENTION WINDOW:

As time is divided into slots.
Station that is ready to send selects random number of slots to wait. The number changes according to binary exponential back off strategy.
This means it is set to one slot for first time and then doubles every time.
The station needs to sense channel after each time slot if channel is busy it doesnt restart process. It just pauses timer and resumes when channel Idle.
This gives ~~longer messages~~ priority ~~as they have~~ to longer wait time

ACKNOWLEDGEMENT

with all these precautions too there may be collision or error during transmission. Thus time-out timer and positive acknowledgements are set in place.

BINARY EXPONENTIAL BACKOFF ALGORITHM

After a collision time is divided into discrete (Tslot) whose length is $2t$, where t is max propogation delay in the network
The station involved in the collision randomly pick an integer from set k i.e {0, 1} This is called contention window
If both station pick same integer contention window size doubles
Now they pick from this window and the process repeats until there is no collision.
Thus this algorithm defines a waiting time for the station involved in collision i.e how much time should a station wait for retransmit.

ERROR DETECTION.

1. SIMPLE PARITY:

Sender 100011

check parity | 100011 | 1 | → Transmit. → compute → Even → accept / odd → reject.

odd ones. make even.

Reciever.

2. Two dimentional Parity check:

sender | 100 | 101 | 111 |

1	0	0	1
1	0	1	0
1	1	1	1
0	0	1	1

check parity → transmit → compute → Even → accept / odd → reject.

Reciever.

3 Check sum:

Sender | 100 | 101 | 111 |

compute:

```
  100
+ 101
-----
 1001
+   1
-----
  010
+ 111
-----
 1001
+   1
-----
  010
```

check sum = 101. → transmit →

Reciever | 100 | 101 | 111 | 101 |

compute:

```
  100
+ 101
-----
  001
+   1
-----
  010
+ 111
-----
  001
+   1
-----
  010
+ 101
-----
  111   =(000)'
```

thus no error.

4. Cyclic redundancy check (CRC)

polynomial x^2+1 ∴ key: 101 ($n-1 = 2$)

n.

Sender | 1001 |

```
  10010
101 | 100100
   @ 101
     00100
   @  101
      0110
    @ 101
       011
```

R bit = 11.

R bits.

Reciever | 1001 | 11 |

```
    1
101 | 1001 11
   @ 101
     00111
   @ 101
      0101
    @ 101
       000
```

∴ Error free data.

@ = EXOR operation.

ERROR CORRECTION

HAMMING CODE

can correct 1 - bit Error and detect position of error.

Sender 1011

7	6	5	4	3	2	1
1	0	1	R_4	1	R_2	R_1

R_4	R_2	R_1	
0	0	0	0
0	0	1	1
0	1	0	2
0	1	1	3
1	0	0	4
1	0	1	5
1	1	0	6
1	1	1	7

$R_1 = 1, 3, 5, 7$

$= r_1\ 1\ 1\ 1.$

$\therefore r_1 = 1$ to make even parity.

$R_2 = 2, 3, 6, 7.$

$= r_2\ 1\ 0\ 1$

$\therefore r_2 = 0$ to make even parity.

$R_4 = 4, 5, 6, 7.$

$= r_4\ 1\ 0\ 1$

$\therefore r_4 = 0$ to make even parity.

Reciever 1010101

The reciever will each check R_1, R_2 & R_4 with parity

if error 1011101.

7	6	5	4	3	2	1.
1	0	1	1	1	0	1.

$R_1 = 1, 3, 5, 7 = 1\ 1\ 1\ 1$

$1 = 1$ as $r_1 = 1$.

$R_2 = 2, 3, 6, 7 = 0\ 1\ 0\ 1$

$0 = 0$ as $r_2 = 0$.

$R_4 = 4, 5, 6, 7 = 1\ 1\ 0\ 1.$

$0 = 1$ as $r_4 = 1$.

but LHS $\neq$ RHS thus position of error = 4.