IP-add-on Network layer

Computer Network

classmate
Priyal Patel

- **Physical Layer** – bits are converted into signals.
- **Computer Network** – Collection of autonomous computers inter connected by a single technology where interconnection means that they are able to exchange the information.

Uses: – Business (Resource sharing), home, Mobile, Social issues

- Business → Client-Server architecture
  - client – request
  - server – reply for the service
- home → all day-to-day e-commerce related operations.

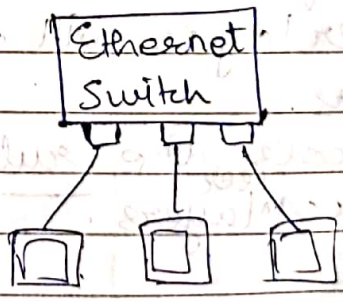
- **Network Hardware:**

(1m) PAN (Personal Area Network) eg:- Bluetooth

10m	Room	Local Area Network
100m	Building	
1 KM	Campus	
10 KM	City	Metropolitan Area Network
100 KM	Country	WAN (Wide Area Network)
1000 KM	Continent	

LAN :-

802.11



Ether (wire)

802.3
802.4
802.5
} Ethernet

802 (IEEE std for defining any network)

802.11 (a), (b) (c), (d), (e) (wireless)

Date ____
Page ____

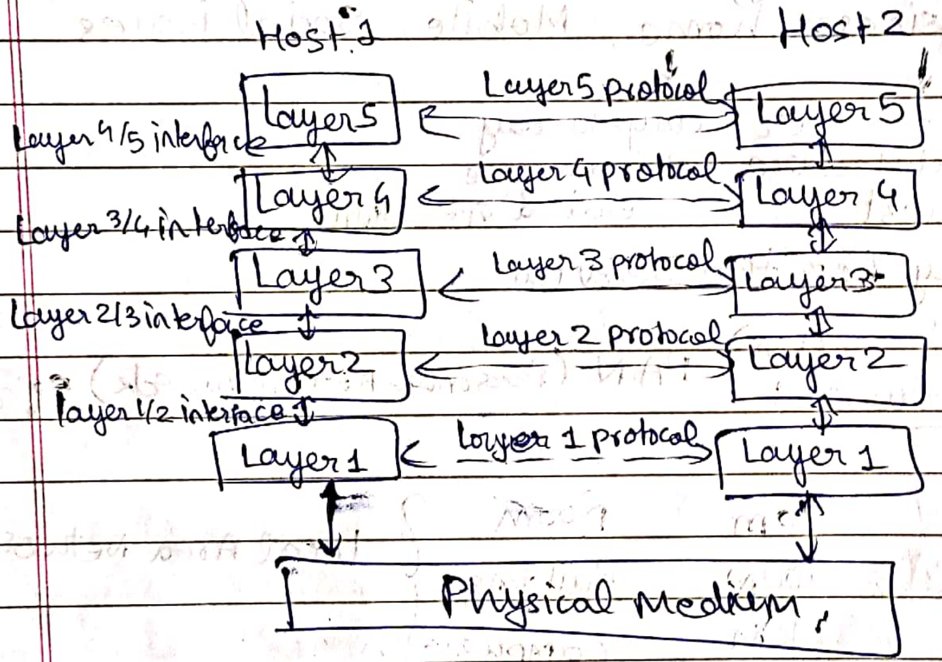
★ (LAN - Switch)

→ WAN - By default it is Router

- Network software :- a) Protocol hierarchies
  ★ b) Design Layer Architecture

- It is a 5 layered architecture.

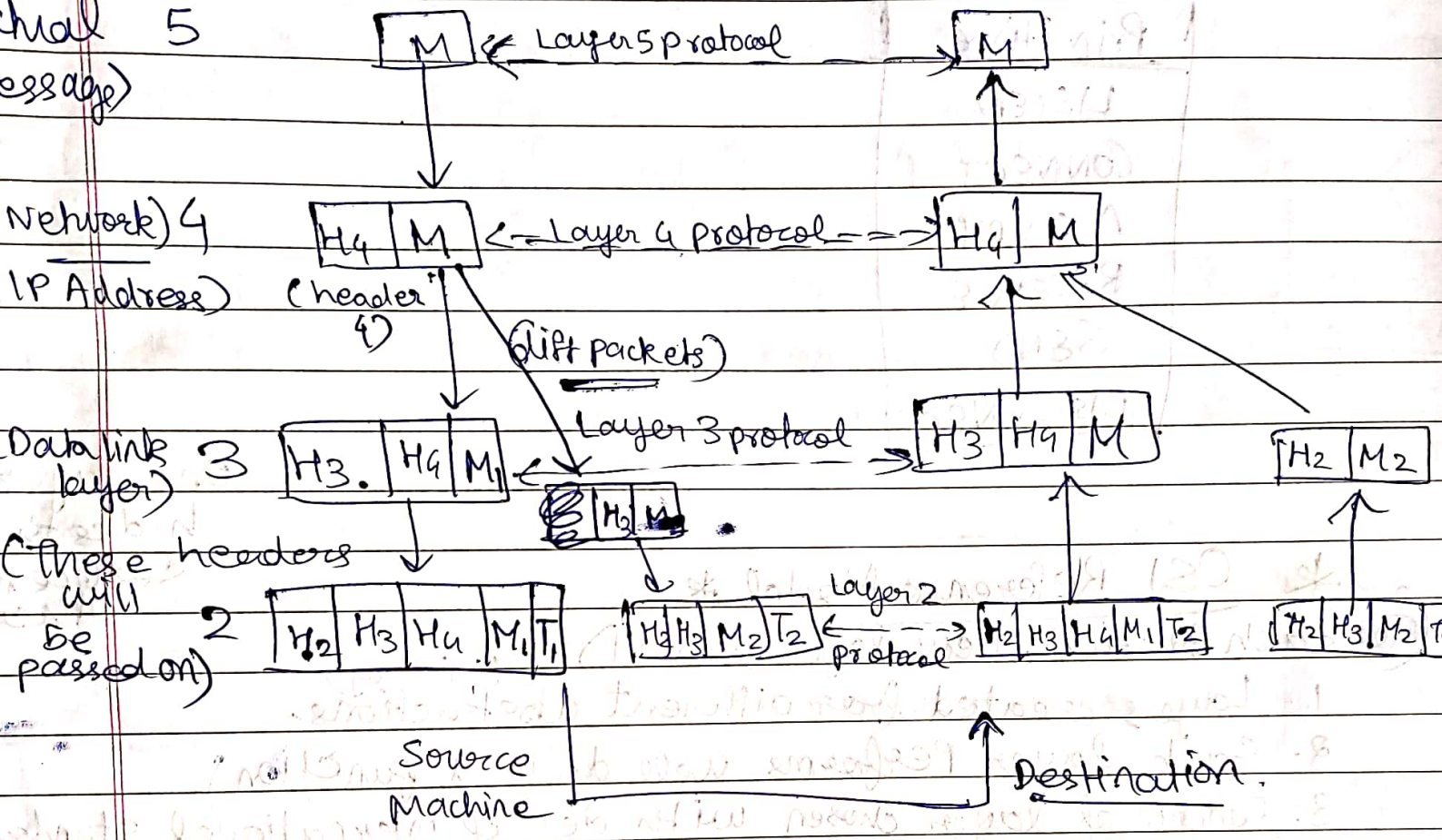
dotted arrows mean virtual communication



- Every Layer has its own seperate & unique functionality which can't merge with each other.

- Interface is also called SAP (Service Access Point)
- Lower Layers will always provide service to upper layers.
- Protocols are rules to handle communication between peer layers.

Layer



* Tail - Error Detection & Correction info.

⇒ Layer 5 Architecture — Both architectures are Compulsory

	Service	Eg
Connection oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection.	Voice over IP
Connection less (UDP) (VS)	Unreliable datagram	Electronic junk mail.
	Acknowledged datagram	Text Msg
	Request-Reply.	Database query.

Service Primitives

Primitive
LISTEN
CONNECT
ACCEPT
RECEIVE
SEND
DISCONNECT

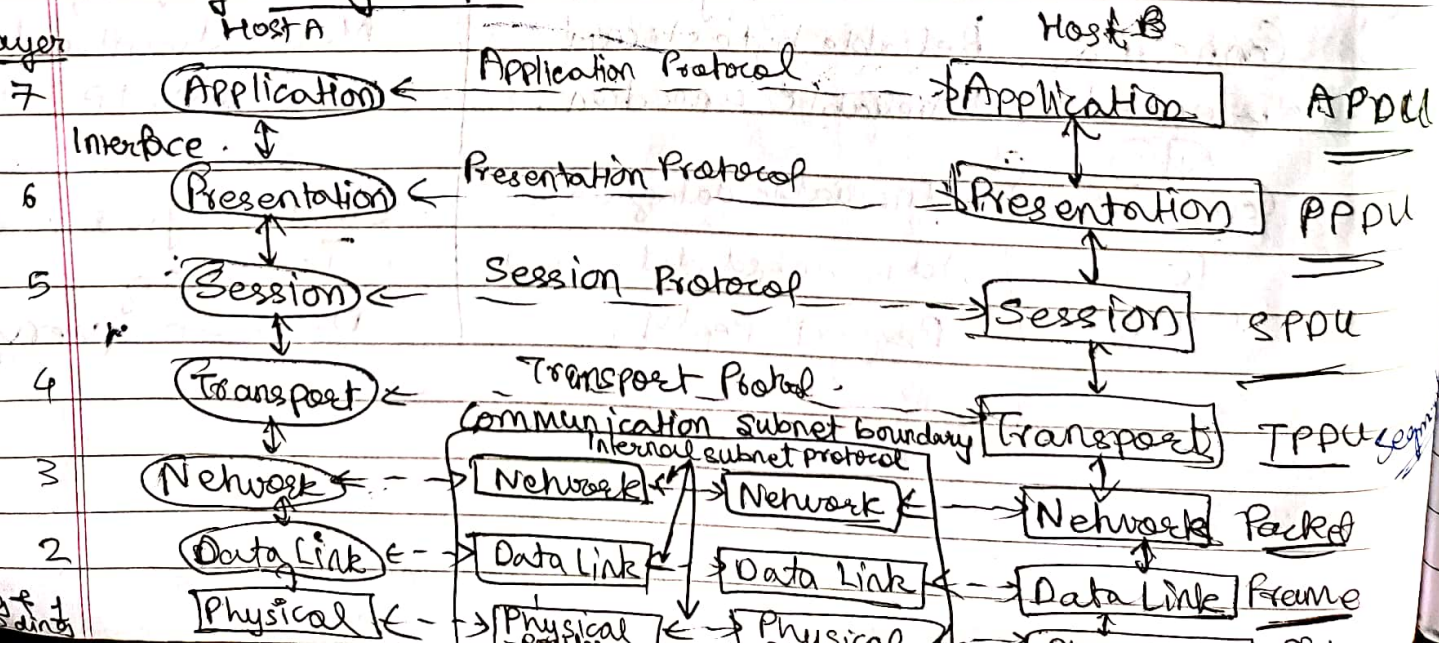
One layer hides the service from offers.

* OSI Reference Model *

(for each function, new layer created) (hiding)

1. Layers created for different abstractions.
2. Each layer performs well defined function.
3. Function of layer chosen with def. of international standard protocols in mind
4. Minimize info. flow across interfaces between boundaries.
5. No. of layers optimum.

* Diag very imp *



- Network Layer :- (i) Routing (ii) Congestion Control (CC) (iii) IP addressing (iv) QoS (Quality of Service) (based on application)

Routing, Congestion control, IP addressing, QoS

- Transport Layer :- (i) Port Addressing (ii) Error handling (iii) Flow Control (NOT Congestion)

↳ & DLL has same functions

it is our interface so it has to provide

* If we don't cross the network layer, then the errors that occur in the middle will be handled by Transport layer.

→ Port Add. { memory location at which that particular process / service is residing.

- 0 to 1023 are reserved for some other applications.

Networ

* Rem :- DLL provides node-to-node, hop to hop delivery

* MAC (Medium Access Control) *

- imp function dealing with physical addressing (MAC add.)

2 Protocols :- (a) ALOHA (b) CSMA/CD (Carrier Sense Multiple Access Collision Detection)

These functions are performed by LLC :-

Protocols :- (i) Stop & Wait (ii) sliding window

→ HDLC & PPP (in DLL)

* Flow control (Fast sender, slow receiver) - to handle we have diff mech in DLL

* Error control (3rd Func.) - Hamming code, CRC, Checksum

2 sub layers - LLC & MAC. Framing, character count, byte stuffing, bit stuffing

→ electrical & mechanical specification of bits. ...

→ Upto session, all the rules are decided / handled by Application. For the lower layers, they are governed by the Operating System.

o Functions of Application, Presentation & Session Layer:

(1) Session Layer handles session management by providing authentication for the session, authorization & checkpoint facility.

(2) Presentation Layer:- a) Translation i.e. code conversion characters & numbers are converted into machine understandable format. (b) Encryption (c) Decryption & (d) Compression of the data.

(3) Application Layer:- It provides network applications such as web browser & the protocols such as ftp, http & serves as the interface between the user and the network.

* Flow control in : DLL - Fast machine within one network, slow router

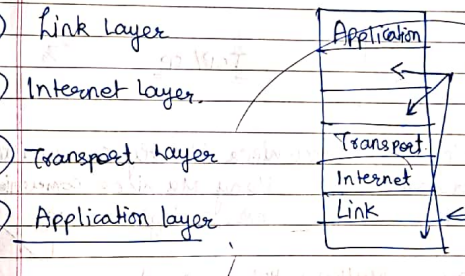
: Transport :- Fast machine in a particular network to slower receiver machine in some other network.

(Transmission Control Protocol) / Internet Protocol

⇒ OSI is a Model. TCP/IP are basically protocols.
↓ 7 layers ↓ 4 layers

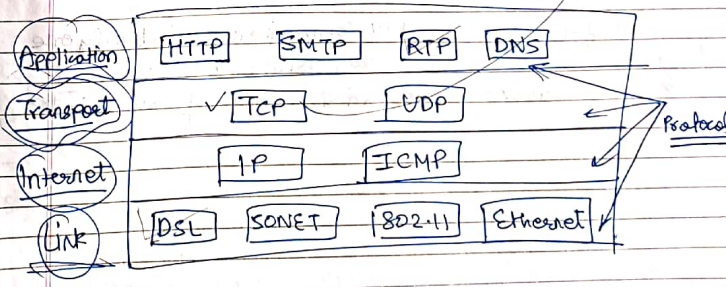
The 4 layers are :-

a) Link Layer
b) Internet layer.
c) Transport layer
d) Application layer



⇒ OSI Supports connection-oriented protocol. TCP/IP at Transport layer provides both connection oriented & connectionless facilities.

⇒ Link layer - Network Interface layer but does not support error & control



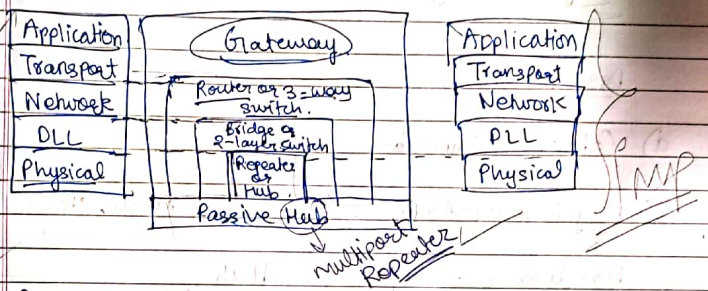
- Internet Control Message Protocol
- Reverse Address Resolution Protocol (ARP) & (RARP)
- UDP (User Datagraph Protocol)
- SMTP (Simple Mail Transfer Protocol)

Differentiate:	OSI	TCP/IP

Point-to-Point – 2 machines directly communicating
* Multipoint Configuration – Many machines communicating over a single server.

* Tree Topology – Multiple Hubs connected.
* Bus Topology –
* Ring
* Hybrid – Combination of diff. Topologies.

- Simplex – One sender – One receiver
- Half-Duplex – 2-way communication, but only one way possible at a time
- Full-Duplex – both can simultaneously communicate



→ Repeater – Amplifies the signal

→ Broadcasting – One to All (Getting data from)

Gateway → Connects 2 Networks together

→ Hub – works by broadcasting

→ Switch – Similar to hub (intelligent hub) as it is present in the next layer. It doesn't forward the data by mere broadcasting but it has a database & will forward the data to selected machines only and thus it is better than hub. Hub unnecessarily increases the traffic.

→ Bridge – Similar to switch but connects only similar networks (eg: Ethernet to Ethernet) (DLL functionality)

→ Router – Unlike bridge, will work with different technologies also. (Network layer)
(Its own OS, table, Routing Algorithms)

→ Application Gateway – takes care of protocol translation.

* Physical Layer *

Design Issues :-

a) Cables & Connectors

b) Physical Topology - Ring, Star, Mesh, etc.

c) Hardware - Repeaters, Hub (eg:- Star (One-to one, but transfer to all))

d) Transmission mode ⇒ Simplex, Half Duplex, Duplex

e) Multiplexing (FDM - tv channels) (TDM)

f) Encoding

→ Circuit Switching - Fixed circuit connections are established.

→ Packet Switching - No fixed connection, reduces wastage of time, multiple packets transferred. (least transmission delay)

→ Message Switching - Entire msg is transferred all at once.

→ they can use any path, and have the destination IP (even if the router is down)

* Transmission Media :-

a) Guided Media

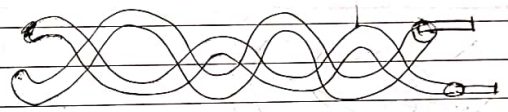
(i) Twisted-pair cable. - UTP (Unshielded) (TP), STP (shielded)

(ii) Coaxial Cable.

(iii) Fiber-optic cable.

TP Cable

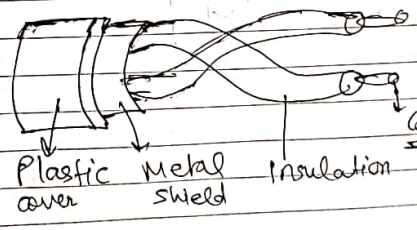
100Hz — 5MHz



⇒ Effect of noise on Parallel Lines. → one is sender, one is grounded

⇒ because of twisting, noise effect gets nullified.

⇒ UTP Connectors - 4 Conductor, 6 Conductor, 8 Conductor

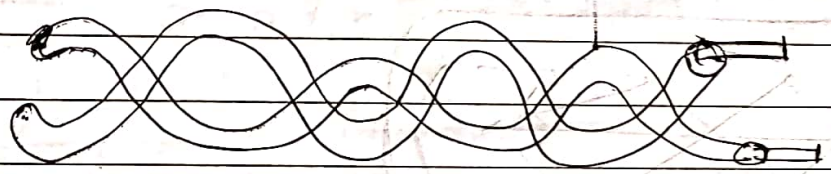


* Transmission Media :-

a) Guided Media

(i) Twisted-pair cable. (TP) – UTP (Unshielded), STP (Shielded)
(ii) Coaxial Cable.
(iii) Fiber-optic cable.

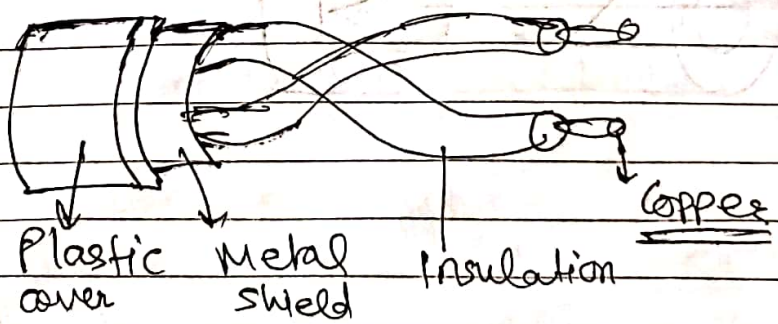
TP Cable
100Hz — 5MHz



⇒ Effect of noise on Parallel Lines. → one is sender, one is grounded

⇒ because of twisting, noise effect gets nullified.

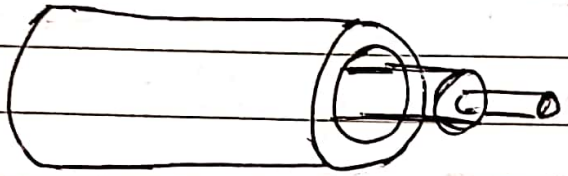
⇒ UTP Connectors – 4 Conductor, 6 Conductor, 8 Conductor

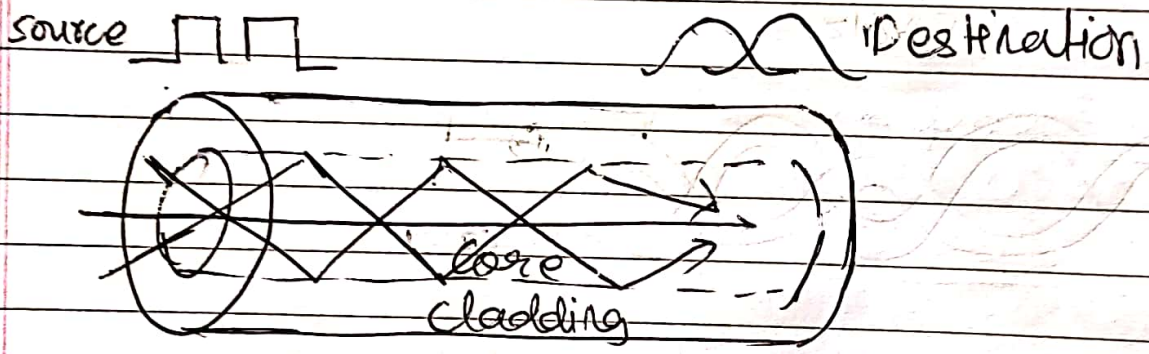


⇒ Coaxial Cable

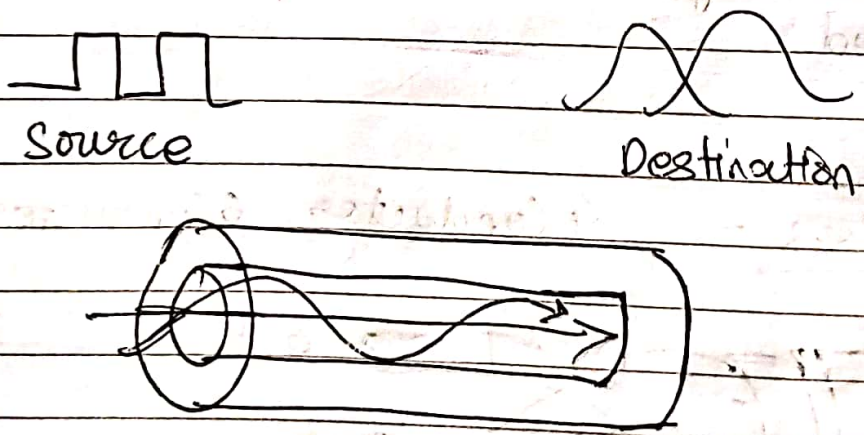
→ Single Mode & Multimode (step index)

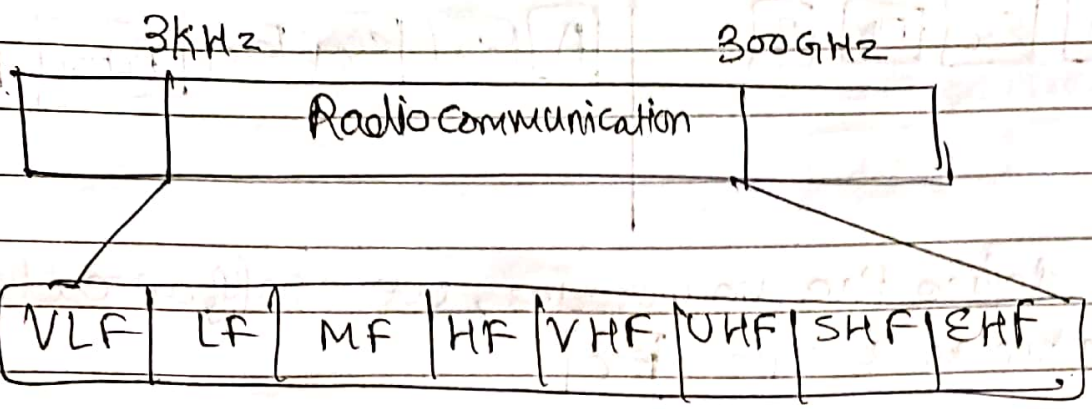
* Fiber Construction :-





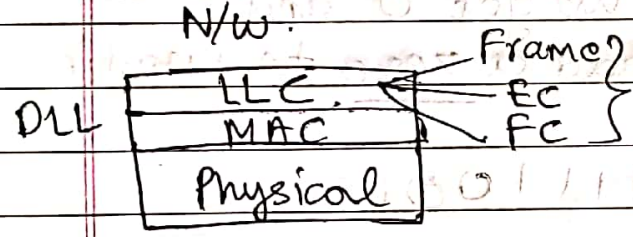
Multimode graded index





Chapter 3: The Data Link Layer ★★ imp

→ LLC - Converts packets into frames once it recei
data from network layer.



Sending machine

Packet

⇒ Byte Stuffing

→ Flags act as delimiters.

Flag	Header	Payload field	Trailer	Flag

⇒ Escape (ESC) is a byte which is stuffed into the dat

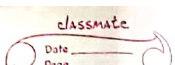
Original

A	Flag	B

After stuffing

A	ESC	Flag	B

Thus the flag in this case will be considered as data.



- to define the boundaries, we stuff an extra byte known as Escape [Esc]

★★ Flag → 01111110 – fixed pattern

→ Bit stuffing

- We break the pattern of the flag 01111110
- So whenever in a pattern we get 0 and 5 consecutive one's, then we add a zero to break it.

01101111111111111111110010

break

011011111 0 - - - - - -

bit stuffing

⇒ CRC

Divisor (4 bits)

Data

1101 | 11110111111000

so we add 3 zeroes

Ex-OR 1101

0011

If we get Remainder = 001 → Now Data is Dividend &

⇒ At receiver – repeat the same process, if we get remainder = 0, then it means it is without any error.

we added these as redundant bits

1101 | 1011110 | 000 If Remainder less than Divisor only then division can occur

= 001

★ Receiver:

data Rem

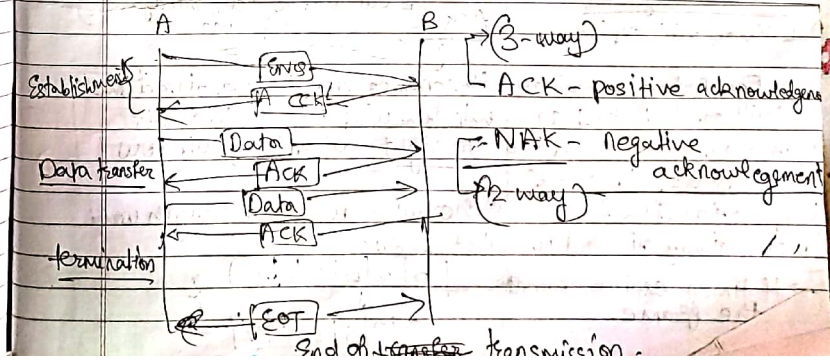
1101 | 1001000 001

1101

0100

1101 ← Rem

- If it is 0, then, discard the last 3 bits and that is data with new error.



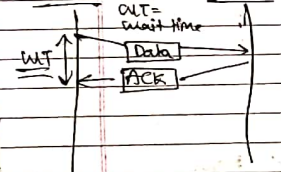
(Timer related functionality)

ARQ
↓
Acknowledgement Repeat Request

(Compulsory)

⇒ Flow Control

(one frame at a time) Stop & wait — always +ve acknowledgement



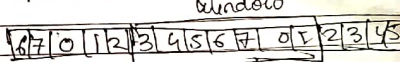
If the data is with errors, Receiver won't send any acknowledgement & timer will expire

→ For Data 0, receiver will send ACK-1 so it means it expects the next Data 1. In case of duplication it will automatically discard it.

→ If timer expires, resend the frame.

Sliding window (send several frames at a time)
- Go back-n
- Selective-reject

window



We can send 7 frames at a time without waiting for acknowledgement

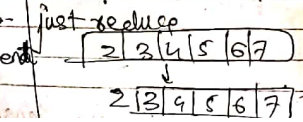
→ After receiving acknowledgement, sender window will slide to the right.

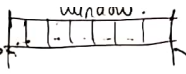
Sender window moves to the right frame by frame, when a frame is sent.

ACK-2 ← cumulative acknowledgement of frames

Whenever ack is received the window will slide one bit to right of end of window.

Otherwise window length will just reduce





This wall moves to right frame by frame when a frame is sent

Moves to right by as many steps for which acknowledgement is received

⇒ M=3 (reserved bits)

2^3 = 8 combinations = 0-7 unique frames

(sender window) $SW = 2^{m-1}$, $RW = 1$ } Go back n

(Receiver window)

For selective repeat :- $SW = 2^{m-1}$, $RW = 2^{m-1}$

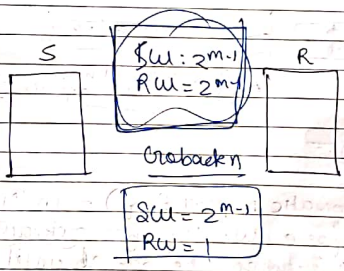
$SW = 2^{m-1}$

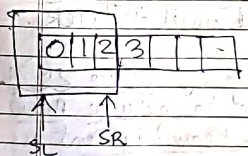
- Window size depends on how many bits are reserved for frame identifier in the protocol.

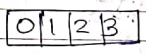
Go back n

m=2

$\Rightarrow 2^2 - 1 = 4 - 1 = 3$

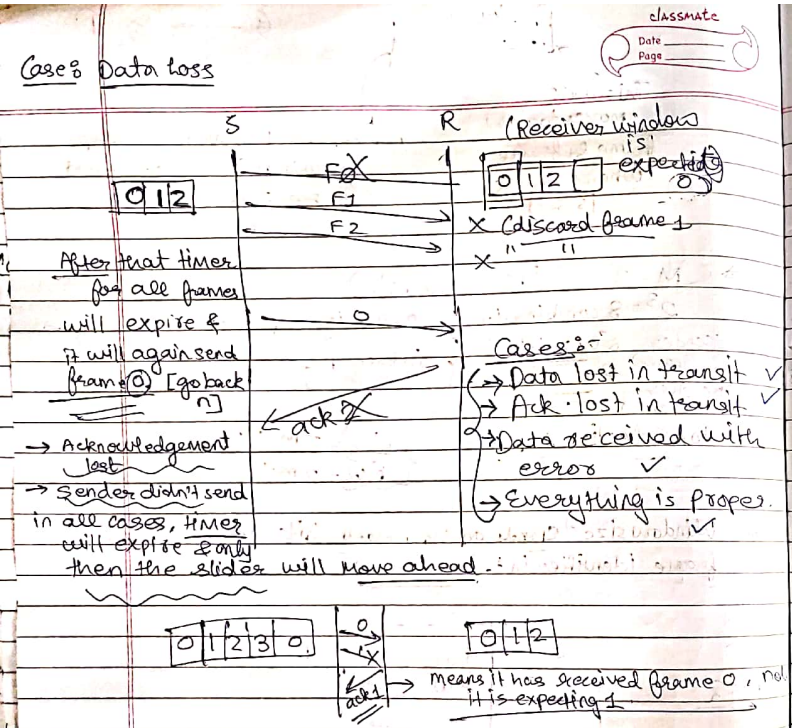






Sender Window.

Case: Data loss



After that timer for all frames will expire & it will again send frame 0 [go back n]

→ Acknowledgement lost
→ Sender didn't send

in all cases, timer will expire & only then the slider will move ahead.

* Go-back n:-

ARQ (Automatic Repeat Req.) - In this m frames are sent before waiting for acknowledgement.

(Copy of all frames are stored until the ack arrives)

Copy of all frames are stored until the ack. arrives.

- Frame numbers have the range of 0 to $2^M - 1$.
- Sender sliding window slides to include new unsent frames when correct acknowledgement is received.
- Receiver sliding window size is always 1, following specific order to accept a specific frame. If this

frame is lost or damaged, out of order, receiver remains silent & discards all the frames until it receives the one it is expecting. ✓

→ Timer of unacknowledged frames expires. Sender goes back and resends all frames. * (Go back n) (sends all frames)

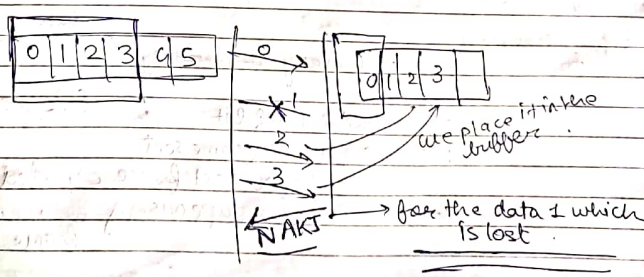
o Case 1:- Damaged frame

Sender goes back and sends a set of frames starting from the damaged one upto the last one sent.

eg:- Sender sends frame 6 timer for frame 3 expires & ack. is lost in transit.
Sender goes back to 3rd frame & sends 3, 4, 5, 6 again.

* Selective Reject (Supports -ve Ack.)

Size = 2^{m-1}
M = 3
$\Rightarrow 2^2$
= 4

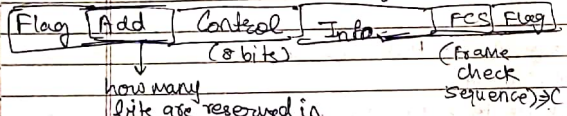


$0 \text{ to } 2^{m-1}$

* Bit oriented protocol *

SDLC | HDLC (High level Data link control Protocol) | LAPIs | LAN's

error : (Supports, CRC)

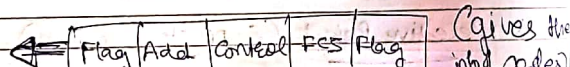


↓ User data coming from upper layer

how many bits are reserved in add-field.

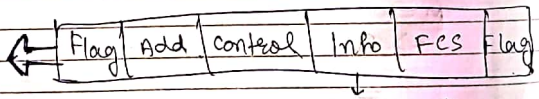
I-frame.

S-frame : (Supervisory)



(gives the info codes)

U-frame : (Unnumbered frame)



Management Data.

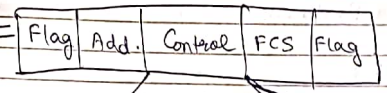
info is related to management of Primary & Secondary.

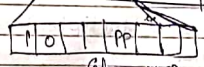
(P=1, ⇐ Primary is secondary)

P/F - Poll & Final bit
N(S) - Seq. no. of frame sent
N(R) Seq. no. of next frame expected
Code - Code for: supervisory or unnumbered frame

⇒ ARQ - data & Ack sent at same time.

CN - 5th edition
Tenanbaum





Code	Command
00	RR Receiver Ready
01	REJ Reject
10	RNA - Receive not ready
11	SREJ - selective reject

⇒ PPT (X) : not there

MAC (Medium Access Control)

Dynamic Channel Allocation in LAN & MAN -

1. Station model. (n-independent stations, all or none can transmit data)
2. Single Channel Assumption -
3. Collision Assumption.
4. (a) Continuous time
   (b) Slotted time
5. (a) Carrier Sense - shared carrier, will sense if some other signal is coming or not
   (b) No Carrier sense

- Multiple Access Protocol
  - Pure
  - ALOHA — slotted.
  - CSMA — Carrier Sense Multiple Access
  - Collision free protocol.

Pure Aloha

1. Assuming n-frames, G is the throughput of the system ($G \geq N$)

because of collision, new frames might be generated.

N = no. of frames. ($N > 1$) $0 < N < 1$

$G \geq N$ $N = 0$ $G = N$

$G > N$, $S = GP_0$; $P_r[k] = \frac{G^k e^{-G}}{k!}$ (from Poisson's Dist)

- G: total load of system (new + old)
- S: total throughput
- P_0: Probability of 0 collision
- $P_r[k]$: probab. of k transmissions

$P[0] =$

$$\boxed{S = Ge^{-2G}}$$

vulnerable time = 2 frames

as G is total load,

$G = 1/2$

$S = \frac{1}{2e} = 18.4\%$.

STEPS

→ For Pure Aloha, 'N' frames per unit time are generated.
→ at higher rate N>1
→ Considering new frames, + retransmission of collision frames, total G frames can be generated. so G ≥ N.
→ At low load, G=N because of no collisions. At higher load G>N.

→ Throughput S for the system with no collisions is given by $S = GP_0$, (P_0 = no collision probability)

→ P_K = Prob of K frames generated. = $\frac{G^K e^{-G}}{K!}$ by Poisson's Dist.

→ If K=0 (i.e. no collisions), $P_0 = e^{-G}$.
Considering Pure Aloha, Vulnerable period is of 2 frame time long.
(Sent + received)

S (throughput) $= Ge^{-2G}$

→ At G = 0.5, S will become $= \frac{1}{2e} = 0.184$
$= 18.4\%$.

which is max throughput of system which gives 18.4% channel utilisation rate.

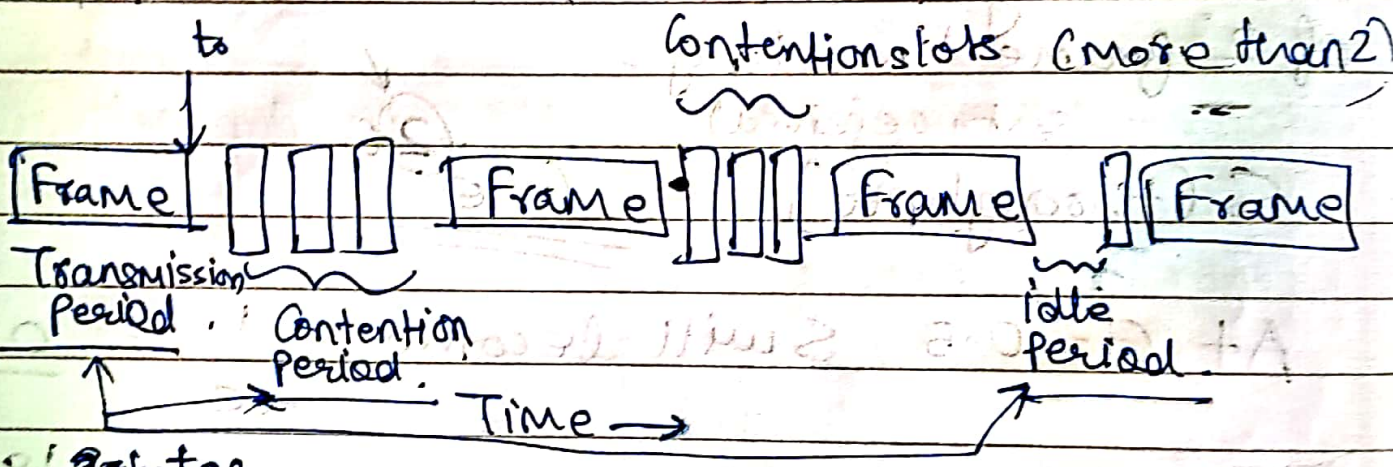
* Slotted Aloha: - Graph
- vulnerable period reduces to 1 frame time.

CSMA

→ Before the transmission, every station will first sense the carrier channel whether it is free or not.

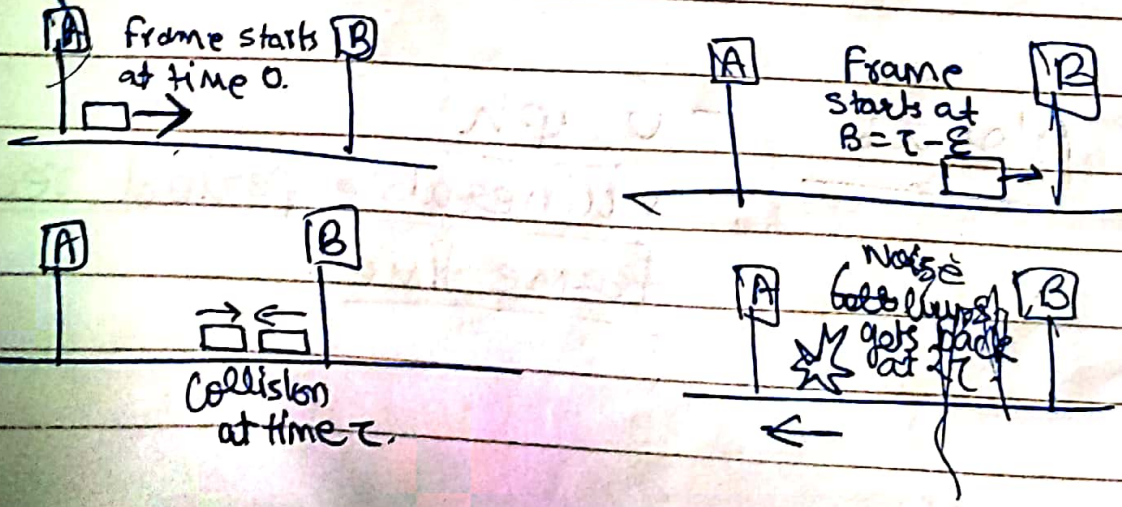
→ 2 different stations will have different randomness for wait.

CSMA with CD (Collision Detection)



3 states

And it takes worst-case 2τ seconds to detect a collision.



- Security
- Strict source
- Loose source
- Record Route
- Timestamp

← 32 bits →

net id	host id
← n bits →	← (32-n) bits →

4 bytes
4 x 8 = 32-bit
1 byte = 8

8888 | 8888 | 8888 | 8888

(ICANN)

IP - network interface

(7)

0	Network	Host
10	16-2=14	
110	24-3=21	
1110	Multicast	
1111	Reserved.	

1.0.0.0
127 255.255.255

128.0.0.0
191.255.255.255

192.0.0.0
223 255

224 2
239

240
255

00 - - - 0 This host

111 - - - 1 Broadcast on this network

127 - - - Loopback

000 10 | Host

Network 1114

Host on this network
- Host on distant network.

- network into 8 subnets
  - ↓
  - We will take 3 extra bits
  - ↓
  - $2^3 = 8$

IP add — Mask Subnet

↓

AND

↓

Network add / Subnet add.

* Store & Forward Packet Switching *

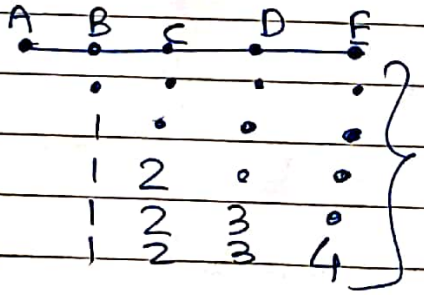
* Shortest Path Algorithm *

* Distance Vector Routing Protocol * (works on the process of info. of neighbours).

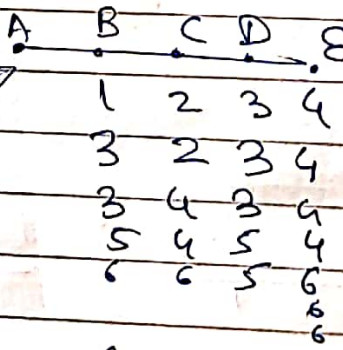
- This algorithm works on the delay metric.
- The 4 tables is the data given by the neighbours (which may ~~be~~ unt...
- The data given below is true. (calculated by J)

* The count-to-infinity problem *

- We have 5 nodes i.e. computers in the network.



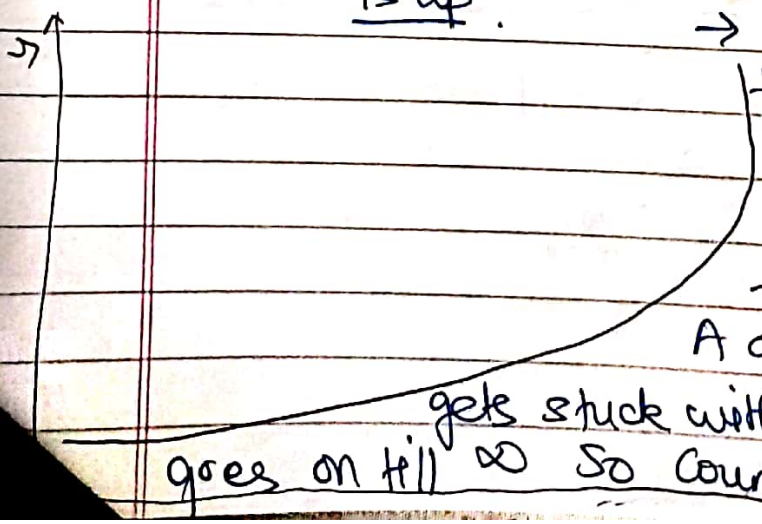
(A which is currently up, is only one hop away from B)



In 4 exchanges, the entire network is up.

(and say the network goes down)

→ Now if A-B link is down, then B will think that it can go via C to A, but B doesn't know that the path to C is through A only. Thus every router gets stuck with some alt. path & this goes on till ∞ So Count to infinity.



(LSR)

* Link State Routing *

(i) Sequence number } 2 parameters in LSR.
(ii) Age (of the packet) }

Structure of Link state Packet:

A	← this compulsory
Seq	
Age	
B | 4	
E | 5	

(Hello packet sent - Ack received)

- Flooding :- Age decrement + same packets sent

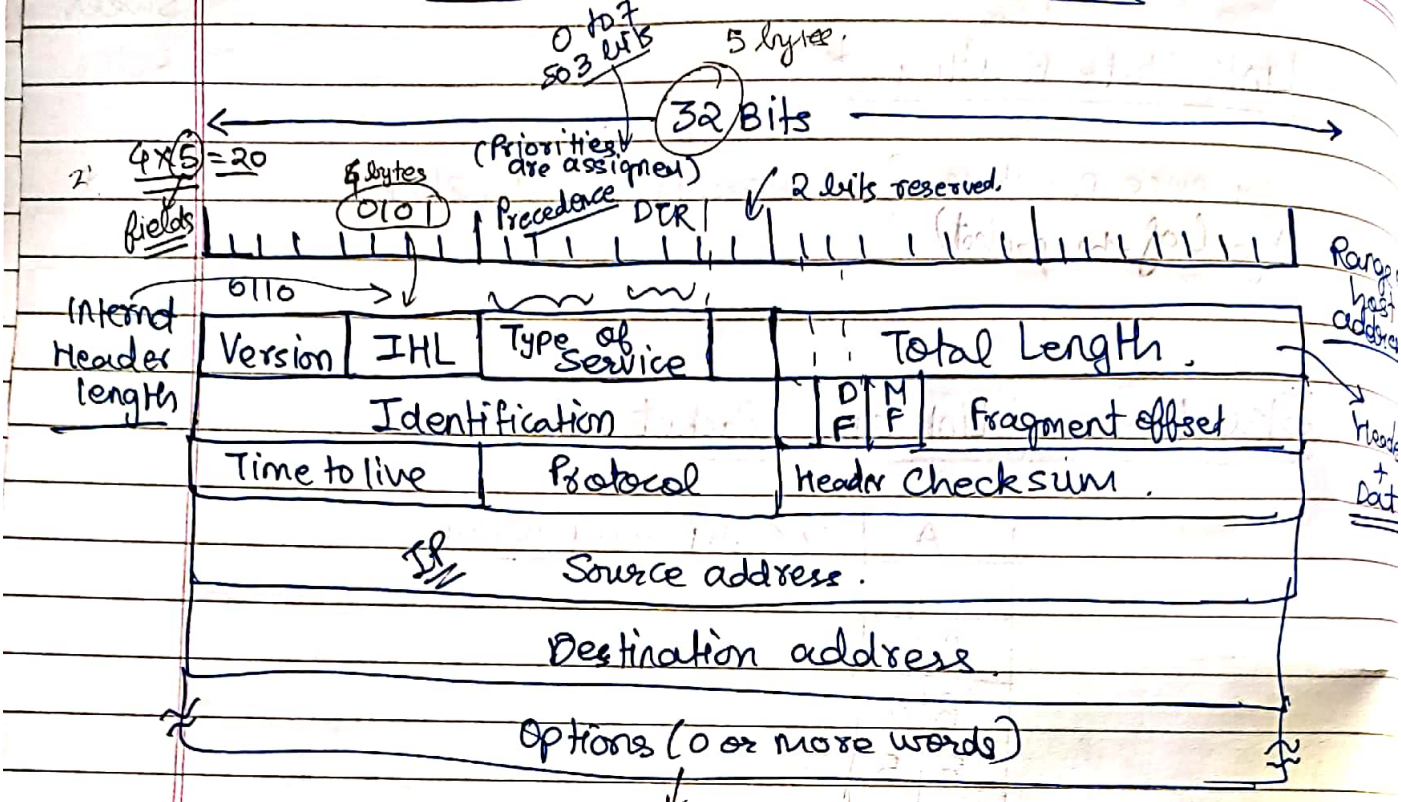
(Even if it's a LAN, we consider it to be a node)

The diag in the slide depicts the current scene.

* Hierarchical Routing *

- Maintains the entire network as a group of small networks.

* The Internet Routing Protocols *



Suppose we dont have options

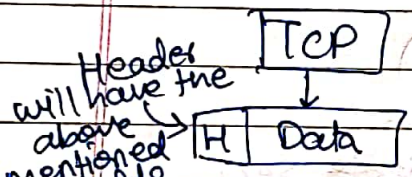
no. of rows = 5

Value of IHL = (5)

Total 5 rows of 4 bytes each

Max = 5x4 = 20

Header will have the above mentioned fields



- DTR = Delayed Throughput & Reliability
  eg:- 1 0 1 (Delay allowed)
- Total length :- 16 bits
  2^{16} = 65536 bytes. x 4 = 262144 ← Combinations
- For Header :- In this case 20 bytes bits
  Data length - T.L - IHL.

If we have 1111 → indicates 15 rows with ones. → 15x4 = 60 bytes (max header length)

⇒ Identification :- All fragments should have the same identification no. of the packet.

⇒ DF - Don't Fragment (Router is out of capacity) MF - More Fragment. (if there is capacity left, all segments except last one will have MF=1)

* Time to live :- 255 sec (it will decrement as per no. of hops)

* Protocol :- TCP or UDP

* Header checksum.

* Source add :- We have reserved 32 bits for source add. (That is why I had 32 bits)

* Some IP options :

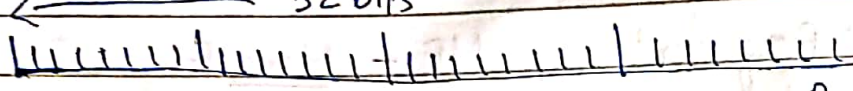
Option
Security
Strict source routing
Loose source routing
Record route
Timestamp.

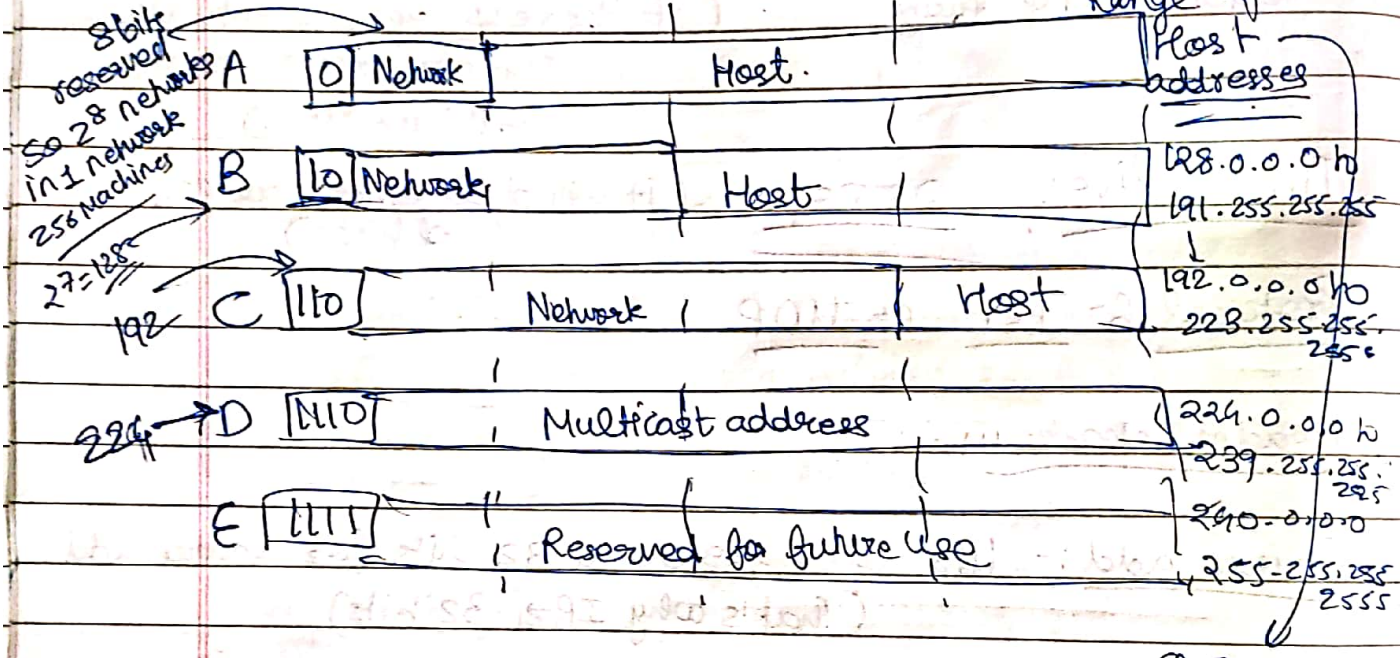
1000 $2^{?}$

divided into network + host (machine identification)

- IPV4

* 32 bits



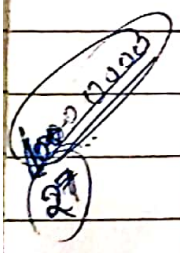


⇒ Public + Private IP addresses

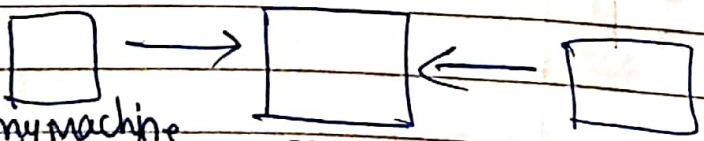
(given by ISPs) (already assigned)

(within the same network, there can't be repetition but others can use)

(192.... range)



⇒



Private (192.134.28.1) → Public (224.something) Mapping done by that → (13.) google

SPECIAL IP Addresses [By default, user can't use this]

Date

→ 127.0.0.1 → assigned for Loopback (designed, so that it can be checked whether that machine is accessible or not)

→ 000000000...0 → This host (Local host)
0000...0 → Host → A host on this network

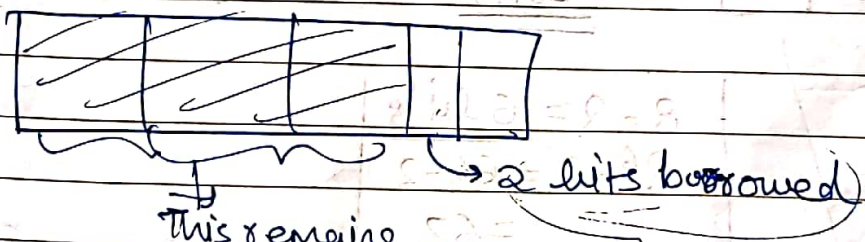
1111 - - - - - 1 → Broadcast on the local network.

* SubNetworking *

- CIDR - Class Less Inter Domain Routing
- Dividing the same network into a no. of subnets - subnetting

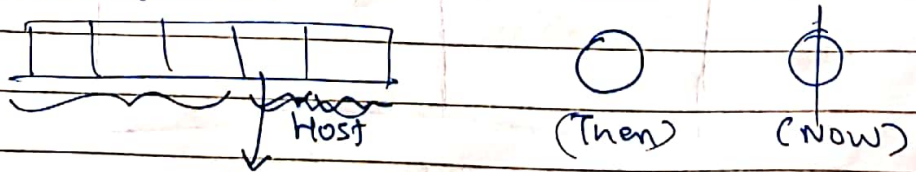
(Concept is to borrow some bits from the Host)
192.168.1.[0] ← This last 3 bits is what we change

eg:-



No. of bits = 26 (after slash) : /26

IP address given :- 200.1.2.0



If we borrow 1 bit
(we will have either 0 or 1 as the possible combination)

	200.1.2.0	200.1.2.128
IP of Subnet		
total IP	2^7 =	
hosts	2^7-2 =	
Range = 200.1.2.	0 0000000 = 0	1 0000000 = 128
	0 1111111 = 127	1 1111111 = 255

7 bits are left for Host, so 2^7 is no. of possible IP addresses

But no. of Machines = $2^7 - 2$ (1 for Network, 1 for Broadcasting)

200.1.2.[ ] will borrow 2 bits so $2^2 = 4$ Combinations

$8-2 = 6$ bits
$2^6 - 2 = 64-2$
$= 62$
(no of Machines)

0-63	64-127	128 to 191	192 to 255

For odd bits (not power of 2)

↓

6 (we take 2 bits) = (4

& then subdivides the 2 parts into further 2 parts

(1) a) 192.168.1.0 (/28) — Class C — 4 bits borrowed — 16 subnets

b) 150.150.0.0 (/30) — Class B — 14 bits borrowed

c) 192.168.1.35 (/27) — class C — 3 bits — $2^3 = 8$ subnets

lies between 32 to 63 ~~we start from the lowest (8 subnets)~~

2 (14) subnets

2 bits left

$2^2 - 2 = 4 - 2 = 2$

Network, Broadcasting

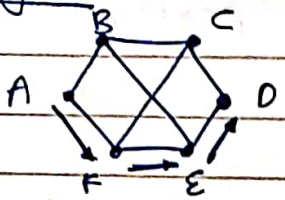
For congestion control:

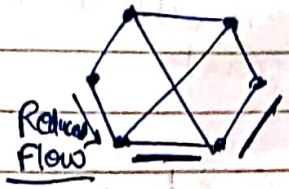
(i) warning bit ×

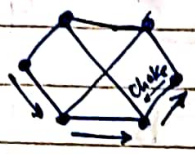
(ii) Choke packet circulation (as soon as the choke packet is received by the sender, the flow will be reduced.)

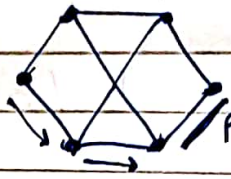
Hop & Hop choke packet (the congestion is avoided everywhere the choke packet passes.)

Type 1

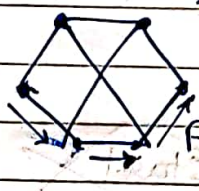

A
B
C
D
E
F

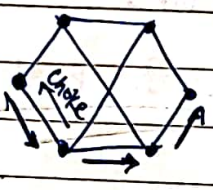

Reduced Flow


Choke

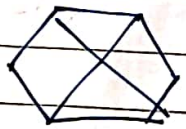

Flow is still at max rate

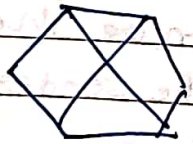

Choke


Flow is reduced


Choke

Type 2





* Types & (i) Open Loop - It takes care of congestion by implementing good design and takes the decision so that congestion won't occur at first step.

(ii) Close Loop - It is a feedback system - allows the congestion to happen, monitor the network, adjust system parameters, pass the info to other routers & detect if any congestion.

* Congestion control in Virtual Circuit -

(a) Admission Control - No new virtual circuit is set up but congestion prevention mechanisms are applied.

(b) New Virtual Circuit is set up. if congestion happens.

* Congestion Control in Datagram

Congestion Prevention Mech. using warning bit and choke packets are implemented.

* The Transport Layer *

1. TSAP (Transport Service Access Point)

Transport Service Primitives

LISTEN
CONNECT
SEND
RECEIVE
DISCONNECT

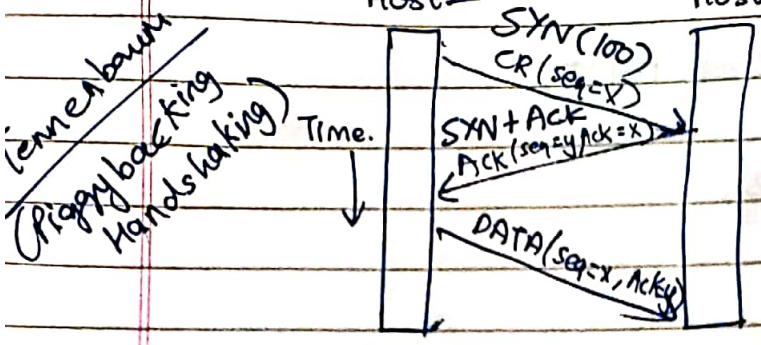
* Main Functions:

1. Port Addressing
2. Connection Establishment
3. Connection Release
4. Error & flow control
5. Multiplexing
6. Crash Recovery

Addressing Hosts will only remember the process server's address. The Process server will remember the address of diff mail servers serving FTP, SMTP, etc. respectively.

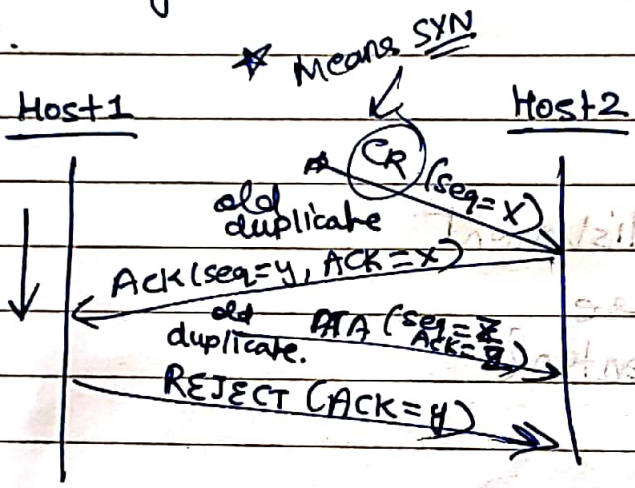
* (Initial Connection Establishment Protocol)

* Connection Establishment (3-way Handshake Mech. for T



* TCP Header req. sequence number of data to be transferred
  - Seqno
  - Ackno

→ Three protocol scenarios for establishing a connection using a 3-way Handshake. CR denotes CONNECTION REQUEST.



⇒ DR - Disconnect Request

* Solutions for Error Control + Flow Control.

(a) Chained - fixed size buffers.
(b) Chained Var. size buffers.
(c) (One large circular buffer per connection instead of a pool of buffers)

Instead, we keep dynamic window size

→ Whenever the receiver has received all data.

if → <ack = 0, buf = 0>

this msg is lost then there is potential Deadlock. (It has got all data)

- S0 → 0 or No pending Ack.
- S1 - 1 outstanding Acknowledgement

- At transport layer, receiver will have the buffer (Fast sender + Slow Receiver)
Sender doesn't need a buffer as if it doesn't get the Ack, it means receiver hasn't received the data.

A = Ack.
W = Write
C = Crash

Whatever is given in the bracket, won't happen.
OK = Protocol functions correctly
DUP = Protocol gen. a duplicate msg.
LOST = Protocol loses a Msg.

AW
First Ack then write

WA
First Write, then Ack.

* TCP Connection Management *

K = KB
WIN = 0 (no more space in buffer window)

* Silly Window Protocol: Receiver is signalling that it has 1 byte of space is free.
(Receiver advertises this & Sender responds)
→ Just for this, we add all headers.