Computer Networks

→ A computer network is a collection of computers and other hardware components interconnected by communication channels that allows the sharing of resources and information

→ Internet being the most well-known example of network of networks.

LAN (Local Area Network) - network in small geographic area
MAN (Metropolitan Area Network) - network in a city
WAN (Wide Area Network) - network spread geographically.

Applications of Networks:

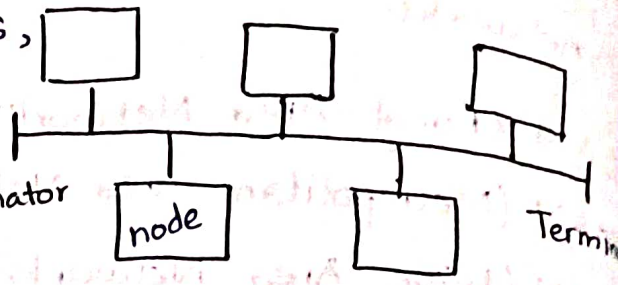
1. Resource Sharing
   → Hardware (Disks, Printers)
   → Software (Application softwares)
2. Information Sharing
   → Easy Accessibility from anywhere (les, databases)
   → Search capability (www)
3. Communication
   → e-mail
   → Broadcast
4. Remote Computing
5. Distributed Processing

Network Topology

→ The network topology denes the way in which computers, printers, and other devices are connected.

→ The network topology describes the layout of the wire and devices as well as the paths used by data transmissions.

1. Bus Topology



→ Commonly referred to as linear bus, all the devices are connected by one single cable.

→ Easy to install, easy to expand.

→ Used for small networks.

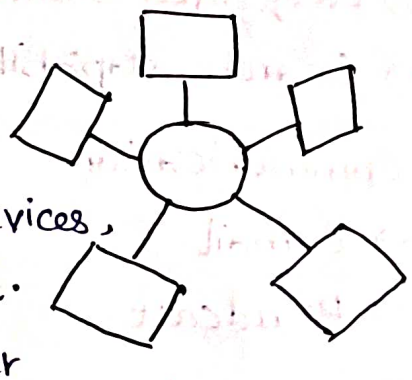
→ Slow speed as only one system can transmit at a time.

→ Faulty cable can bring down whole network.

→ As more workstations are connected, performance will become slower because of data collisions.

→ Every workstation on the network sees all the data on the network, this is a security risk.

2. Ring Topology



→ Each device is connected to two other devices, this forms a ring for the signals to travel.

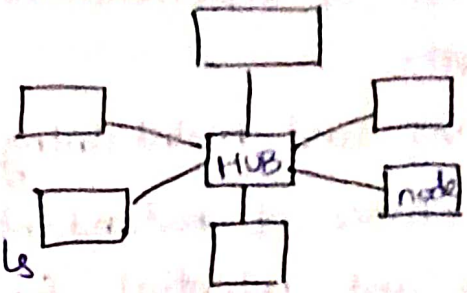
→ Token passing mechanism, performs better than bus under heavy traffic.

→ Faulty cable can bring down whole network.

→ Reduced chances of data collision, no need of server to control connectivity among the nodes.

→ In unidirectional ring, a data packet must pass through all the nodes.

3. Star Topology



→ Each device on the network has its own cable that connects to a switch or hub.

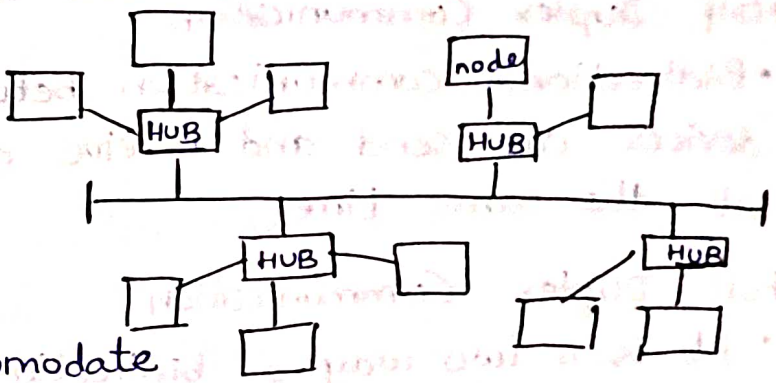
→ Very reliable if one cable or device fails then all others continue to work.

→ High performance due to no data collisions.

→ Expensive to install as this uses the most cable, Extra hardware is required (hubs/ switches) which adds to cost

→ If hub or switch fails, all the devices have no network.

4. Tree Topology



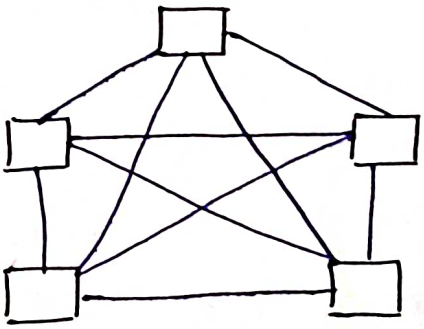
→ Combination of a star and bus topology.

→ Scalable as leaf nodes can accomodate more nodes

→ Other hierarchial networks are not affected if one of them gets damaged.

→ Easier Fault finding, huge cabling and maintainence required

5. Mesh Topology



→ Network setup where each computer and device is interconnected with one another.

→ Manages high amount of traffic, because multiple devices can transmit data simultaneously.

→ Failure of one device doesnot cause a break in network or transmission of data.

→ Adding additional devices doesnot disrupt data transmission between other devices.

→ The cost of implementation is higher, making it a less desirable option.

→ Building and maintaining the topology is difficult and time taking

→ The chance of redundant connections is high, which adds to high costs and potential for reduced efficiency.

Types of Communication

Simplex Communication

- Unidirectional communication between two devices in which one device is sender and the other is receiver.

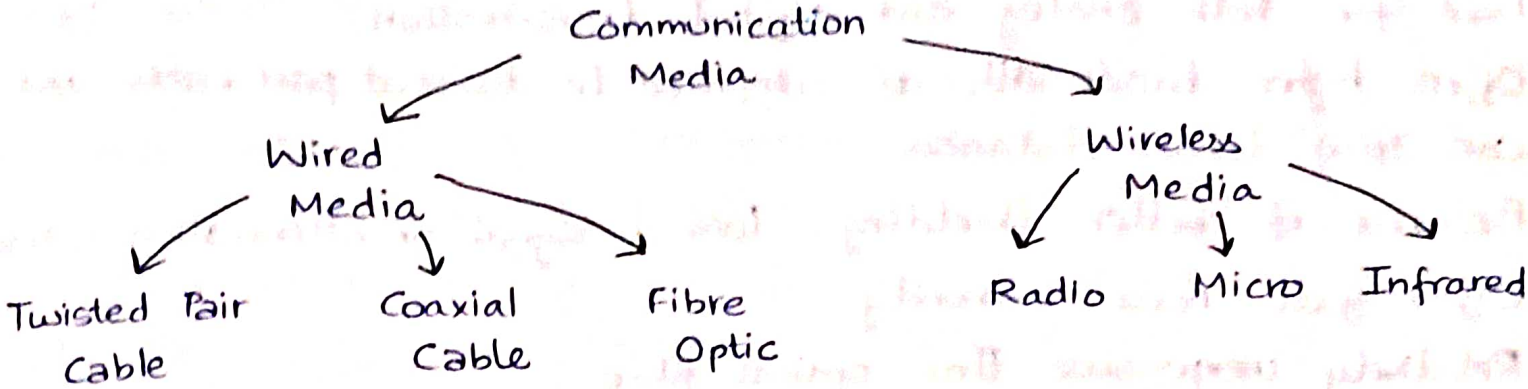
Half Duplex Communication

- Bidirectional communication between two devices in which both devices can send and receive data in both directions but not at the same time.

Full Duplex Communication

- It is a two way or bidirectional communication in which both devices can send and receive data simultaneously

Transmission Media



- Anything that can carry data between source and destination
- In guided transmission, there is physical link, wherein unguided transmission, data travels in air in EM waves using an antenna

Twisted Pair Cable

Unshielded Twisted Pair

- Least expensive
- Easy to install
- High speed capacity
- Susceptible to external interference.
- Lower capacity and performance in comparison to STP.
- Short distance transmission due to attenuation

Shielded Twisted Pair

- More expensive
- Better performance at a higher data rate
- Eliminates crosstalk
- Comparitively faster
- Comparatively difficult to install and manufacture
- Bulky

Coaxial Cable

(i) Baseband - transmits signal one at a time at very high speed

(ii) Broadband - transmits many simultaneous signals using different frequencies.

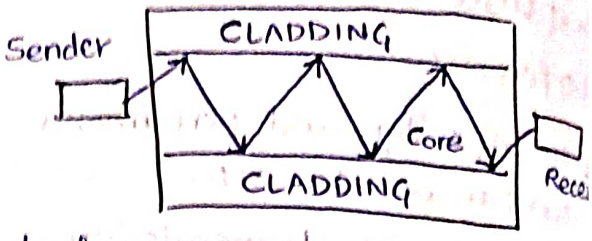
* Coaxial cables provides better immunity, frequency range than twisted pair.

Advantages of Coaxial cable

- Used for both analog and digital transmission
- Offers higher bandwidth as compared to twisted pair cable
- Can span longer distances
- Because of better shielding, loss of signal or attenuation
- Offers good noise immunity
- Relatively inexpensive than optical fibre
- Offers lower error rates than twisted pair, it is also not to bulky as twisted pair as it contains plastic jacket

Fibre Optics

- Uses concept of reflection of light through a core made up of plastic or glass
- The cable can be unidirectional, bidirectional
- Offers increased capacity, bandwidth, less signal attenuation.
- Fibre optics is light weight, resistant to corrosive materials, difficult to install, maintain and they are fragile



Radio Waves

- Waves of frequency range 3 KHz - 1 GHz
- Omnidirectional, susceptible to interference
- Radio waves of frequency 300 KHz - 30 MHz can travel long distances.
- Radio waves of frequency 3 - 300 KHz can penetrate walls
- Used in AM and FM radio, TV, cordless phones

Microwaves

→ EM waves of frequency range 1 GHz - 300 GHz
→ Unidirectional, cannot penetrate solid objects
→ Needs line-of-sight propagation, i.e, both communicating antenna must be in direction of each other
→ Used in point-to-point / unicast communications
→ provides very large information carrying capacity

Infrared waves

→ EM waves of frequency range 300 GHz - 400 THz
→ very high frequency waves, cannot penetrate solid objects
→ Used for short distance point-to-point communication

Line Coding Techniques

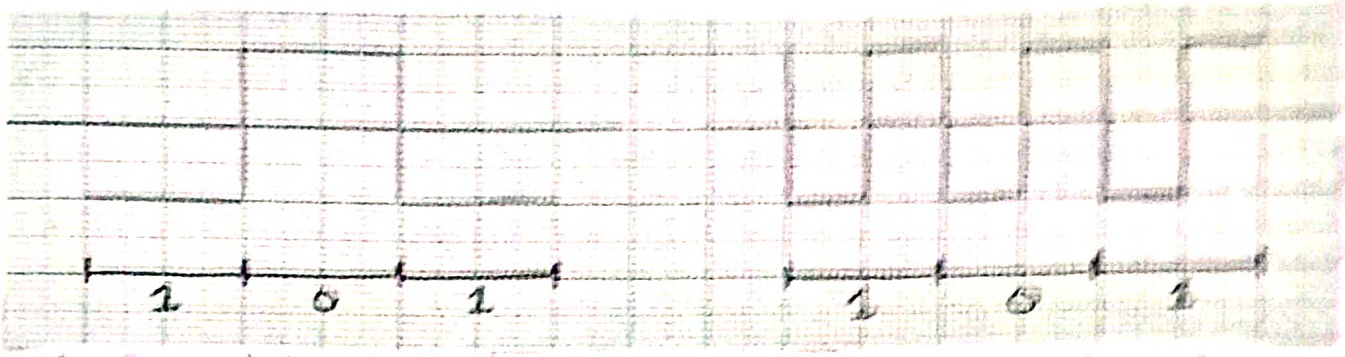
→ Converting a string of 1s and 0s (digital data) into a sequence of signals that denote digital data

→ High voltage +V could represent 1
Low voltage (0 or -V) could represent 0

→ A data symbol can be coded into signal element, one or multiple elements.

1 → +V 0 → -V
1 → +V / -V
0 → -V / +V

→ The ratio 'r' is the number of data elements carried by a signal element



(a) One data element per one signal
r = 1

(b) One data element per two signals
r = 1/2

Baseline Wandering

→ A receiver will evaluate average power of received signal, called baseline and use that to determine value of incoming data elements.

→ If the incoming signal does not vary over a long period of time, baseline will drift and cause errors in detection of incoming data elements

DC Components

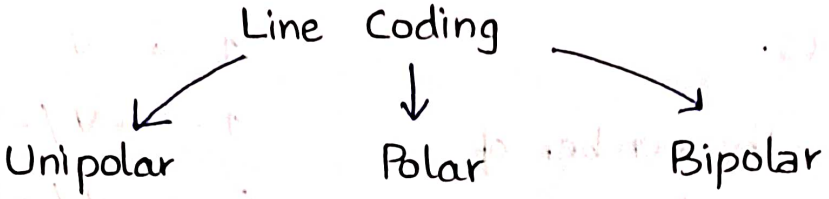
→ When voltage remains constant for long periods of time, there is an increase in low frequencies of signals. Most channels bandpass and may not support low frequencies

→ This will require removal of DC component of transmitted signals.

Self Synchronization

→ The clocks at sender and receiver must have same bit interval

→ If the receiver clock is faster or slower, it will misinterpret the incoming bit stream.



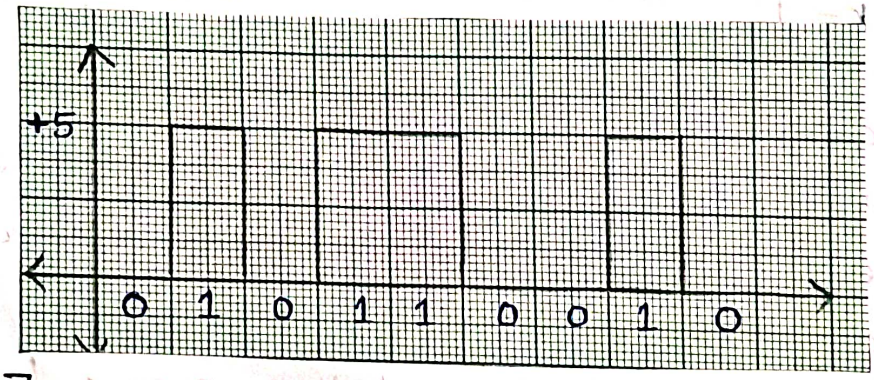
Unipolar Encoding – ON-OFF keying

Non Return to Zero

→ Logic High (1) → +5 V
Logic Low (0) → 0 V

→ Voltage level remains constant during bit interval

→ The start or end of a bit will not be indicated and it will maintain same voltage state, if values of previous bit and present bit are same.



Return to Zero

→ NRZ is less effective when sender and receiver are not synchronized. If original data contains consecutive 0s and 1s then receiver can lose its powerplace.

→ Binary data is represented by pulse having transition exactly at center of bit period rather than constant level voltage.

Advantages

→ Simple coding technique

→ Requires less bandwidth

→ Spectral line present at the symbol rate can be used as a clock (RZ).

Disadvantages

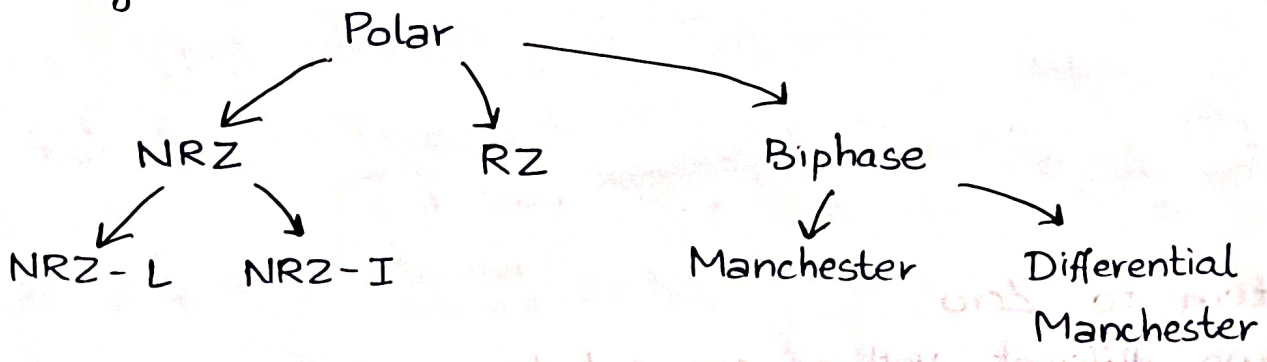
→ Normalized power is double that for polar NRZ

→ If receiver clock is not in synchronization with sender, it will misinterpret the incoming bit

→ Average amplitude of unipolar signal is non-zero.

- creates DC component
- signal cannot travel through medium which cannot handle DC component.

Polar Encoding

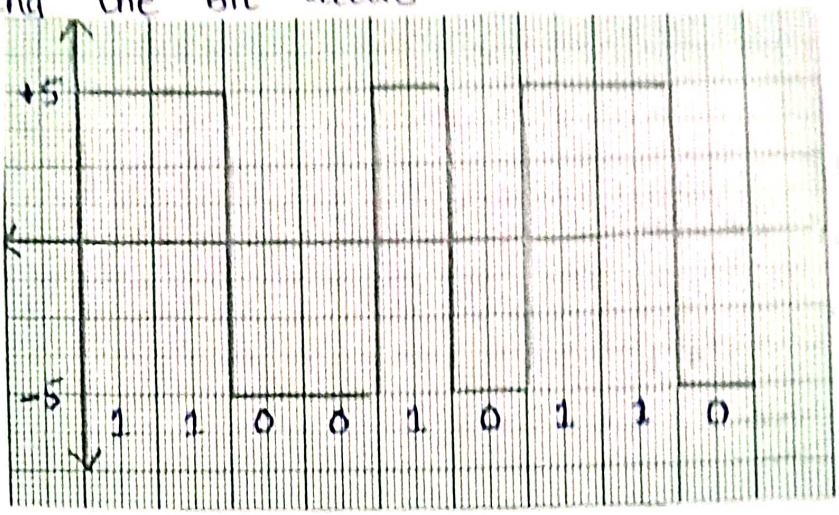


* By using two voltage levels, an average voltage level is reduced, and DC component problem of unipolar encoding scheme is alleviated.

Non Return to Zero - Level

→ Logic high (1) → +5 V
Logic low (0) → -5 V

→ If long sequence of 0s and 1s are present, then average signal is weakend. The receiver might have difficulty for regenerating the bit value

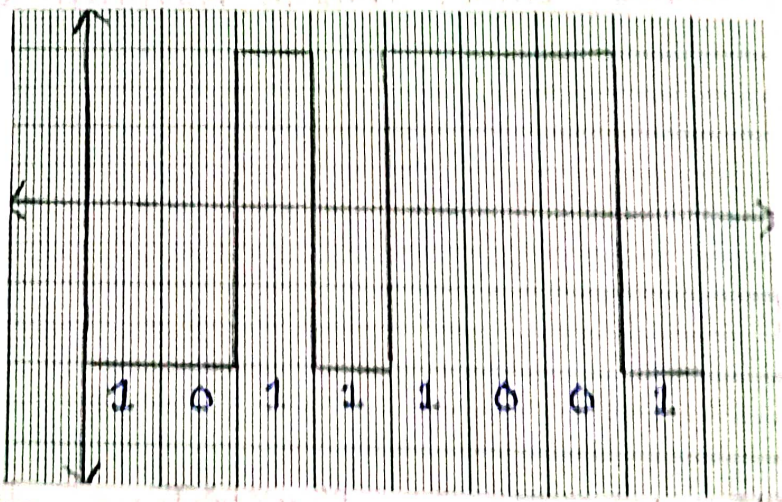


Non Return to Zero - Inverted

→ 0 bit represent no change

→ An Inversion of voltage represent 1 bit

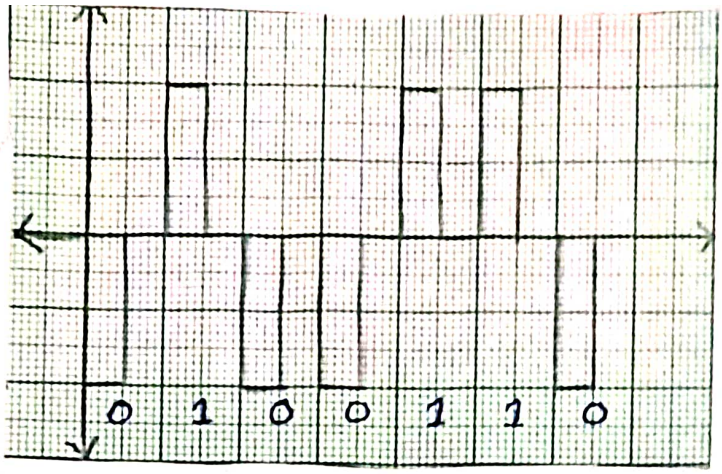
→ It is transition between +ve and -ve that represent 1 bit string of 0s still causes a problem



Return to Zero

→ Two different voltage are used to represent binary value

→ Logic High (1)
Logic Low (0)



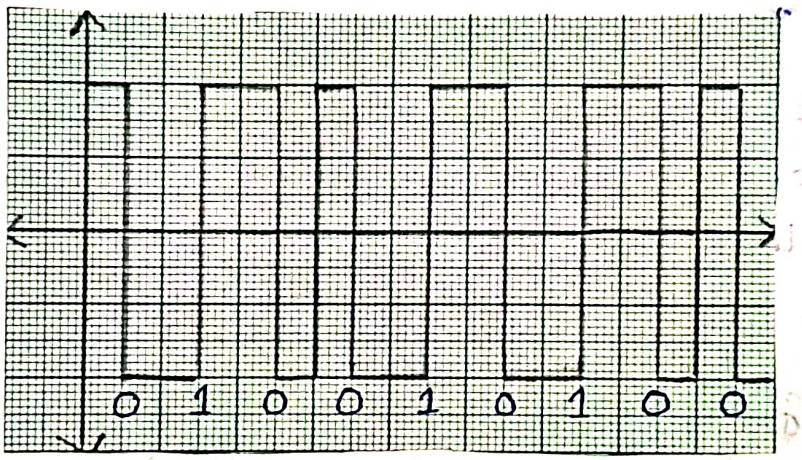
Disadvantages

→ Continuous part is non-zero at 0 Hz, causes 'signal droop'.
→ Doesnot have any error correction capability.
→ Doesnot possess any clocking component, clock can be extracted by rectifying the received signal
→ Occupies twice as much bandwidth as polar NRZ

Manchester Encoding

→ Combination of RZ and NRZ-L
→ Transition is used at middle of each bit period.
→ Transition is used as clock edge and data mapping both.

Zero - ⌉⌊
One - ⌊⌉



→ Signal synchronizes itself, minimizes error rate and optimises reliability
→ More bandwidth is consumed

Differential Manchester Encoding.

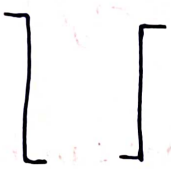
→ Combination of RZ and NRZ - I

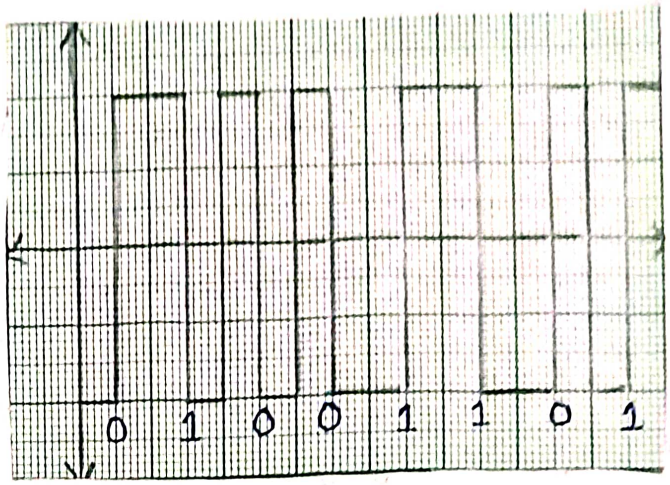
→ Bit time is divided into two halves

→ Transmits in middle by bit and change phase when different phase is encountered.

Zero -

One -





Advantages

→ Provides guaranteed midbit transitions. Hence it offers synchronizatio facility at receiver. It is called self clocking codes

→ No DC components present

→ Provides error detection by detecting absence of expected transitions.

Disadvantages

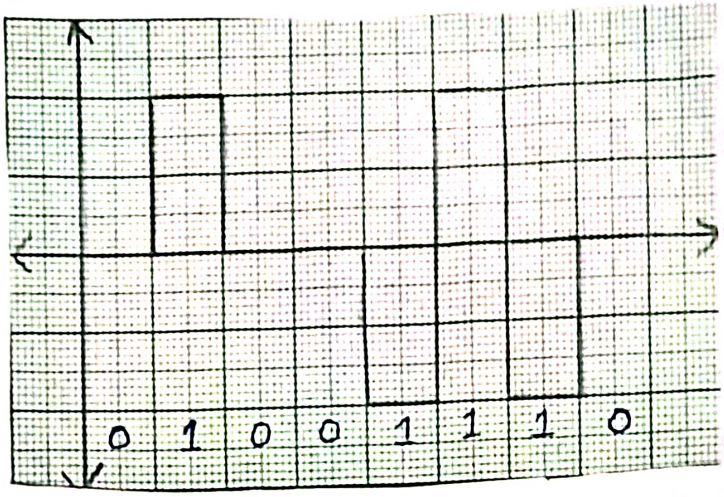
→ Used over short distances (in LANs)

→ Maps atleast one transition per bit time and possibly two bi More bandwidth required as modulation/ signal rate is two ti that of NRZ.

Bipolar Encoding

→ RZ line code, where two non-zero values are used, so tha the three values are +, −, and zero.

→ Designed to be DC balanced, the line always return to 'zer level to denote optionally a bit separations or to denote idleness of line.



→ If we have a long sequence of 1s, the voltage level alternates between positive and negative, it is not constant Thus, no DC component

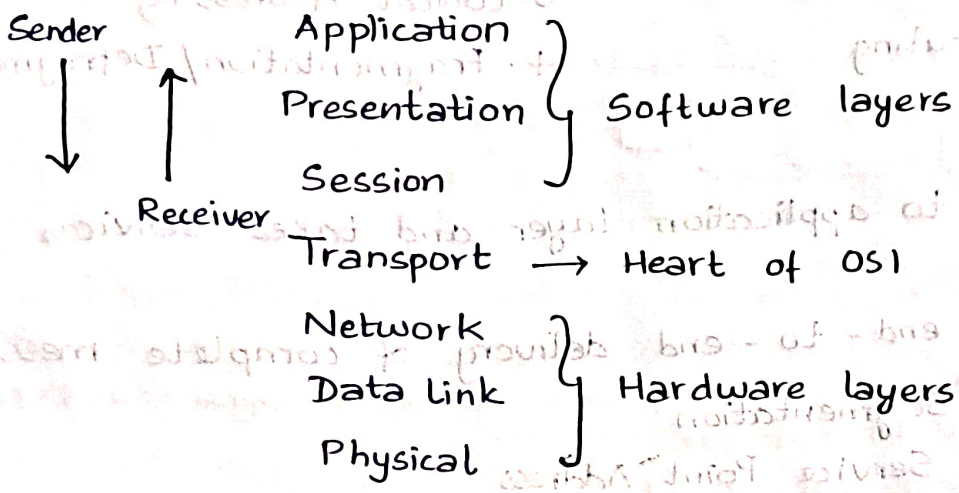
→ If we have a long sequence of 0s, voltage remains constant but its amplitude is zero, which is same as having no DC Component.

→ A sequence that creates a constant zero voltage doesnot have a DC component.

ISO - OSI Model (Open System Interconnection)

→ 7 layer architecture with each layer having specific functionality to perform.

→ All these 7 layers work collaboratively to transmit data from one device to another



Physical Layer

→ responsible for actual physical connection between devices.

→ contains information in the form of bits

Functionalities :
1. Bit synchronization
2. Bit rate control
3. Physical topologies
4. Transmission mode / medium
5. Communication mechanism

Data Link Layer

→ responsible for node-to-node delivery of the message.

→ transmits packets to the host using its MAC address

→ data link layer is divided into logical link control (LLC) and media access control (MAC)

Functionalities :
1. Framing
2. Physical addressing
3. Error control
4. Flow control
5. Access control

Network Layer

→ works for the transmission of data from one host to the other located in different networks.

→ take cares of packet routing, i.e, selection of shortest path from number of routes available.

Functionalities : 1. Packet
2. Routing
3. Logical Addressing
4. Fragmentation / Defragmentation

Transport Layer

→ provides services to application layer and takes services from network layer.

→ responsible for end - to - end delivery of complete message

Functionalities : 1. Segmentation
2. Service Point Address
3. Multiplexing / Demultiplexing
4. Flow control
5. Error control

Session Layer

Functionalities : 1. Message
2. Dialog control - allows system to enter comm.
3. Synchronization

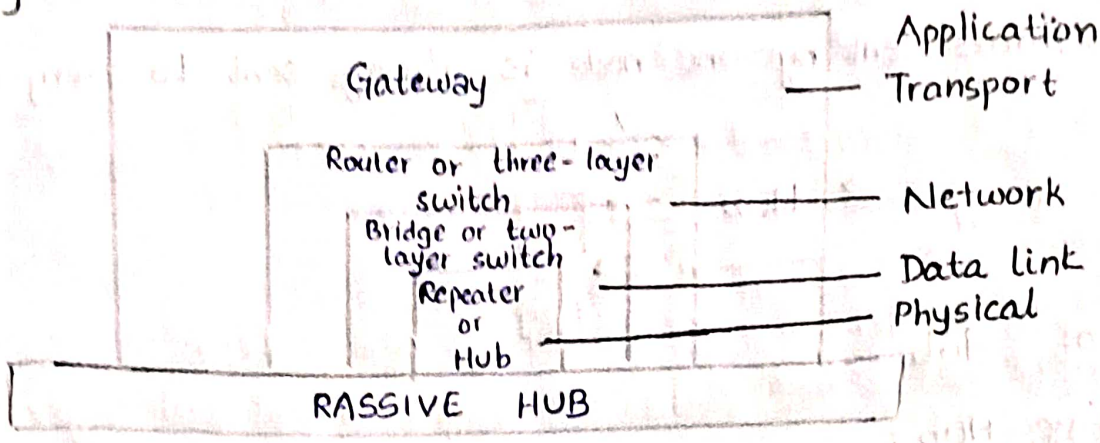
Presentation Layer

Functionalities : 1. Translation
2. Encryption / Decryption
3. Data compression
4. Message

Application Layer

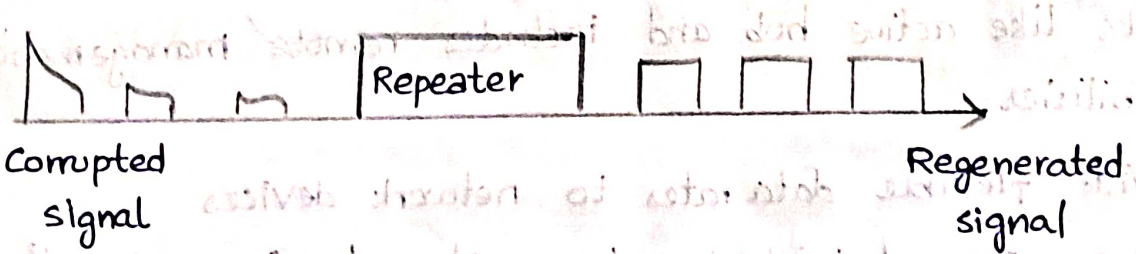
Functionalities : 1. End user applications (gmail, youtube)
2. Network Virtual Unit terminal

Networking Devices

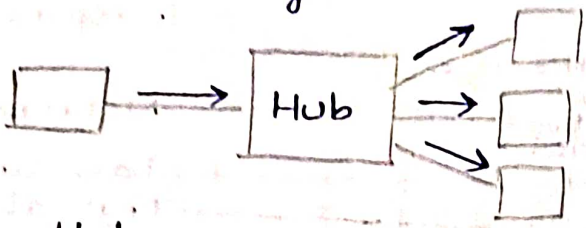


Repeater

→ operates at physical layer
→ 2- port device
→ regenerates the signal over same network, before the signal becomes too weak or corrupted so as to extend length to which the signal can be transmitted over same network.
→ do not amplify the signal.
→ when signal becomes weak, they copy the signal bit-by-bit and regenerate it at the original strength.
→ connects segments of a LAN.
→ forwards every frame, it has no filtering capacity.



→ Multiport repeater
→ connects multiple wires coming from different branches
→ Hubs cannot filter data, so packets are sent to all connecting devices
→ A frame sent by one node is always sent to every other node



Types of Hub

1. Active Hub:
   → have their own power supply and can clean, boost and relay the signal along with network
   → serves as both repeater and wiring center
   → used to extend maximum distance between nodes
2. Passive Hub:
   → Hubs that collect wiring from nodes and power supply from active hubs.
   → relay signals onto network without cleaning and boosting
   → cannot be used to extend distance between nodes
3. Intelligent Hub:
   → works like active hub and includes remote management capabilities.
   → provides flexible data rates to network devices
   → enables an administrator to monitor traffic passing through hub and to configure each port in the hub

Bridge

- → operates at data link layer
- → repeater with filtering content by reading MAC addresses of source and destination
- → used for interconnecting two LANs working on same protocol
- → 2-port device
- → has a table used in filtering decisions
- → doesnot change MAC physical addresses in a frame

Types of Bridges

1. Transparent bridges
   - → stations are completely unaware of bridge's existence
   - → makes use of bridge forwading and bridge learning
2. Source Routing bridges
   - → routing operation is performed by source station and the frame specifies which route to follow
   - → host can discover frame by sending a special frame called discovery frame, which spreads through entire network

Switch

- → operates at data link layer
- → multiport bridge with a buffer with boosted efficiency
- → can perform error checking before forwarding data, forwards good packets selectively to correct port only
- → divides collision domain of hosts, but broadcast domain remains same.
- → LEARNs location of each node by looking at source address of each incoming frame and builds a forwading table
- → FORWARDs frame to port where destination is
  - (i) reduces collision domain
  - (ii) more efficient use of wire
  - (iii) dont waste time checking frames

Routers

→ switch that routes packets based on their IP Addresses

→ operates at Network layer

→ connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing data packets

→ divide broadcast domain of hosts connected through it.

Brouters

→ Bridging routers - combines bridge and routers

→ operates at either data link layer or network layer

→ working as a router, it is capable of routing packets across networks, and working as bridge, it is capable of filtering traffic

Gateway

→ passage to connect two networks together that may work upon different networking models

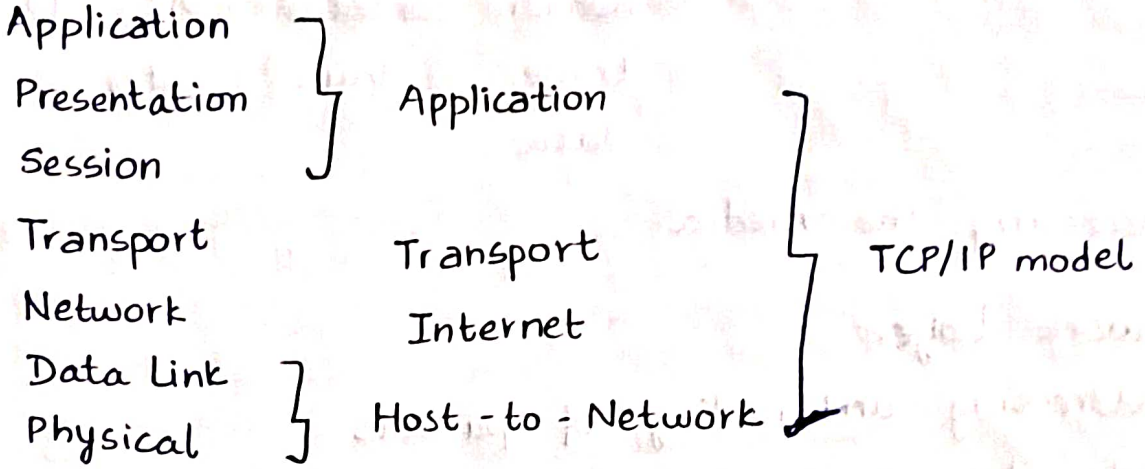
→ messenger agents that take data from one system, interpret it and transfer it to another system.

→ also called protocol networks and can operate at any Network layer.

→ generally more complex than switches or routers.

TCP / IP

Transmission Control Protocol / Internet Protocol



TCP/IP Layers:

Application		Data / HTTP
Transport		Data / HTTP / TCP
Internet		Data / HTTP / TCP / IP
Network Access	Data Link / Physica layer	Data / HTTP / TCP / IP / Ether

Physical Layer:

→ transmitting bits over a channel
→ deals with electrical and procedural interface to transmission

Data Link Layer:

→ Grouping of bits into frames
→ Dealing with transmission errors
→ Regulating flow of frames
→ Regulating multiple access to medium

(i) Logical Link Layer

→ Framing (start and stop)
→ Flow control – restricts amount of data that sender send
→ Error control – error detection and retransmission

→ Medium Access Control Layer

→ Data Encapsulation - adds header and trailer to IP packet
- header contains MAC address
- trailer contains 4 bytes of error checking data

→ Accessing the media

Network Layer

→ Addressing and routing of packets

→ Path determination

Transport Layer

→ end-to-end connection characteristics

→ retransmissions, sequencing and congestion control

→ TCP - reliable connections
UDP - fast streaming

→ assign port numbers to applications to deliver data

TCP	UDP
* Slow compared to UDP	* Fast compared to TCP
* Reliable network	* Not Reliable
* Less overhead	* More overhead
* Connection establishment	* No connection establishment
* Acknowledgement	* No acknowledgement
* Resend Lost data	* Streaming

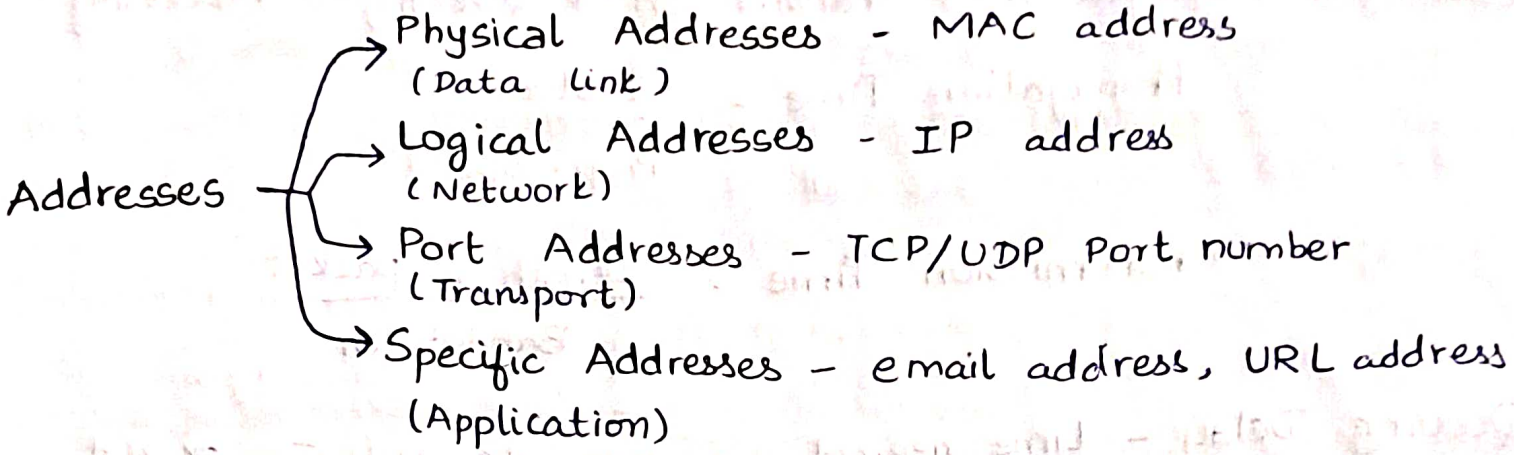
Data Transmission via TCP

Connection Establishment
↓
Data Transfer → Detection of lost packet → Handling order
↓ ↓
Connection Termination Discarding duplicate

Application Layer

→ Deals with providing services to users and application developers

→ Protocols are building blocks of network architecture



* The physical address will change from hop-to-hop, but the logical addresses remain the same. Also, the port addresses remains same.

Performance Metrics

1. Bandwidth
   - measures network performance

* bandwidth in hertz - range of frequencies a channel can pass
* bandwidth in bits per second
  - number of bits per second that a channel can transmit

2. Throughput
   - measure of how fast we can actually send data
   - bandwidth is a potential measurement of a link, while throughput is actual measurement

3. Latency

- denes how long it takes for an entire message to complete arrive at destination from the time the first bit is sent

Latency = Propagation + Transmission + Queuing + Processing

$$\text{Propagation Time} = \frac{\text{Distance}}{\text{Prop. Speed}}$$

$$\text{Transmission Time} = \frac{\text{Length of packet}}{\text{Bandwidth}}$$

Queuing Delay - time needed for each intermediate or end device to hold message before it can be processed.

Processing Delay - time routers take to process packet

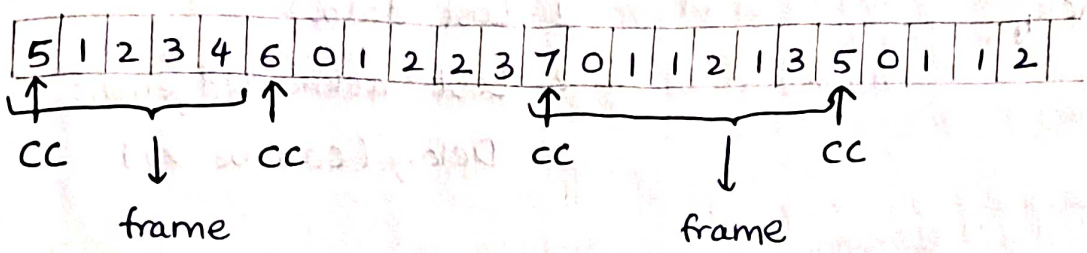
Framing

. – break stream of bits into discrete frames

Methods:

1. Use of time gap – unacceptable, too risky
2. Fixed size framing – character count
3. Variable size framing – character stuffing
   – bit stuffing

Character Count



→ rarely used

→ frame contains length as first bit

→ out of synchronisation if error

Character Stuffing

→ frame starts with special sequence of chars

→ additional DLE before each DLE (Data Link Escape)

DLE	STX	A	B	DLE	DLE	C	DLE	ETX

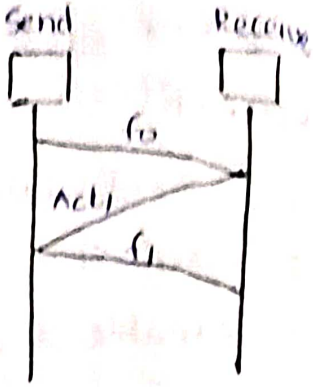
Bit Stuffing

→ special bit pattern at start / end of frame

→ add '0' after 5 consecutive '1'

Flow Control Mechanisms

1. STOP & WAIT



Sender : 1. One data packet can be sent at a time
2. Once acknowledgement is received, then next frame is sent

Receiver : 1. Send acknowledgement after receiving and consuming packet

$F_1 \longrightarrow Ack_2$

$F_{n-1} \longrightarrow Ack_n$

Drawbacks :
1. Lost data
2. Lost acknowledgement
3. Delay (can be ∞)

2. STOP & WAIT AUTOMATIC REPEAT REQUEST (ARQ)

→ We need sequence number for both frame and acknowledgement, else we wont be able to distinguish frame or acknowledgement at sender or receiver

No. of sequence numbers required = 2 {0, 1}

Total Time = T_t (frame) + T_p (frame) + T_q (ack) + T_p (ack) + $T_{process}$ (Ack) + T_t (ack)

$\approx T_t(f) + T_{propag}(f) + 0 + 0 + T_{prop}(Ack) + 0$

$\approx T_t(f) + T_{propag}(f) + T_{propa}(ack)$

$\approx T_t + 2T_{propagation}$

Total time = $T_t + 2T_p$

Efficiency = $\frac{T_t}{T_t + 2T_p} = \frac{1}{1+2a}$ $\quad a = \frac{T_p}{T_t}$

Throughput = $\eta \times$ Bandwidth = $\frac{L}{2 \times d/v}$

3. SLIDING WINDOW - GO BACK 'N'

Window size : Sender - N
Receiver - 1

Cumulative Ack. = 1 Ack for all N frames

→ A window size of N is transmitted over the channel one by one. If a packet is lost, then window starting from that packet will be resent.

→ If receiver is waiting for packet 1 and receives packet 2, then it discards packet 2 until packet 1 is received.

$$\text{Round Trip Time (RTT)} = 2T_p$$

$$\text{Timeout Timer} = 2(\text{RTT})$$

$$\text{Min. no. of sequence numbers} = N + 1$$

$$\text{No. of bits} = \lceil \log_2(N+1) \rceil$$

$$\text{No. of bits that represent sequence numbers} = 2^N - 1$$

→ Cumulative & Independent acknowledgement
- ↳ Reduced Traffic
- ↳ Lesser reliability

4. SLIDING WINDOW - SELECTIVE REPEAT

Window size : Sender - N
Receiver - N

Independent Acknowledgement

→ Same as Go back 'N'

→ When packet is lost, only that packet is resent. This protocol accepts out of order packets

→ Retransmissions reduced

→ Sorting required at receiver's end

$$\text{Min. No. of sequence numbers} = 2N$$

$$\text{No. of bits} = \lceil \log_2(2N) \rceil$$

$$\eta(\text{Go back 'N'}) = \eta(\text{Selective Repeat}) = N\left(\frac{T_t}{T_t + 2T_p}\right)$$

Access Control Mechanisms

→ prevent collision or deal with it and ensures smooth flow of traffic on network

→ implemented at data link layer

Media Access Control

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

Random Access Mechanism

→ all stations have equal priority to send data over channel

→ one or more stations cannot depend on another station nor any station control another station.

Controlled Access Mechanism

→ method of reducing data frame collision on shared channel.

→ each station interacts and decides to send a data frame by particular station approved by all other stations

Channelisation Access Mechanism

→ allows total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distances and codes.

→ can access all stations at same time to send data frames to channel.

ALOHA

→ designed for wireless LAN but can also be used in a shared medium to transmit data

→ any station can transmit data across a network simultaneously

→ doesnot require any carrier sensing

→ collision and data frames may be lost during transmission

→ Acknowledgement of frames exists. No collision detection

→ requires retransmission of data after some random amount of time

Pure ALOHA

$\eta = 18.4\%$

→ send data whenever it is available

→ when each station transmits data to a channel without checking whether channel is idle or not, collisions may occur.

→ when data is transmitted, pure Aloha waits for acknowledgement. If not received within specified time, the station waits for random amount of time, called backoff time T_b

→ retransmits frame until all the data are successfully transmitted to receiver

Slotted ALOHA

$\eta = 36.8\%$

→ shared channel is divided into fixed time intervals, SLOTS.

→ if a station wants to send frame to shared channel, the frame can only be sent at beginning of slot and only one frame is allowed to be sent to each slot. If not, the station will have to wait until the beginning of slot for the next time

Sense Multiple Access (CSMA)

→ Sense traffic on channel before transmitting data
→ If idle, station can send data from to the channel. Otherwise, it has to wait until channel becomes idle
→ reduces chances of collision on transmission medium

1 - persistant :

→ first sense the channel and if channel is idle, immediately send the data
→ else must wait and keep track of status of channel to be idle and broadcast frame unconditionally as soon as the channel is idle

Non - persistant :

→ If channel is idle, immediately send the data
→ else must wait for a random time, and when channel is found to be idle, it transmits the frame

P- persistant

→ If channel is idle, sends a frame with p - probability
→ else waits for random time and resumes frame with next time slot.

CSMA / Collision Detection

→ sense the channel, if idle, it transmits a frame to check whether transmission was successful.
→ if succesful, the station sends another frame
→ if any collision is detected, the station sends a jam / stop signal to shared channel to terminate data transmission
→ It waits for random time before sending a frame to channel

$T_t \geq T_p$

$T_t \geq 2T_p$

$L \geq 2\frac{d}{v}B$

$T_{propagation} = X + T_p + T_p$

$= 2T_p + X$

Efficiencies :

1. Pure Aloha

T_f → frame time (processing transmission)

S → average number of successful transmissions

G → average number of total transmissions per T_f

D → average delay between packets

$$S = G \times (\text{probability of good transmissions})$$

Vulnerable time $= 2T_f$

λ → arrival time

$$P_k(t) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$$

for slotted aloha $t = T_f$

$t = 2T_{fr}$, $k = 0$

$$\Rightarrow P_0(2T_{fr}) = \frac{(\lambda 2T_f)^0 e^{-\lambda 2T_f}}{0!}$$

$$P_0(2T_{fr}) = e^{-2G}$$

$$S = G e^{-2G} \quad \text{where } \lambda = \frac{G}{T_f}$$

2. CSMA/CD

$$\eta = \frac{\text{useful time}}{\text{total time}}$$

Useful time $= T_t$

Wasted time $= 2T_p$

. Total time = Wasted time + Propagation time

$$= 2cT_p + T_p \qquad (c \rightarrow \#\text{ collisions})$$

$$\eta = \frac{T_t}{2cT_p + T_p + T_t}$$

Average no. of collisions before successful transmissions $= e$ //

Error Detection Techniques

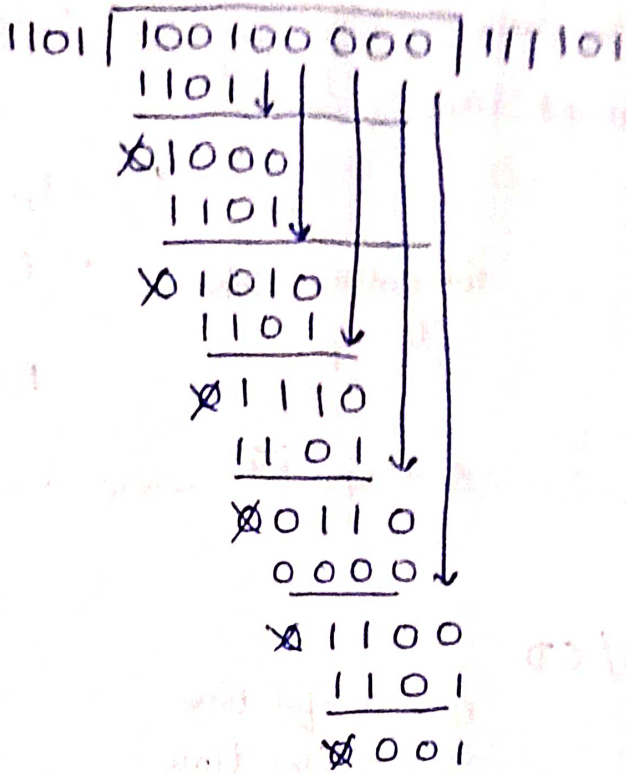
1. Cyclic Redundancy Check (CRC)

Generator Polynomial $x^3 + x^2 + 1 \Rightarrow 1+1+0+1 \Rightarrow 1101$

1. find length of polynomial L
2. append 'L-1' bits to message
3. perform binary divison (bitwise EXOR operations)
4. add remainder bits to original message and send

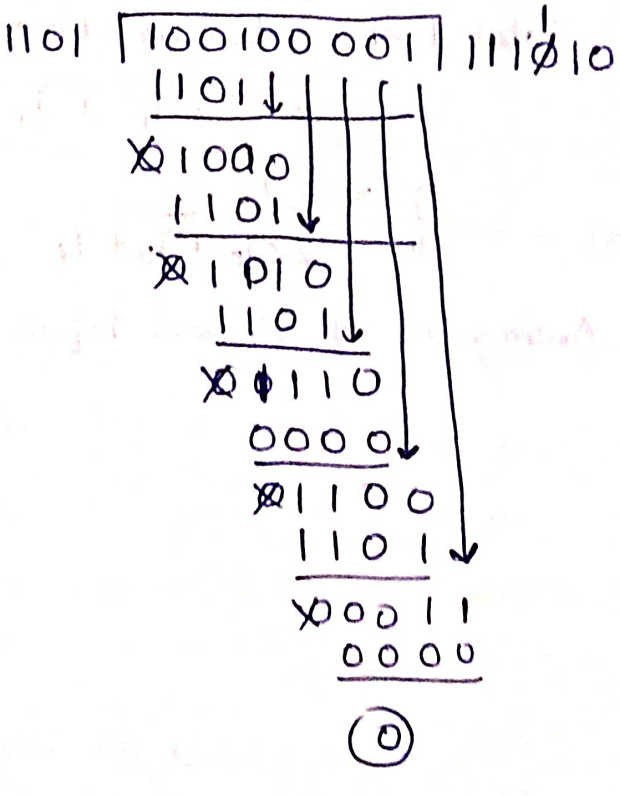
Message = 100100

Polynomial = 1101



Sent message = 100100 001

Checking Receiver's Side



Remainder = 0

Correctly sent

(0)

2 Checksum

1 Segment the message into 2^n bits

2. Perform addition

3 If carry bit is obtained, add it to LSB

4 Perform 1s complement to sum and add (append) it to last

Message : 1010|0110|1010|0100

```
  1010          0001
  0110          1010
 ------        ------
 (1)0000        1011
    ->1
 ------
  0001
  0110
 ------
  0111
  1010
 ------
  0001
```

1s complement ≈ 0100

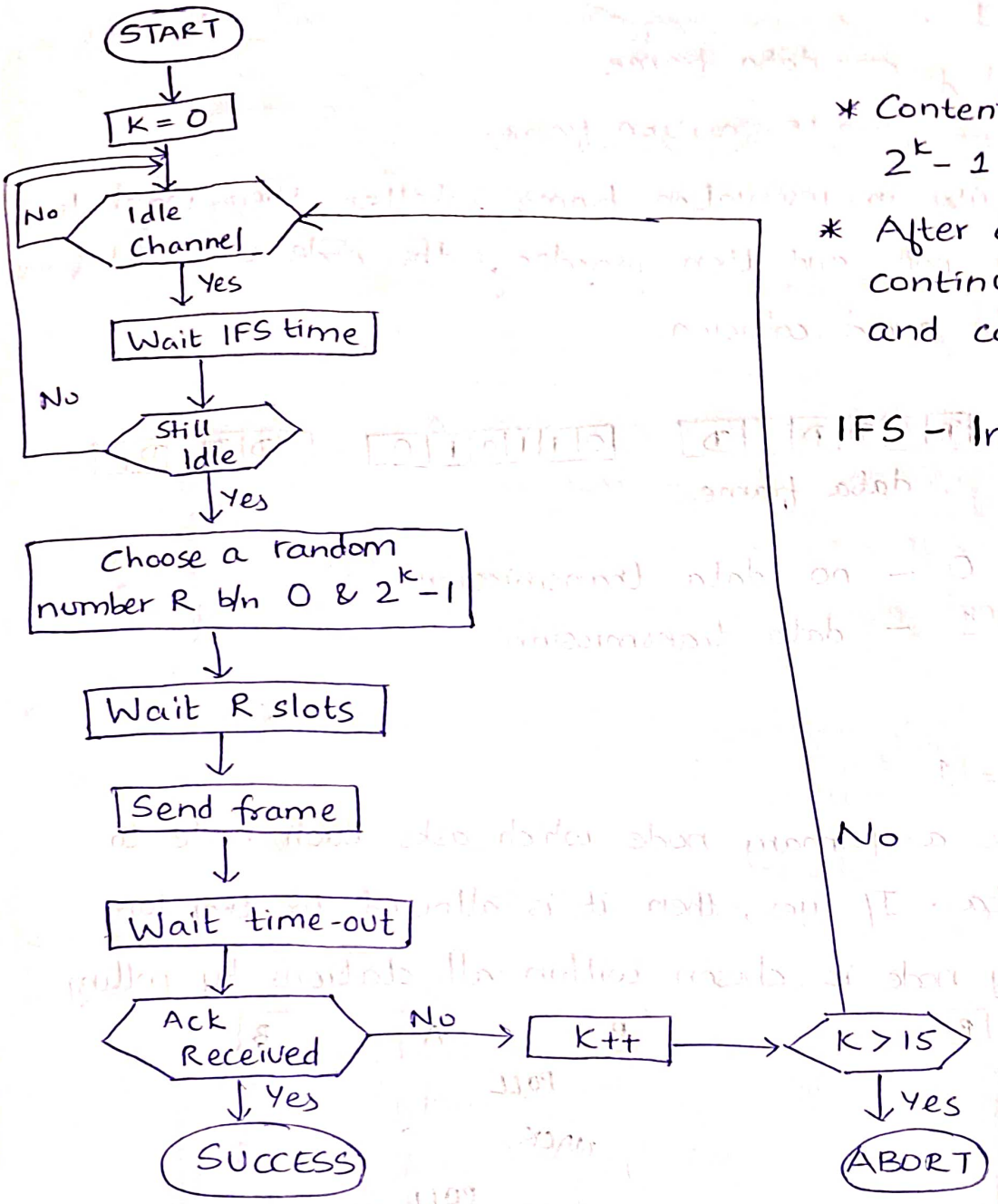
Checking receiver's side

```
  1010
  0110
 ------
  0000
     1
 ------
  0001
  1010
 ------
  1011
  0100
 ------
  1111
```

1s complement ≈ 0000

Correctly sent

CSMA / Collision Avoidance



* Contention window size is $2^k - 1$
* After each slot, if idle, continue, if busy, halt and continue when idle.

IFS - Inter Frame Space

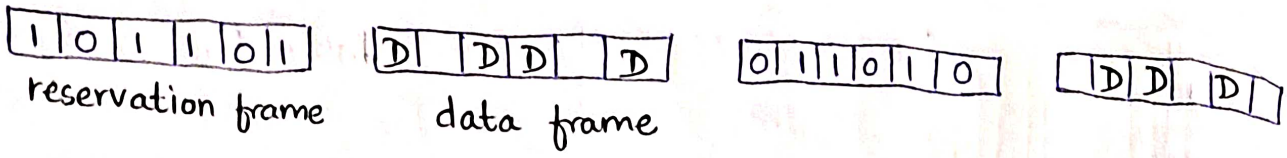
* CSMA/CA is used in wireless LAN, wifi and IEEE 802.11
* In CSMA/CA, the IFS can be used to define priority of a station or frame
* If the station finds the channel busy, it doesnot restart timer of contention window, it stops timer and restarts it when the channel becomes idle

Reservation

→ packet size = 1

→ 2 frames needed ⟶ data frame
↳ reservation frame.

* Nodes give their priority in reservation frame whether they want to use data frame or not and then inorder, the node uses dataframe to transfer data to avoid collision.



reservation frame data frame

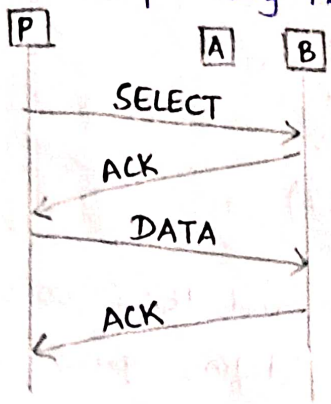
Bit 0 – no data transmission
1 – data transmission.

Polling

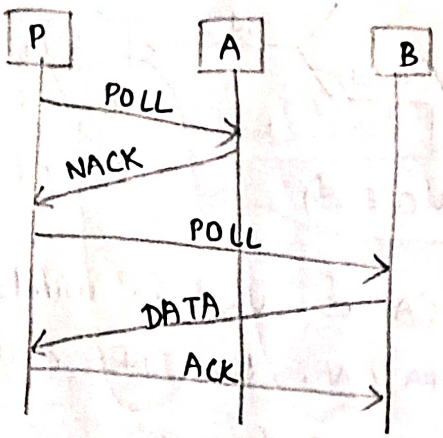
→ packet size = 1

→ there will be a primary node which asks each node to transfer data. If yes, then it is allowed to transfer.

→ the primary node is chosen within all stations by polling



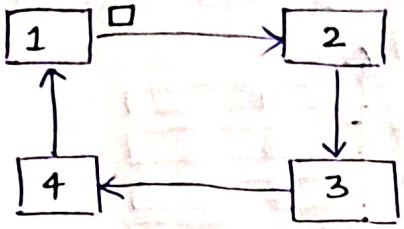
Select Function



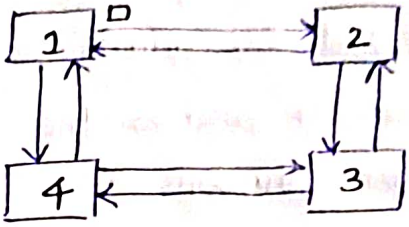
Poll Function

$$\eta = \frac{T_t}{T_{poll} + T_t + T_p} \approx \frac{T_t}{T_{poll} + T_t}$$

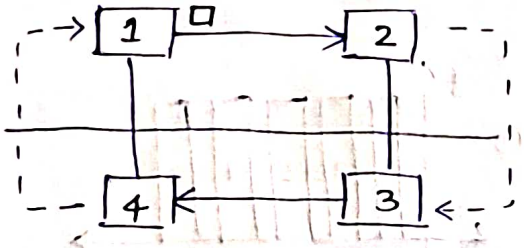
Token Passing



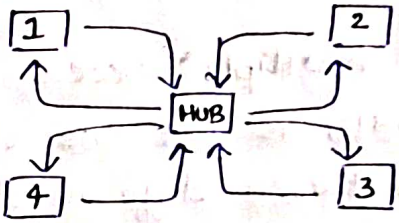
Physical Ring



Dual Ring



Bus Ring



Star Ring

* Node having token should only transfer data. If a node wants to transfer data, then it should capture token.

$$\text{Ring Latency} = T_p + (N * b)$$

$$= \frac{d}{V} + \frac{Nb}{BW} \quad \text{(sec)}$$

$$= \frac{d}{V} \times BW + Nb \quad \text{(bits)}$$

N - number of stations
b - number of bits

Delay Total Handling, $THT = T_t + RL = T_t + T_p$

Early Total Handling, $THT = T_t$

$$\text{Total Cycle Time} = \frac{d}{V} + (N * THT)$$

$$THT = T_t + T_p + (N * b)$$

$$\text{Total Cycle Time} = T_t + T_p$$

both mean the same

$$\eta = \frac{NT_t}{T_p + N \times (T_t + T_p)}$$

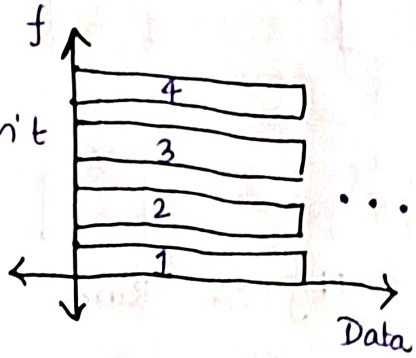
$$\eta = \frac{1}{1 + \left(\frac{N+1}{N}\right)a}$$

For ∞ active hosts,

$$\eta = \frac{1}{1+a}$$

Frequency Divison Mulliple Access (FDMA)

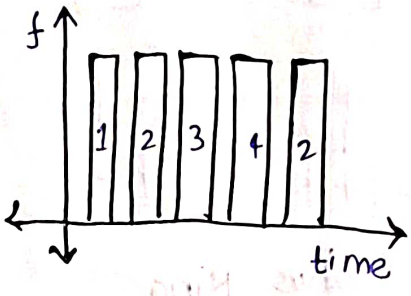
* The available bandwidth of common channel is divided into bands that are separated by guard bands
* The guard bandwidth ensures the data doesn't interfere with other divisons
* Data is uniformly sent but data with higher bandwidth cannot be sent.



$$B_t = NB_c + 2B_{guard}$$

Time Divison Multiple Access (TDMA)

* The bandwidth is just one channel that is timeshared between different stations.
* Data can be sent out at high frequency, but data cannot be sent continually.



Coded Divison Multiple Access (CDMA)

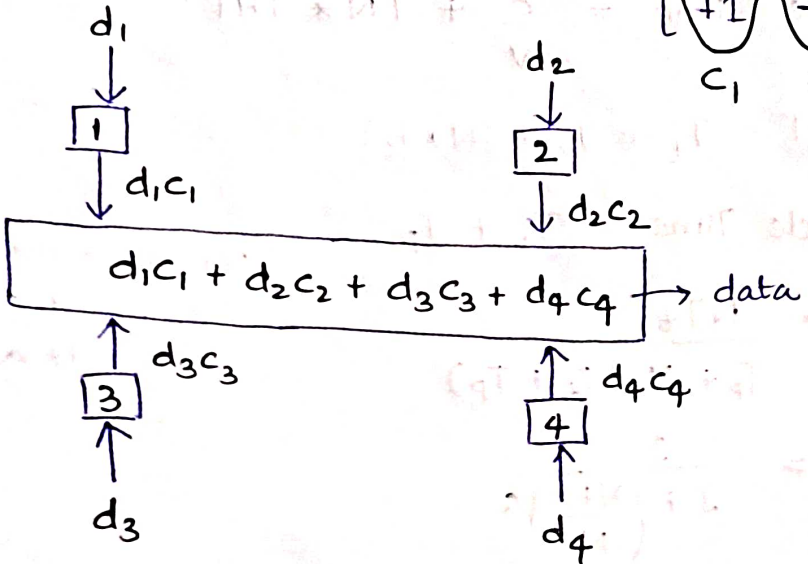
Walsh Tables

$$W_1 = [+1] \qquad W_{2N} = \begin{bmatrix} W_N & W_N \\ W_N & \overline{W_N} \end{bmatrix}$$

$$W_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$$

$$W_4 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$$

C_1 C_2 C_3 C_4



* For station of 2^N elements, generate walsh table and get the codes for each element column-wise

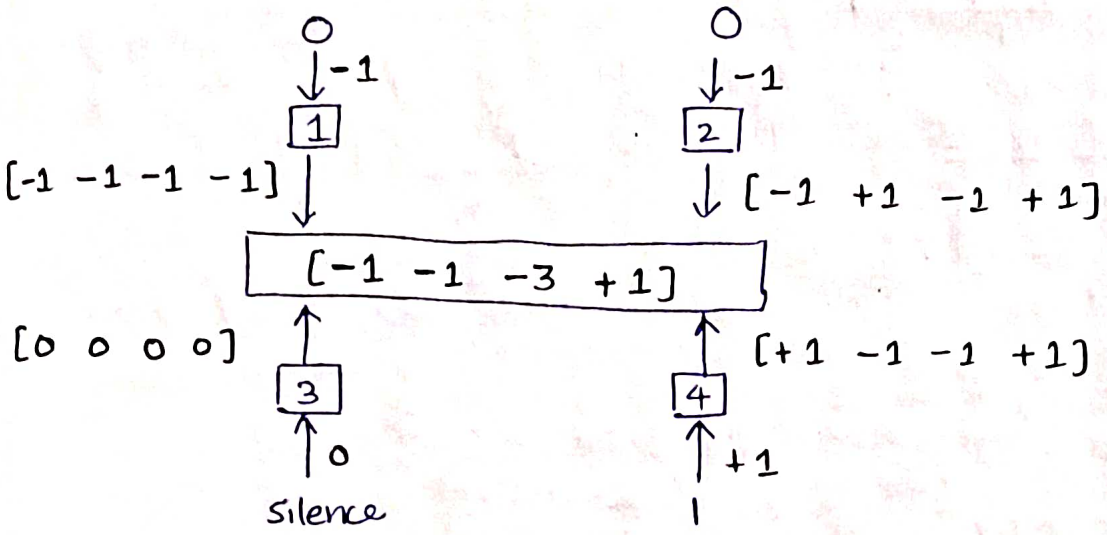
* For a station of 4 elements, the codes are as follows

$$C_1 = [+1 \quad +1 \quad +1 \quad +1]$$
$$C_2 = [+1 \quad -1 \quad +1 \quad -1]$$
$$C_3 = [+1 \quad +1 \quad -1 \quad -1]$$
$$C_4 = [+1 \quad -1 \quad -1 \quad +1]$$

* Data Bit 0 $\longrightarrow$ -1

1 $\longrightarrow$ +1

Silence $\longrightarrow$ 0

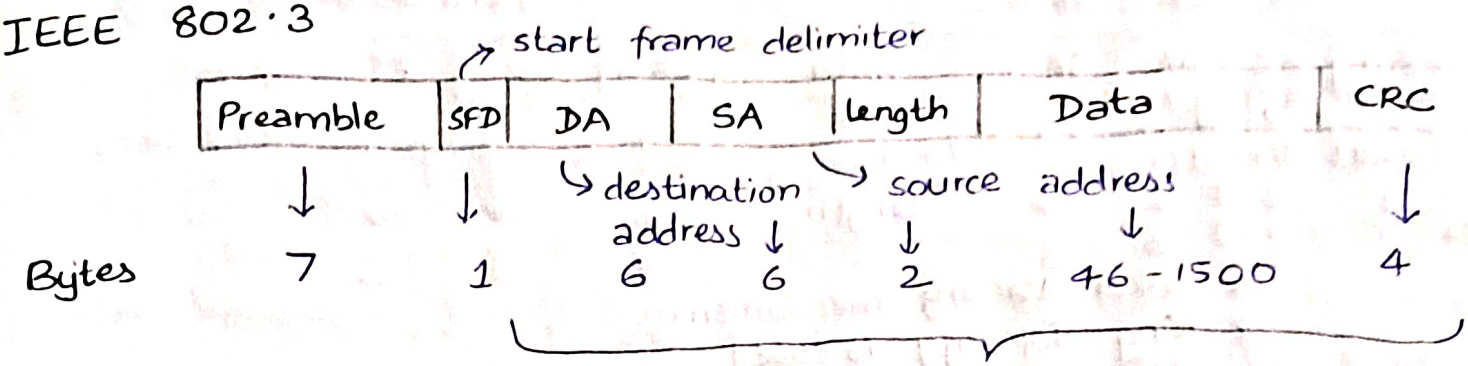


Token Passing, Early token, $\eta = \frac{1}{1 + \frac{a}{N}}$

Delay token, $\eta = \frac{1}{1 + \left(1 + \frac{a}{N}\right)}$

Ethernet Frame Formats

IEEE 802.3



* CSMA/CD is used
* Bus Topology is used
* Manchester Encoding is used
* Minimum size of frame = 6 + 6 + 2 + 46 + 4 = 64 bytes
  Maximum size of frame = 1518 bytes
* During transmission, destination address is reversed in original frame

DA → FF : FF : FF : FF : FF : FF → Broadcast

DA → 6A : 2B : 3C : 4D : 5E : 6F

01101010 → reverse → 01010110

0 - unicast
1 - multicast

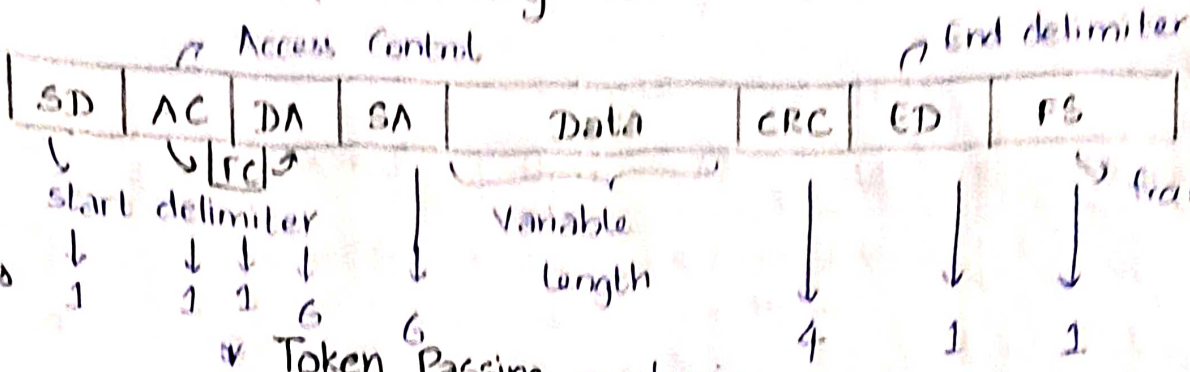
10 base 5 → 10 Mbps bandwidth, thickness of cable
10 base 2
10 base 1
10 Base T
10 base F
10 base G

Preamble - 101010 ... 10

SFD - 10101011

* Preamble and SFD are added by Physical layer
  Preamble is used to synchronise sender and receiver
* Acknowledgement is not considered and ethernet has no priority.
* Cannot be used for realtime and interactive applications, client server applications.

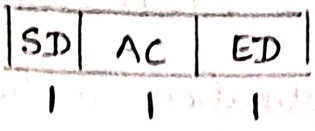
IEEE 802.5 (Token Ring Frame Format)



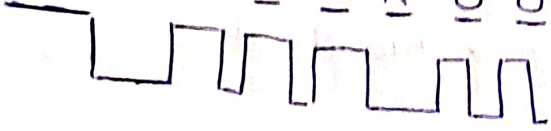
* Token Passing mechanism
* Ring Topology is used
* Differential Manchester Encoding is used

→ When (i) source / destination is down
(ii) errors between addresses occur, monitor station is selected and discards token.

Token Frame



SD - J K 0 0 J K 0 0



ED - J K 1 1 J K I

intermediately frame

error frame

AC - P P P T M R R R

token

priority

monitor

reservation

Token - 0 - data / control bit
1 - token frame

Frame Control (FC) - _ _ _ _ _ _ _ _

alive / dead information from monitor

0 0 → data
1 1 → control

Frame State - A C 0 0 A C 0 0

available

copied

* Acts as acknowledgement

1 1 → destination available & message copied
1 0 → destination available & message not copied
0 1 } not possible
0 0 }

IEEE 802.5 problems

- Source → orphan - source is down after transmission
  - stray - source address is modified
- Destination → destination is down
  - destination is busy
- Token
  - Monitor → monitor is down
- Token ring

(i) Token monopolisation
(ii) Token lost
(iii) Token error

} Monitor waits for RL + N(THT) time and creates a new token

* Token ring can be used in real time, interactive and client-server applications.
* Token ring has priority

IEEE 802.3

Ethernet, $\eta = \frac{1}{1+(6.44a)}$

TDMA, $\eta = \frac{1}{1+a}$

Effective length to be added = $\frac{V}{B}$

Internet Protocol Address - Network Layer

IP Addresses → IPv4
IP Addresses → IPv6

	IPv4	IPv6
Length	32	128
Octet	4	8
Range	0 to 255	0 to FFFF
Number	4 billion (2^{32})	340 trillion 2^{128}

IP Address → Network ID
IP Address → Host ID

IP Address → Classfull
IP Address → Classless
a.b.c.d/n

Classfull IP Addresses

Class A 0 _ _ _ _ _ _ _ . b.c.d
class B 1 0 _ _ _ _ _ _ . b.c.d
class C 1 1 0 _ _ _ _ _ . b.c.d
class D 1 1 1 0 _ _ _ _ . b.c.d
class E 1 1 1 1 _ _ _ _ . b.c.d

class A : range 2^7 : 0 to 127
class B : range 2^6 : 128 to 191
class C : range 2^5 : 192 to 223
class D : range 2^4 : 224 to 239
class E : range 2^4 : 240 to $247 + \frac{16}{2} \Rightarrow$ 240 to 255

* The starting ID of each class is used to identify NID
The ending ID of each class is used for broadcast / experiment.
So, the practical available NIDs would be $2^k - 2$

class A : 0.0.0.0 - broadcast request
127.0.0.0 - loopback request

class A : a . b . c . d
NID HID

class B : a . b . c . d
NID HID

class C : a . b . c . d
NID HID

class D : a . b . c . d
NID

* class D is used for multicasting and class E is unused for researchers' later use.

HID : 0000 0000 0000 0000 0000 0000 — identifies NID

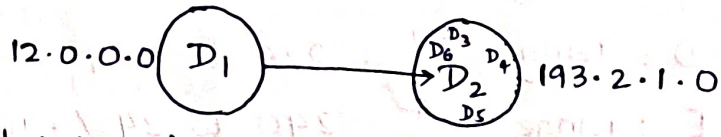
HID : 1111 1111 1111 1111 1111 1111 — broadcast.

class A : 2^{24} IP addresses – $(2^{24} - 2)$ Host addresses
class B : 2^{16} IP addresses – $(2^{16} - 2)$ Host addresses
class C : 2^{8} IP addresses – $(2^{8} - 2)$ Host addresses

Types of Casting

1. Unicast
2. Broadcast → Limited
   → Direct
3. Multicast

Unicast
DIP : dest. IP of reciever
SIP : source. IP of sender



Direct Broadcast : send infomation to every station in dest. network
DIP : 193.2.1.255
SIP : IP of source

Limited Broadcast : send information to every station in same network
DIP : 255.255.255.255
SIP : IP of source

Subnetting

→ dividing a network into small networks

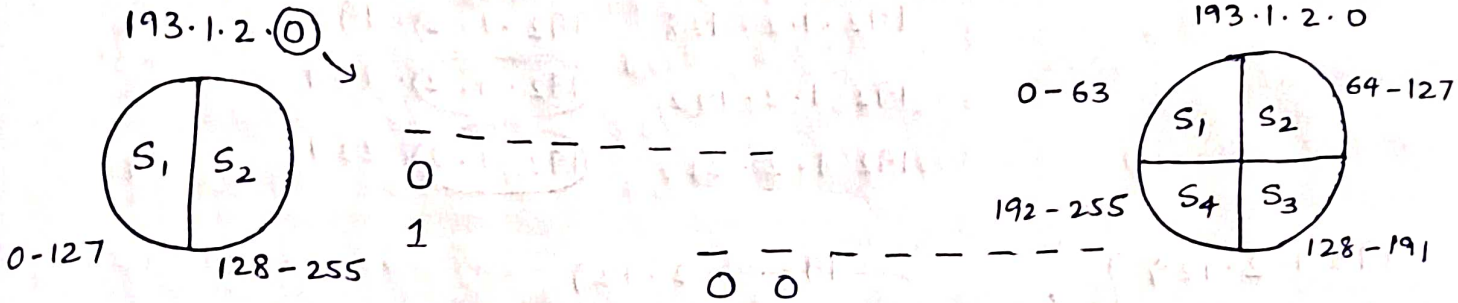
→ easy maintainence and improved security

→ unused IP address if less systems are connected.

Fixed Length Subnetting

→ subnetting can be done only in the power of 2

→ if divided into 2^k subnets, k bits must be borrowed from HID.



S_1 : 193.1.2.0 → SID

193.1.2.127 → direct broadcast

Subnet Mask:

255.255.255.11000000

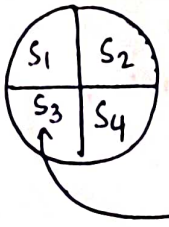
S_2 : 193.1.2.128 → SID

193.1.2.255 → direct broadcast

* To locate any DIP to which subnet it belongs, bitwise AND of DIP and subnet mask gives SID.

Subnet Mask: NID + k bits + HID

(NID + k bits: 1s; HID: 0s)



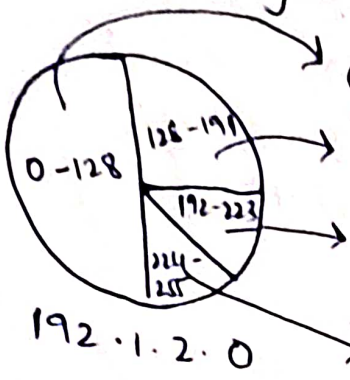
255.255.255.11000000

193.1.2.11000001

193.1.2.192

Routing Table	SID	Subnet Mask	Interface
	192.1.2.0	255.255.255.192	I_1
	192.1.2.64	"	I_2
	192.1.2.128	"	I_3
	192.1.2.192	"	I_4

Variable Length Subnetting



0 _ _ _ _ _ _ _ — 192.1.2.0

1 0 _ _ _ _ _ _ — 192.1.2.128

1 1 0 _ _ _ _ _ — 192.1.2.192

1 1 1 _ _ _ _ _ — 192.1.2.224

Routing Table

SID	Subnet mask 255.255.255	Interface
192.1.2.0	192.1.2.128	I_1
192.1.2.128	192.1.2.192	I_2
192.1.2.192	192.1.2.224	I_3
192.1.2.224	192.1.2.224	I_4

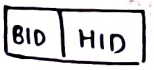
193.1.2.129
193.1.2.128 } X

193.1.2.129
255.255.255.128
193.1.2.128 → I_2

Classless Inter Domain Routing (CIDR)

* No class
* Blocks

IPv4



$x.y.z.w/n$ ← number of bits used to represent block/network
↳ mask

1. Addresses should be contiguous
2. Number of addresses must be in power 2
3. First address of every block must be evenly divisible with size of block

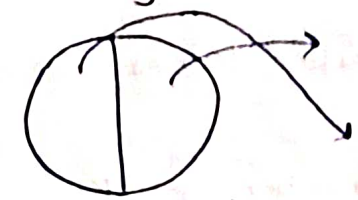
$x.y.z.w/n$

NID – n bits
HID – (32 – n) bits

193.1.2.0
193.1.2.1
193.1.2.2
⋮
193.1.2.63
} 2^6

IP address : 193.1.2.0/26

Subnetting in CIDR



0 _ _ _ _ _ _ → 193.2.1.0/26 to 193.2.1.31/26

1 _ _ _ _ _ _ → 193.2.1.32/26 to 193.2.1.63/26

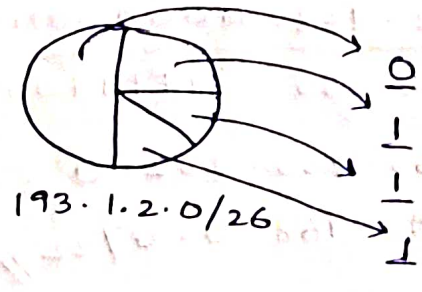
193.2.1.0/26

S_1 : SID – 193.2.1.0/26
DBA – 193.2.1.31/26

S_2 : SID – 193.2.1.32/26
DBA – 193.2.1.63/26

Subnet Mask – 255.255.255.11100000/26

↳ 26 1s + 1 1s + 5 0s



193.1.2.0/26

0 _ _ _ _ _

1 0 _ _ _ _

1 1 0 _ _ _

1 1 1 _ _ _

S_1 : SID – 193.2.1.0/27
S_2 : SID – 193.2.1.32/28
S_3 : SID – 193.2.1.48/29
S_4 : SID – 193.2.1.56/29

SID	Subnet mask	Interface
193.2.1.0/27	255.255.255.224/27	I_1
193.2.1.32/28	255.255.255.240/28	I_2
193.2.1.48/29	255.255.255.248/29	I_3
193.2.1.56/29	255.255.255.248/29	I_4

Supernetting

* Combining subnets to avoid problems of routing tables, memory

1. All networks should be contiguous
2. All networks should be having same size and number of IP addresses should be in power of 2.
3. Total size of the network should be divisible by first network address.

Supernet Mask

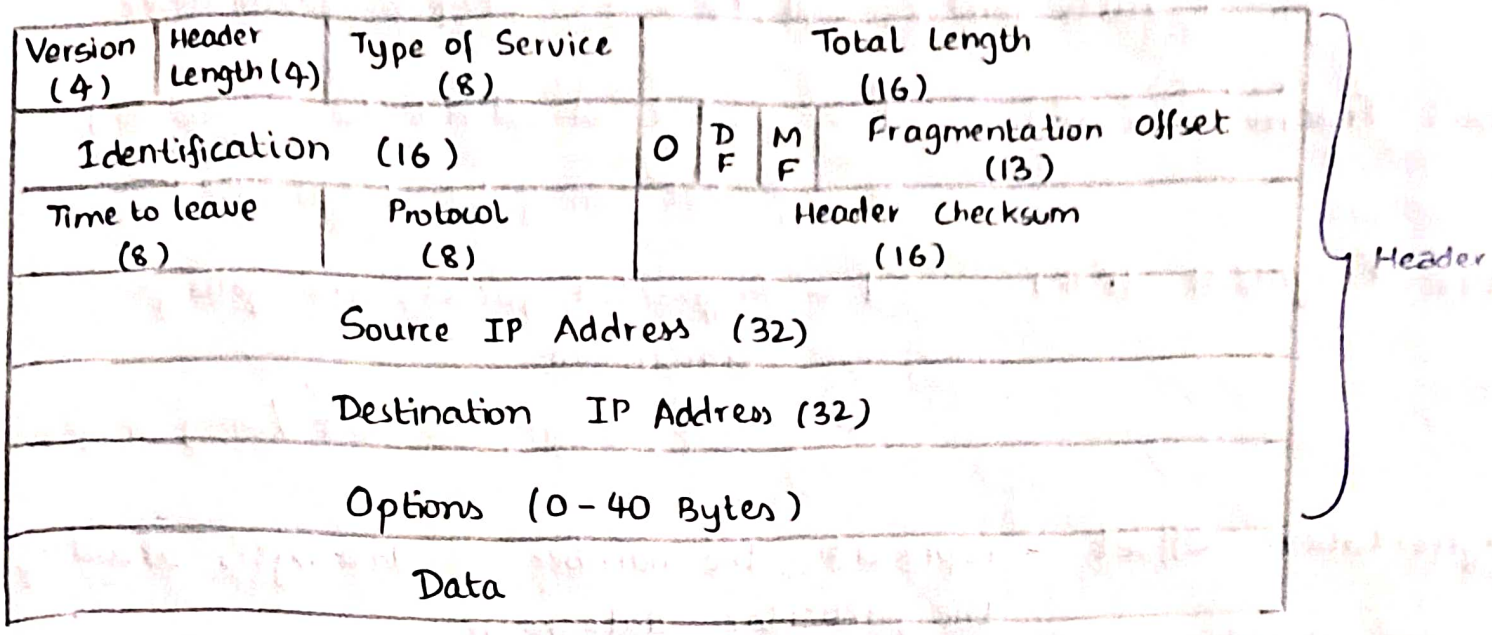
fixed bits → 1
variable bits → 0

192.168.1.0/24	192.168.00000000.
192.168.2.0/24	192.168.00000001.
192.168.3.0/24	192.168.00000010.
192.168.0.0/24	192.168.00000011.
	255.255.11111100.

Supernet mask - 255.255.252.0

NID - 192.168.0.0/22

IPv4 frame format



Version 0100 – IPv4
0110 – IPv6

Header Length – Size of header

Minimum header length = 20 B
Maximum header length = 60 B

* Since only 4 bytes are allocated, the actual header length can be divided by 2

$20/4$ – 0101

$60/4$ – 1111

* If header length is not divisible by 4, perform padding to yield header length in next nearest multiple of 4

$30\ B \approx \underbrace{30 + 2}_{\text{padding}} \approx 32\ B$

Total length – Header length + Data

$2^{16} - 1 = 65,535\ B$

Maximum data = 65,535 – 20

= 65,515 B //

Identification - identify datagrams and packets
- each packet will have its unique ID number

Don't Fragment (DF)
1 - packet should not be fragmented
0 - packet may be fragmented

More Fragment (MF)
1 - fragmented packets are getting transmitted
0 - last fragmented bit / only fragme

Fragmentation Offset - represents the number of databytes ahead of the particular datagram

Time to leave - time expected to live in transmission

Protocol - name of the protocol to which the data is to be passed

Network Layer : IP, ICMP, IGMP
Transport layer : TCP, UDP

ICMP > IGMP > UDP > TCP

* If networks require the datagram to be fragmented to travel further but settings do not allow, then it is discarded
* An error message is sent to sender saying that the datagram has been discarded.
* Fragmentation Offset - indicates position of fragmented datagram in original unfragmented IP datagram
- first fragment of datagram has offset 0.
* Time to leave - maximum number of hops a datagram can tate
- prevents looping in routing
* Identification - when IP datagram is fragmented, each fragment is same number ID number, which is useful during reassembly of fragments

Type of Service

P P P D T R C O → reserved always zero

P P P : Precedence
D : Delay
T : Throughput
R : reliability
C : cost

Delay & Cost : 0 - normal
1 - minimise

Throughput & Reliability : 0 - normal
1 - maximise

Priority :

0 0 0 - Routing	1 0 0 - Flash override
0 0 1 - Priority	1 0 1 - CRITIC / ECP
0 1 0 - Immediate	1 1 0 - Internetwork control
0 1 1 - flash	1 1 1 - Network Control

Options – 1. Record route
- record IP address of routers through which datagram passes on its way

2. Source route
- traverse through specified route only

3. Padding

Fragmentation

Packet
2000 B → MTU = 500B

P1: 480 | 20
P2: 480 | 20
P3: 480 | 20
P4: 80 | 20

$\frac{480}{8} = 60$

Scaling $\frac{2^{16}}{2^{13}} = 2^3 = 8$

Fragmentation Offsets : $P_1 \rightarrow 0$, $P_2 \rightarrow 60$, $P_3 \rightarrow 120$, $P_4 \rightarrow 180$

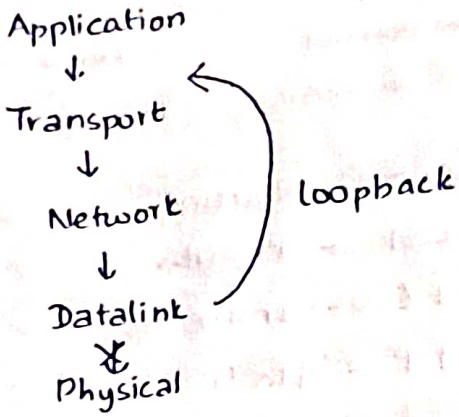
1. Check fragment or not
2. Identify 1st fragment and subsequent fragment
3. Repeat (2) until MF = 0
4. Current datagram = $\frac{\text{Payload}}{8}$ + Fragmentation Offset

Loopback Addresses

127.0.0.1 to 127.255.255.254

→ mocks TCP/IP server - client on the same system

→ Used for testing network connectivity and to find device on the network



Address Resolution Protocol (ARP)

* ARP maps IP address to MAC address
* ARP can occur b/n host to host, host to router, router to host, router to router.

ARP request: Broadcast a packet over network to validate whether the destination MAC address is encountered or not.

Physical Address of Sender - same

Receivers - all 1s

IP Address of Sender & Receiver - same ~~as de~~

ARP reply: MAC address response that the source receives from destination which aids in further communication of data.

ARP Cache: After resolving MAC address, ARP responses are stored for future reference.

ARP Cache Timeout: Indicates time for which MAC address in ARP Cache can reside

Reverse Address Resolution Protocol (RARP)

* RARP maps MAC addren to IP addres
* RARP is used to find IP address of source itself

RARP request : Source MAC address : same

Destination MAC addren : all 1s (broadcast)

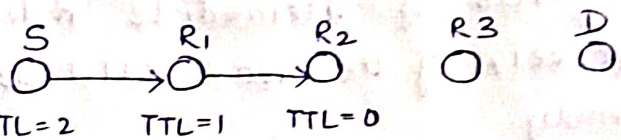
The request is broadcasted to RARP server.

Internet Control Message Protocol (ICMP)

→ Network Layer protocol

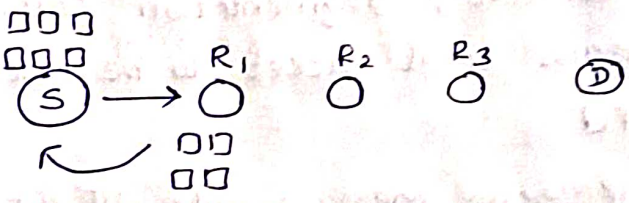
ICMP feedback and error

1. TTL exceeded (11)



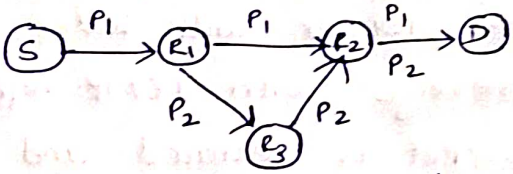
2. Parameter problem (DF & MF) (12)

3. Source quench (4)



4. Source redirect (15)

5. Destination unreachable (3)



IP → ICMP

ICMP ↛ ICMP

If P_2 is followed, retrace back to follow better path

* ICMP is not reliable, lost ICMP message cannot generate another ICMP message.

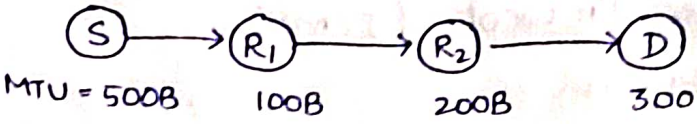
ICMP request and reply

1. Echo request & reply (8/0)
2. Timestamp request & reply (13/14)
3. Network mask request & reply (17/18)
4. Router Solicitation (10/9)
   &
   Advertisement

ICMP header

Type (8 bit)	Code (8 bit)	Checksum (16 bit)
Rest of ICMP header (32 bit)		
Data section		

Maximum Transmission Unit (MTU)



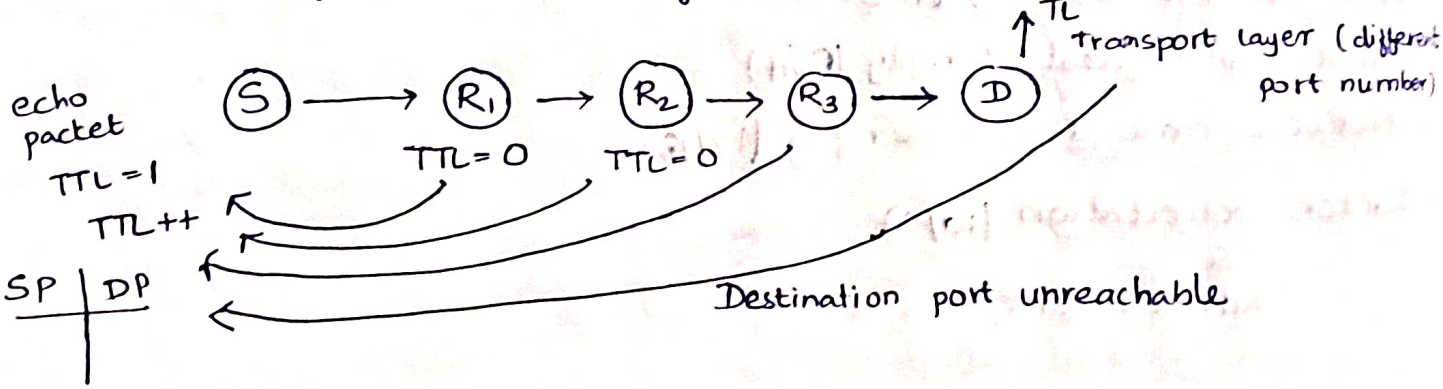
* If the MTUs of intermediate nodes are known, the source could send packets of the least MTU size to avoid fragmentation and reassembly.
* This is because, fragmentation causes more overhead, one fragment lost means total packet to be resent.

Finding MTU

1. An ICMP echo message with DF bit-1 and source MTU is sent and the router with lesser MTU is encountered, it sends back the message with ICMP reply of router MTU.
2. The packet is retraced and the packet is sent with new MTU.

Trace Route

→ allows you to trace every router that a packet has traverse during its journey
→ packet travels through several routers before it reaches its destination.
→ TTL field, error message in a packet



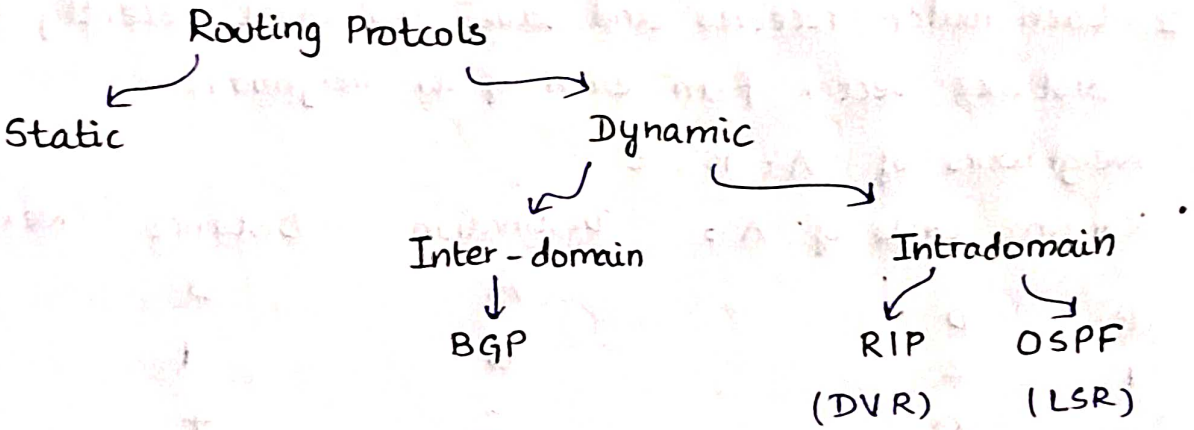
Routing

→ In order to transfer packets from source to destination, the network layer must determine the best route through which packets can be transmitted

→ The process of forwarding packets from source to destination but the best route to send packets is determined by routing algorithm

Flooding

→ Non- Adaptive routing technique; when a data packet arrives at a router, it is sent to all outgoing links except the one it has arrived on.



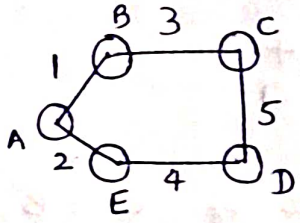
Distance Vector Routing Algorithm

A:

Destination	Distance	Next hop
A	0	A
B	1	B
C	∞	-
D	∞	-
E	2	E

B:

A	1	A
B	0	B
C	3	C
D	∞	-
E	∞	-



1. A router transmits its distance vector to each of its neighbours in a routing packet.

C → A to B, B to C = 4
A to E, E to C = ∞

C : A ∞ -
B 3 B
C 0 C
D 5 D
E ∞ -

D: A ∞ -
B ∞ -
C 5 C
D 0 D
E 4 E

E : A 2 A
B ∞ -
C ∞ -
D 4 D
E 0 E

2. Each router receives and saves the most recently received distance vector from each of its neighbours

Neighbours of A : B , E

Routing table of A :

Destination	Distance	Next hop
A	0	A
B	1	B
C	4	B
D	2	D
E	6	D

B D
1 2
0 ∞
3 ∞
∞ 4
∞ 0

Neighbours of C : B , D

Routing table of C :

Destination	Distance	Next hop
A	4	B
B	3	B
C	0	C
D	5	D
E	9	D

B D
1 ∞
0 ∞
3 5
∞ 0
∞ 4

3. A router calculates its distance vector when
   (i) It receives a distance vector from neighbour containing different information than before.
   (ii) It discovers that a link to neighbour has gone down.

* Distance Vector Routing Algorithm is known as Bellman-Ford Algorithm.
* The routing table is constructed using local knowledge
* The convergence is slow.