# COMPUTER NETWORKS

Neso academy, Gate Smashers, Gate Academy

* Imp

for revision only this

* together with this read theory of gate book (wiley)

Read wiley & solve its questions / some theory there

## INTRODUCTION

- A computer network is set of nodes connected by communication links.
- A node can be a computer, printer or any other device capable of sending / receiving data generated by other nodes in the network.

- Basic characteristics of COMPUTER NETWORK
  1) Fault Tolerance
  2) Scalability
  3) Quality of Service (QoS)
  4) Security

- Fault Tolerance
  1) Continue working despite failures
  2) Ensure no loss of service.

- Scalability
  1) Grow based on needs
  2) Have good performance after growth.

- Quality of Service (QoS)
  The ability to:
  1) Set priorities
  2) Manage data traffic to reduce data loss, delay etc.

- Security
  ability to prevent:
  1) Unauthorized access 2) Misuse 3) forgery
  ability to provide:
  1) Confidentiality 2) Integrity 3) Availability

## Network Protocols and communications

- Data flow
  Flow of data from one node to another via a communication link

  3 types:-
  - Simplex
  - Half Duplex
  - Full Duplex

- **Simplex**
  → Communication is unidirectional
  → One device can transmit and other device will recieve.
  eg Keyboards, Traditional monitors.

- **Half Duplex**
  → Communication is in both directions but not at same time
  → If one device is sending, other can only recieve and vice-versa.
  eg: Walkie - Talkies

- **Duplex**
  Communication is in both direction simultaneously.
  eg: Telephone line

## ⇒ Protocol

- Set of rules that govern data communication.
- Protocols used in network communication also defines:
  1) Message encoding
  2) Message timing
  3) Message formatting and encapsulation
  4) Message size
  5) Message delivery options

- Peer-to-Peer Network
  - No centralized administration
  - All peers are equal
  - Simple sharing applications
  - Not scalable

- Client Server Network
  - Centralized administration
  - Request-response model
  - Scalable
  - Server may be overloaded

# COMPONENTS OF A COMPUTER NETWORK

1) Nodes 2) Media 3) Services

## 1) Nodes

Can be end nodes or Intermediary nodes

## 2) Media

- Wired Medium (Guided Medium) : eg Fibre optic cable, ethernet cable, USB cable, Coaxial cable
- Wireless Medium (Unguided Medium) : Infrared, radio, Microwaves, satellite

3) Services

Email
Online game
world wide web
Video telephony
voice over IP
File sharing
Messaging
Storage services

# Network Topologies

Topology → Arrangment of nodes of computer network.
(Layout)

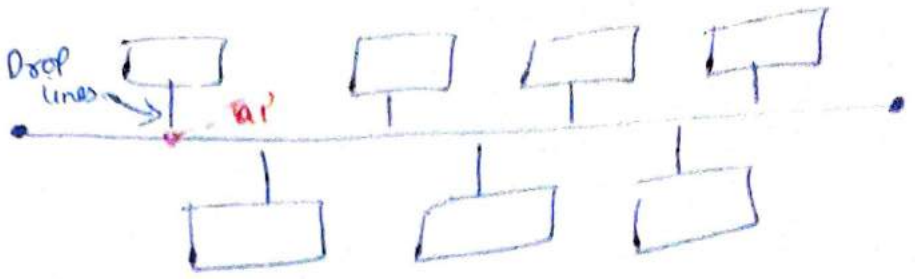
1) Physical Topology - Placement of various nodes
2) Logical Topology - Deals with data flow in network.

Types :-
1) Bus 2) Ring 3) Star 4) Mesh
5) Hybrid

## ⇒ Bus Topology

- All data transmitted between nodes in network is transmitted over this common transmission medium and is able to be received by all nodes in this network simultaneously

eg




No of cables = n + 1
↑
Center (Coaxial) Cabel

## Advantages

- Only one wire (less expensive)
- Suited for temporary network
- Nodes failure does not affect others

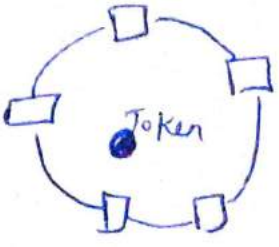
## Disadvantages

- Not fault tolerant (no redundancy)
- Limited cable length
- No security.

## ⇒ Ring Topology

- A ring Topology is bus topology in closed loop
- Peer-to-Peer LAN topology
- Unidirectional
- Sending & receiving data takes place with help of token.

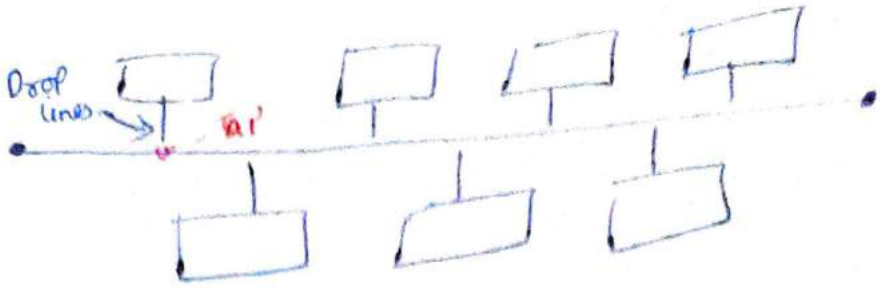
→ one having token has chance to send data, one by one token is passed.




## Advantages

- All nodes with equal access
- Perform better than ~~ring~~ Bus topology
- Can cause bottleneck due to weak links

eg




No of cables = n + 1
↑ center (coaxial) cable

## Advantages

- Only one wire (less expensive)
- Suited for temporary network
- Nodes failure does not affect others

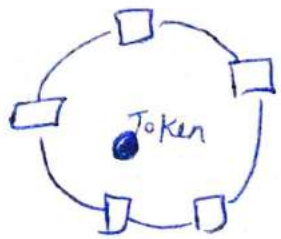
## Disadvantages

- Not fault tolerant (no redundancy)
- Limited cable length
- No security.

## ⇒ Ring Topology

- A ring Topology is bus topology in closed loop
- Peer-to-Peer LAN topology
- Unidirectional
- Sending & receiving data takes place with help of token.

→ one having token has chance to send data, one by one token is passed.




## Advantages

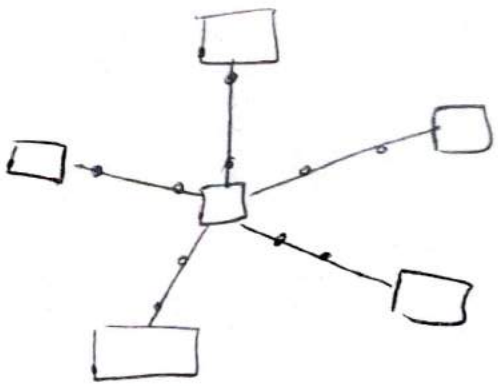
- All nodes with equal access
- Perform better than ~~ring~~ Bus topology
- Can cause bottleneck due to weak links

Disadvantages

- No security
- more load → less performance
- Unidirectional. Single point of failure affect whole network.

## ⇒ STAR TOPOLOGY

- Every node is connected to central node called a hub or switch.
- Centralized Managment
- All traffic must pass through hub



Advantages

- Easy to design & implement
- Centralized administration
- Scalable

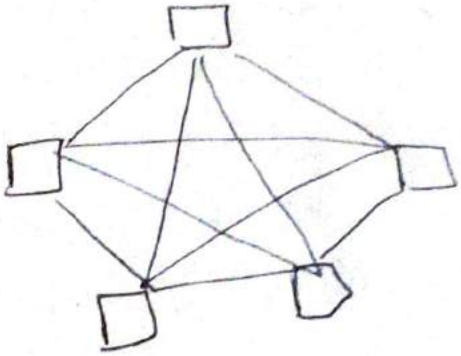
Disadvantages

- Single point of failure affects whole network
- Bottlenecks due to overload switch / hub.
- Increased cost due to switch / hub.

## ⇒ MESH TOPOLOGY

- Each node is directly connected to every other nodes in network, Point to point communicaton.
- Fault tolerant and reliable

eg



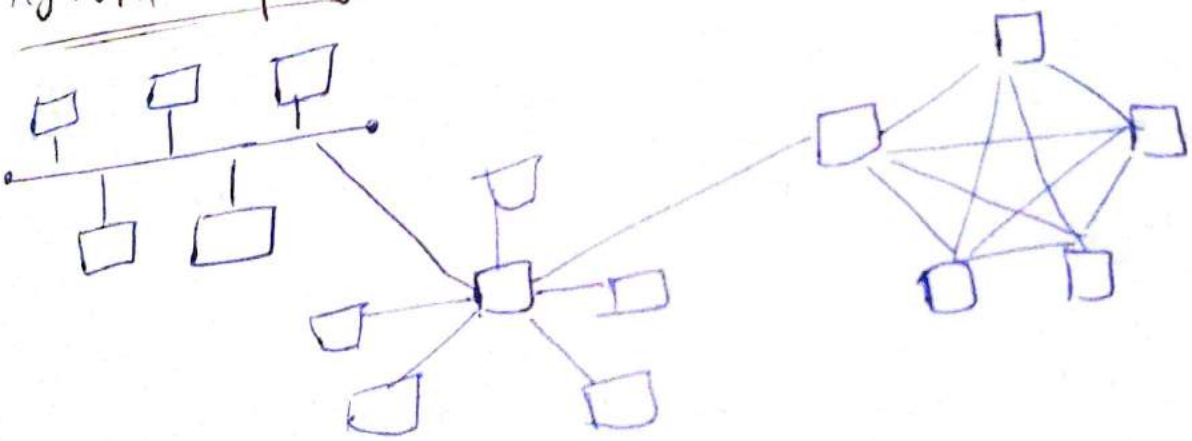
Advantage

- Fault tolerant
- Reliable

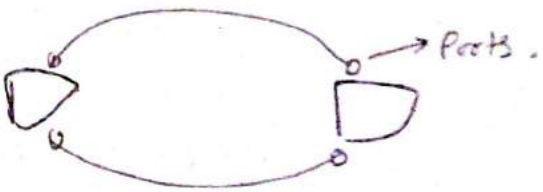
Disadvantages

- Issue with broadcasting messages
- Expensive & impractical for large networks.

- Hybrid Topology



Ports




Ports → connection port

here = 4 ports.

Note

- To connect same type of devices :- Ethernet cross over cable.
- To connect diff. type of devices :- Ethernet cable Straight - Through

# Basic of IP Addressing

IP - Internet protocol

→ Every node in the computer network is identified with the help of IP address.

→ Logical address (can change)

→ Can change based on location of device

→ Assigned manually or dynamically.

## IPV4

- Represented in decimal & has 4 octets (x.x.x.x)
- 0.0.0.0 to 255.255.255.255 (32 bits)

## MAC address

- MAC stands for Media Access Control.
- Every node in the LAN is identified with the help of MAC address.
- IP address = Location of a person
- MAC address = Name of a person

→ Every node in LAN is identified with help of MAC address.

→ Physical Address or Hardware Address (can't change)

→ Unique, can't be changed, Assigned by Manufacturer

→ represented in hexadecimal eg, 70-20-84-00-E0-FC (48 bits)

→ Seperator: hyphen (-), period (.), colon (:)

# Port Addressing

Let see analogy

Parcel sent from London to Mumbai

→ So one address to reach city, one for apartment, & one for your location in apartment.

- Reaching our city = Reaching our network (IP address) → needed by router
- Reaching our apartment = Reaching our host (MAC address) → by switch/LAN
- Reaching right person = Reaching right process (Port address) → by OS

## Port address or port number

→ In a node, many processes will be running

→ Data which are sent / received must reach right process.

→ Every process in node is uniquely identified using port numbers.

→ Port = communication endpoint

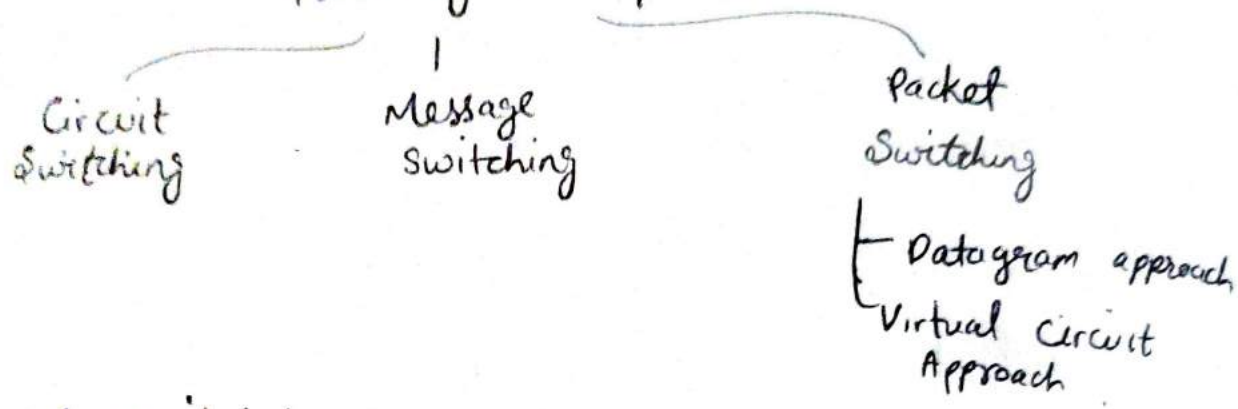
→ Fixed port numbers & dynamic port numbers (0 - 65535)

eg Fixed port numbers : 25, 80 etc

OS assigned dynamic port no. : 62414

# Switching techniques

Switching in computer network helps in deciding the best route for data transmission if there are multiple paths in larger network.




## 1) Circuit switching

- A dedicated path is established betn sender & receiver
- Before data transfer, connection will be established first.
  eg Telephone network.

3 phases in circuit switching

1) Connection establishment
2) Data transfer
3) Connection Disconnection

## 2) Message switching

- Store & forward Mechanism
- Message is transferred as a complete unit & forwarded using store and forward mechanism at intermediary node.
- Not suited for streaming media and real-time applications.

3) Packet switching

- Internet is packet switched network.
- message is broken into individual chunks called as packets
- Each packet is sent individually.
- Each packet will have source & destination IP address with sequence number.
- sequence number will help receiver to
  - record the packets
  - Detect missing packets
  - Send acknowledgements.

2 approach

a) Datagram approach.

- also known as connectionless switching. Each independent entity is called datagram.
- Datagram contain destination info & intermediary devices uses this info to forward datagrams to right destination
- In datagram Packet switching, path is not fixed
- Intermediate nodes take routing decisions to forward process.

b) Virtual circuit approach.

- also known as connection-oriented switching
- a preplanned route is established before messages are sent.
- Call request & call accept packets are used to establish connection between Sender & receiver.
- In this approach, path is fixed for duration of logical connection

# Layering in Computer Networks

1) OSI reference Model , 2) TCP/IP model.

## 1) OSI reference model

- OSI = Open system Interconnection
- It is model for understanding & designing a network architecture that is flexible, robust & interoperable.
- Developed by International Standards for Organizations (ISO)
- OSI model is not a protocol but only a guidelines.
- OSI model was never fully implemented.

## 2) TCP / IP model

- = Transmission Control Protocol / Internet Protocol.
- was developed prior to OSI model, therefore layers in TCP/IP protocol suite not exactly match with OSI model.
- TCP /IP is hierarchial protocol made up of interactive modules, each of which provides a specific functionality.

- Layering → Means decomposing problem of building a network into more managable components (Layers).

# OSI Reference Model

- The purpose of OSI model is to facilitate communication betn different systems (diff OS, type of device etc) without requiring changes to the logic of underlying hardware and software.

## 7 layers of OSI model

| | | |
|---|---|---|
| 7 | Application layer | Away |
| 6 | Presentation layer. | Pizza |
| 5 | Session layer | |
| 4 | Transport layer | Sausage |
| 3 | Network layer | Throw |
| 2 | Data link layer | Not |
| 1 | Physical layer | Do |
| | | Please |

to learn ↑

Working ↓ to send password

7) AL → abc @ 132

6) Presentation layer → odkf*3dqctv ←

5) Session Layer → odkf*3dqctv (session created)

4) TL → TL INFO - odkf*3dqctv

3) NL → NL INFO - TL Info - odkf*3dqctv

2) DL → DL INFO - NL info - TL info - odkf*3dqctv

1) Physical Layer → 0|000|0|0|00|0|0|1|1|00|0|1

↳ into waves or signals etc.

## 1) Application Layer

- It enables the user to access network resources.

Services provided are -

1) file transfer & access managment (FTAM)
2) Mail services
3) Directory services. (access to data globally)

## 2) Presentation Layer

- It is concerned with syntax & semantics of information encharged between two systems.

Services

1) Translation
2) Encryption
3) Compression

## 3) Session Layer

It establishes, maintains and synchronizes the interaction among communication devices.

Services

1) Dialog control (decides either duplex, half duplex etc for a given process)
2) Synchronization (add checkpoints in communication)

4) Transport layer

It is responsible for process to process delivery of entire message

Services

1) Port addressing (source & destination port no. is added to message)
2) Segmentation & reassembly
3) Connection control
4) End-to-end flow control (speed matching)
5) Error control

5) Network layer

It is responsible for delivery of data from original source to destination network.

Services → Logical addressing (IP address)
Routing (finding best path)

6) Data link layer

It is responsible for moving data (frames) from one node to another node

Services

1) framing
2) Physical addressing (MAC addressing)
3) Flow control
4) Error control
5) Access control (If more than 2 devices connected to same link this decides which will have control over it).

# 7) Physical layer

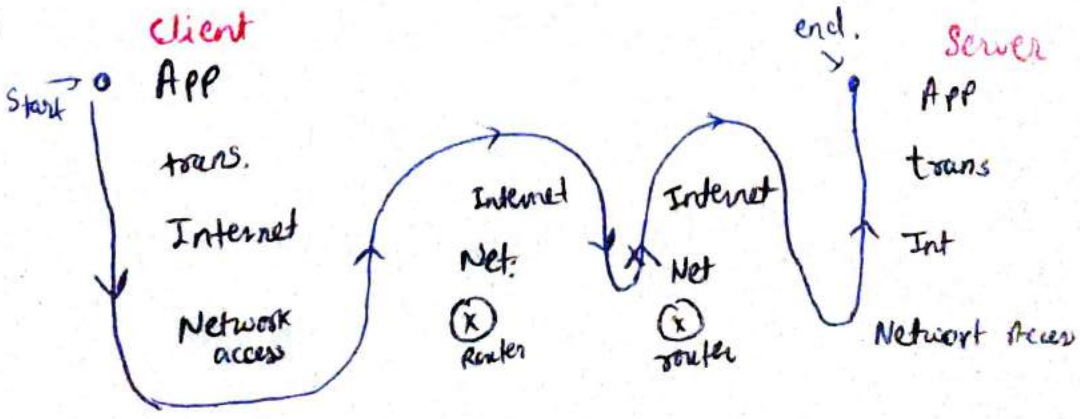
It is responsible for transmitting bits over a medium
It also provides electrical & mechanical specifications

Services

1) Physical characteristics of media (cables & connectors)
2) Representation of bits
3) Data rate
4) bits synchronization
5) Line configuration (Point to point or Point to multi)
6) Physical topology. (star, mesh etc).
7) Transmission mode (half duplex, duplex etc)
8) multiplexing
9) Encoding. (like digital to analog etc)
10) Hardwares (Repeaters, Hubs)

Let TCP/IP 4 layer

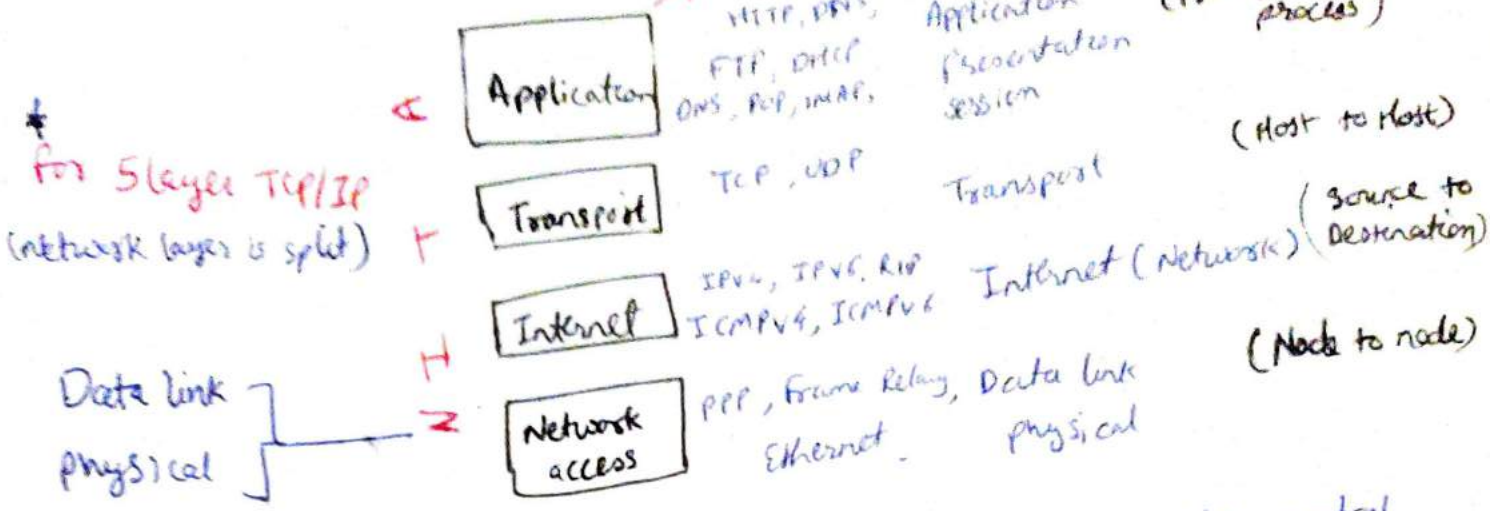
how this works.



# TCP/IP protocol Suite

4 layer TCP/IP

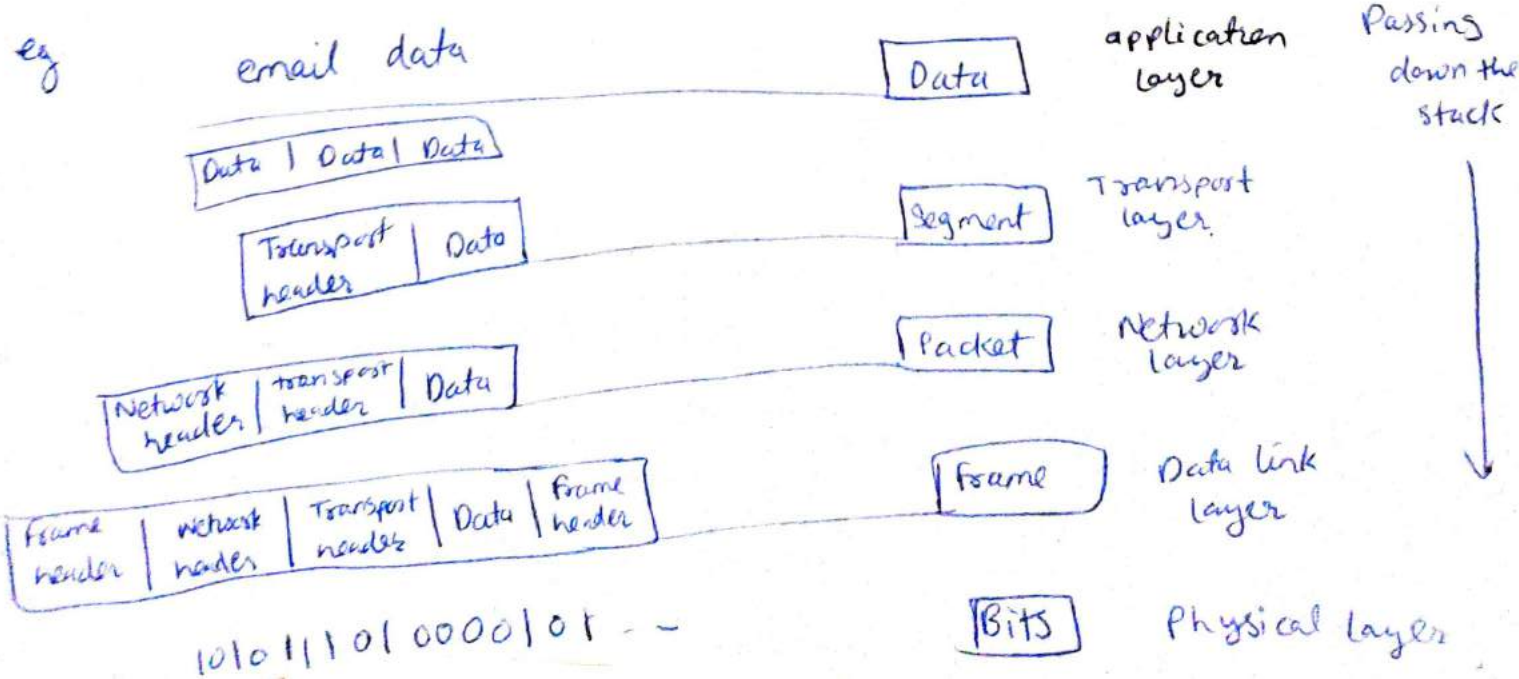
OSI comparision




- Application → Represents data to user, plus encoding & dialog control
- Transport → Supports communication betn diverse devices across diverse networks
- Internet → Determines best path through network.
- Network access → Control hardware devices & media that make up the network.

- **PDU** (Protocol Data unit)

PDU's are named according to protocols of TCP/IP suite : data, segment, packet, frame & bits.



# #Basic networking commands

1) ipconfig
returns ip configuration. — details of Layer 3 (Network layer) Network layer uses IP Address.

2) ipconfig/all
gives Layer 2 (Data link layer) info. about MAC address.

3) nslookup
gives ip address of site to access.

>nslookup
> www.khanacademy.com. ) get ip address.

4) ping
can be used to know if 2 computers are reachable to each other or not
it sends n packages & if it receive n packages so they are reachable.

> ping 192.169.217.12
→ target IP address.
or
> ping www.facebook.com.

5) Tracert
generate path followed by package to reach from your device to target

tracert 192.169.217.12

## Various devices

1) cables
2) repeaters
3) hubs
] Hardware (on physical layer)

4) Bridges
5) Switches
6) Routers
} H/w & S/w

7) IDS
8) Firewall
] Security

9) modem (for analog to digital & vice versa)

## HUB

→ aka network hub, work like multiport repeater.
→ Hub works at physical layer of OSI model (Layer 1)
→ Used to set up LAN → has no memory
→ has multiple ports
→ star topology → half duplex
→ when a packet arrives at one port, it is copied to other ports so that all segments of LAN can see all packets.

## SWITCH

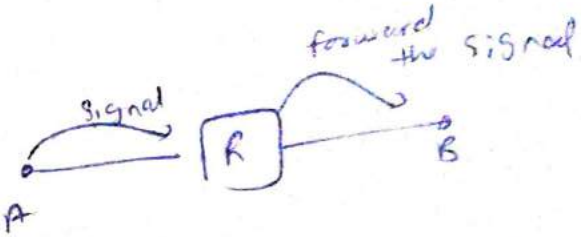
- A Switch is a networking hardware that connects devices on a computer network to establish local area network.
- Unlike hub, switch has memory.
- Store MAC address Table
- Layer 2 DEVICE for setting up LAN.
- works at Data Link layer.

## Router

- A router is a networking device that forwards data packets betn computer networks.
- It is a layer 3 (Network layer) device
- A router is connected to at least two networks, commonly 2 LAN's or WAN's or LAN & its ISP (Internet service provider) network.
- Stores routing table., Store & forward method
- decision taken based on IP address. (Internet)

## • Repeater

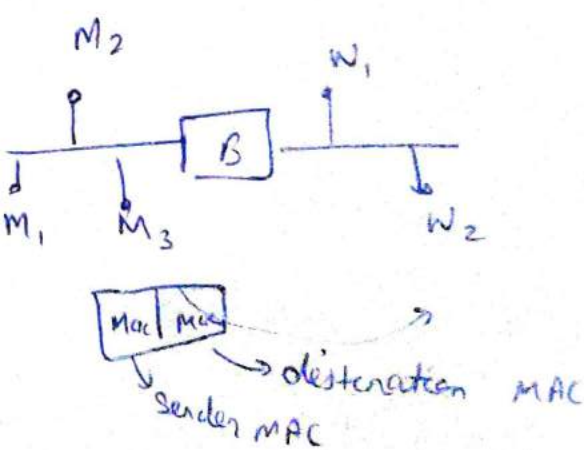
- The data signals generally become too weak or corrupted if they tend to travel a long distance
- Repeater regenerates signal over same network
- It operates at physical layer
- They do not amplify the signal
- It is a 2 port device
- is pure hardware
- Repeater can do forwarding




- Repeater can do filter (remove certain signals since is h/w)
- maximum collisions = no. of devices connected)

## Bridges

- Physical & data link layer
- Connect two different LAN's
- Do forwarding, can do filtering
- No collision inside, as use store & forward method (maintain buffer)



# Cables

- Unshielded twisted pair cable
  - 10 Base T , 100 Base T
- Coaxial cable
  - 10 Base 2 ---> 200 meter
  - 10 Base 5
- Fiber optic
  - 100 base Fx ---> ≈ 2 km

10 Base T → 100 m (after 100 m strength of signal decrease) [attenuation]

10 Mbps → Bandwidth

Base → at a time 1 signal

Broad → broadband, multiple signal at a time

Q For any cable with n devices

max collision = n

collision domain

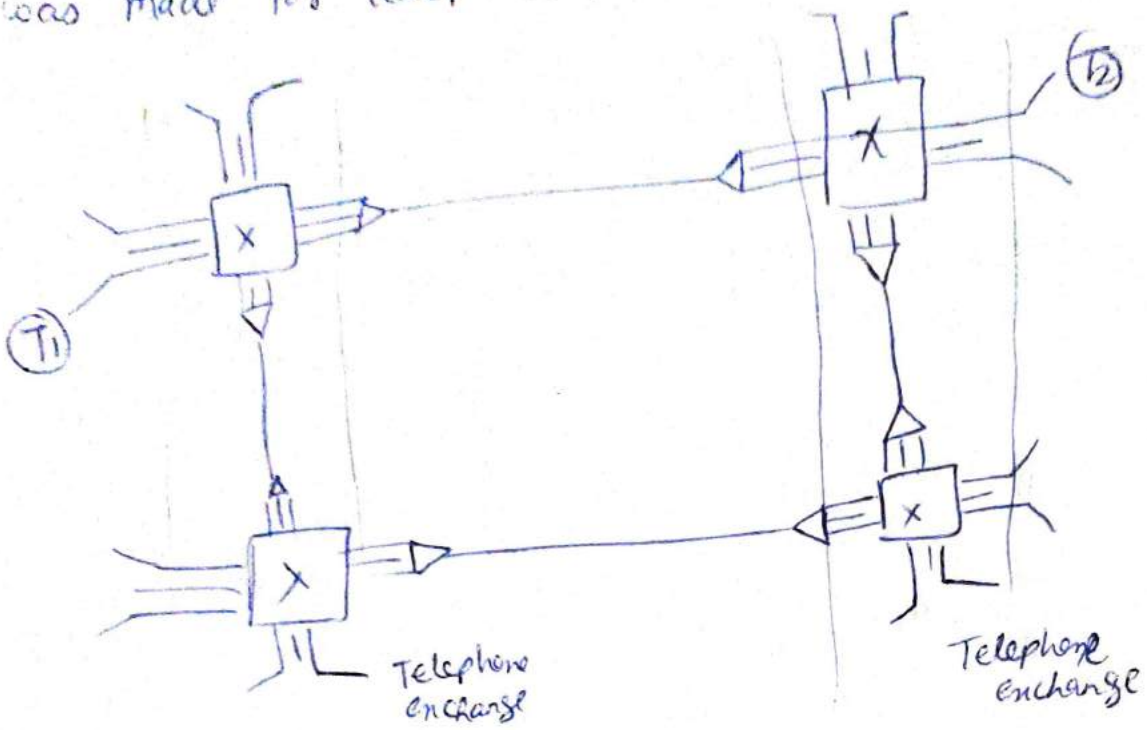
- cables can't do filter, used in physical layer.

# Gateways

It is a networking system capable of interconnecting one or more networks that has different base protocol. Gateway serves as a entry & exit point. Gateway sometimes called as protocol converter is used in different layers. eg. gateway can be used to convert a TCP/IP packet to Netware IPX packet.

# Circuit Switching

was made for telephones.



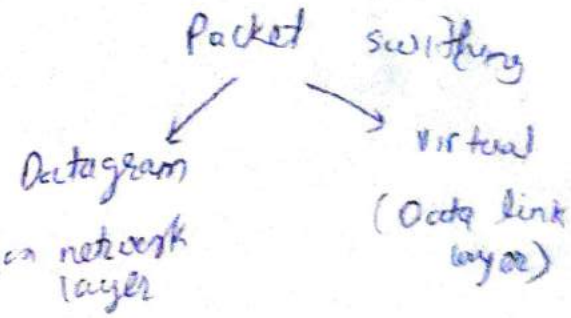

- dedicated path (when $T_1$ connect to $T_2$ single path is made betn them)
- continues flow (no packets etc)
- data is send in order
- Efficiency less

$$\text{Total time} = \text{Setup time} + \text{Transmission time}\left(\frac{\text{message}}{\text{bandwidth}}\right) + \text{Propagation delay}\left(\frac{\text{Distance}}{\text{velocity}}\right) + \text{Peer Down time}$$

(time to free connections at end)

# Packet Switching

- Data devided in packet
- Data link & network layer.
- Store & forward
- So more efficiency.
- Delay is more (as stored in buffer)
- we use pipelining here.




Total time = Transmission Time + Propagation delay

## Datagram Switching

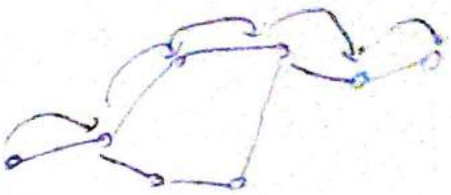
- Connectionless (no reservation of resources)
- Out of order (packet 4 can be came before packet 1)
- high overhead
- Packet loss is high (since all packets follow different path)
- Used → internet
- Cost ↓
- Delay ↑

## Virtual circuit

- Connection oriented (before sending packet resources like switch etc is reserved)
- in order
- Less overhead
- Packet loss less (all packet singl path)
- Used → ATM
- Cost ↑ (reservation)
- Delay ↓

# Message Switching

→ Hop to Hop delivery →



→ Store & forward

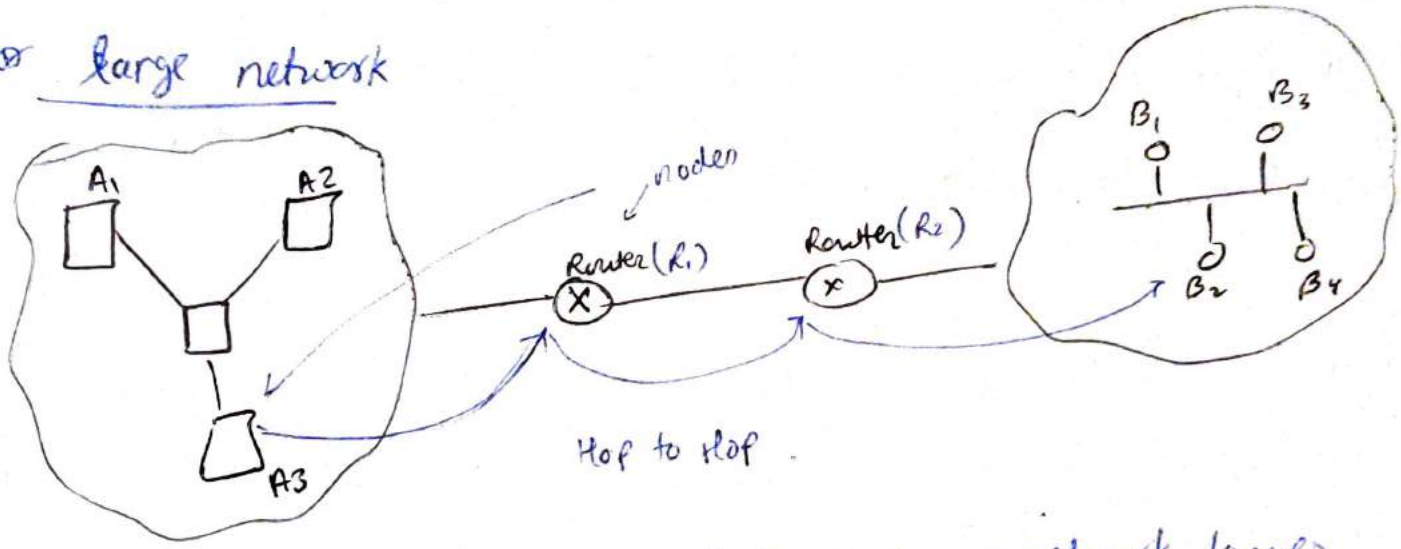
→ Delay ↑
as each hop stores

• in content switching full path was reserved.

# Datalink layer

- for communication within a network, Datalink layer is sufficient
- used for node to node or Hop to Hop delivery.

For large network




- for direct communication of A3 to B2 → network layer
- for A3 → R1 → R2 → B2 (Hop to Hop) → Data link layer

(uses mac address)

2) also does flow control (speed of sending) for hop to hop.
uses Stop & wait, GBN (Go Back N), SR (selective repeat)

3) Error control (CRC, checksum, parity)
CRC → in data link
checksum → in transport

4) Access control (CSMA/CD, Aloha, Token ring & bus)

5) Physical address (MAC) [is fix]

6) Framing : data unit at data link is called frame

Error Control : It is a mechanism which informs sender about retransmission of a damaged & lost frames during transmission. It is method of error detection & correction. Automatic repeat request (ARQ) is a process in which whenever an error is detected, the receiving device sends request for retransmission to sender.

## • Flow Control

### 1) Stop & wait :

→ Only 1 frame sent at a time

→ sender window = 1 ( 1 frame send )

→ receiver window = 1 ( 1 frame received )

→ Retransmission = 1

* when acknowledgment (ACK) not received with given time again 1 frame is send.

→ Efficiency :-

(Tt) Transmission time = $\frac{\text{Message size}}{\text{Bandwidth}}$

(PD) Propagation delay = $\frac{\text{Distance of link}}{\text{velocity}}$

• Efficiency, link utilization of sender or throughput

$$\eta = \frac{T_t}{T_t + 2 \times PD} = \frac{1}{1 + 2a} \qquad a = \frac{P_D}{T_t}$$

time for round trip → frame

## 2) Go-back-N

- Multiple frames, sliding window
- Sender window $= 2^k - 1$ or $N - 1$
- Receiver window $= 1$
  ∴ so fills the pipe

N = Window size
k bits count to represent window size

- Commulative acknowledgement eg: 1, 2, 3 → in window; ← 4 as ACK, next expected
- Retransmission $= 2^k - 1$
- $\eta = 2^k - 1 \times \frac{1}{1 + 2a}$
- frames send in order

## 3) Selective Repeat

- Multiple frames
- Sender window $= 2^k - 1$ (frames)
- reciver window $= 2^k - 1$
- Commulative & independent ACK
- Retransmission $= 1$
- $\eta = (2^k - 1) \times \frac{1}{1 + 2a}$
- frames send out of order.

# Error Detection & Correction

1) Sirgl bit Error 101 → 100
(1 bit change)

2) Burst Error

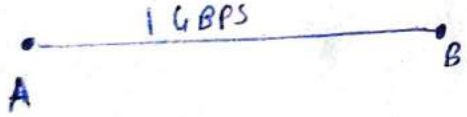
Length of error = 5

bits changed = 2 > 1
So ↗ Burst error

Detection
- Simple Parity (Even, odd)
- 2D parity check
- checksum
- CRC (cyclic Redundancy check)

Correction
- Hamming codes

Q If bandwidth of channel is 1 Gbps then for how much duration error should last?




$10^9$ bits → 1 sec

1 bit = $\frac{1}{10^9}$ sec = 1 ns

So if error stays for more than 1 ns chances of single bit error

So if error stays for $\frac{1}{1000}$ sec So error count = $\frac{1}{1000} \times 10^9 = 10^6$ bits

## • Simple Parity

→ Append a single parity bit to a sequence of bits.
Can be even or odd parity

eg Even parity

if 1010 → 10100

2 bits = 1
already even count of 1

1110 → 11101 } at end even 1 count

- Can detect only change occured or not
  but can't find location

- Can find odd no. of changes

eg 1110 1 → (3) → 0000 1

x for even parity
So error detected.

1110 1 → (1 change) → 0110 1
detect

1110 1 → (2 change) → 0010 1
fine for even parity
can't detect

# CRC (cyclic Redundancy check)

- most widely used error detection
- Based on Binary division

→ bits send - $m$ + $r$ (redundancy bits)
(message bits)

let given divisor = $x^4 + x^3 + 1$ & dividend = 1010101010
can be given directly

→ for $r$ → max power $(x^4 + x^3 + 1) = 4$

so append 4 0 bits at end.

also $x^4 + x^3 + 1 = 1.x^4 + 1.x^3 + 0.x^2 + 0.x^1 + 1.x^0$

$\equiv 11001$

so $\equiv$ 11001 ) 1010101010 0000 (

need to find remainder

do XOR ↳

Start from leading 1

```
11001
-----
01100
 11001
-----
00001010
  xor 11001
-----
00011000
   11001
-----
0000100
```

take last 4 bit = 0010

so r = 0010
not 0000

efficiency $\frac{m}{m+r} \times 100$

here - $\frac{10}{14} \times 100$

receiver gets = 1010101010 0010

if for this → do division remainder gets 0, if remainder not = 0 so error would be occured.

# Hamming code for error detection

here both data parity bits (p) are fitted

eg

| position | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|
| bit | $d_3$ | $d_2$ | $d_1$ | $p_2$ | $d_0$ | $p_1$ | $p_0$ |

data = $d_3\ d_2\ d_1\ d_0$

parities are placed on positions → $2^0, 2^1, 2^2, 2^3$ ... ↓ 1, 2, 4, 8 ...

$p_2 = d_3 \oplus d_2 \oplus d_1$ , $p_1 = d_3 \oplus d_2 \oplus d_0$

$p_0 = d_3 \oplus d_1 \oplus d_0$

$p_0$ at position 1 so $p_0\ p_1\ d_0\ p_2\ d_1\ d_2\ d_3$ (1 gap)

$p_1 = p_1\ d_0\ p_2\ d_1\ d_2\ d_3$

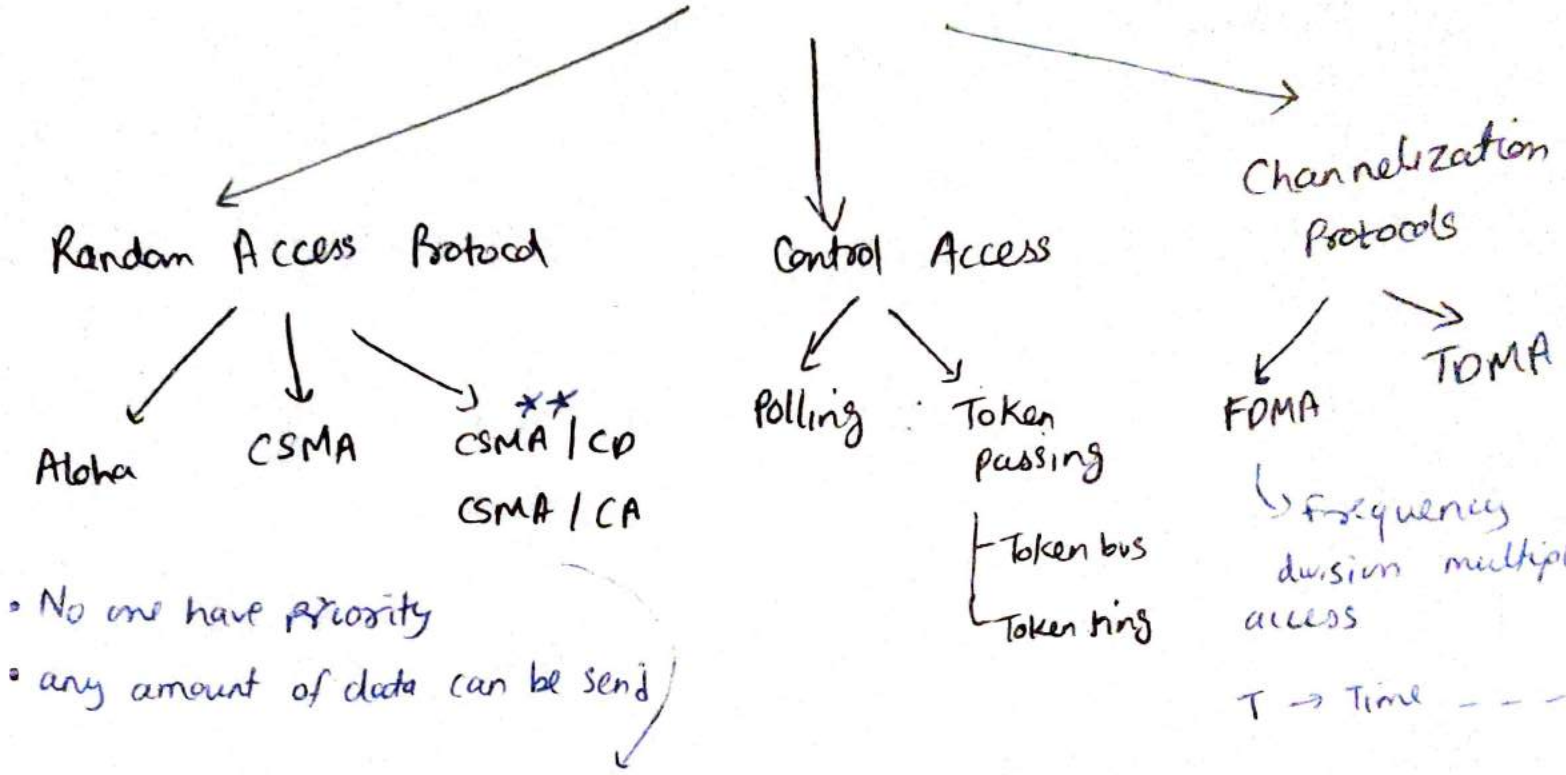
$p_2$ at 4th = $p_2\ d_1\ d_2\ d_3$

size : $d_1 \oplus d_2 \oplus d_3$

according to max parity ko possible size

# helps in correction also

# MAC (medium access control) Protocol




- No one have priority
- any amount of data can be send

CD → collision detection
CA → collision Avoidance

## Aloha

## 1) Pure Aloha

- Random Access protocol
- It says whenever a station has a data, they can send immediatly.
- LAN based.
- Only transmission time, No propogation time.

$T_T$ = transmission time = $\frac{\text{Frame size}}{\text{Bandwidth}}$ = G

- Vulnerable time : time at which collision occurs.

$T_P$ = Maximum propagation time = $2 \times T_T$

= $\frac{\text{Distance betn 2 stations}}{\text{Velocity}}$

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

for max S

$\frac{dS}{dG} = G \times e^{-2G}(-2) + e^{-2G} = 0$

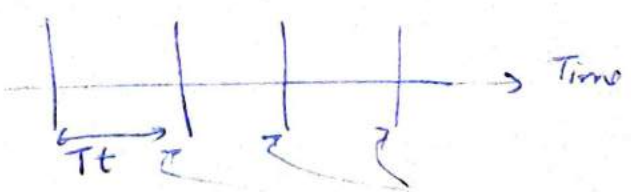
$G = 1/2$ & $S_{max} = 0.184$ or 18.4%.

So if let 10 stations, for $S_{max}$ half → 5 stations should send

## 2) Slotted Aloha

here time is devided on basis of $T_T$

$T_T$ = $\frac{\text{Frame size}}{\text{Bandwidth}}$ } fix




- every station starts transmission from start of its slot
- It says that if stations are ready with data, they have to wait for the required time slot & can transmit data exactly at the timeslot.

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

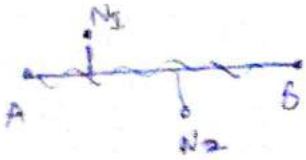
Vulnerable time = $T_t$

$S_{max} = 36.8\%$.

# • Carrier - Sensor Multiple access (CSMA)

If a station is ready with data, it senses the channel, & if channel found idle, data is transmitted, otherwise the station has to wait for random amount of time.

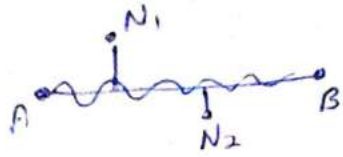
## 1 persistent




→ when A & B transmission stops without delay N1 & N2 starts transmitting.

• check again & again non stop if transmission stopped or not.

## 0- persistent




→ N1 & N2 fixes specific time duration after which they check if transmission stopped.

→

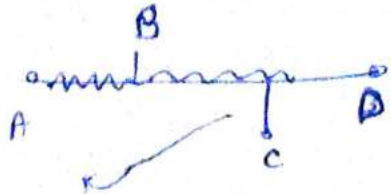
## P - peristent

is betn 0 & 1

P = probability they transmit or not with given probability P.

# • CSMA / CD (collision detection)

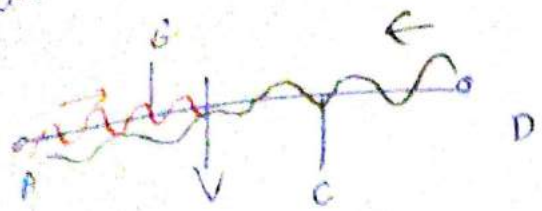
• we don't send acknowledgment, as it will increase collision




If again ack

So ↑ collision

⊙ to detect collision

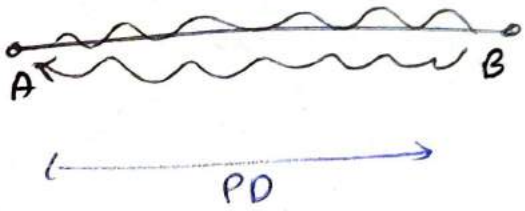



here collision occured

now since A received collided frequency ($\simeq$ combined) it tells collision occured.

So at given time of transmissim, if received data $\neq$ collision occured.

For detection




$Tt \geq 2 * PD.$

after this can't detect

$\Rightarrow \frac{\text{Length}}{\text{Bandwidth}} \geq 2 * PD \Rightarrow \boxed{L \geq 2 * PD * Bd}$

& $\eta = \frac{1}{1 + 6.44a}$ $\left(a = \frac{PD}{Tt}\right)$ $\left(PD = \frac{D}{V}\right)$

- Ethernet (wired) use CSMA/CD

Φ Consider CSMA/CD network that transmits data at a rate of 100 Mbps over 1 km cable with no repeaters. If minimum frame size required for this network is 1250 bytes. What is signal speed (km/sec) in cable?

100 Mbps = $100 \times 10^6$ (bits per sec) = $10^3$.

$TT \geq 2 * PP$

$\frac{L}{Bw} \geq 2 * \frac{D}{V}$ ⇒ $V = \frac{2 * D * Bw}{L}$

$V = \frac{2 * 1 * Km * 10^8}{1250 \times 8 \rightarrow bits} = 20000$ Km/sec

- **CSMA / CA (collision avoidance)**

used in WLAN (wifi)
↳ wireless Lan.

- uses ~~inter~~ frame space (IFS), where wait till no collision
- Uses acknowledgement.

some states → IFS, RTS (ready to send)
CTS (clear to send)

- collision window

# NETWORK LAYER

1) Host to Host data transfer
   (from one network to other)
2) uses IP address (logical address)
3) Routing → select path (use of Router & switch in network layer)
4) Fragmentation
5) Congestion control.

→ Packets delivery can be accomplished by using either a connection-oriented or a connectionless network service. In connection oriented protocol, the connection is established before sending packet. eg used in ATM.

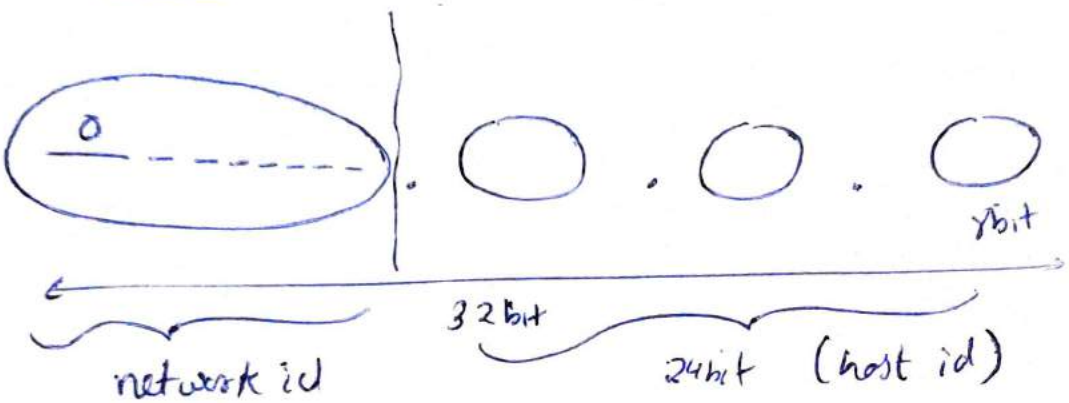
→ In connectionless protocol, network layer protocol treats each packet independently. The packets in message may or may not follow same path. used in Internet

# Classful addressing

- here for IPv4 (32 bit)
- uses Dotted Decimal format

IP address = network id + host id

## Class A

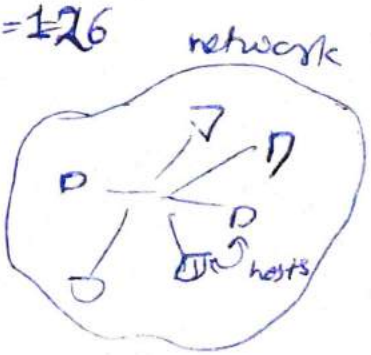



- Net id → 7bit $2^7$ 0 to 127

→ No. of Networks in CA = $2^7$ = 128

but 00000000 and 01111111 → so possible = 128 − 2 = 126

not given — for diagnostic




→ host possible = $2^{24}$

but in real = $2^{24} - 2$

eg → 64.0.0.0 → for representing network address of network

& 64.255.255.255 → for broadcasting within it's network

First host for network 64.0.0.0 ⇒ 64.0.0.1

Q find network address for 64.0.0.8

$\rightarrow$ <127 so class A

for class A mask = 255.0.0.0

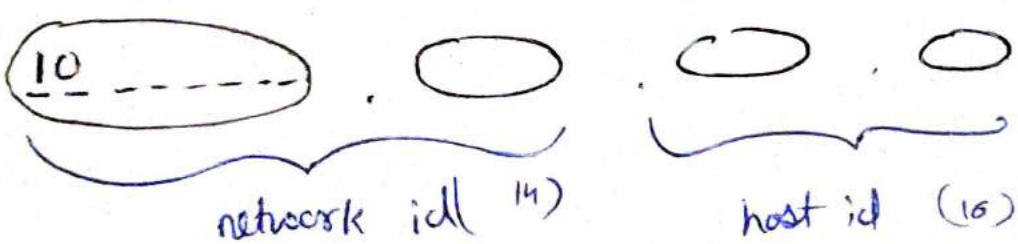
do and of given address with mask

get 64.0.0.0 network address

or basically ___.0.0.0
Net id

- All possible count of IP addresses
  only 1 bit out of 32 fixed so $2^{31}$ possible ways.

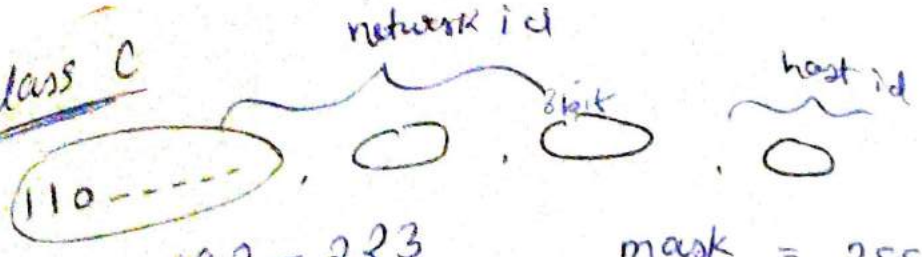
## Class B




- range → 128 – 191
- No. of address = $2^{30}$
- No. of networks = $2^{14}$
- No. of host = $2^{16} - 2$
- mask = 255.255.0.0

→ moderate count of host
So prefered in colleges, universities

- **Class C**




range = 192 – 223 mask = 255.255.255.

no. of networks = $2^{21}$

No. of hosts in each network = $2^8 - 2$

- **Class D**


range = 224 – 239

- No network, no host
- This class is reserved for multicasting, email/broadcast.

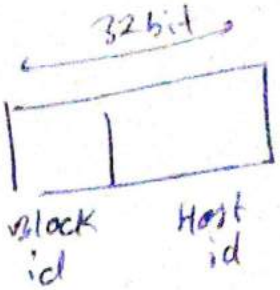
- **Class E**


- range → 240 – 255.
- no net & host.
  as reserved for military purpose.

⇒ So many reservation & thus so many ip address are getting waste.

→ Maintenance is time consuming

# Classless addressing



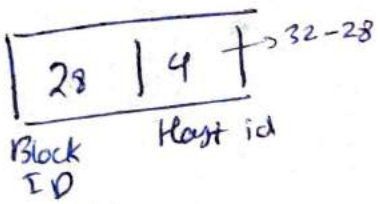

- no class, only blocks.

→ Notation

n.y.z.w /n → mask (no. of bit represent block)

eg 200.100.20.40 /28

So




- No. of host $= 2^4 = 16$

for network address, mask 28 bits

11111111.11111111.11110000

and 200. 100 . 20 . 00101000 (40)

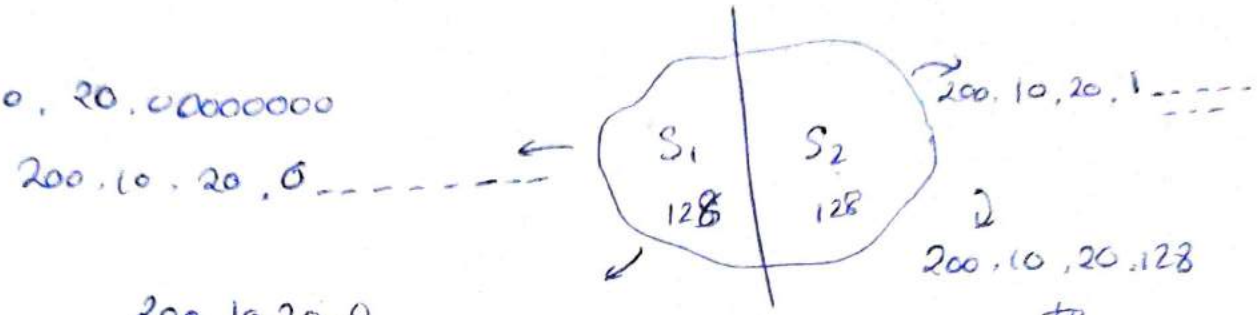
block id → 200. 100. 20. 32 /28

# Subnetting

- deviding the big network into small networks.

eg 200.10.20.0 class C
network

now
200.10.20.00000000




for $S_1$ valid ips = 126
but 2 again 1 for $S_1$ & .127 for broadcast
usable $S_1$ = 128 - 2 = 126

for $S_2$
200.10.20.128 represent $S_2$
& 255 broadcast
usable $S_2$ = 126 - 2 = 126

total = 252

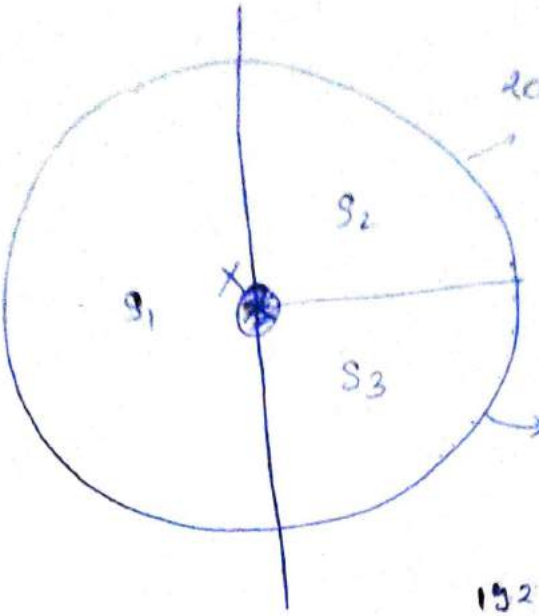
- for selling if $S_1$ or $S_2$.
So subnet mask.
1 bit reserved so
255.255.255.10000000

subnet mask
255.255.255.128.

→ All this task done according to class.

# Variable length Subnet masking (VLSM)

- to divide in 2 parts reserve 1 bit.




eg

200.10.20.0 ----

range

$S_1$
200.10.20.0
to
200.10.20.127
usable → 128-2 = 126

200.10.20.10 ----
128 ↔ 191
usable 64-2

200.10.20.11 ----
↑
2 bit reserved

192-255.
usable $S_3$
= 64-2
= 62

total = 126 + 62 + 62.

- X is router which use subnet mask.

for $S_1$ → 255.255.255.1 0 0 0 0 0 0 0 (1 bit fix)
= 255.255.255.128.

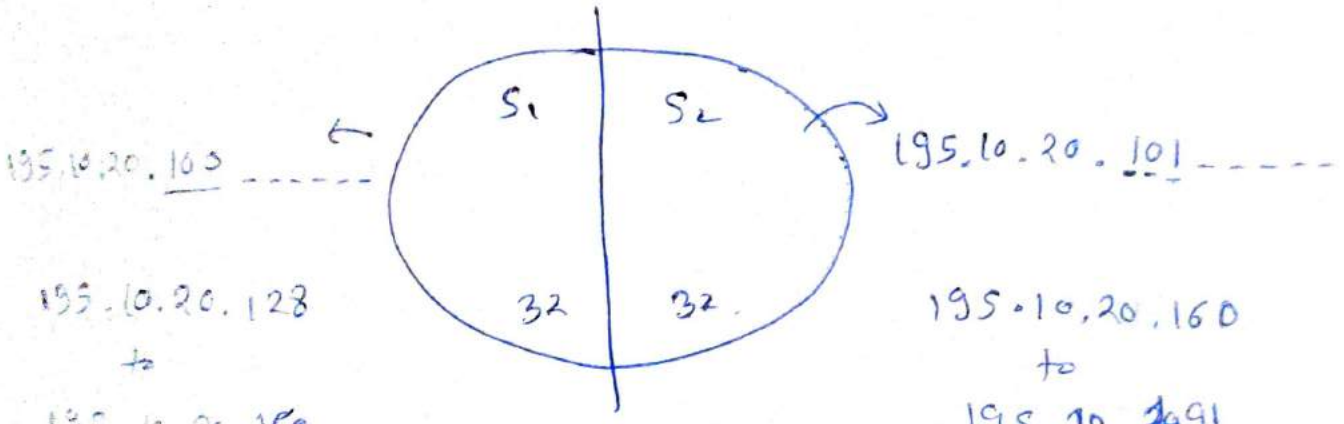
for $S_2$ 2 bit fix
$S_3$ 255.255.255.11 000000
= 255.255.255.192

# Subnetting in classless interdomain Routing (CIDR)

- given host id → convert to network id
- 195.10.20.129/26 → 195.10.20.128/26

195.10.20.10 000000
- 26 bit
- host id

for subnetting fix bits of host id.




mask

195.10. ⇒ 255.255.255.11 1 00000 /27

- of net id
- 1 bit fix of net
- /27 ↑ since 27 bits got fixed

= 255.255.255.224/27

- Can even do VLSM in CIDR

# IPv4 header

## About IP

- IP is a connectionless datagram protocol with no guarantee of reliability.
- It is host to host network layer delivery protocol designed for internet.

| VER 4 | HLEN 4 | Type of service (DSCP) 8 | Total length 16 |
|---|---|---|---|
| Identification bits 16 | | | Flag 3 / Fragment offset 13 |
| Time to LIVE TTL (8) | Protocol 8 | | Header checksum 16 |
| Source IP address 32 bits | | | |
| Destenation IP address 32 bits | | | |
| → options & padding | | | |

IPv4 header

Size → 20 – 60 bytes  payload = 0 – 65515 bytes

- only options & padding is optional.

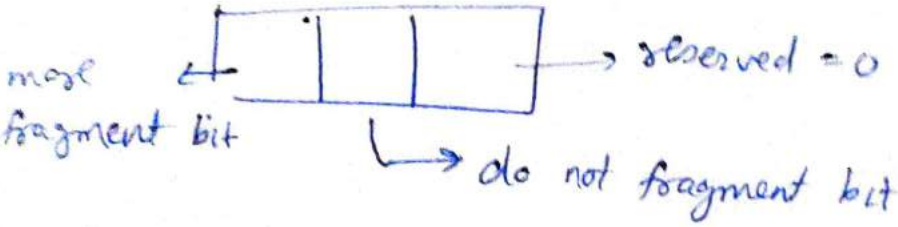
- Ver (version) : IPv4 (↓ 0100), IPv6
- HLEN (Header length) : length of datagram, multiple of 4, (multiply by 4) → max 1111 = 15, max size 15×4 = 60
- DS (Differential service) : defines class of datagram for quality of service

- Total length :- defines total length of IP datagram. total length includes length of header as well as data field. ( max $2^{16}-1$ = 65535 )

- Identification, flag & offset :- defines in fragmentation.

→ Identification : When datagram is fragmented, value of identification field is copied to all fragments. Identification number helps destination in reassembling fragments of datagram.

→ Flags.




→ offset → Shows relative position of this fragment with respect to whole datagram.

- TTL :- controls maximum no. of routers visited by datagram. Helps in preventing congestion

- Protocol :- defines higher-level protocol used with IP eg TCP/IP

- header checksum :- error prevention.

C

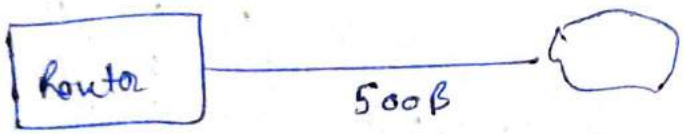
- options & padding :- optional, used for network testing & debugging

→ IP provides several optional features, allowing packets sender to set requirements on path it takes, trace route a packet takes & label packets with security features.

Q A datagram of 3000B (20B of IP header + 2980 IP payload) reached at Router & must be forward to link with MTU of 500B. How many fragments will be generated & also write MF, offset, total length of all.

Datagram ← header
← data (payload)

we need to send 2980 data & medium can handle 500B.




480B + 20B
header

So no. of fragments = $\left\lceil \frac{2980\,B}{480\,B} \right\rceil$ = 7 pack

| $P_7$ | $P_6$ | $P_5$ | $P_4$ | $P_3$ | $P_2$ | $P_1$ | ← Total length | ← More fragment flag |
|---|---|---|---|---|---|---|---|---|
| (100+20) | (480+20) | (480+20) | (480+20) | (480+20) | (480+20) | (480+20) | | |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | | MF |
| ← packet 360 comes after P7 so MF=0 | 300 | 240 | 180 | 120 | 60 | 0 | | ↑ if any packet is follow then MF = 1 |

480 + 480 / 6 → 120

↑ offset

Eg $P_2$ को before 480 data
normalize by 8 (always)
480/8 = 60

# IPv6

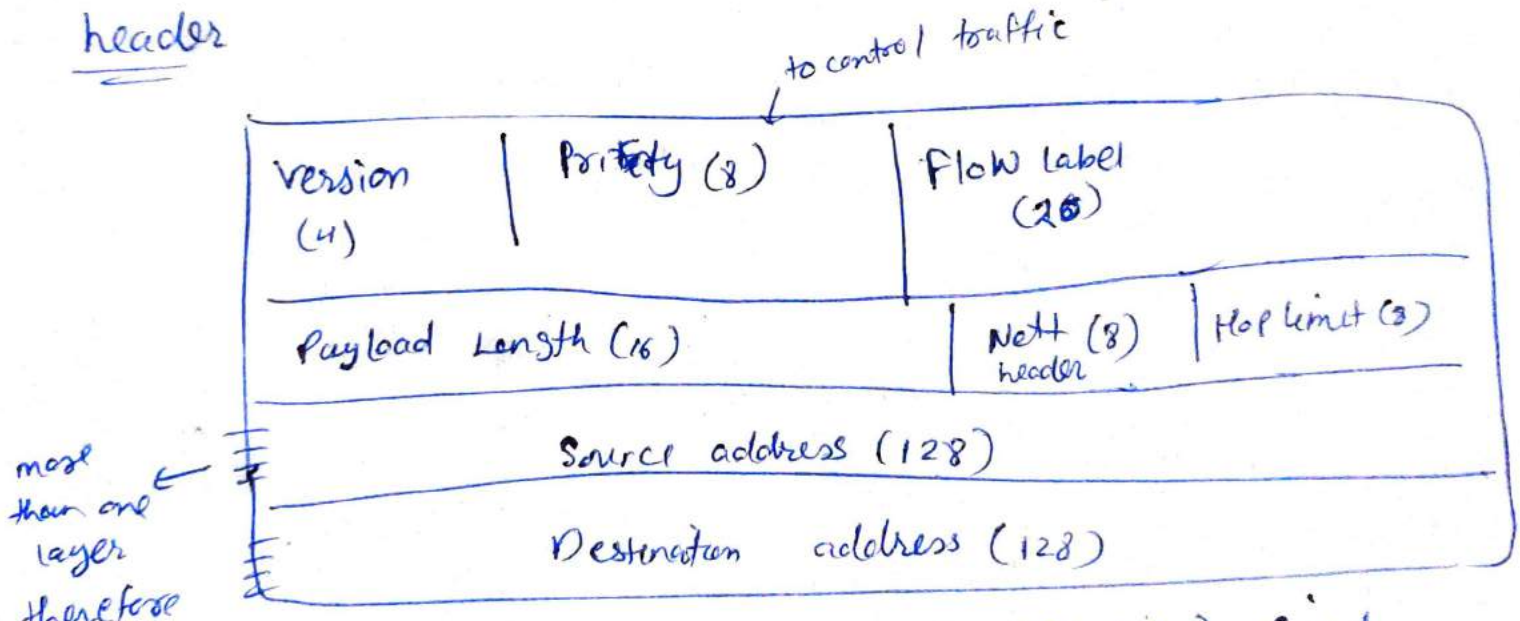
- due to increase in demand of IP addresses, we need more IP address so used IPv6.
- 128 bit address space
- is hexadecimal format

eg AC81 : 9840 : 0086 : 3210 : 000A : BBFF : 0000 : FFFF

0086 → drop, 000A → drop, 0000 → drop

can drop consecutive 0's.

## header



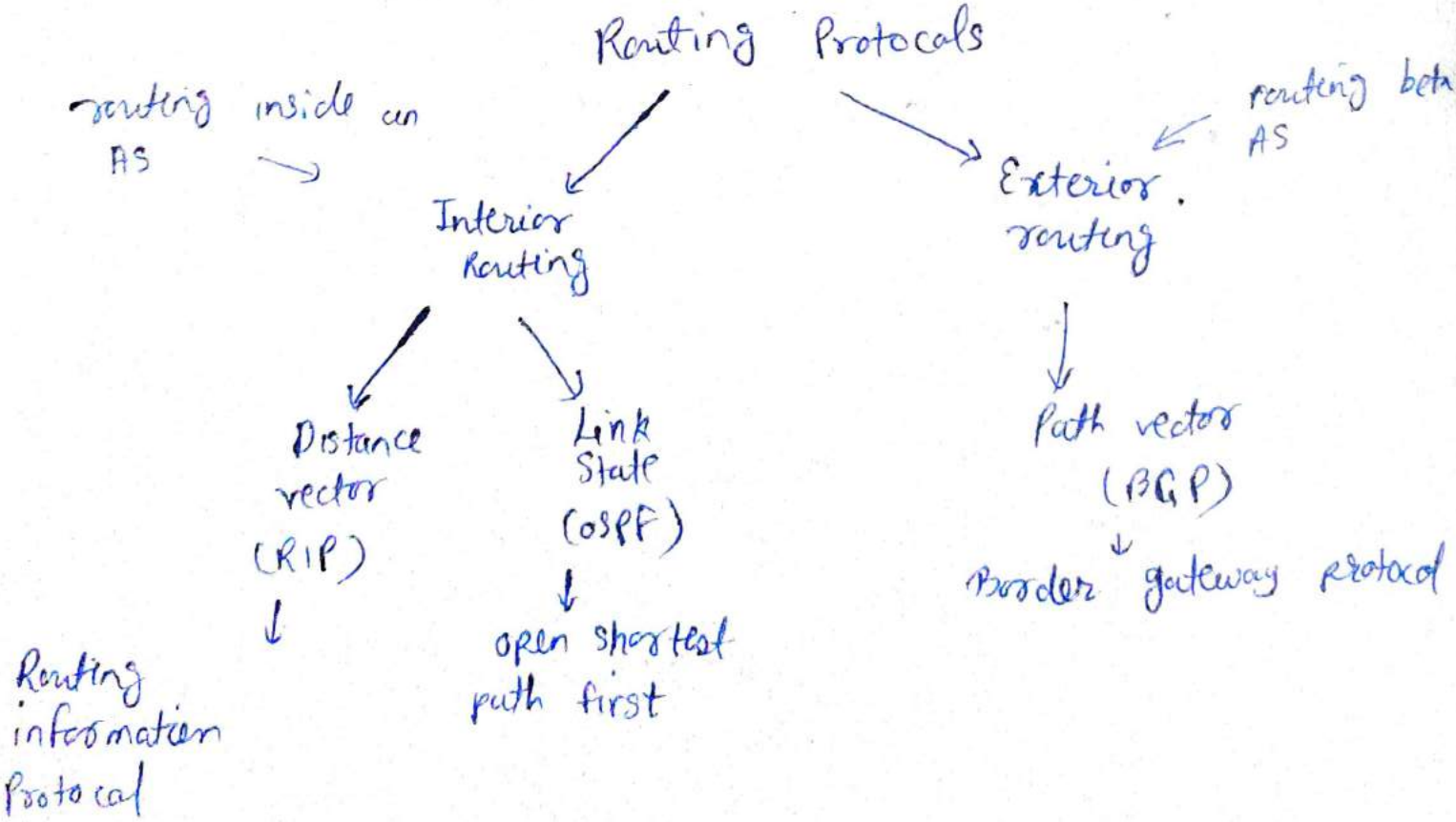

- Header size = 40 bytes (320 bits) fixed.

# • Routing & its protocals

routing :- deciding route which packet travels to reach destination.
done by using routing table.

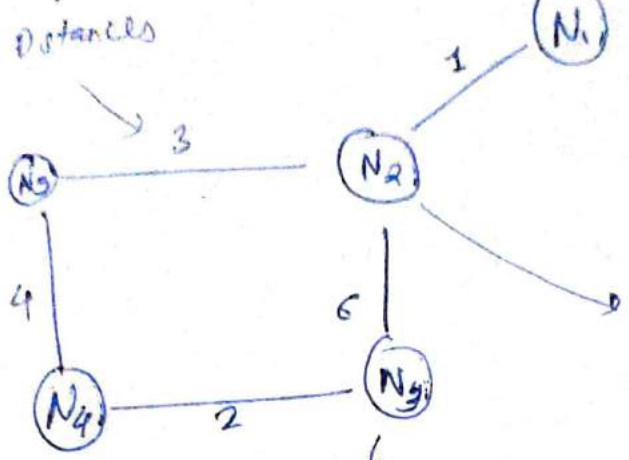
• descised below protocals are for unicasting.
In unicast routing there is one source and one destination and relation betn source & destination is one to one.

⇒ An internet is so large that one routing protocal can not handle task of updating routing tables of all routers.
⇒ So an internet is devided in autonomous systems (AS) which is a group of networks & routers.



# RIP
## Distance vector routing (DVR)

at first round




Same for N5 & N4

| Destination | Distance | Nxt |
|---|---|---|
| $N_1$ | 0 | $N_1$ |
| $N_2$ | 1 | $N_2$ |
| $N_3$ | ∞ | – |
| $N_4$ | ∞ | – |
| $N_5$ | ∞ | – |

if no direct path so at first round distance = ∞.

| Dest | Dist | Nxt |
|---|---|---|
| $N_1$ | ∞ | – |
| $N_2$ | 6 | $N_2$ |
| $N_3$ | 0 | $N_3$ |
| $N_4$ | 2 | $N_4$ |
| $N_5$ | ∞ | – |

| Dest | Dist | Nxt |
|---|---|---|
| $N_1$ | 1 | $N_1$ |
| $N_2$ | 0 | $N_2$ |
| $N_3$ | 6 | $N_3$ |
| $N_4$ | ∞ | – |
| $N_5$ | 3 | $N_5$ |

routing table

- for 2nd round all nodes will share only Distance vector with their neighbours

eg $N_1$ will share with $N_2$ its distance vector, $N_2$ will share with $N_1$, $N_3$, $N_5$.

- $N_2$ gets from $N_2$ table for $N_1$

| $N_2$ |
|---|
| 1 |
| 0 |
| 6 |
| ∞ |
| 3 |

$N_1 \to N_2 \to N_2$ ≡ $N_2$ (1 + 0)

$N_1 \to N_2 \to N_3$ (1 + 6) ← $N_3$

$N_1 \to N_2 \to N_5$ ← $N_5$

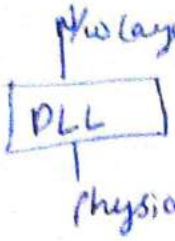
| Destination | Distance | Nxt |
|---|---|---|
| $N_1$ | 0 | $N_1$ |
| $N_2$ | 1 | $N_2$ |
| $N_3$ | 7 | $N_2, N_3$ |
| $N_4$ | ∞ | – |
| $N_5$ | 4 | $N_2, N_5$ |

for all tables do this

Parth Sir class notes

# Data link layer

In data link layer data is called → Frame — header, Data




DLL (2 layers) — Logical Link control LLC
— Medium access control (MAC)

- **Services** :

1) Framing
2) Unacknowledge connectionless (with ack packet & no special connection made in advance both two before message trasfer)
3) acknowledged connectionless
4) acknowled connection oriented
5) Addressing.
6) Error control
7) flow control (speed of transfer)
8) Medium access control

} 3 are services

others are functions

- Addressing (link layer address)

MAC / physical address ⇒ 48 bit

24 bit (org. unique identifier) ↳ IEEE

24 bits (organization assigned by company)

3) Error control

↳ Error detection → cyclic redundancy check (CRC) * polynomial code * in H/w
→ checkSum (in software)

↳ error correction

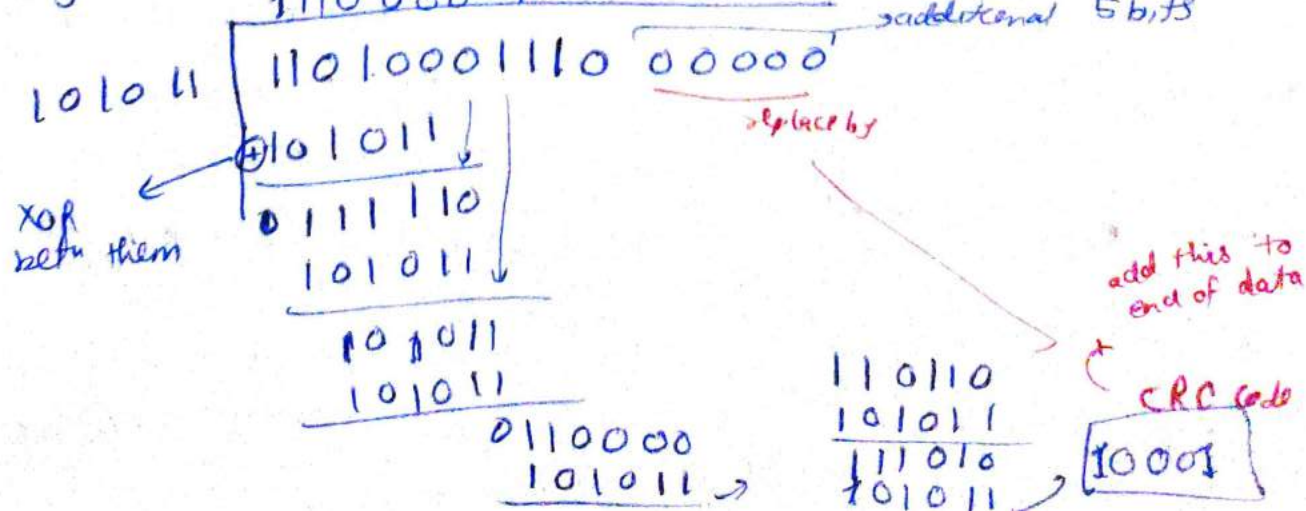
for error detection send some extra bits eg sum of digits, or number of occurance of 1 etc, and at receiver end calculate it & check again. if equal so no error else you detect an error & notify sender.

- **Cyclic Redundancy check (CRC)**
  - frame content (actual data)
    ⇒ 1101011110 (11 bit)
  - Generator (known to sender & receiver)
    ⇒ 101011 ⇒ $x^5 + x^3 + x^1 + 1$
    5 4 3 2 1 0

(if x5 (6 bits divisor) So extra bits added = 5)

Additional data size ⇒ 5 bit (max degree of generator)
Should be less than 50% of size of original data.

to get original data



- MTM uses CRC-16 $(x^{16} + x^{13} + x^2 + 1)$
  IP use CRC 32 $(x^{32} + x^{24} \ldots$
  other is CRC-CCITT ?

$x^{32} \rightarrow$ uses 32 flip flop in designing

CRC 32 uses 32 flip flops

CRC detects
1) Single bit error
2) burst error of length <= size of frame check last (eg = 5)

CRC only detects

## LLC

- Error correction technique

→ additional data
→ size of additional data
→ position of additional data

m → message's size
r → redundancy / checkbit / parity
n = m + r (code word)

datalink gets n & sends m to network layer

Hamming code

use hamming distance to see bits changed.

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

Hamming distance

$C_1 \rightarrow 1\,0\,1\,0\,1\,0\,1$
$C_2 \rightarrow 1\,0\,1\,0\,0\,1\,1$
xor → Sum 0 0 0 0 1 1 0

2 bits 1
hamming distance = 2

given $m = 1010$

Find size of r

$4 + r + 1 \leq 2^r$

$r + 5 \leq 2^r$

put $r = 3$

$r = 3$

$m + r = 7$

$n =$ _ _ 1 _ 0 1 0 ← actual data

① ② 3 ④ 5 6 7 → powers of 2

this bits are reserved for parity bits

1 2 3 4 5 6 7

for bit 1 → 1 3 5 7 → take 1 leave 1 take 1 leave 1

for bit 2 → 2 3 6 7 → 2 3 4 5 6 7 take 2 break of 2

4 → 4 5 6 7 → 4 5 6 7 — break of 4 — take 4 as present

- Now let even parity

for bit 1 → 1 3 5 7

add 1 to make even parity → 1 1 0 0

- for bit 2 → 2 3 6 7

for even parity → 0 1 1 0

- for 4th bit → 4 5 6 7

1 0 1 0

so $n =$ code ward $= 1\ 0\ 1\ 1\ 0\ 1\ 0$ (r, m)

at receiver, it removes parity bits & again ~~check~~ calculate all parity bits.

if some error from received one then error occurs. take intersection & see which unique bit is present in wrong ans received bit where

$m = 1010$

- Hamming code

can correct single bit error only.
It can only detect burst error.

eg K → 1 0 1 1 0 1 0 (even parity)
1 2 3 4 5 6 7

① 1 3 5 7 ⇒ 1 + 0 + 0 + 0 ⇒ 1 ✗
② 2 3 6 7 ⇒ 0 + 0 + 1 + 0 ⇒ 1 ✗
③ 4 5 6 7 ⇒ 1 + 0 + 1 + 0 ⇒ 2 ✓

common bcth them = 3 ✓

if in 5, 6, 7 error would have occured it would be seen in ③rd also but not present so in 3 only.

## Error Control

Errors Detection → CRC - implemented in hardware

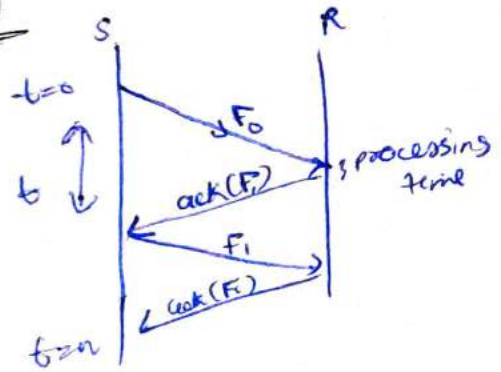
errors correction → Hamming code

# Flow control

to have efficient connection
sender speed of transmission should ideally be equal to receiving speed of receiver.
if sender speed is more, some frames will be lost at receivers end.

→ Stop & wait (SW)
→ Sliding window (SLW)

## ① SW




Round trip propagation delay

wait for acknowledgment

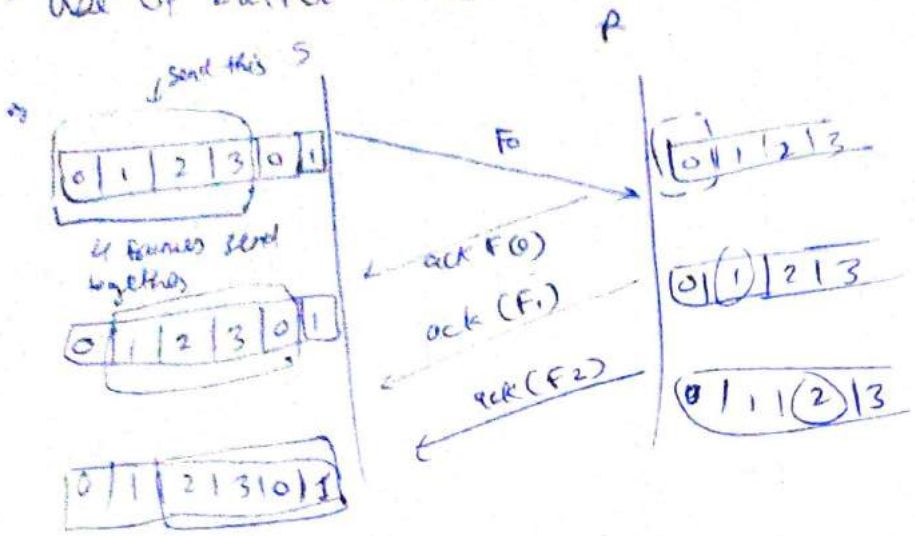
- Transmission time (TT) = time to send frame onto the link = $\frac{\text{Frame size}}{\text{Bandwidth}}$ → capacity of channel

- Propagation Time (PT) = $\frac{\text{distance}}{\text{speed}}$ → $2 \times 10^8$ m/sec

time of travelling in link

## SLW

- better than SW as lesser time wastage. or better link utilization
- in place of single frame, a collection of frames is send.
- use of buffer at receiver.




eg transmission speed = 50 kbps.

Round trip propagation delay (RTPD) = 500 msec

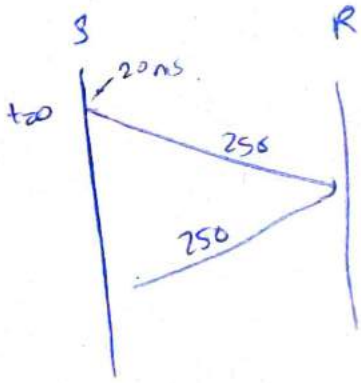
Size of Frame = 1000 bits

**SW** (stop wait)

$TT = \frac{1000}{50 \text{ kbps}} = 20 \text{ ms}$

$PT = 250 \text{ ms}$.

↓ half of RTPD




total time = 20 + 250 + 250 = 520

wastage (usage here) $\frac{500}{520} = 96\%$.

in Ethernet → half duplex (Bus topology)

→ full duplex (flow control is optional)

now we have 2 channels & can send data & ack together

$\frac{\text{data (frames)}}{\text{control (ack)}}$ → called piggybacking

# ARQ (Automatic repeat Request)

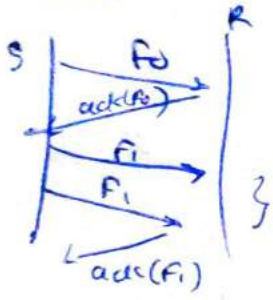
Error correction → forward (Hamming code)
→ Backward (ARQ)

Differ in window size:
1) Stop & wait ARQ
2) Go Back (N) "
3) selective Repeat ARQ

1) handles
- lost frame
- lost ack & damaged frame
- delayed ack

## ① Stop & wait ARQ

window size Receiver & sender = 1




} not received ack within threshold time resend.

## ② Go Back N

Sender window = $2^k - 1$ receiver window = 1

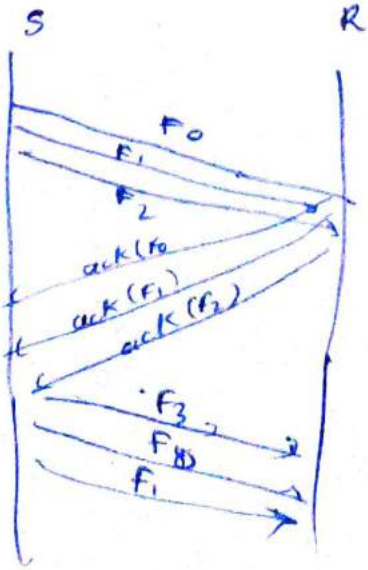
K = sequence no. alloted.

Let k = 2

w = 3

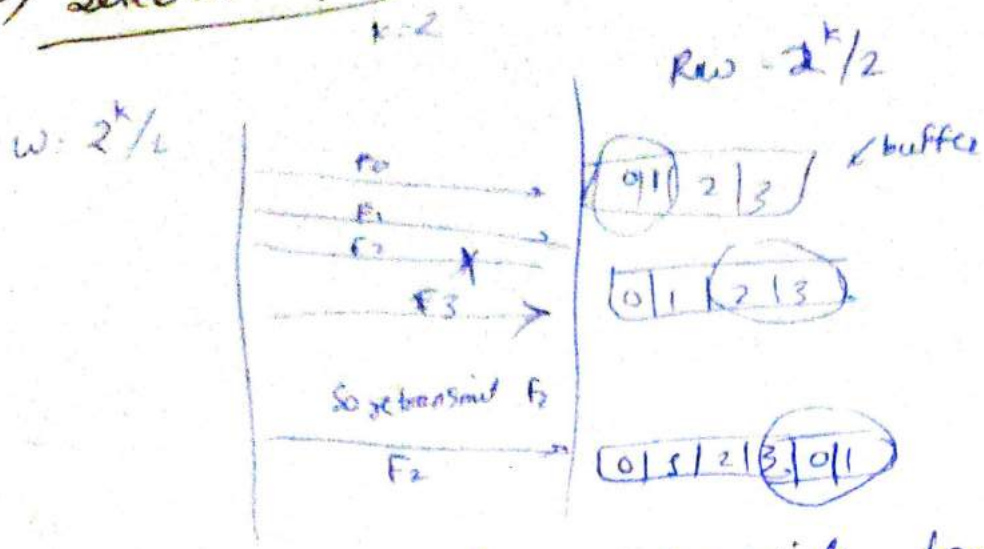

Send 3 windows without waiting ack

move window when receive ack. of all




- if not received all 3 acknowledgment
- Let ack($F_2$) is lost Send starting from $f_2$ again. If at given time other frames were send discard them.

## 3) selective repeat




- on receiving both only window slide, from buffer frames send to memory.
- window ≡ buffer

- link → point to point
- link → broadcast (much collision)

- Ethernet (half duplex) is like broadcast.
- Bus, ring topology ≡ broadcast
- Satellite communication is also broadcast

- Who is going to access shared medium

Who → centralized / distributed

How → Synchronous (Tight coordination) (Fixed pattern) → FDMA / TDMA
How → Asynchronous → STDMA

MAC protocol
- fixed Partitioning — FDMA
  - TDMA
- Random Access — Aloha
  - CSMA/CD
- Reservation — Bitmap
  - (Binary counter)

1) ALOHA

- Pure (unslotted) ALOHA : simpler, no synchronization.
- pkt needs transmission :
  - Send without awaiting for beginning of slot
- Collision probability increase.

- $P^{pure}$ (success by given node) = P (node transmits) ·
  P(no. other node transmits in $[p_0-1, p_0]$) ·
  P(no other node transmits in $[p_0-1, p_0]$)
  $= p(1-p)(1-p)$

- Slotted aloha
  - time is devided in equal slots
  - node with new arriving pkt : transmit at beginning of next slot.

2) CSMA (carrier sense multiple access)

- CSMA - Listen before transmit
- If channel sensed idle : transmit entire pkt
- If channel sensed busy; defer transmission
  - Persistent CSMA : retry immediatly with probability p when channel becomes idle
  - Non persistent CSMA : retry after random interval.

CSMA / CD

detect the collision


Half duplex

transmission time = 2t → t : propagation delay

if $TT > 2(P.T)$

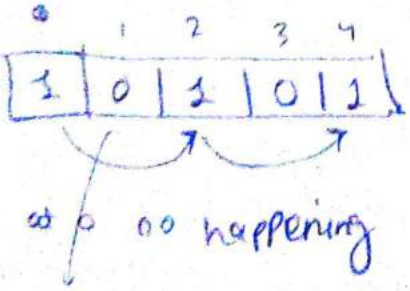
so collision has occured. can be detected if this condn is satisfied.

- in transmission period during CSMA/CD no collision
- collision in contention period

⊙ Ethernet ✓half duplex ⇒ IEEE 802.3 use CSMA/CD

now we use WLAN (Full duplex)

- **Bitmap**
- is reservation type
- to avoid those collision during contention period (CP) we are using reserve band.




- good at high load
- bad at low load (↓ efficiency)

- Problem with wireless connection

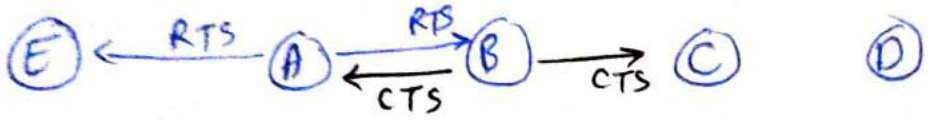
1) reflection 2) absorption 3) Interference

for wireless we use ↑ CSMA/CD can't work due to this

CSMA / CA ( collision avoidance )

RTS → request to send
CTS → clear to send

⇒ before sending data control frames (RTS, CTS) are send.




B told I am receiving data (CTS) from A so don't send me data hence collision is avoided.

- DCF (distributed control function)

PC → point coordinator (master slave) : master decide whom to transfer.

## 802.11 Frame
### for wireless communication

have frame control
Duration
Address
sequence control
Data
FCS.

MACA → multiple access ^ collision avoidance

MACAW → multiple access collision avoidance with acknowledgement

# 802.11 Frame

| Bytes | 2 | 2 | 6 | 6 | 6 | 2 | 0-2312 | 4 |
|---|---|---|---|---|---|---|---|---|
| | Frame control | Duration | Address 1 (receipient) | Address 2 (transmitter) | Address 3 | Sequence | Data | Check Sequence |

- 802.11 allows frames to be fragmented, each with its own checksum.

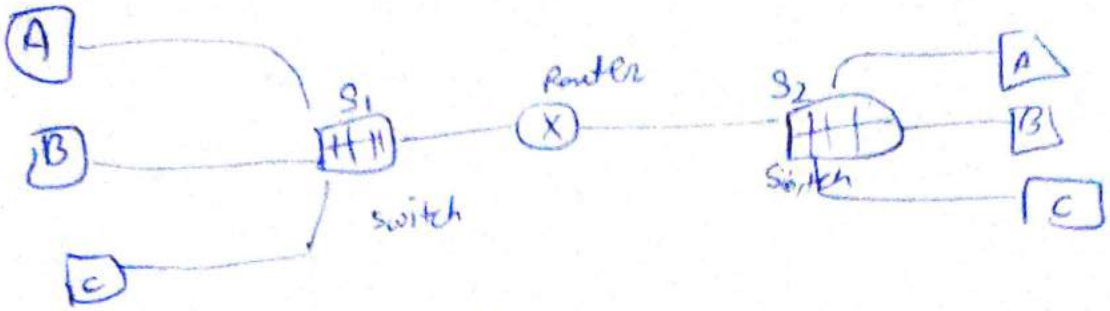
- DCF → fragmentation of frames.
- Fragments are individually numbered & ACKed using Stop-and-wait protocol.
- Once channel has been acquired using RTS & CTS, multiple fragments sent in a row.
  - Sequence of fragments called fragment burst.
- fragmentation increase the throughput.

PCF (point coordination function) mode

→ Base station polls other stations, asking if they have any frames to send.
Since centralized station, so no collision ever occur

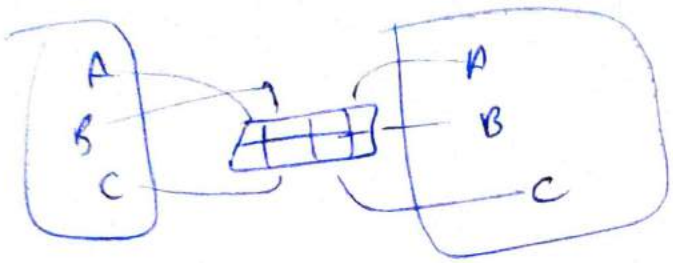
→ Base station broadcasts beacon frame periodically. Beacon frame consists of
  - hop sequence
  - dwell time (for FHSS), clock synchronization etc.

# Virtual Lan




very costly

- we can decrease cost by joining all in one switch




here comes concept of virtual LAN.

VLAN frame
802.1 $Q_5$
(42 - 1500)

VLAN used to partition network in same network.