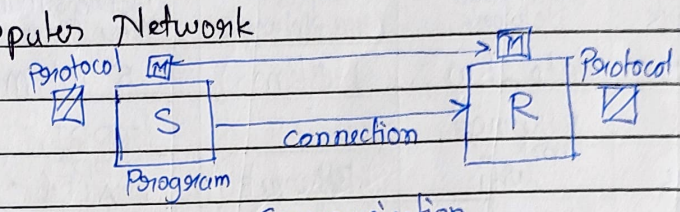
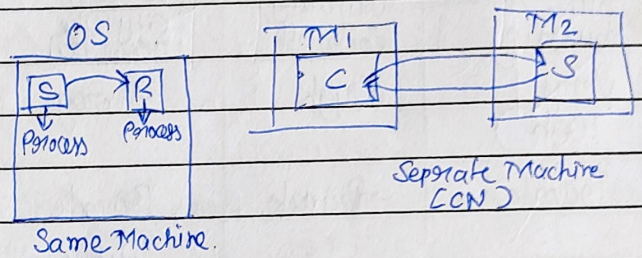
Computer Network and Network Design

Computer Network



Communication

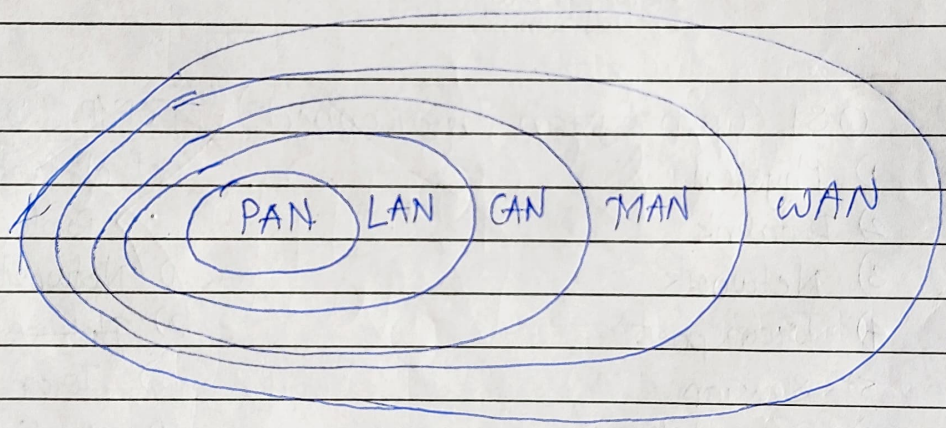


Functionalities

- Mandatory
  - Error Control
  - Flow control
  - Mux, Demux
- Optional
  - Encryption, Decryption
  - Checkpoint

OSI (Open System Interconnect)	TCP/IP (Transmission Control Protocol / Internet Protocol)
1) Physical	1) Network Interface
2) Datalink	
3) Network	2) ~~Network~~ Internet
4) Transport	3) Transport
5) Session	
6) Presentation	4) Application
7) Application	

	PAN	LAN	CAN	MAN	WAN
Full form	Personal Area Network	Local Area Network	Campus Area Network	Metropolitan Area Network	Wide Area Network
Range	1-100 meter	Upto 2km	1-5km	5-50km	Above 50km
Technology	Bluetooth, IrDA, Zigbee	Ethernet and wifi	Ethernet	FDDI, CDDI, ATM	Leased line, Dial-Up
Area	Within a Room	Within office building	Within University, Co-op off	Within City like Mumbai	Within Countries
Transmission Speed	Very High	Very High	High	Average	Low
Ownership	Private	Private	Private	Private or Public	Private or Public
Maintenance ~~Maintain~~	Very Easy	Easy	Moderate	Difficult	Very Difficult
Error Rate & Cost	Very Low	Low	Moderate	High	Very High

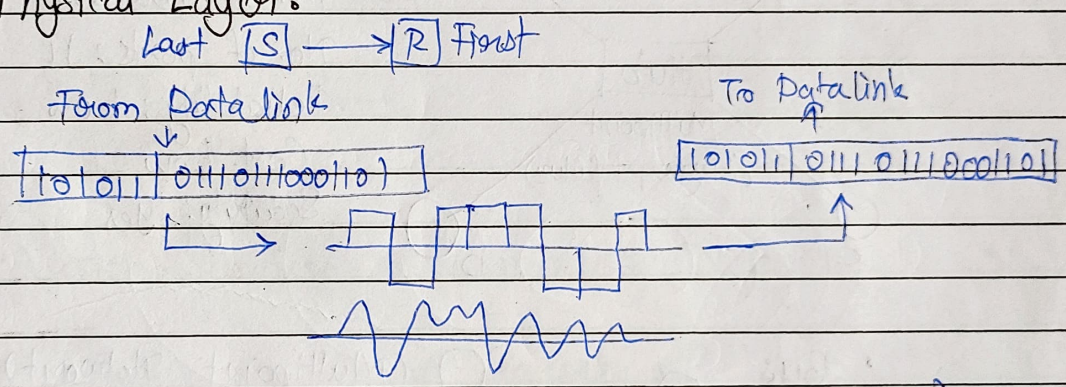


	TCP/IP-5	OSI	TCP/IP-4	
Process to Process	Application	Application Presentation Session	Application	Data
Host to Host	Transport	Transport	Transport	Segment
Source to Destination	Network	Network	Internet	Packet
Node to Node	Datalink	Datalink	Network Access	Frame
	Physical	Physical		

TCP/IP Protocol suit or Internet Protocol

- Developed by ARPANET
- Supports client-server and peer to peer

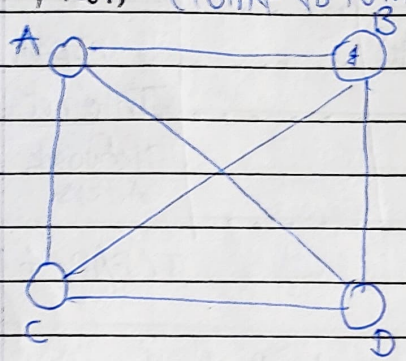
Physical Layer:



- Cables and Connectors (Wired / Unwired Media)
- Physical topology (Star, Mesh, Bus, ...)
- Hardware (Repeaters, Hub, Switch, ...)
- Transmission mode (Simplex, Half Duplex, Duplex)
- Multiplexing (S) Demultiplexing (R)
- Encoding

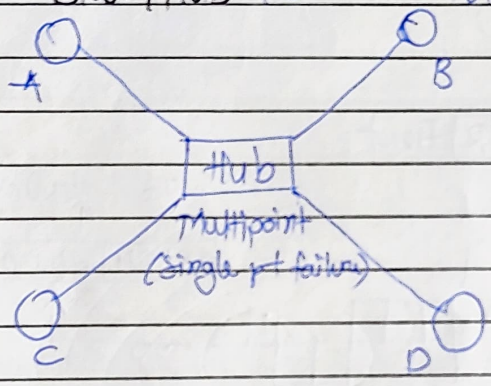
Topology:

- **Mesh** (Point to Point ~~Connection~~ Communication)



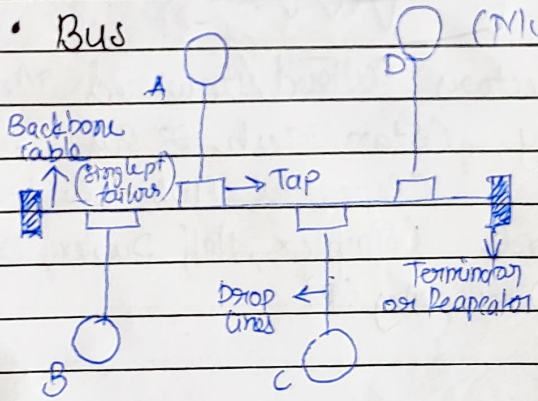
n = no. of nodes
No. of cables: $\frac{n(n-1)}{2}$
No. of ports: $n(n-1)$
Reliability: Highest
Cost: High
Security: Yes
Maintenance: High

- **Star / Hub** (Point to Point Communication)



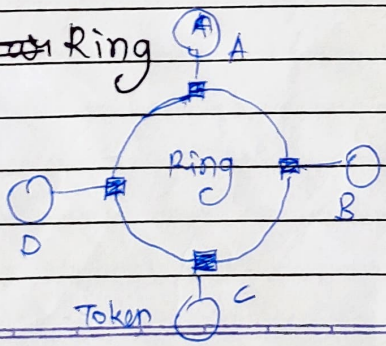
n = no. of nodes
No. of cables: n
No. of ports: n
Reliability: Low
Cost: Low
Security: Yes

- **Bus** (Multipoint Network)



Collision: n
No. of cables: n+1
No. of ports: n
Reliability: No
Cost: Cheap
Security: No

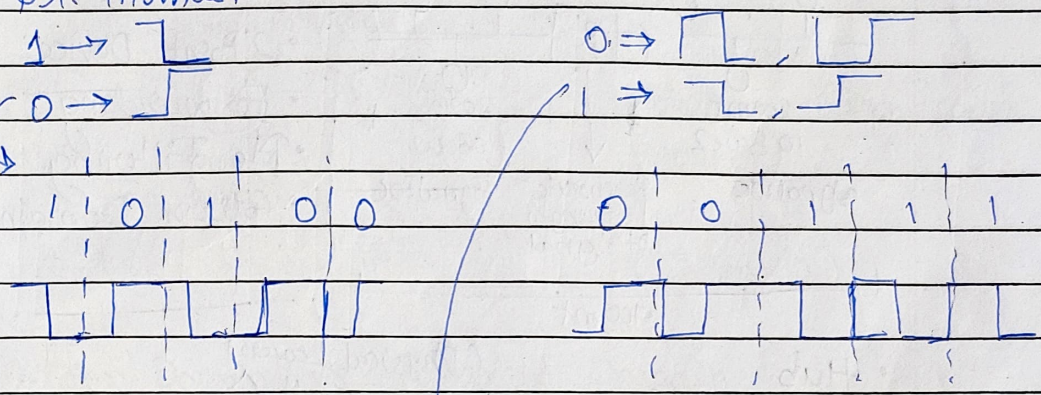
- ~~Star~~ **Ring**



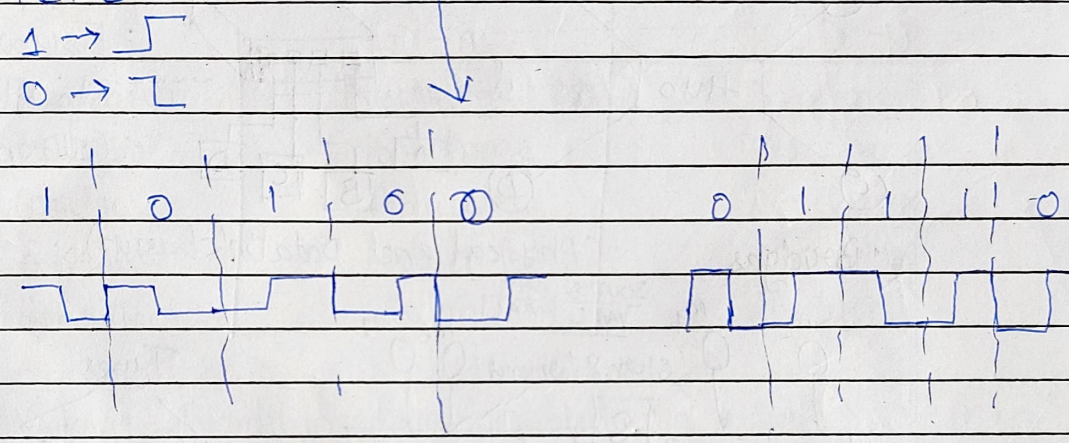
Collision: n
No. of cables: n+1
No. of ports: n
Reliability: No
Cost: Cheap
Security: No

• Manchester Vs. Differential Manchester Encoding

Dr. Thomas:



IEEE:



• Various Devices in Computer Network

H/W
1) Cables
2) Repeaters
3) Hubs

H/W + S/W
4) Bridges
5) Switches
6) Routers

7) Gateway
8) IDS
9) Firewall
} security
10) Modem

• Cables

→ Unshielded twisted pair cable — 10 Base T / 10 Mbps / 100mt

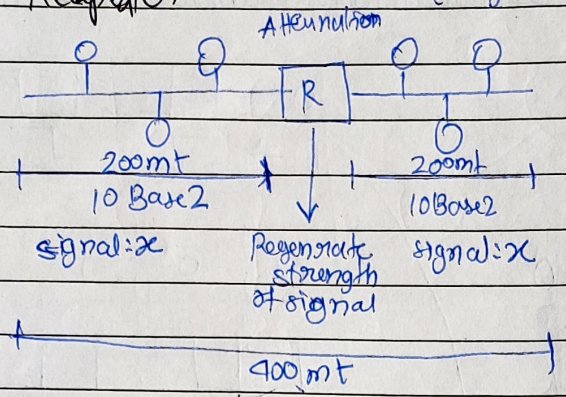
100 Base T, 10 Base T (LAN)

→ Co-axial cable ← 10 Base 2, 10 Base 5

→ Fibre optics — 100 Base Fx — Fx / 2km

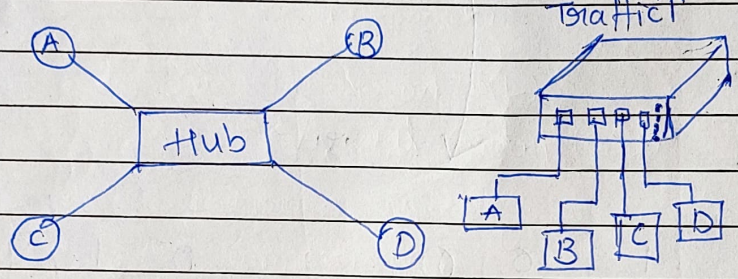
Collision : n ← Filter:

- **Repeater** (Physical Layer)



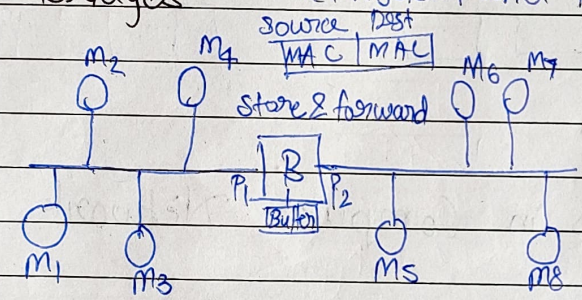
- 2 Port Device
- Forwarding
- No Filtering
- Collision Domain (n)

- **Hub** (Physical Layer)



- Multiport Repeater
- Forwarding
- No Filtering
- Collision Domain 1

- **Bridges** (Physical and Datalink Layer)

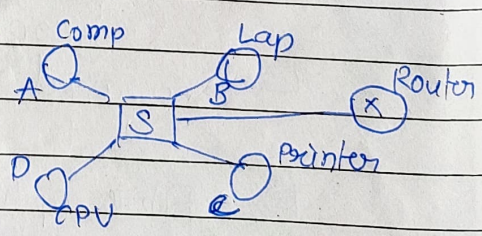


Types
- Static — Data manually added
- Dynamic or Transparent

MAC	Port
M1	P1
M2	P1
M3	P1
M4	P1
M5	P2
M6	P2
M7	P2
M8	P2

- Connect two different LANs
- Forwarding
- Filtering
- Collision Domain (0)
- Bridge Data Unit Protocol
  uses spanning tree to remove loops

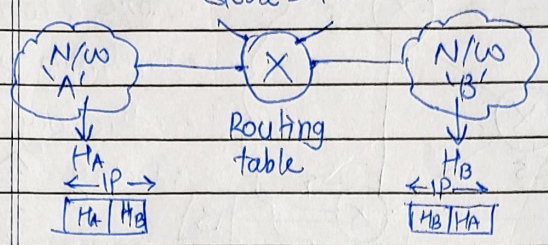
- **Switch** (Datalink Layer)
- Multiport Bridge
- Full Duplex Links
- Traffic is minimal
- Collision Domain (0)



- Routers (Physical, Datalink, and Transport Layer)

'Internet' ← IP

Store & Forward



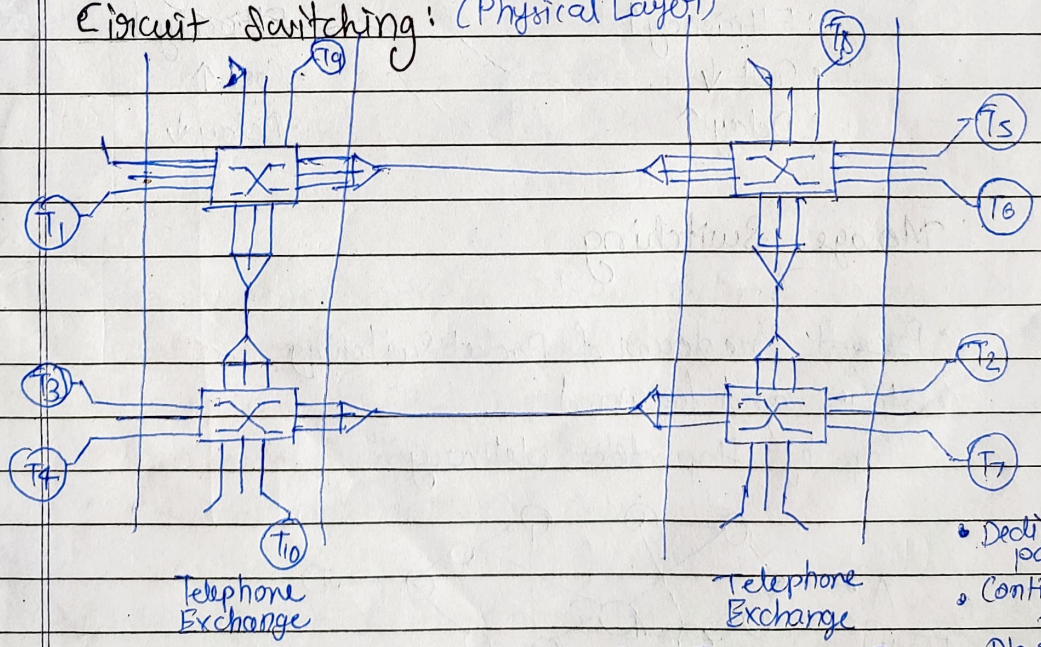
- Forwarding
- Flooding (Broadcast)
- Filtering
- Routing
- Collision (D)

Collision Domain vs Broadcast Domain

	CD-n	BD-n
Repeater	No change	No change
Hub	No change	No change
Bridge	Reduce	No change
Switch	Reduce	No change
Router	Reduce	Reduce

Gateway - Transition from one device to other (CD - BD) ✓

Circuit Switching: (Physical Layer)



- Dedicated path
- Contiguous flow (123 123)
- No readers
- Efficiency less
- Delay less

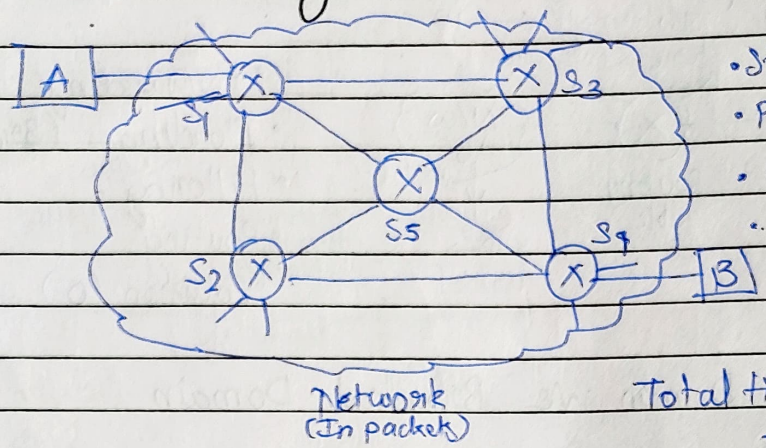
Total time = Setup time + TT + PD + Tear Down Time

TT → Transmission time → $\frac{M}{BW}$ (M: message, BW: Bandwidth)

PD → Propagation delay → $\frac{D}{V}$ (D: distance, V: velocity)

Tear Down Time → Terminate time

• Packet Switching (Datalink & Network Layer)



- Store & Forward
- Pipelining used
- Efficiency ↑
- Delay ↑

Total time $= n(TT) + PD$

- n → no. of switches
- TT → Transmission time → $\frac{m}{BW}$
- PD → Propogation Delay → $\frac{D}{V}$

Types — Datagram (NL)
— Virtual Circuit (DLL)

Datagram Switching

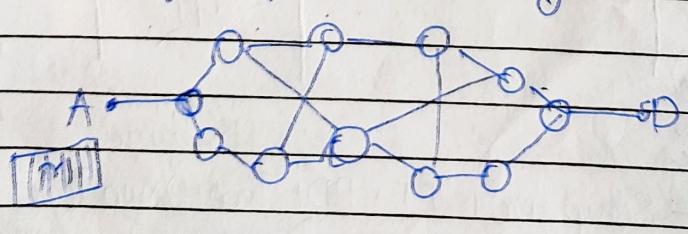
- Connectionless
- No Reservation
- Out of Order
- High overhead
- Packet lost ↑
- Used in Internet
- Efficiency ↑
- Cost ↓
- Delay ↑

Virtual Circuit

- Connection-oriented
- Reservation
- Same order
- Less overhead
- Packet lost ↓
- X.25, ATM
- Efficiency ↓
- Cost ↑
- Delay ↓

Message Switching

- ~~Pseudo~~ Predecessor of Packet Switching
- Store and forward
- Hop by Hop ~~deliv~~ delivery

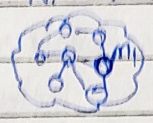


Types of Casting

cast - file shared b/w how many peep?

- Unicast (one to one)

N/w 'A'



90.0.0.0

N/w 'B'

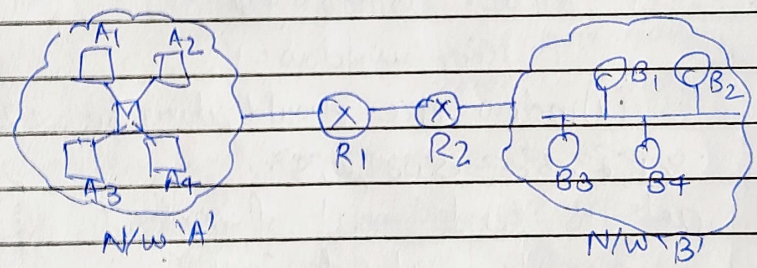
92.0.0.0

- Broadcast
  - Limited
    255.255.255.255
    (message in same n/w)
    (m1 to N/w A)
  - Direct broadcast
    92.255.255.255
    (message ~~at~~ to other n/w)
    (m1 to N/w B)
- Multicast
  To a specific grp

DataLink Layer:

(Works within N/w)

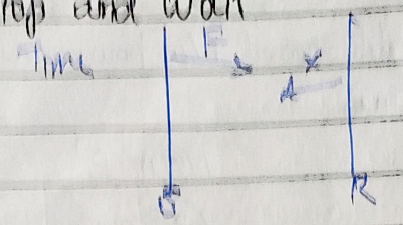
- ~~Hop to Hop / Node to Node Delivery~~



- Hop to Hop / Node to Node Delivery (Source to Router) (Router to Dest)
- Flow control (Stop & wait, Go back N, Selective Repeat) - Node level
- Error Control (CRC, Checksum, Parity) - Node level
- Access Control (CSMA/CD, ALOHA, Token Ring)
- Physical address (MAC)

Data are divided in frames.

Stop and Wait



Round trip time = frame sent + ack sent

Sender window : 2
Reciever window : 2

Time-out then restart previous frame to send again

ack failed - resend frame (Discard duplicate)

Error correction in Stop-and-Wait ARQ is done by keeping copy of the sent frame and retransmitting of the frame when timer expires.

Go Back N

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

~~The send window is an abstract concept defining an imaginary box of size $2^m - 1$ with the variables S_f, S_n~~ size

Sender window = $2^m - 1$

Reciever window = 1

Window size should always be $< 2^m$

~~0, 1, 2, 3 → 0, 1, 2, 3~~

~~ack is sent out of order~~

accepts out of order

discard frames if order is not matched

Selective Repeat

Sender Window = Reciever window = 2^{m-1}

Window size should be = 2^{m-1} & not >

accepts out of order frame

Gives NAK - negative ack

If frame is lost NAK is sent

$k \rightarrow$ no. of bits to rep WS

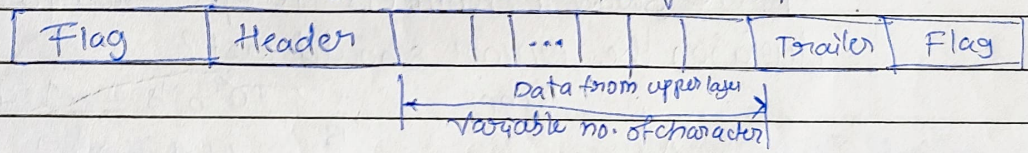
Stop & Wait	Go Back N	Selective Repeat
• Only 1 frame transmit	• Multiple frame	• Multiple frame
• Sender Window = 1	• Sender Window $= 2^k - 1$	• Sender Window $= 2^{k-1}$
• Reciever Window = 1	• Reciever Window = 1	• Reciever Window $= 2^{k-1}$
• $\eta = \frac{1}{1+2x} = \frac{TT}{TT+RTT}$	• $\eta = (2^k - 1) \cdot \frac{1}{1+2x}$	• $\eta = 2^{k-1} \cdot \frac{1}{1+2x}$
$x = \frac{T_p}{T_t}$	• Cumulative ACK	• Commulative & Independent ACK
• Re-transmission = 1	• Retransmis $= 2^k - 1$	• Retransmission = 1
• ASN $= W_s + W_R$ Available Sequence Number		

Framing

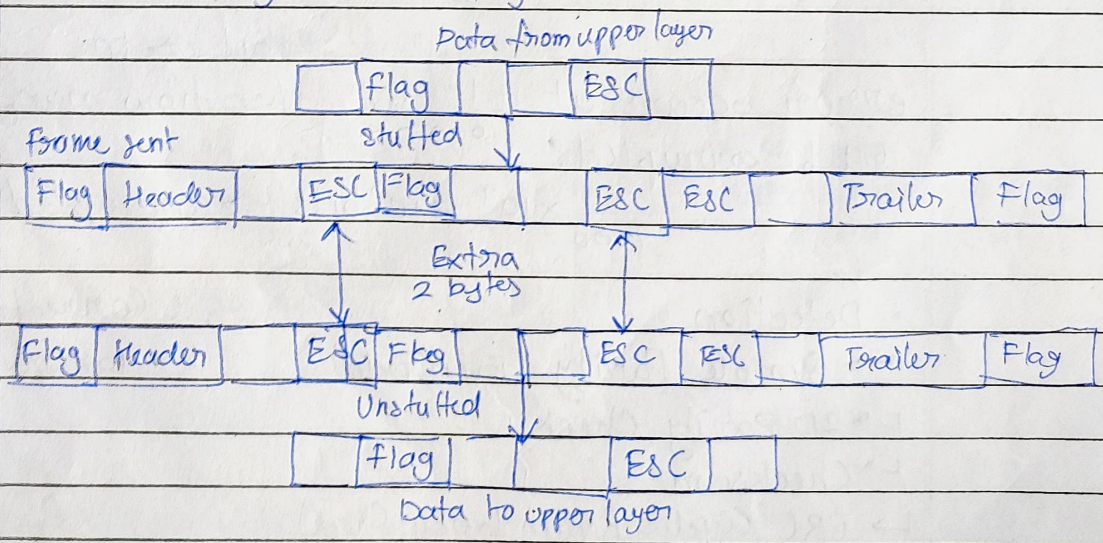
The data link layer needs to pack bits into frames, so that each frame is distinguishable from another.

Envelope $\rightarrow$ seprates letter $\rightarrow$ delimiter

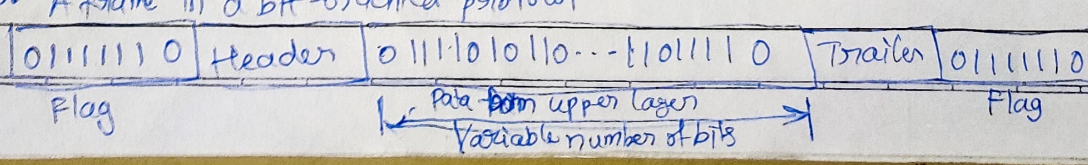
1. A frame in a character-oriented protocol



2. Byte stuffing and unstuffing



3. A frame in a bit-oriented protocol



1

1. Bit stuffing and unstuffing

Data from upper layer

| 00011111110011111 01000 |

Stuffed

| Flag | Header | 00011111011 00111110 01000 | Trailer | Flag |

Extra 2 bits

| Flag | Header | 00011111011 00111110 01000 | Trailer | Flag |

Unstuffed

| 00011111110011111 01000 |

Data to upper layer

Error Detection and Correction

Sender Reciever

↳ Single bit Error 100 → 101

↳ Burst Error 101010 → 111101 length of error = 5bi

- If the BW of a channel is 1Gbps then for how much duration the error should last?

A —— 1Gbps —— B

10^9 bits → 1 sec

1 bit → $\frac{1}{10^9}$ sec

1 bit → 1ns

error occurs at $\frac{1}{1000}$ sec then how many bits will be corrupted?

$\frac{1}{1000} \times 10^9 = 10^6$ bits → corrupted

- Detection
  - ↳ Simple Parity (Even, Odd)
  - ↳ 2D Parity Check
  - ↳ Checksum
  - ↳ CRC (Cyclic Redundancy Check)

- Correction
  - ↳ Hamming Code

Single Parity Bit

$m \rightarrow$ message bits

- $m+1$ bits
- Even Parity
- Can detect all single bit errors in code word
- Can detect all odd no. of errors

Hamming Distance

Minimum Hamming dist = 2

```
 0000        0101
 1111  (XOR) 1000
 1111        1101
 ----        ----
   4           3
```

Hamming dist = d

Error detection length = d-1

Cyclic Redundancy Check (CRC)

- Can detect all odd errors, single-bit, burst error of length equal to polynomial degree
- Based on binary division

  Total bits = $(m + r)$ → message bits, → redundant bits

- Polynomial should not be divisible by x
- also not with $(x+1)$

$x^4 + x^3 + 1$

Polynomial

$1x^4\ 1x^3\ 0x^2\ 0x\ 1x^0$

11001

(Append highest 0's = highest power)

```
11001 ) 1010101000
        11001
        -----
        011000
         11001
        ------
        000011110
           11001
        ---------
        00000000
            11001
        ---------
        00001010
```

At receiver if remainder of code word/divisor is 0 then no error

$\eta = \frac{10}{14} \times 100$

Valid code word: 1010101000010

Hamming Code

7-bit → 4bit (data) + 3 bit (parity)

2^nth	Position	7	6	5	4	3	2	1
	Bit	d_3	d_2	d_1	P_2	d_0	P_1	P_0

$P_0 = d_3 \oplus d_1 \oplus$
$P_1 = d_3 \oplus d_2 \oplus d_0$
$P_2 = d_3 \oplus d_2 \oplus$

Example: | d | d | d | r_8 | d | d | d | r_4 | d | r_2 | r_1 |

i/p data = 1001101

$r_1 = 1,3,5,7,9,11$ $r_2 = 2,3,6,7,10,11$ $r_4 = 4,5,6,7$

$r_8 = 8,9,10,11$

	11	10	9	8	7	6	5	4	3	2	1
Adding r_1	1	0	0	r_8	1	1	0	r_4	1	r_2	1
Adding r_2	1	0	0	r_8	1	1	0	r_4	1	0	1
Adding r_4	1	0	0	r_8	1	1	0	0	1	0	1
Adding r_8	1	0	0	1	1	1	0	0	1	0	1

o/p data = 10011100101

10111100101 – ~~error~~ msg

r_1 – 0 , r_8 – 0

Multiple Access Protocol (MAC)

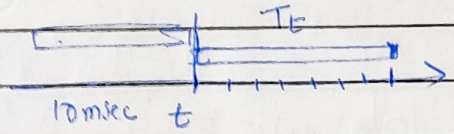
Datalink → Logical Link Control Layer
→ Media access control Layer

MAC

- Random Access Protocol
  - ALOHA
    - Pure Aloha
    - Slotted Aloha
  - CSMA
  - CSMA/CD
    CSMA/CA
- Control Access
  - Polling
  - Token Passing
- Channelization Prot.
  - FDMA
  - TDMA

Pure ALOHA

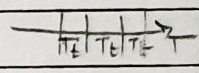
- Random Access Protocol
- ACK is there
- Retransmission, Collision
- LAN based
- Only transmission time no propogation time
- Vulnerable time = $2T_t$
- Efficiency = $\eta = G \times e^{-2G}$ $G \rightarrow$ no. of st who want to transmit data at specific time



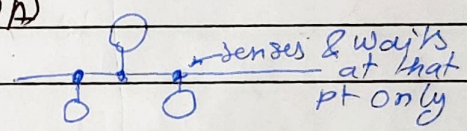
$TT = \frac{M}{BW} = \frac{1000 bit}{100 kb/s} = 10 msec$ $\times 10^{-3}$

Collision is min @ $G = 1/2$ ie $\eta = 18.4\%$

Pure ALOHA	Slotted ALOHA
• Any time transmission	• Beggining of slot
• $VT = 2 \times T_t$	• $VT = T_t$
• $\eta = G \times e^{-2G}$	• $\eta = G \times e^{-G}$
• 18.4% ($G = 1/2$)	• 36.8% ($G = 1$)



Carrier Sense Multiple Access (CSMA)



CSMA

- **1-Persistent**
  continously senses
  (high chances of collision)
- **0-Persistent**
  wait for some random time
  (less collision)
- **P-Persistent**
  senses & ~~waits~~ transmission depends on value of P
  $0 < P < 1$
  (less collision)

CSMA/CD (Collision Detection)

- No ACK system
- Sender recives collided data
- after complete transmission it can't be said if collided frequency is of its or other
- $TT > PD$
- $TT \geq 2 \times PP \rightarrow$ Worst case

$$\eta = \frac{1}{1 + 6.44a}$$

$$a = \frac{PD}{TT}$$

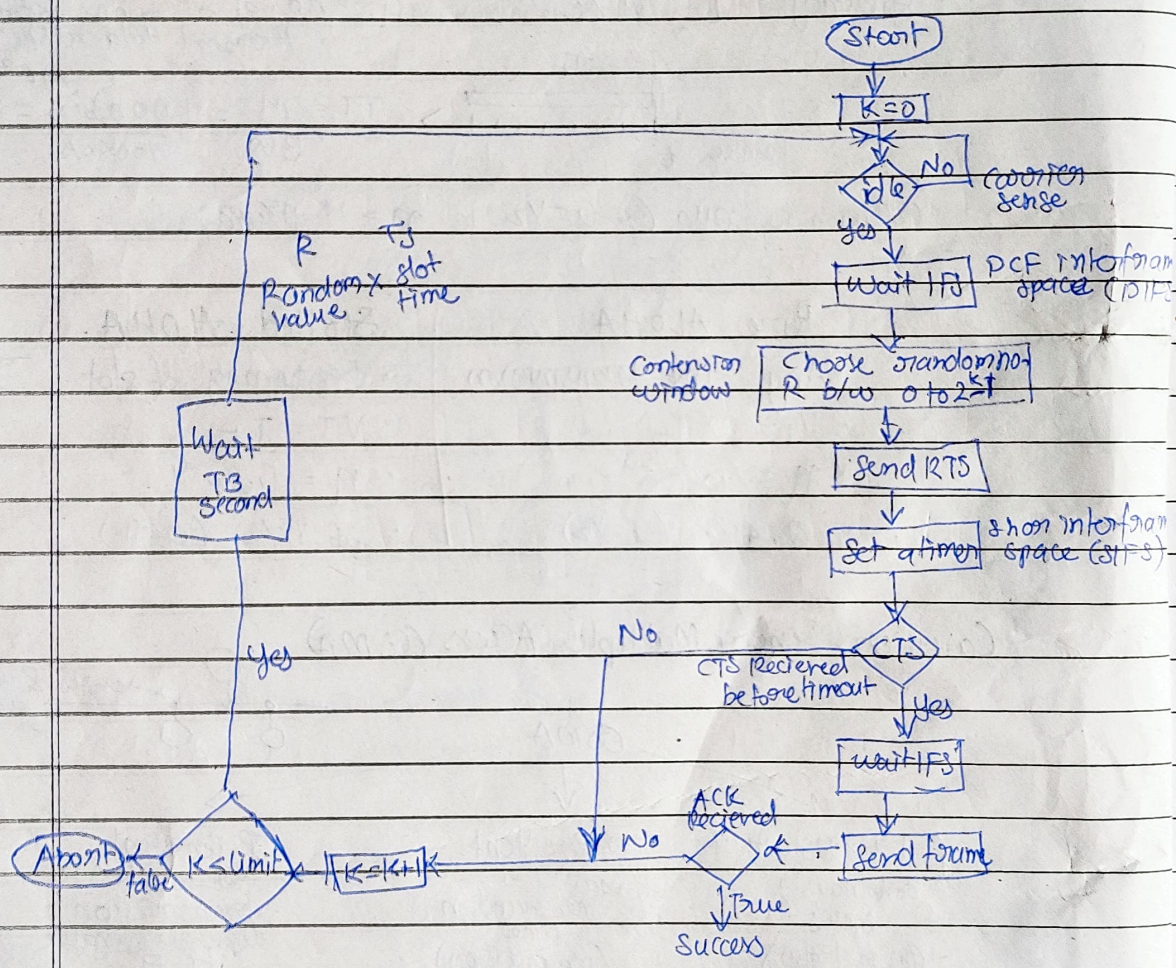
CSMA/CA (Collision Avoidance) (WLAN used)

- interframe space
- collision window
- ACK

K = no. of attempt T_B = Backoff time

IFS = interframe space RTS = ready to sent

CTS = Clear to send



Consider a CDMA/CD network that transmits data at a rate of 100 Mbps (10^8 bits per second) over 1km cable with no repeaters. If the minimum frame size required for this network is 1250 bytes. What is the signal speed (km/sec) in the cable?

A] 8000 B] 10000 C] 16000 D] 20000

$$TT \geq 2 * PD$$

$$\frac{L}{BW} \geq 2 * \frac{D}{V}$$

$$V \geq \frac{2 * D * BW}{L}$$

$$V \geq \frac{2 * 1 * 10^8}{1250 * 8}$$

$$V \geq 20000$$

$$\eta = \frac{1}{1 + 6.44a}$$

$$= \frac{1}{1 + 6.44\left(\frac{TT}{PD}\right)}$$

Ethernet Frame Format (IEEE-802.3)

- Datalink protocol
- 10 Base2 — Thin
  10 Base5 — thick
  10 Base T
  100 Base Fx — Fast
  10G Base-T · Gigabit
- Topology — Bus, Star
- 1 Mbits/sec — 400 Gbits/sec : Rate

MAC

PREAMBLE	SFD	DA	SA	Length	DATA	CRC
7B	1B	6B	6B	2B	46B-1500B	4B

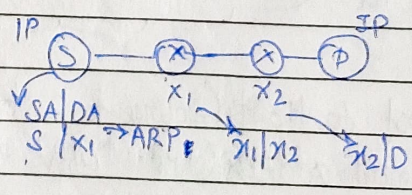
0 – $2^{16}-1$ / 0 – 65535

min – 64 bits (PL excluded)
max – 1518 bits

← PL →

56 bits
101010...10
8 bits
10101011

~~Dest address~~



Token Ring (IEEE - 8025)

- Ring Topology is used
- Access control method used is token passing
- Token ring is unidirectional
- Data Rate used is 4Mbps & 16 Mbps
- Piggybacking acknowledgement is used
- Differential Manchester encoding is used
- Variable size framing
- Monitor station is used

↳ Data Frame Format

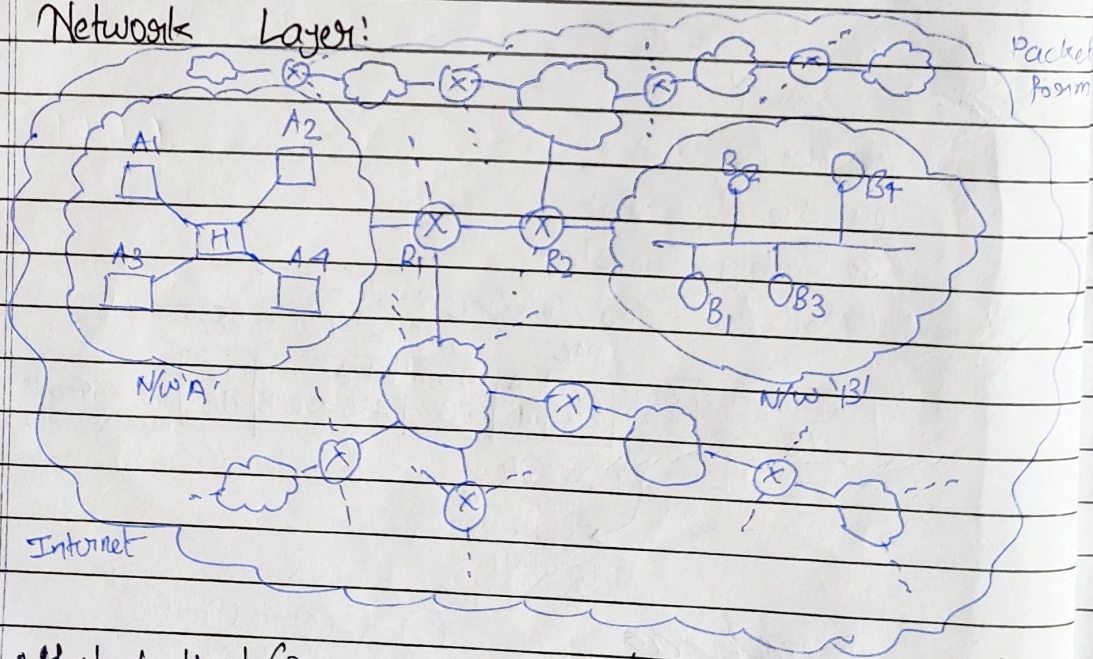
SD(1)	AC(1)	FC(1)	DA(6)	SA(6)	DATA	CRC(4)	ED(1)	FS(

DATA ↓ depends upon token holding time (tht)

↳ Token Frame Format

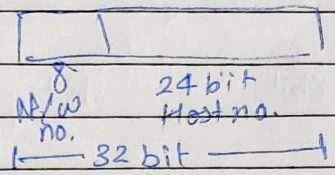
SD(1)	AC(1)	ED(1)

Network Layer:

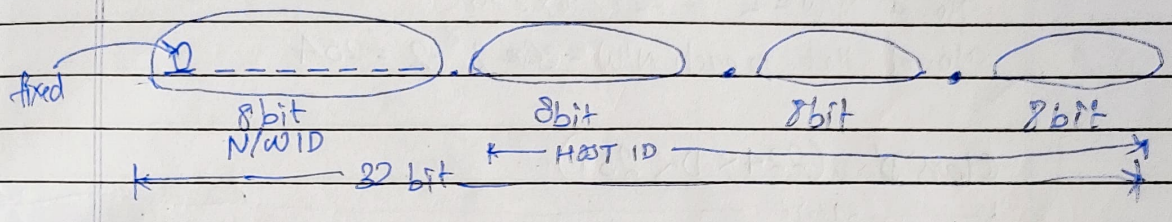


- Host to Host (Source to Destination / Machine to Machine Delivery
- Logical address (IP) ← Network, Host
- Congestion Control
- Routing (RIP, OSPF)
- Fragmentation

Classful Addressing



Class 'A' $(0 < A < 127)$ Default Mask = 255.0.0.0



Dotted decimal representation

Possible IP address in Class A = 2^{31}

notused ← 00000000, 01111111 — null and loopback address

No. of N/W in Class A = $2^7 = 128 - 2 = 126$

No. of host possible in every N/W = $2^{24} - 2$

1st address

- 64.0.0.0 – 1st IP address represents Network address

Last address – 64.255.255.255 – last address represents broadcast address

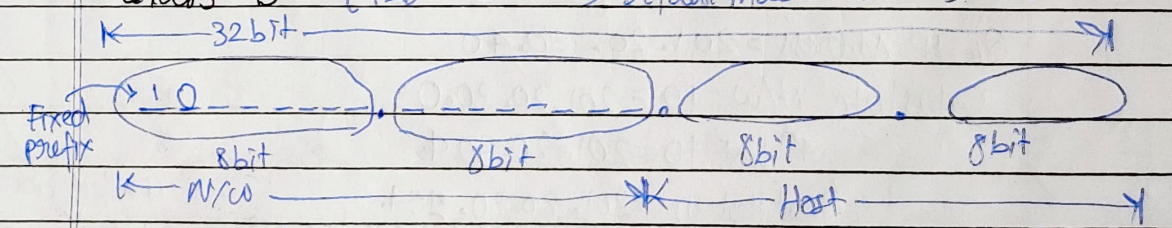
1st address = 64.0.0.8 i.e. 01000000.0.0.00001000 AND

Default mask = 255.0.0.0 i.e. 11111111.0.0.00000000

01000000.0.0.0

↳ 64.0.0.0 → N/W address

Class 'B' $(128 < B < 191)$ Default mask = 255.255.0.0



Range = 128 – 191

1st – 128.0.0.0
last – 128.0.255.255 } Eg.

No. of Network = $2^{14} = 64 \times 256 = 16384$

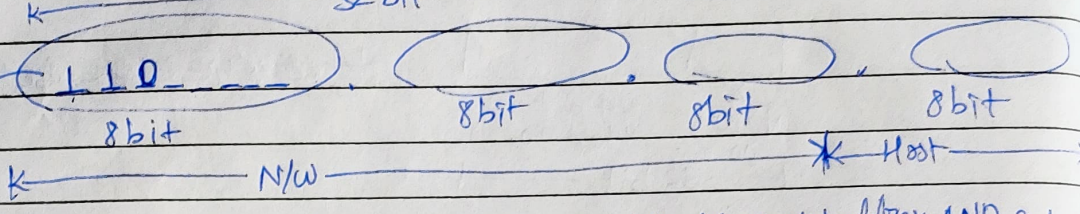
No. of host in each N/W = $2^{16} - 2 = 65534$

No. of address = 2^{30}

N/W address = 1st address AND Default mask

Date
Page

Class 'C' (192 < C < 223) Subnet mask = 255.255.255.0



Range = 192 - 223

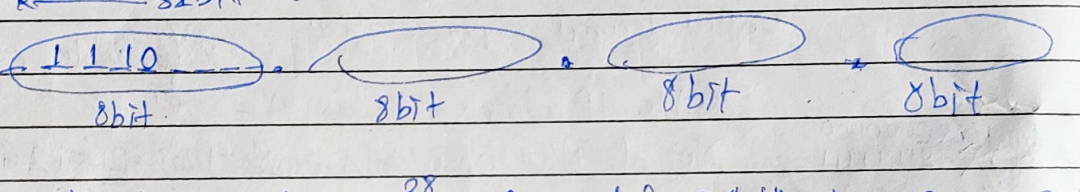
N/W address = 1st address AND Subnet mask

No. of IP Address = 2^{29}

No. of N/W = 2^{21} = 32 × 256 × 256

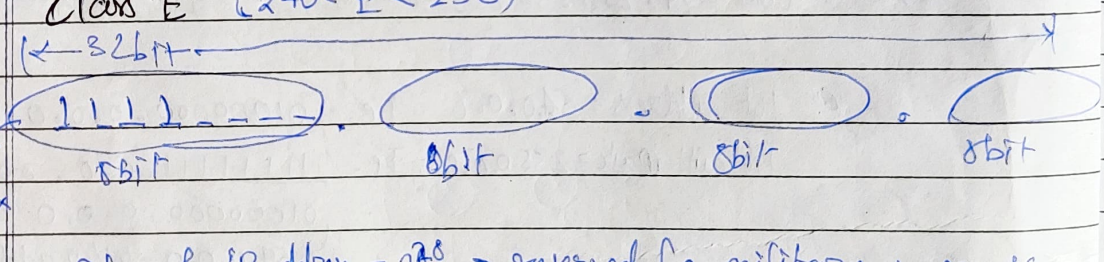
No. of Host in each N/W = $2^{8} - 2 = 254$

Class 'D' (224 < D < 239)



No. of IP address = 2^{28} → Reserved for Multicasting, Group Emo Broadcast

Class 'E' (240 < E < 255)



No. of IP address = 2^{28} → reserved for military purpose

Q. IP Address = 201.20.30.40

Calculate N/W ID = 201.20.30.0

4th host ID = 201.20.30.4

last Host ID = 201.20.30.254

Broadcast Add = Limited 255.255.255.255 — limited address when host is in the n/w

~~Direct 201.20.30.255~~ — direct when host is from other n/w

201 → C class

N/W ID = 201.20.30.40 AND 255.255.255.0 = 201.20.30.0

0000 0000
0000 0001
0000 0010
0000 0100

201.20.30.255 — last broadcast — reserved

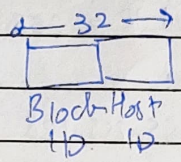
∴ last host = 201.20.30.254

Disadv of Classful Addressing

- Wastage of IP Address
- Maintenance is time consuming
- More prone to errors

Classless Addressing

- No classes
- Only blocks
- Notation



x.y.z.w/n

n → no. of 1's (mask)

n → no. of bits represents block/network

No bits to represent host = $2^{(32-n)}$

~~NW ADD = IP AND mask~~ Keep n bits same and make remaining bits zero to get N/W address

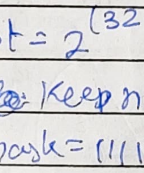
if n=28 then mask = 11111111.11111111.11111111.11110000

= 255.255.255.240

or → AND IP

e.g. 200.10.20.40/28

200.10.20.00010000 (28 bits | make all 0)



$2^4 = 16$

N/W add: 200.10.20.00100000

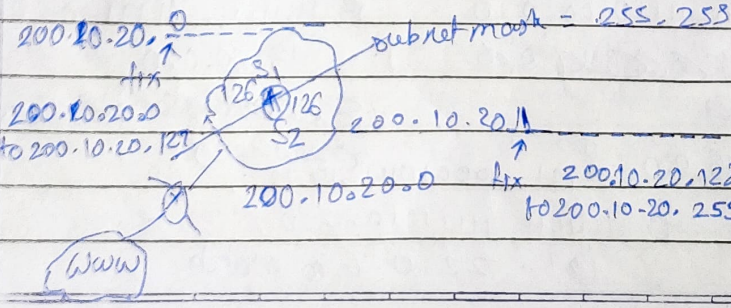
200.10.20.32/28

Rules:

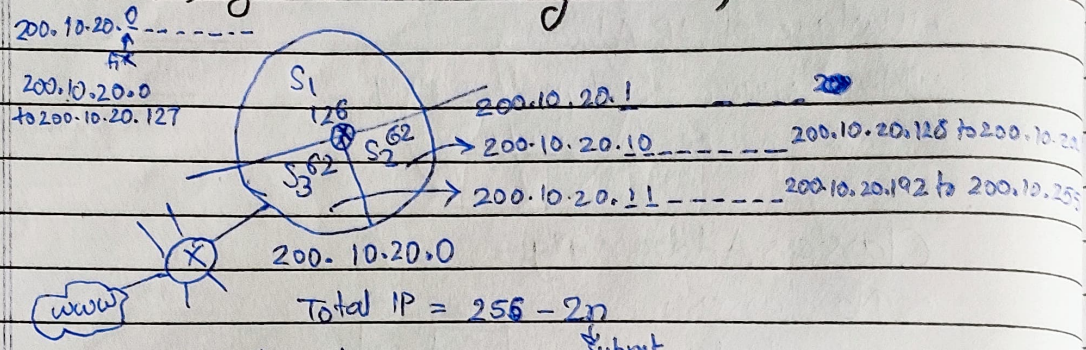
- Address should be contiguous
- No. of address in a block must be a power of 2
- First address of every block must be evenly divisible with size of block. (last 4 bit should be 0)

Subnetting

Dividing big network into small network



Variable length subnet masking (VLSM)



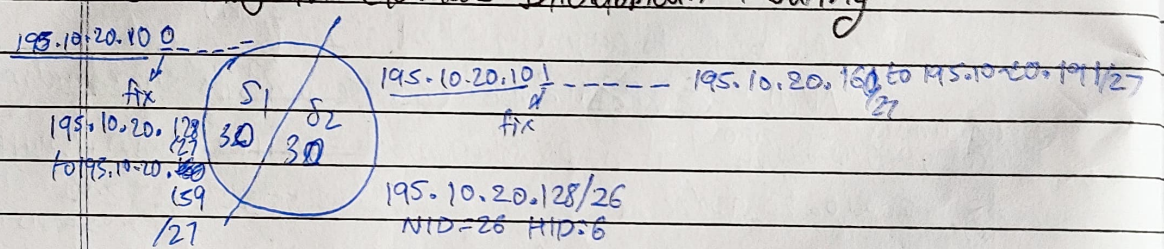
Total IP = 256 − 2n
subnet

Subnet mask:

S_1 : 255.255.255.128

S_2 : 255.255.255.192

Subnetting in Classless Interdomain Routing



Q CIDR receive a packet within address 131.23.151.76. The Regotab routing table has following entries:

	Prefix	O/P Interface
A	131.16.0.0/12	3 ✓
B	131.28.0.0/14	5 ✗
C	131.19.0.0/16	2 ✗
D	131.22.0.0/15	1 ✓

* Mark the prefix with higher number

Packet will be forwarded to which interface. D

00010111

131.23.151.76

131.00010111.151.76

A 11111111.11110000.0.0

B 11111111.11111100.0.0

131.20.0.0

match 131.16.0.0

131.00010111.151.76 → wrong

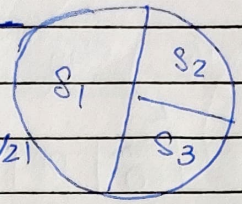
D 11111111.11111110.0.0

131.22.0.0 match

VLSM in CIDR

245.248.10000 ---
N/W bit ↓ fix

245.248.128.0/21
to 245.248.135.255/21



245.248.128.0/20
NID = 20 HID = 12

24
245.248.10001 → fix
245.248.10001.0 ---
fix
245.248.136.0/22
to 245.248.139.255/22
245.248.100011 ---
fix
245.248.140.0/22
to 245.248.140.255/22

IPv4 Header

- Connectionless
- Datagram Service

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				
Destination IP Address 32 bits				
Options & Padding				

Datagram ← Header Size = 20-60 Bytes
+
Payload = 0-65515 Bytes

VER- Version HLEN - ~~Header~~ Header Length (X4)

Type of service:

Differentiated Services code Point (DSCP)

P	P	P	D	T	R	C	O

Precedence, Delay, Throughput cost, Reliability, Reserved

Explicit Congestion Notification

DSCP	ECN
0 – 5	6 – 7

Total length = 2^{16} = 65535

2nd row - Fragmentation part

Time to Live = 2^8 = 255 will drop packet once 0 drop 1 at every step

Protocol - TCP/IP, UDP protocol usage of upper layer

Checksum - error detection of Header

Options & Padding - To add extra data

Fragmentation of IPV4 Datagram

Identification bits 16	Flag 3	Fragment offset 13

no. of bits ahead

Res.	DF	MF
0		

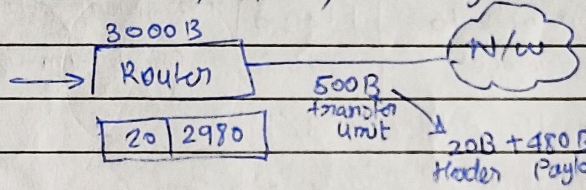
DF: Donot fragment
MF: More fragment

tells packet no.

Fragmented: 0 0, 0 1

Not fragmented: 1 0, 1 1

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



$\frac{2980B}{480B} = 7$

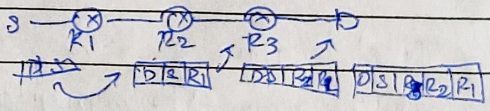
P_7	P_6	P_5	P_4	P_3	P_2	P_1	
100+20	410+20	480+20	480+20	480+20	480+20	480+20	
120	500	500	500	500	500	500	total length
0	1	1	1	1	1	1	MF
360	300	240	180	120	60	0	offset → scale of 8 i.e. $\frac{Data}{8}$

$480/8 = 60$

Options & Padding in IPv4

Option : 0-40 bytes

- Record Route
  // Can store up to 9 router location



- Source Routing (Packet tell routing route)
  - → Strict Source Routing (Tell complete path)
  - → Loose Source Routing (Incomplete)
- Padding
  - Scale of header is 4
  - So if 23 it will add 1 extra byte

IPv6 Header (128 bit address)

Base Header	Extention 1	. . . . .	Extention N	Data

VERSION (4)	Priority (8)	Flow label (20)	
Payload length (16)		Next (8) Header	Hop (8) Limit
Source address (128)			
Destination address (128)			

Base Header = 40 Bytes (320 bits) // Fixed

Priority/Traffic type - Congestion control
Flow label - real time data processing (ensures no delay)
converting Datagram into a Virtual circuit
follows single path (makes reservation)
Payload length - 65535B cand add extra using extention
Next header - holds extension header
Hop limit - same as time to Live (drops packets when 0)

Extention Headers:

1) Routing Header (43) (Route ~~path~~ path by source)
2) Hop by Hop option (0) (provides info to hop)
3) Fragment Header (fragementation) - by source not router
4) Authentication Header (51) (to maintain data integrity)
5) Destination options (60) (address read only by destination)
6) Encapsulating Security Payload (50) (for security ie encrypt decrypt)

Routing Protocols

Routing Protocols

Internet divided in autonomous sys (same admin)
(Do make dynamic routing tables)

(within autonomous) Intradomain

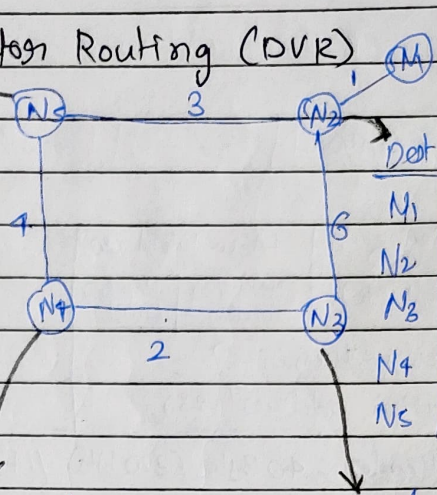
Interdomain (b/w autonomous)

Distance Vector (RIP)

Link State (OSPF)

Path Vector (BGP) } Unicasting algos

Distance Vector Routing (DVR)



Dest	Dist	Next
N_1	∞	–
N_2	3	N_2
N_3	∞	–
N_4	4	N_4
N_5	0	N_5

Dest	Dist	Next
N_1	1	N_1
N_2	0	N_2
N_3	6	N_3
N_4	∞	–
N_5	3	N_5

Dest	Dist
N_1	0
N_2	1
N_3	∞
N_4	∞
N_5	∞

Dest	Dist	Next
N_1	∞	–
N_2	∞	–
N_3	2	N_3
N_4	0	N_4
N_5	4	N_5

Dest	Dist	Next
N_1	∞	–
N_2	6	N_2
N_3	0	N_3
N_4	2	N_4
N_5	∞	–

- only neighbour share
- shares distance vector (Dist array)

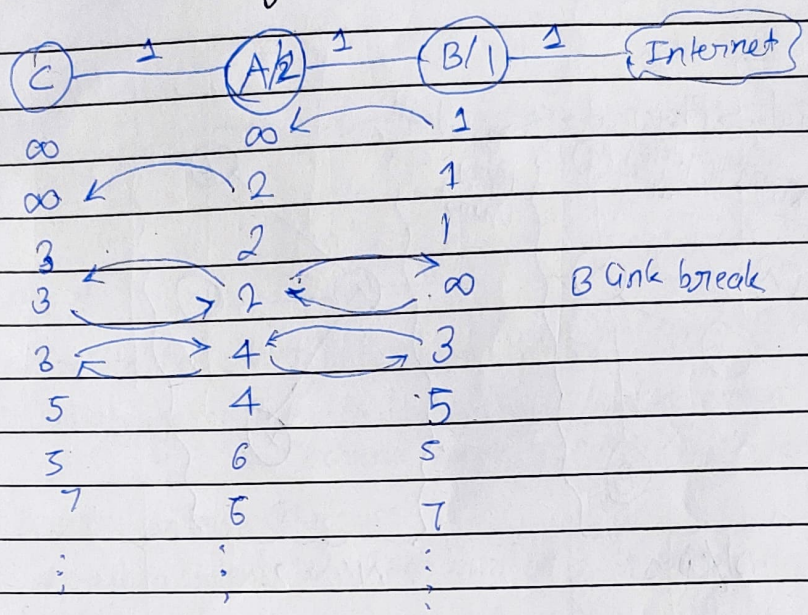
Updating N_1: N_2 — N_1 New Routs

N_2	Dest	Dist	Next	
1	N_1	0	N_1	
0	N_2	1	N_2	$N_1 \to N_2 + N_2 \to N_2$
6	N_3	7	N_2, N_3	$N_1 \to N_2 + N_2 + N_3$
∞	N_4	∞	–	$N_1 \to N_2 + N_2 \to N_4$
3	N_5	4	N_2, N_5	$N_1 \to N_2 + N_2 \to N_5$

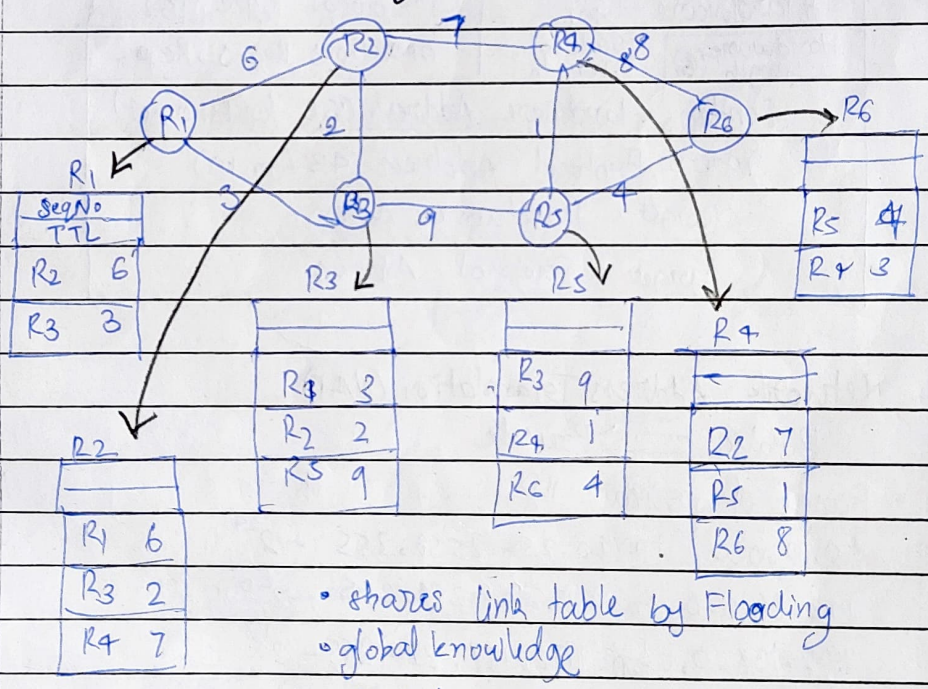
Updating N_5: N_2 — N_5 New RT

N_2	N_4	Dest	Dist	Next	
1	∞	N_1	4	N_2, N_1	$N_5 \to N_4 + N_4 \to N_1$ $N_5 \to N_2 + N_2 \to N_1$
0	∞	N_2	3	N_2	
6	2	N_3	6	N_4, N_3	$N_5 \to N_4 + N_4 \to N_3$ $N_5 \to N_3 + N_3 + N_3$
∞	0	N_4	4	N_4	
3	4	N_5	0	N_5	

Count to Infinity problem in DVR



Link state routing



- shares link table by Flooding
- global knowledge
- Dijkstra path

	R2	R3	R4	R5	R6
R1	6	3	∞	∞	∞
R1 R3	5	3	∞	12	∞
R1 R3 R2			12	12	∞
R1 R3 R2 R4			12	12	21
R1 R3 R2 R4 R5					16

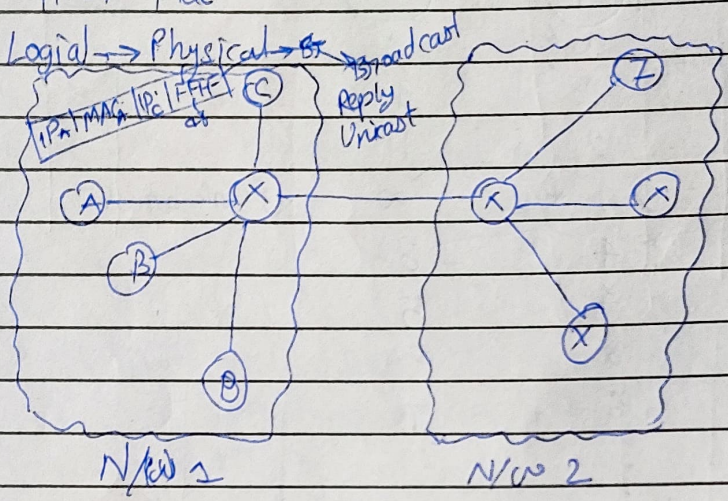
		via
R1	0	R1
R2	5	R1
R3	3	R1
R4	12	R3 R2
R5	12	R3
R6	16	R3 R5

Address Resolution Protocol (ARP)

IP → Mac

Logial → Physical → Broadcast

Reply Unicast



← 8 →	← 8 →	← 16 bits →
Hardware Type		Protocol Type (16)
Hardware Length (6)	Protocol Length	Operations Req-1, Rep-2
Sender Hardware Address (6B for Ethernet)		
Sender Protocol Address (4B for IP)		
Target Hardware Address		
Target Protocol Address		

Network Address Translation (NAT)

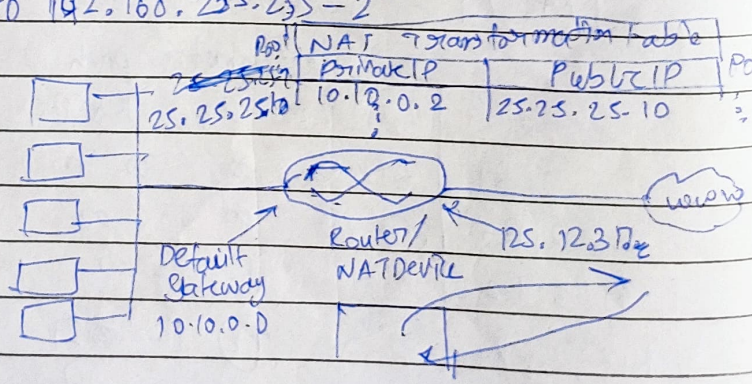
Public ⇄ Private

- Range of private IPs

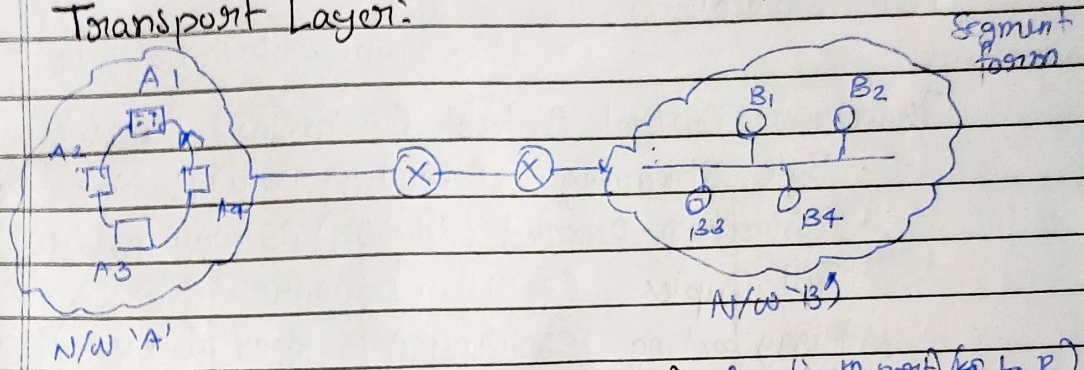
10.0.0.0 to 10.255.255.255 -2^{24}

172.16.0.0 to 172.31.255.255 -2^{20}

192.168.0.0 to 192.168.255.255 -2^{18}

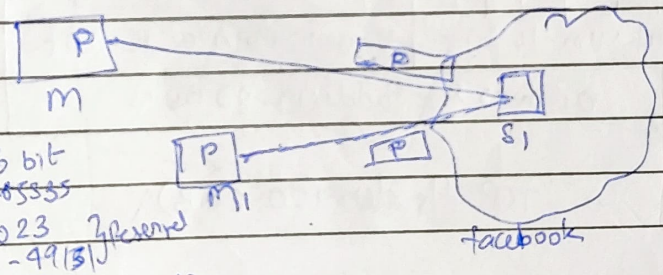


Transport Layer:



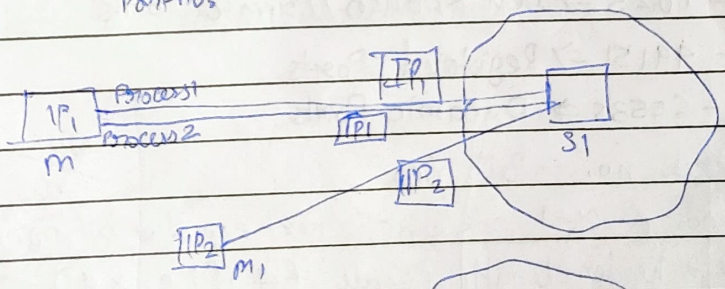
- End to End delivery (Port to Port) (Application port) (S to R)
- Reliability (In order delivery)(Equal no. of segment delivered) (Achieved using TCP/UDP) (No loss of data)
- Error Control (Checksum - TCP)
- Congestion Control (Advertising Window) (AIMD method)
- Flow control (Stop and Wait, Go Back N, Selective Repeat)
- Segmentation
- Multiplexing, Demultiplexing (Data from many application to 1) (Increase at R)

Socket Address (IP address + Port no.)

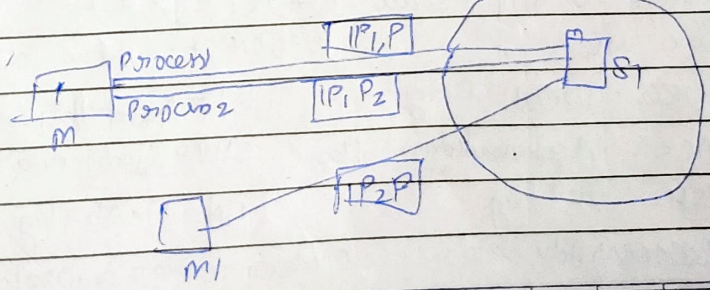


only port no. connection

16 bit
0 - 65535
0 - 1023 Reserved
1024 - 49151
49152 - 65535 - Machine Port no.



only IP address



IP + Port
32 + 16 = 48 bits

TCP Protocol:

segment - collection of bytes

Transmission Control Protocol (Transport Layer)

- Byte Streaming (Continous Data) (Convert into segments)
- Connection-Oriented (Reliability) (3-way handshake)
- Full Duplex (Both can transmit data @ same time)
- Piggy backing (Sending ACK along with Data) (GBN, SR)
- Error Control (Checksum)
- Flow Control
- Congestion Control (Take care of Recvr and network)

TCP Header

Source Port 16 bit								Destination Port 16 bit
Sequence no. 32 bit								
Acknowledgement no. 32 bit								
HLEN 4bit		U R G	A C K	P S H	R S T	S Y N	F I N	Window Size 16 bit
Checksum 16 bit								Urgent Pointer 16-bit
Options & Padding 40 Bytes								

TCP Header (20-60 B)

** 0 – 1023 ⇒ Well known / Private Ports

1024 – 49151 ⇒ Registered Ports

49152 – 65535 ⇒ Dynamic Ports

Sequence no. — Bit no.

ACK no. — x+1 ack sent (next expected bit no.)

HLEN - header length (Scale of 4) (i.e. x 4)

6 bit - future use

URGEN PT - Where is urgent data

URG - Urgent flag

RST - Reset flag

ACK - Acknowledgment flag

SYN - Synchronization flag

PSH - Push flag

FIN - Finish flag

Opt Padd - Extra bit

Window size - Adv window

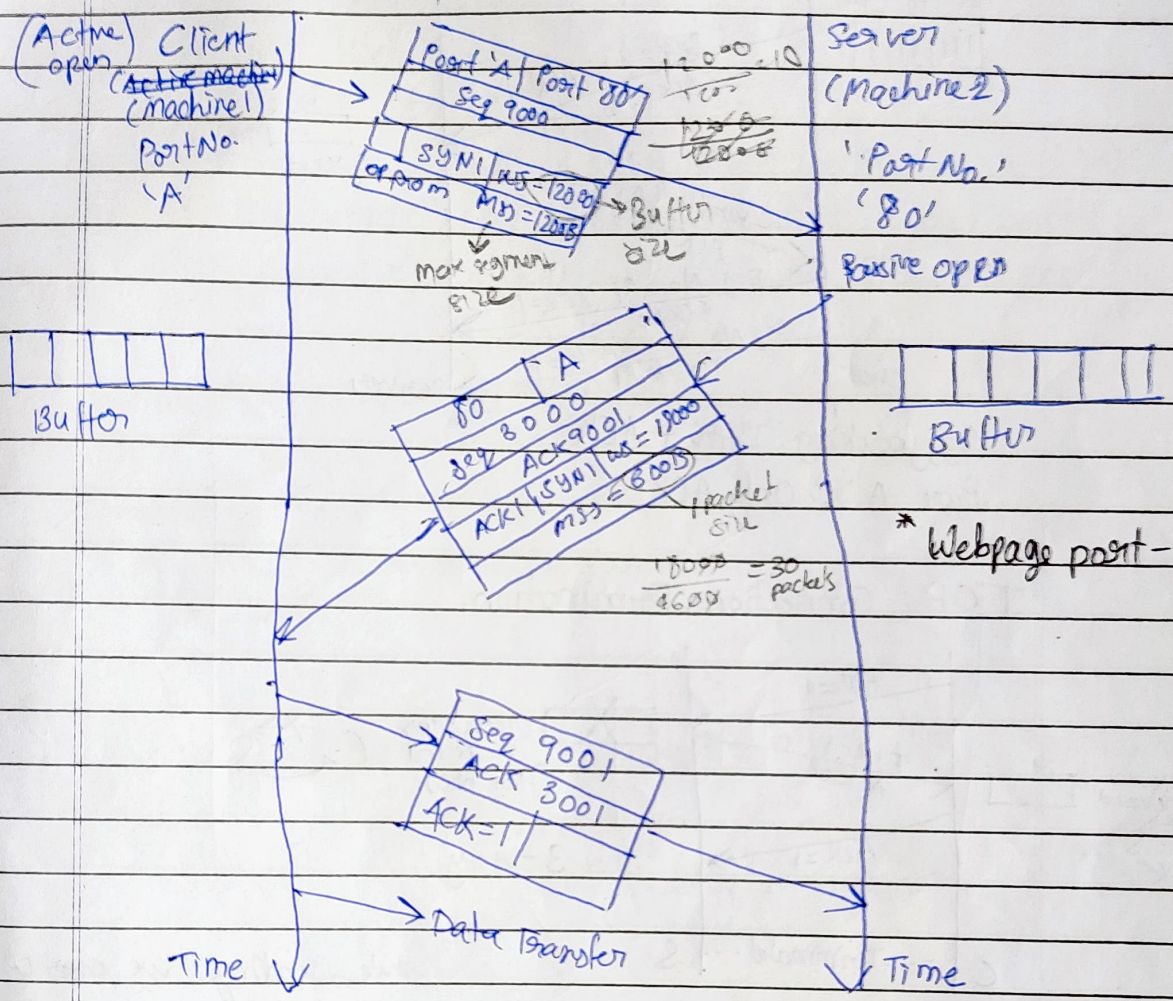
Checksum - error control

MSS

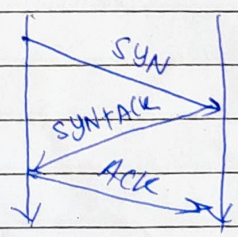
segmentation

TCP connection - Establishment and Termination

- Full duplex (3-way handshake)
- CPU, buffer, etc are reserved

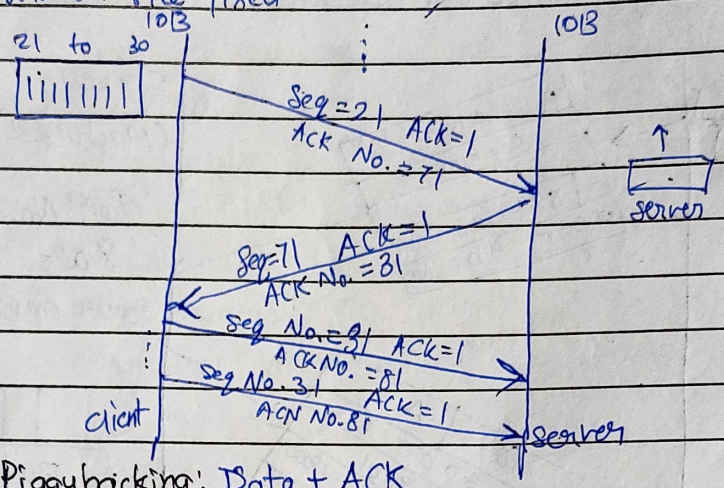


1st packet - connection establishment segment



TCP Data Transfer

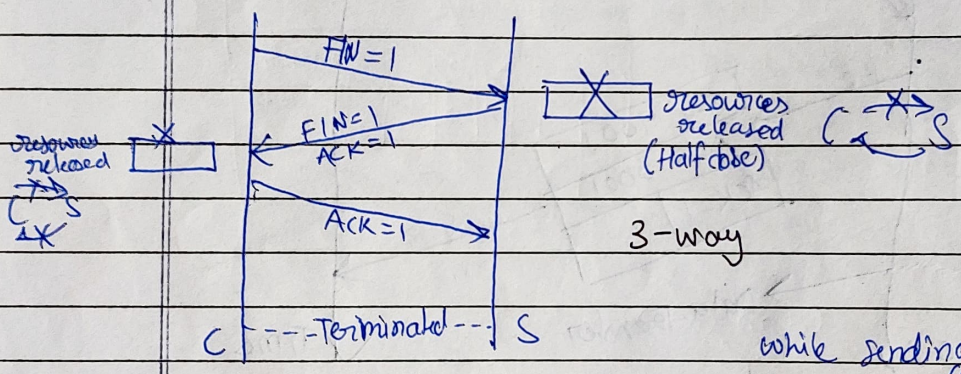
- Duplex mode [C ⇄ S]
- Windox size fixed



- Piggybacking: Data + ACK

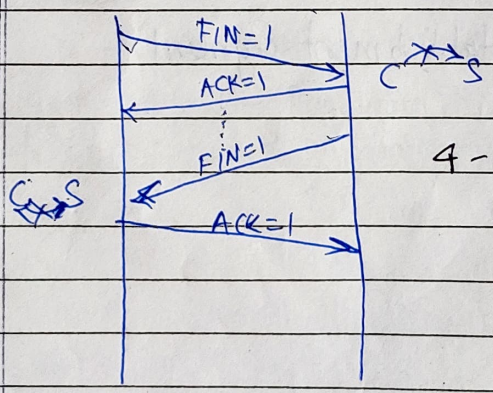
  Pure ACK: Only ACK

TCP: Connection Termination



3-way

while sending we use expected seq no. and use it again later for sending data.



4-way

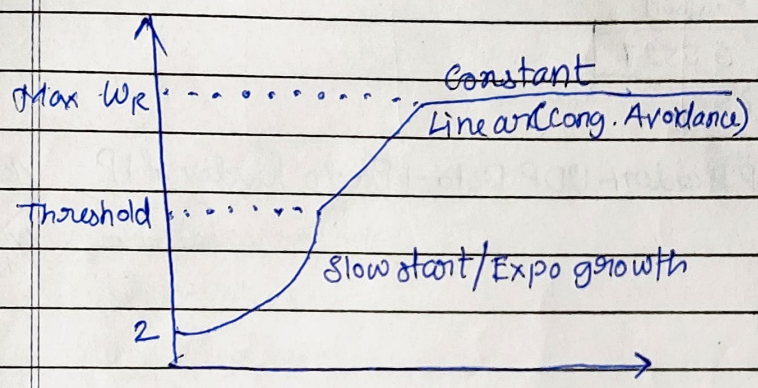
TCP Congestion Control

Let the size of congestion window of a TCP connection in two cases when

Case 1: Timeout occur (Severe)

Case 2: 3 ACK Received (Light)

is 32 KB. The RTT of a connection is 100 msec and MSS = 2 KB. The time taken (msec) by TCP Connection to get back to 32 KB congestion window is 1200 & 900 respectively



Case 1: 32 KB ↑ 2 (Timeout) Threshold = $\frac{32}{2}$ = 16 * Take node value if pt.

(start

4 → 8 → 16 stop

↳ Linear

↳ 18 – 20 – 22 – 24 – 26 – 28 – 30 – 32

12 × 100 = 1200 msec

segment RTT

(Round trip time)

Case 2: 32 ↑ 16 ← start

18 – 20 – 22 – 24 – 26 – 28 – 30 – 32

9 × 100 = 900 msec

segment RTT

UDP (User Datagram Protocol) header

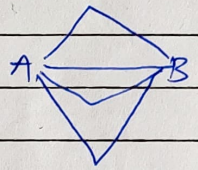
- Connectionless Protocol (Unreliable) • No ordering
- ~~TCP~~ UDP header + Payload

Source Port 16	Destination Port 16
Length 16	Checksum 16

Length: H | Payload
8 | 65527
65535

Checksum = UDP Header + UDP Data + Pseudo header of IP
↓ value that doesn't change

//Optional in IPv4
///Comp in IPv6



UDP Application

1] Query respons protocol (one request one reply) [DNS] [DHCP]
domain name
↳ my MAC address
IP — www
IP address

2] Speed (online games, voice over IP)

3] Broadcasting / Multicast [RIP] → Routing Information Protocol

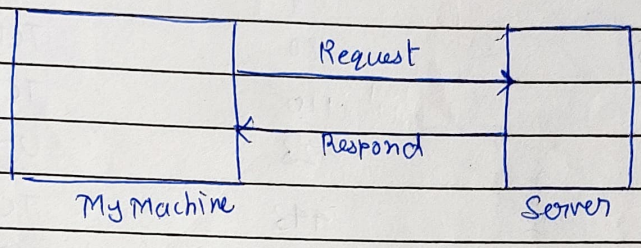
4] Continous Speed [Skype, Youtube] (stateless).

TCP	Vs.	UDP
• Connection oriented		• Connectionless
• Reliable		• Less Reliable
• Error control mandatory		• Error control is optional
• Slow transmission		• Fast transmission
• More overhead		• Less overhead
• Flow control & congestion control		• No flow control & congestion control

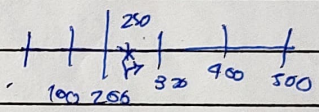
TCP-UDP Application

TCP	UDP
HTTP	DNS
FTP	BOOT P
	DHCP
	RIP

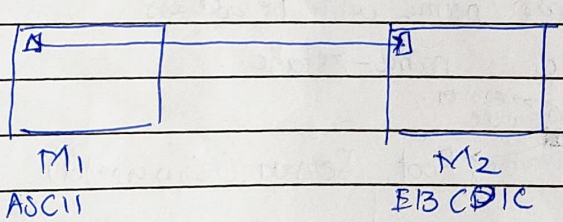
Session Layer



- ~~Session~~
- Authentication
- Authorization
- Session Restoration (Check point) – Session beans
- Webinar *flow control & synchronization



Presentation Layer



- Code Conversion (Formatting)
- Encryption/Decryption
- Compression

Application Layer

	Protocol Name	Port No.	Transport Protocol
Connectivity check To check RTT	Echo	7	TCP/UDP
File transfer protocol	* FTP	20/21	TCP
Secure key security	Secure Shell (SSH)	22	TCP
Remote login	* Telnet	23	TCP
Simple mail transfer protocol	* SMTP	25	TCP
To get IP — Domain name system	* DNS	53	UDP
Dynamic IP provides — Dynamic host control Protocol	DHCP	67/68	UDP
Trivial file transfer Protocol	TFTP	69	UDP
Hyper text transfer protocol	* HTTP	80	TCP
To pop mail — Post office protocol	POP	109 old/post 110	TCP
Syn time — N/w time protocol	NTP	123	UDP
Secured version of HTTP (SSL)	HTTPS	443	TCP
Routing Information protocol	RIP	520	UDP

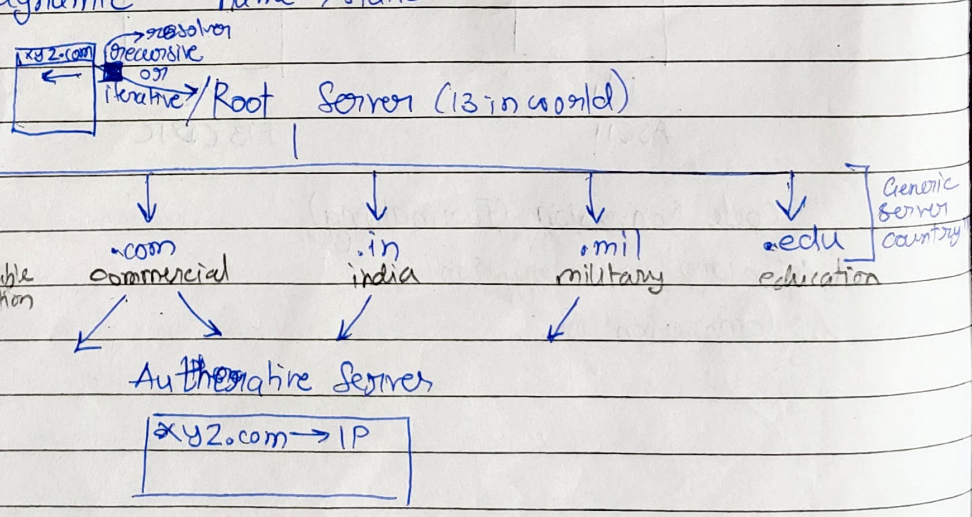
0 - 1023 - Well defined

1st port - data transfer
2nd port - control commands
out of line protocol

Domain Name System

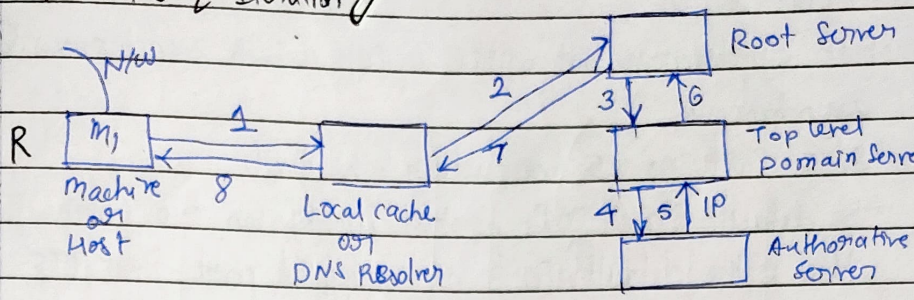
To map domain name with IP address

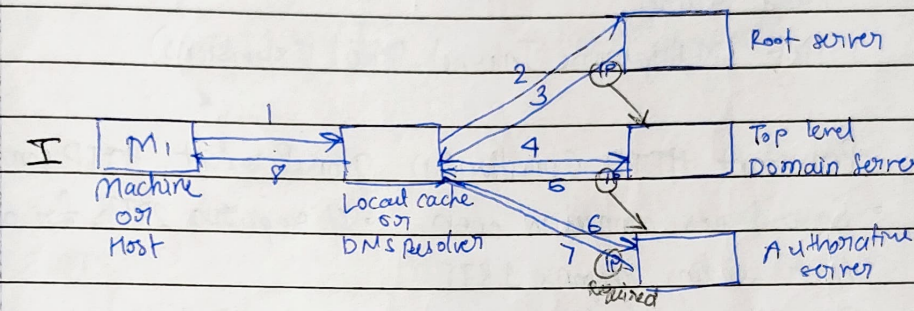
IP → dynamic name → static



Date
Page

Reaursive & Iteration





HTTP

- Port no. 80
- Itself not reliable but use TCP to achieve reliability
- Inband protocol (Commands & Data using same port)
- Stateless (Doest save request)
- HTTP 1.0 Non-Persistent (Re-write data once connection lost)
- HTTP 1.1 Persistent
- Commands (Head, Get, Post, Put, Delete, Connect)
  metadata

FTP

- Port no. 20(DATA) & 21 (Control)
- Data connection is non-persistent
- Control connection is persistent
- Not Inband
- Reliable
- Stateful

SMTP & POP

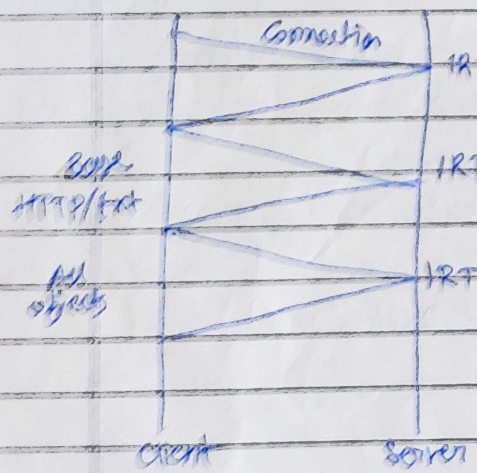
- FTP synchronous but SMTP & POP is both synchronous & asynchronous
- SMTP Port no 25 for pushing the mail
- By default, the POP3 protocol works on two ports: Port 110 - this is the default POP3 non-encrypted port. Port 995 - this is the port you need to use if you want to connect using POP3 securely
- MIME (Multipurpose Internet Mail Extensions)

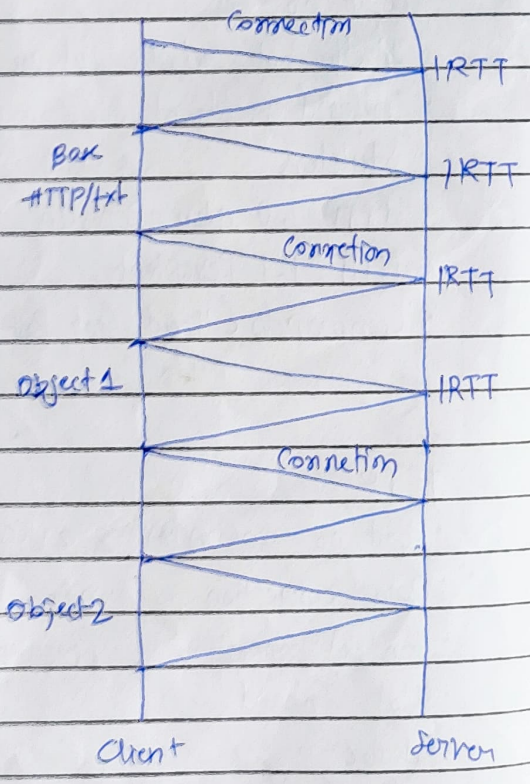
Persistent HTTP Connection (1.1)

- Server leaves connection open after sending response 1 RTT for all referred object
- Less overhead

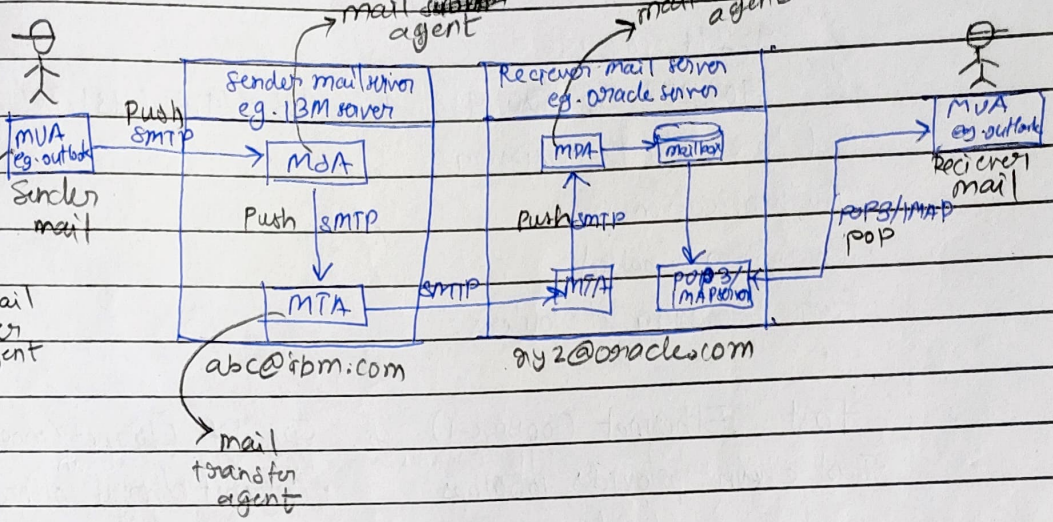
Non-Persistent HTTP Connection (1.0)

- It requires 2RTTs for object
- More overhead





SMTP vs POP3 vs IMAP → internet message access protocol



SMTP	POP	IMAP
• Simple Mail Transfer Protocol	• Post office protocol	• Internet message access protocol
• Send mail (PushMail)	• Retrieve Mail (Pop Mail)	• Retrieve Mail (Pop Mail)
• Port no = 25	• Port no = 110 (Default) 995 (SSL)	• Port no = 143 (Default) 993 (SSL)
• TCP/UDP Default	• TCP/UDP will delete from mailbox	• TCP/UDP will send a copy and keep mail in mailbox and can be retrieved.

Socket Programming (How applicatn will communicate over internet)

↳ node

Domain, Type, Protocol

Active end point

Server		Client
SOCKET()		
BIND()		SOCKET()
LISTEN()	←	CONNECT()
ACCEPT()	Connection Established	
SEND() (write)	→	RECV() Read
RECV() (read)	←	SEND() write
CLOSE()	Terminate	CLOSE()

SOCK_STREAM - TCP
SOCK_DGRAM - UDP

Socket address = IP + Port

Date
Page

Need of IPv6 (IPng) → IP next generation

- Limitation in IPv6 addresses
  2^{32} - 4,294,967,296
  2^{128} - 340,282,366,920,938,463,463,374,607,431,768,211,456
- Real time data transmission
- Authentication
- Encryption enabled
- Fast Processing at routers.

Fast Ethernet (100Base-T) vs. Gigabit Ethernet (1000 Base X)

Fast Ethernet (100Base-T) IEEE 802.3u	Gigabit Ethernet (1000 Base X) 802.3z, 802.3ab, ah
• Fast ethernet provides 100Mbps speed & introduced in 1995	• Gigabit ethernet offers 1Gbps speed. It came to use in 1999
• 100 Base-T4 (twisted cable), 100Base -Tx (2), 100 Base -FX → fiber optic base (2)	• 1000 Base-SX (Fibre short), 1000 Base -LX (long), 1000 Base -Cx, 1000 Base -T (twisted copper)
• Fast ethernet generate more delay comparitively	• Gigabit ethernet generate less delay than fast ethernet
• The coverage limit of fast ethernet is up to 10km.	• While the coverage limit of gigabit ethernet is up to 70km
• Fast ethernet is the successor of 10-Base-T ethernet	• Gigabit ethernet is successor of fast ethernet.