Computer Networks

Computer Networking refers to interconnected computing devices that can exchange data and share resources with each other.

Sending data

Sender [S] → [R] Reciever

[For sending data their must be some connection present between two devices, which is handled by Computer Networking]

⊛ Their must be some protocols between the sender and reciever which must be followed during data transferring.

⊙ Sometimes the sender and reciever should be in the same machine, then the communication is called inter-process communication which is handled by OS.

⊙ If the sender sending the data from another device or server and reciever fetching the data from another device then it is handled by Computer Networking.

Functionalities

- Mandatory
  - Error Control
  - Flow Control
  - MUX/DeMUX
- Optional
  - Encryption/Decryption
  - Checkpoint

Based on these functionalities there are some model presents in the theory of computer Network. Among them the most basic models are,

(i) OS-I Model (ii) TCP/IP Model.

In OS-I model functionalities are divided into some layers ~~&applications~~. 7 layers are there -

Physical layer → Data link → Network → Transport → Session → Presentation → Application

⊙ Types of Computer Network -

1) PAN (Personal Area Network):

→ Technology used: Bluetooth, IrDA, Zigbee.
→ Range: 1-100 Meter
→ Transmission Speed: Very High
→ Area: Small [withing a room]
→ Ownership: Private
→ Maintenance: Very easy.
→ Error rate & Cost: Very low.

2) LAN (Local Area Network):

→ Technology used: Ethernet and Wi-Fi
→ Range: Approximately upto 2KM
→ Transmission Speed: Very High
→ Area: Withing office, building
→ Ownership: Private
→ Maintenance: Easy
→ Error rate & Cost: Comparatively low.

3) CAN (Campus Area Network):

-> Technology used: Ethernet
-> Range: 1-5 km
-> Transmission Speed: High
-> Area: Within University, Corporate offices
-> Ownership: Private
-> Maintenance: Moderate
-> Error rate & Cost: Moderate

4) MAN (Metropolitan Area Network):

-> FDDI, CDDI, ATM
-> Range: 5-50 KM
-> Transmission Speed: Average
-> Area: Within City like Kolkata/Mumbai
-> Ownership: Private/Public
-> Maintenance: Difficult
-> Error rate & Cost: High Comparatively

5) WAN (Wide Area Network):

-> Technology Used: Leased Line, Dial-up.
-> Range: Above 50 KM
-> Transmission Speed: Comparatively low
-> Area: Within Countries
-> Ownership: Private Or public
-> Maintenance: Very difficult
-> Error Rate & Cost: Very High.

⊙ OS-I Model:

(i) **Application layer:** Provide Services for Network Applications with the help of protocols to perform user activities.

[HTTP, HTTPs, FTP etc.]

Services like, File transfer (FTP), Emails (SMTP), Web Surfing (HTTP/s), Virtual Terminals (Telent).

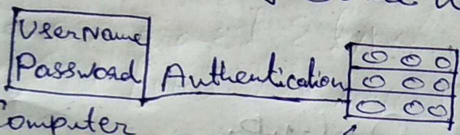
(ii) **Presentation Layer:** Recieves data from app. layer in the ~~the~~ form of Charracters and numbers. This layer Convert the data to binary format (ASCII ↳ EBCDIC)

⊛ This ~~tran~~ convertion is also known as Translation.

DFGJUYRG
6457899 5412 → $\boxed{\text{Translation}}$ → 10001110 1101 → $\boxed{\text{Compression}}$ → 10101101 → $\boxed{\text{Encryption}}$ → 10011011 → [SSL → Secure Socket Layer is used]

10011011 → $\boxed{\text{Decryption}}$ → 10101101

(iii) **Session layer:** Helps to communicate between two devices using some helpers known as APIs.



[Authentication is the process of knowing "who you are?"]

After authentication, authorization is cheked whether the data can be accessible or not?

Both authentication and authorization is done by Session layer. This layer keep tracks on which data is retrieved from where.

(iv) Transport layer: Segmentation, Flow Control, Error Control

1) Segmentation:

Session layer
↓ recieves data
data

Each segment has its ~~each~~ Seq. and Port Number.

Seq. Port Data | Seq. Port Data | Seq. Port Data

Broken down into segments

WP. Fb. Chrome

[Using Port Number] [Data can go into the apps]

2) Flow Control: The speed (Mbps) is check while transfering data between two devices.

[Stop & Wait
Go Back N
SR]

Computer → Data Transfer → Mobile

50 MBPS | 10 MBPS

Transport Layer helps to incr./decr. data speed ↑↓

3) Error Control:

Computer | D1 D2 D3 | D1 ← Missing → D3 | Mobile

[Automatic Repeat Req. is generated by Transport layer to resolve the loss]

CheckSum method is used here.

Transport layer

Service		Protocols:
Connection Oriented Transmission	→	Transmission Control Protocol (T
Connection less Transmission	→	User Diagram Protocol (UDP)

* UDP is faster than TCP

UDP [No feedback]

[No need to recieve all data]

Ex: Video Games, Movies, Audio clip etc.

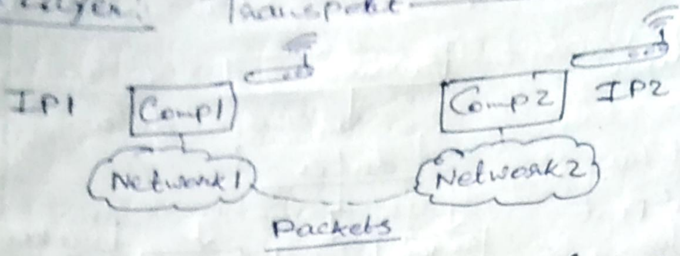
TCP [Feedback]

[Full data recieve is must]

Ex: WWW, Emails, FTP etc

TCP ~~f~~ provides reliability in the system as well as msgs are also inorder.

(v) <u>Network Layer:</u> Transport $\xrightarrow{\text{Segments}}$ Network layer.



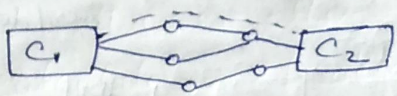
<u>Functionalities:</u> 1) Logical Addressing (IP Addressing)

$C_1 \xrightarrow[\text{using}]{\text{Routing}} C_2$
IP Address

[Sender IP & Reciever IP is assigned to each segment to form IP Packet]

2) <u>Routing:</u> Process of sending and recieving data is done using Routing. Routing use those IP addresses to deliver correct data on correct ~~Cost~~ device.

3) <u>Path determining:</u>



Various Paths are present

[The process of choosing Shortest path is Path determining]

<u>Protocols:</u>

- OSPF (Open Shortest Path First)
- BGP (Border Gateway Protocol)
- IS-IS (Intermediate System - Intermediate System)

(vi) <u>Data link layer:</u> ~~Data~~ Network layer $\xrightarrow{\text{Data packets}}$ Data link layer

↓

[This packet contains IP addresses]

Address are of 2 types.

- Logical [Network layer]
- Physical [Data link layer]

This packets are framed by data link layer. Each frame contains:

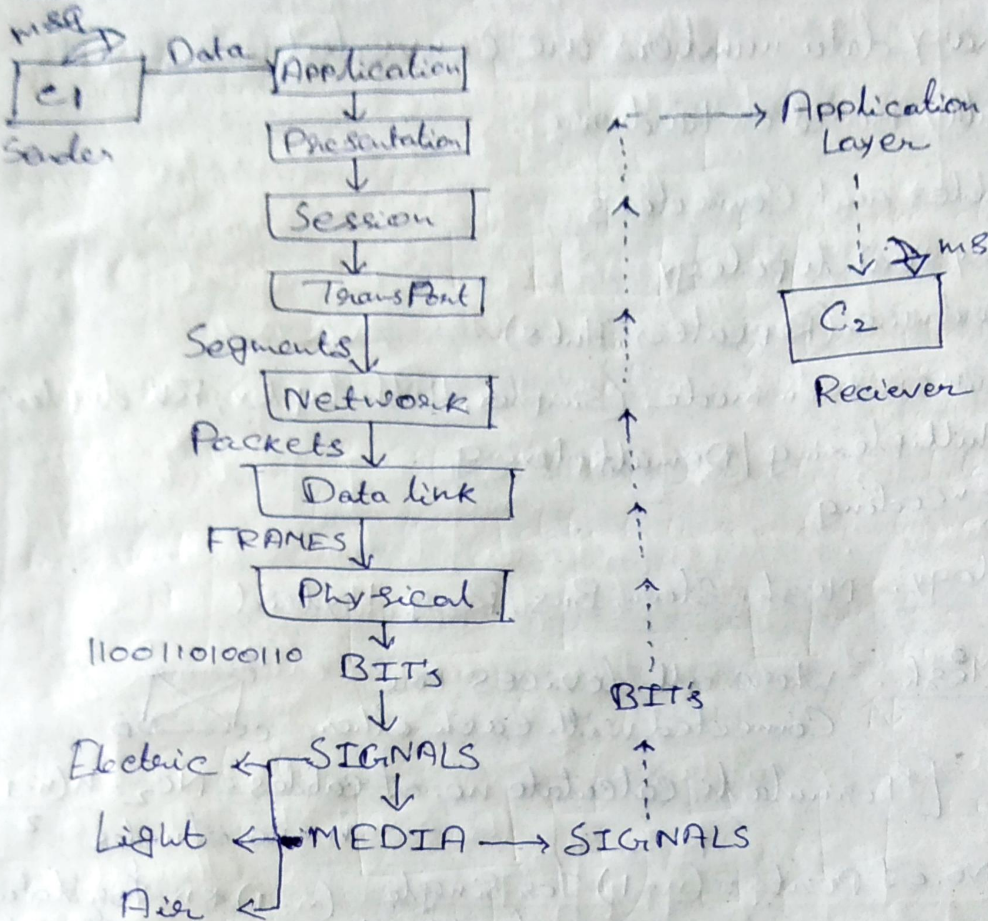
Source MAC	Destination MAC	Packet	FCS

<u>FRAME</u>

[This increases reliability]

(vii) <u>Physical layer:</u> ~~Convert~~ Collect those binary seq. of data from frames and convert it into signal which is further transmitted to the media.

Shortcut OS-I



TCP/IP protocol with OS-I model

TCP/IP	OS-I	TCP/IP	
Application layer	App layer Presentation layer Session layer	Application layer	Process to Process
Transport layer	Transport layer	Transport layer	Host to Host
Network layer	Network layer	Internate layer	Source to Destination
Data link layer	Data link layer	Network Access layer	Node to Node
Physical layer	Physical layer		
5 layer		4 layer	

- OS-I → Theory Model developed by ISO.
- TCP/IP → Implementation model developed by Arpanet.

Physical layer & it's functionalities:

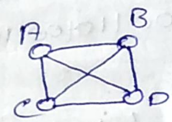
Binary data numbers are converted into signal.

Totally Based on hardware.

→ Cables and Connectors
→ Physical topology
→ Hardware (Repeaters, Hubs)
→ Transmission mode (Simplex, Half-duplex, Full-duplex)
→ Multiplexing / Demultiplexing
→ Encoding

• **Topology:** Mesh, Star, Bus, Ring, Hybrid

i) **Mesh:** Where all devices are connected with each other.

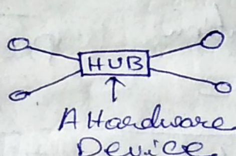


[*Formula to calculate no. of cables = $NC_2 = \frac{n(n-1)}{2}$]
n = no. of nodes

[* No. of Ports = $(n-1)$ for single device, $(n-1) * n$ for total devices]

* Highest Reliability ↑
* Cost is also high ↑
* Provides Security
* Maintenance is high.
* Supports point to point Communication (Dedicated)

ii) **Star:** Where all devices are connected with hub

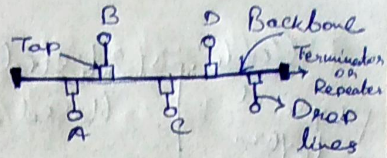


No. of Cables → n

No. of Ports → total n

* Less Reliability
* Cost is comparatively low
* Less Security
* Maintenance is low
* Supports point to point Communication (Dedicated)

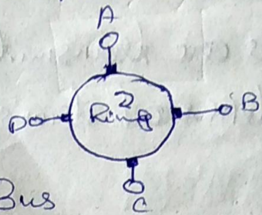
iii) Bus: All are connected with a backbone cable with high bandwidth



- No. of Cable = n+1
- No. of ports = n
- Low Reliability
- Low Security
- Low Cost
- Multipoint Communication

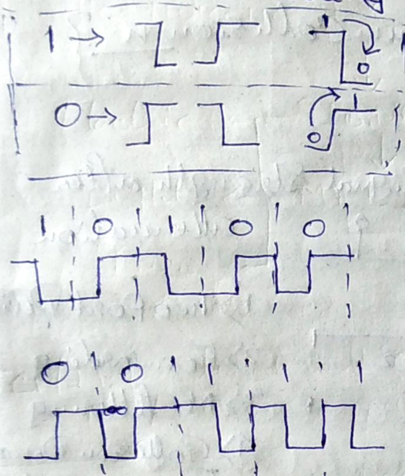
(*) Here Collision occurs due to multipoint communication.

iv) Ring: All are connected with a backbone cable ~~[illegible]~~ in a shape of ring.

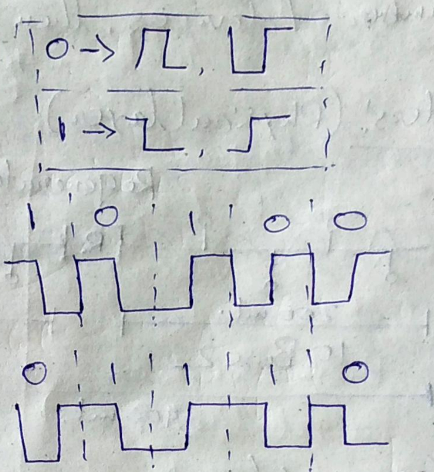


- All points are same as Bus topology.

Manchester Encoding:



Differential Manchester Encoding:



Various Devices in Computer Networks

1) Cables
2) Repeaters
3) Hubs
} Hardware

4) Bridges
~~5) Switches~~
5) Switches
6) Routers
} Hardware & Software

7) Gateway
8) IDS
9) Firewall
} Security

10) Modem

Cables — Physical layer

→ Unshielded twisted pair Cable [10 Base T, 100 Base T] (10 Base T → 10mbps, 100 mt; 100 Base T → 100mbps)
(Used in Ethernet LAN)

→ Coaxial Cable < 10 Base 2 → 200mt. / 10 Base 5 → 500mt.

→ Fibre Optic – 100 Base Fx ≃ 2Km
(100 → 100mbps; Fx → Fibre Channel)

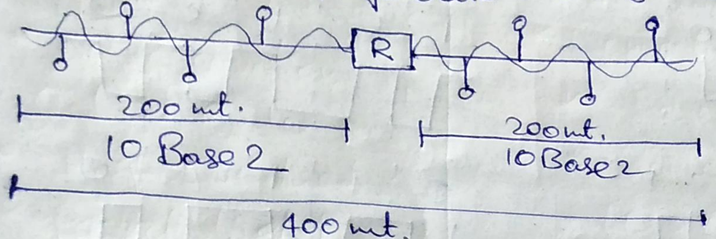
Signals are transmitted into Cables

- Two types of transmission: BaseBand, BroadBand
  - BaseBand → [At a time one Signal]
  - BroadBand → [Multiple Signal Parallely]
- Attenuation: After a particular distance every Signal's strength gets down.

{n number of devices, then maximum Collision n}

Repeaters: (Physical layer)

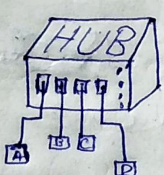
Regenerate the Signal Strength after attenuation

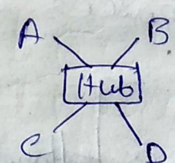


1) Two Port Device
2) Forwarding
3) No filtering
4) Collision Domain [Same as Cable 'n']

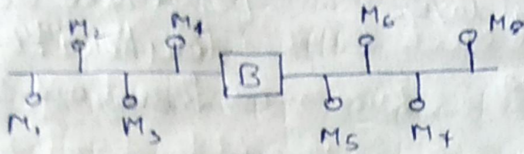
Hub: (Physical layer)

1) Multiport Repeater [Where Repeaters are two port devices]
2) Forwarding
3) Traffic high ↑
4) No filter
5) Collision Domain 'n'.





Bridges (Physical & Data link layer).



Types of bridge → Static, Dynamic

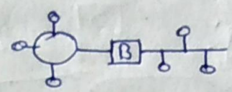
Each msg has two part

MAC	MAC
Source	Destination

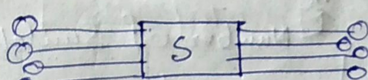
[$M_1 \rightarrow M_6$ | M_1 | M_6]

MAC	PORT
M_1	P_1
M_2	P_1
M_3	P_1
M_4	P_1
M_5	P_2
M_6	P_2
M_7	P_2
M_8	P_2

Filtering technique

- Connect two different lans 
- Forwarding ✓
- Filtering ✓ [Repeater or Hub can't do this]
- Collision cannot be ~~done~~ occured because bridge has buffer in it and it use the Store and forward strategy.
- Bridges use data unit protocol to prevent the loop condition.

Switch :-



[We can create it into a layer 3 device but by default it is 2 layer device]

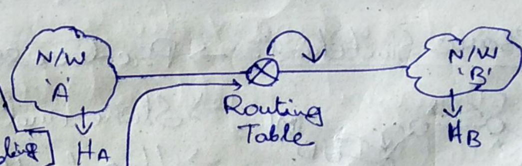
- Layer-2 (Data link layer) Device
- Multiport Bridge
- Full Duplex Links
- Traffic is minimal
- Collision Domain is Zero (0). All the signals are running Parallely.
- Security is high.

Routers :- (Physical, Data-link, Network layer) layer-3 Device

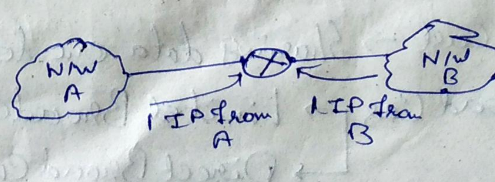
Router can check IP address as well as Mac addresses.

- Forwarding ✓
- Filtering ✓
- Routing ✓
- Flooding / Broadcasting
- Collision Domain Cannot Occur because of Store and forward strategy

If there is a problem in forwarding



Source | H_A | H_B | Destination



Circuit Switching: It's a type of telephone network.
[Just like we use a telephone to call our friend and send data]

- Works in Physical layer
- Contiguous flow
- No headers
- Efficiency less
- Delays less

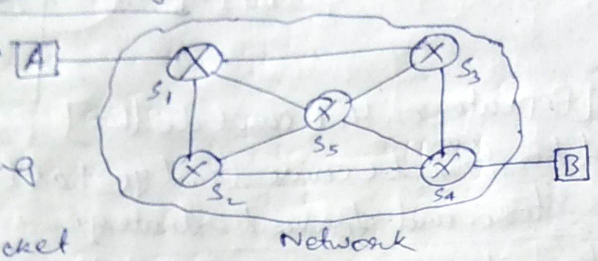
Total time = Setup time + TT + PD + Tear Down time

[Transmission time = $\frac{Msg}{Bandwidth}$]

[Propagation Delay = $\frac{Distance}{Velocity}$]

Packet Switching:

Divided into Packets



Network

1) Data link and Network layer ~~analysing~~
2) Store & forward
3) Pipeline used
4) Efficiency ↑
5) Delay ↑

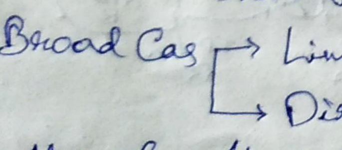
Packet Switching → Datagram, Packet Switching

Total time = n(TT) + PD
↑ Number of switches

Datagram	Virtual Circuit
* Connectionless	* Connection Oriented
* No Reservation	* Reservations
* Out of Order	* Same Order
* High Overhead	* Less Overhead
* Packet lost ↑	* Packet lost ↓
* Used in Internet	* X.25, ATM

Circuit Switching → Message Switching → Packet Switching

Message Switching:



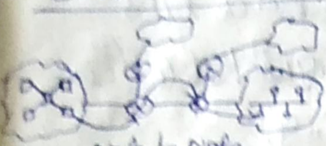
→ Predecessor of packet switching
→ Store and forward
→ Hop by Hop delivery
→ Delay, Efficiency ↑

UniCast → Sharing data one to one

BroadCast → Limited Broadcast [Broadcasting under same network]
→ Direct BroadCast [" under another network]

Multicast → Sharing data to a group [Similar kind of people]

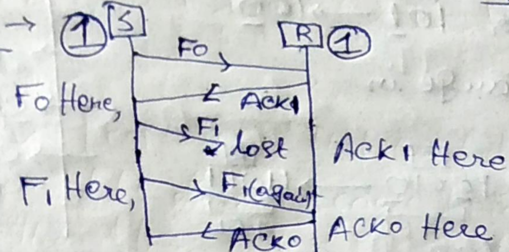
• Data link layer: (i) Node to Node Delivery, (ii) Flow Control
(iii) Error control (Node to Node)
[Methods: CheckSum, C.R.C, Parity]
CheckSum → Transport; C.R.C → Data link
(iv) Access Control & (v) Physical Address (MAC)

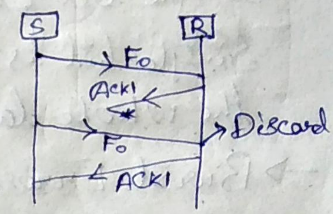


Node to Node

[In Stop-and-wait ARQ, the acknowledgement number always announces in module-2 arithmetic the sequence number of the next frame expected]

Stop & Wait →





[In the Go-Back-N Protocol, the sequence numbers are modulo 2^m, where m is the size of sequence number field in bits.] Sender size $2^m - 1$ / Reciever size 2^m
[Gate Smashers Lec-23]

Selective Repeat ARQ

Sender size 2^{m-1} / Reciever size 2^{m-1} [G.S.M Lec-24]
m → [No. of bits to represent VS]

Flow Control points:

Stop & Wait	Go back N	Selective Repeat
→ Only 1 frame transmit	→ Multiple frames	→ Multiple frames
→ Sender window = 1	→ Sender Window = $2^m - 1$	→ Sender window = 2^{m-1}
→ Reciever " = 1	→ Reciever " = 1	→ Receiver window = 2^{m-1}
→ $\eta = \frac{1}{1+2a}$, a → T_p/T_t	→ $\eta = (2^m - 1) \times \frac{1}{1+2a}$, a → $\frac{T_p}{T_t}$	→ $\eta = 2^{m-1} * \frac{1}{1+2a}$, a → $\frac{T_p}{T_t}$
→ Retransmission = 1	→ Commulative Ack	→ Commulative & Independent Ack
→ Seq No. = SW + RW = 1 + 1 = 2	→ Retransmission = $2^m - 1$	→ Retransmission = 1
	* Cannot be out of order	* Can be out of order
		→ NAK is also transmitted

FRAMING: The data link layer needs to pack bits into frames, so that each frame is distinguishable from another. The process is known as framing.

Fixed-Size ← Framing → Variable Size [LEC-26] Video Gs

Flag	header	D_1	D_2	ESC	Flag	D_3	ESC	Flag	Trailer	Flag

Error Detection & Correction

→ Single bit Error $\boxed{S}$ 101 → $\boxed{R}$ 100

Single bit is change in the whole data

→ Burst Error $\boxed{S}$ 10010 → $\boxed{R}$ 11011 (4 EL, 4 EL)

More than one bit is changed

Here only two bits are changed but the error length is 4 [0010]

Detection
- → Single Parity (Even, odd)
- → 2D Parity Check
- → Check Sum
- → CRC (Cyclic Redundancy Check)

Correction
- → Hamming Codes

Single Parity

→ n+1 bits

10100
11101

→ Even Parity no. of '1' even

→ Can detect all single bit errors in the code word

→ Can detect all odd no. of errors also.

Haming Distance:

0000
1111 [XOR]
1111

0101
1000 [XOR]
1101

[If Haming dis = d
Then no. of error detect = d-1]

Cyclic Redundancy Check (CRC):

→ Based on binary division [total bits = (n+r)]

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

→ Can detect all odd errors, single bit, burst error of length equal to polynomial degree.

Divisor $= x^4 + x^3 + 1$ → Convert into bin.

$1.x^4 + 1.x^3 + 0.x^2 + 0.x^1 + x^0.1$

$= 11001$

Dividend $= 1010101010$ → Take 0000 extra bits as x^4.

→ Append it into Dividend

```
11001 ) 10101010100000
    XOR 11001
        011000
    XOR  11001
         000011010
    XOR      11001
             00011000
    XOR         11001
                000010
```

000010 — Last 4 LSBs → Append Here

Final ans. → 10101010100010

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

Data link → LLC, MAC

Multiple Access protocol (MAC)

- Random Access Protocol
  - * Aloha
    - Pure
    - Slotted
  - ** CSMA
  - ** CSMA/CD
  - CSMA/CA
- Control Access
  - Polling
  - * Token Passing [TOKEN RING]
- Channelization Protocols
  - FDMA
  - TDMA

Pure Aloha -

- Random Access Protocol [Collision is possible]
- Ack is there
- LAN based [Re-transmission is possible]

  * Back of method
- Only transmission time
  No propagation time
- Vulnerable time: $2 \times TT$ → Msg/Bandwidth
- Efficiency, $\eta = G \times e^{-2G}$ [value of $e = 2.71$]

$$\max \eta = \frac{d\eta}{dG} = \frac{d(G \times e^{-2G})}{dG}$$

$$\Rightarrow G.(-2)e^{-2G} + e^{-2G}(1) = 0$$

$$\Rightarrow e^{-2G}(-2G+1) = 0$$

$$\Rightarrow G = \frac{1}{2}$$

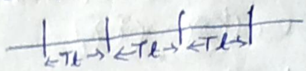
$\therefore G \times e^{-2G}$

$= \frac{1}{2} \times (2.71)^{-2 \cdot \frac{1}{2}}$

$= \frac{1}{2} \times (2.71)^{-1}$

$= 18.4\%$

Slotted Aloha: ~~Each station can~~

- The network is divided into slots and the length of each slot is the transmission time. Each station can send msg into one slot. 

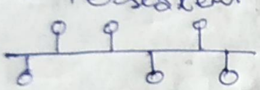
- ~~Each transmission can start transmission at the~~
- Each transmission can be started only at the beginning of a slot.
- Vulnerable time = TT
- Efficiency, $\eta = G \times e^{-G}$

$$\frac{d\eta}{dG} = 0 \Rightarrow G(-1)e^{-G} + e^{-G}(1) = 0$$
$$\Rightarrow e^{-G}(-G+1) = 0$$
$$\Rightarrow G = 1$$

$$= 1 \times e^{-1}$$
$$= 1 \times (2.71)^{-1}$$
$$= .368 = 36.8\%$$

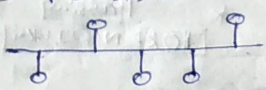
Carrier-Sensor Multiple Access (CSMA)

1-Persistent

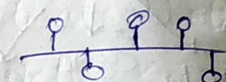


All time check the media and immediate release data if found media is free [High Collision]

0-Persistent

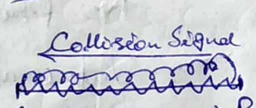


Check after a particular amt. of time and release data if found media is free [Low Collision]

P-Persistent 

Highbrid version of previous two. Check all time but release data based on probability [not instantly] if found media is free. [Low Collision]

CSMA-CD (Collision Detection):



$TT > PD$

For worst case: $TT \geq 2 * PD$

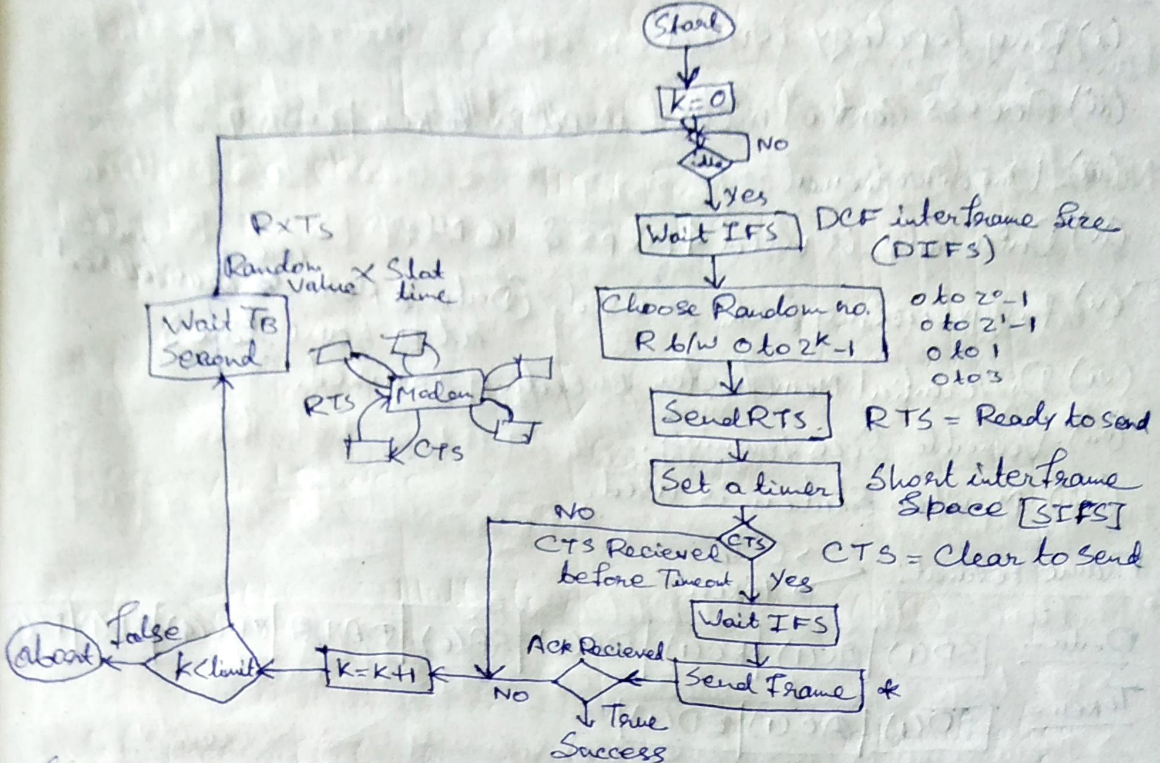
$$\Rightarrow \frac{L}{BW} \geq 2 * PD \rightarrow \frac{D}{V}$$
$$\Rightarrow L \geq 2 * PD * BW$$

[Efficiency, $\eta = \frac{1}{1 + 6.44a}$, $a = \frac{PD}{TT}$]

Gate Smashers [Lec: 35]

[for wire CSMA/CD
for wireless CSMA/CA]

⊙ CSMA-CA (Collision Avoidance):



100 Mbps (10^8 bits/per second) D = 1 Km min. frame size = 1250 byte

$\frac{L}{BW} = \frac{1250 * 8}{10^8} = 10^{-4}$ ⎮ $TT \geq 2*PD$

$\frac{L}{BW} = 2 * \frac{D}{V}$ $\frac{D}{V} = \frac{1}{2 \times 10^4}$

$\Rightarrow V = 2 * \frac{D}{L} * BW = \frac{2*1*10^8}{1250*8} = \frac{10^8 \times 2}{10^4} = 20000$

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

$= \frac{1}{1+6.44(PD/TT)} = \frac{1}{1+6.44\left(\frac{1}{2\times10^4} \times 10^4\right)}$

$= \frac{1}{1+3.22} = \frac{1}{4.22} = 0.24$

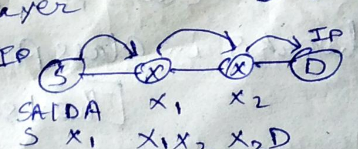
⊙ Ethernet frame format (Used in LAN) CSMA-CD technology used.
(IEEE 802.3) - 1983

- ✓ 10 Base 2 - Thin
- ✓ 10 Base 5 - Thick
- ✓ 10 Base T
- ✓ 100 Base Fx - Fast
- ✓ 10G Base-T-Gigabit
- ✓ Topology - BUS, Star
- ✓ 1 Mbps - 400 Gbps

10101010 --- 10 format MAC Add.

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

Physical Layer [2 byte = 16 Bits]



Token Ring (IEEE 802.5)

(i) Ring topology is used
(ii) Access control method used is token passing
(iii) Uni directional
(iv) Data rate is used 4 Mbps & 16 Mbps
(v) Piggybacking Ack. is used. (Data & Ack. are transferred at a same time)
(vi) Differential manchester encoding is used.
(vii) Variable size framing.
(viii) Monitor station is used.

Frame Format: → Data, → Token

Data –

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

Token –

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

Network layer:

1) Host to Host (Source to Destination) Delivery
2) Logical Address (IP Add.) → Network id, → Host id
3) Routing → RIP, → OSPF [Used to find the shortest path]
4) Fragmentation
5) Congestion Control [Leaky Bucket, Token Bucket]

Class full IP Addressing (1980):

(i) Class-A, (ii) Class-B, (iii) Class-C, (iv) Class-D, (v) Class-E.

1) Class-A IP Add →

8 bits	24 bits
Network id	Host id

0 → First bit is always zero in Network id Class A

Total no. of IP addresses $= 2^{31}$ [As the first bit is always 0]

No. of networks in Class A $= 2^7 = 128$ [As 1st bit is fixed 0]

Total used networks in Class A $= 128 - 2 = 126$
[The 1st and last bit ~~does~~ doesn't used]

No. of Host possible in every network $= 2^{24} - 2$
[The 1st and last bit doesn't given]

IP address = 64.0.0.0 . | 64.0.0.1 → The first host id of the Network

Network id [Should be in 0-127]

Host id

[The first and last id are not given to any host because the 1st id [0.0.0] represent the IP address of the whole network in front of www and the last id [255.255.255] is known as Directed Broad Cast Address].

* Default Mask = 255.0.0.0

2> Class B IP Add:

8b	8b	8b	8b
Network		Host	

10 ____ | ______

Always 1st 2bit '10'

Range: 128-191 (64)

No. of IP Addresses = 2^{30} [25%]

No. of Networks = 2^{14} No. of possible Hosts = $2^{16}-2$

IP address = 132.2.3.4 → Network = 132.2.0.0

Default Mask = 255.255.0.0

1st host = 132.2.0.1 | Brodcast Network = 132.2.255.255

Last host = 132.2.255.254

3> Class C IP Add:

8b	8b	8b	8b
Network			Host

110 ___ | ____ | ____

Always 1st 3bits '110'

Range: 192-223 (32)

No. of IP Addresses = 2^{29} [12.5%]

No. of Networks = 2^{21} No. of possible Hosts = 2^8-2 = 254

IP Address = 194.3.4.5 → Network = 194.3.4.0

Default mask = 255.255.255.0   Broad Cast = 194.3.4.255

1st host = 194.3.4.1   Last host = 194.3.4.254

4) **Class D IP:** | 8b | 8b | 8b | 8b |

Range: 224-239 (16)

[No concept of Network & Host.]

Starts with '1110' in 1st 4 bits

No. of IP Add. = 2^{28} [6.25%]

* Reserved for Multicasting / Group Email / Broadcasting

5) **Class E IP:** | 8b | 8b | 8b | 8b |

Range: 240-255 (16)

[Same as Class D]

Starts with '1111' in 1st 4bits

No. of IP Add. = 2^{28} [6.25%] * Reserved for Army Purposes

◉ **Problems with classful Addressing:**

→ Wastage of IP addresses → Not flexible

→ Maintenance is time consuming → Security decreases

→ More prone to errors

◉ **Classless Addressing: (1993)**

→ No classes

→ Only blocks

← 32 →	
Block ID	Host ID

→ Notation

x.y.z.w/n → mask or no. of bits represent block/network

Rules:

→ Address should be contiguous

→ No. of addresses in a block must be in power of 2

→ First address of every block must be evenly divisible with size of block.

Ex ⇒

200.10.20.40/28

28	4

← 32 →

→ No. of Host $= 2^4 = 16$

n=28. h=4 [28 '1' and 4 '0']

∴ Default mask = 11111111----0000

In this case = 255.255.255.240

Network id: 200.10.20.40/28

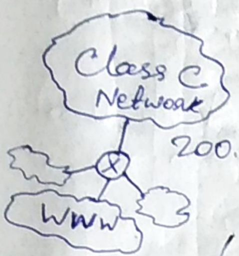
→ $\underbrace{200.10.20.0010}_{N}\underbrace{1000}_{h}$

∴ 200.10.20.00100000

= 200.10.20.32

⊙ Subnetting → Dividing the big network into small networks.

~~It is used to~~ It provides easiness to maintain a network.



[Lec 48: GS]

200.10.20.-------

200.10.20.0

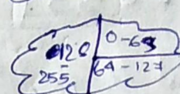
200.10.20.0 ------ | 200.10.20.1 ------

200.10.20.127 | 200.10.20.255

200.10.20.0 to 200.10.20.63

200.10.20.64 to 200.10.20.127

→ VLSM (Variable Length Subnet Masking)



Lec-48, 49

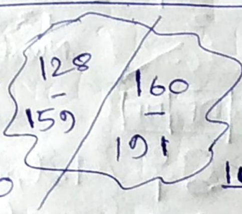
• Subnetting in CIDR:

10 000000

10011111

32-2 = 30

195.10.20.128/27



30

101 00000

10111111

195.10.20.160/27

195.10.20.128/26

$\underbrace{8\ \ 8\ \ 8}_{24}$ 8

24 + 2

10 000000 2^6 Host = 64 Host

Usable = 62.

Q> CIDR recieve a packet with address 131.23.151.76.
The Router's routing table has following entities:

Prefix	OI
131.16.0.0/12	3
131.28.0.0/14	5
131.19.0.0/16	2
131.22.0.0/15	1

131.23.151.76

131.00010111.151.76
255.11110000.0.0
131.00010000.0.0
✓ 131.16.0.0

131.00010111.151.76
255.11111110.0.0
131.00010110.0.0
✓ 131.22.0.0

Packet will be forwarded to which interface 1

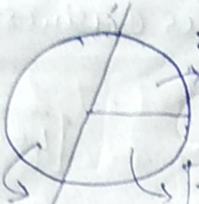
Small host is selected always.

VLSM in CIDR:

245.248.128.0/20

$245.248.\underline{1000,0000}.0/20$

$2^{12}-2$ Host



$2^{11}-2$ Host

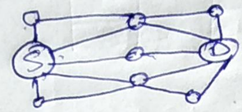
[245.248.128.0/21
⋮
245.248.135.255/21]

[245.248.136.0/22
⋮
245.248.139.255/22] $2^{10}-2$ Host

[245.248.140.0/22
⋮
245.248.143.255/22] $2^{10}-2$ Host

IPv4 Header: → Connection less → Datagram Service.

[LEC 53]



Any way Can be Choosed

- Fragmentation:

Identification bits	flag	fragment offset
16	3	13

fragment offset → Number of bits ahead

flag:

Res 0	DF	MF

frag < 0 0 / 0 1

No frag < 1 0 / 1 1

} 1st, middle, or last packet

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

300B → [Router] —500B— {N/W}

20	2980

$\frac{2980}{480} \approx 7$ fragments

360×8 = 2880

	P_7	P_6	P_5	P_4	P_3	P_2	P_1
Total length =	100+20	480+20	480+20	480+20	480+20	480+20	480+20

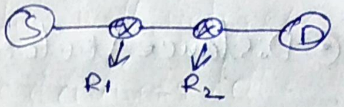
480×6 = 2880

2980 − 2880 = 100

$\frac{480+480}{8} = 120$ $\frac{480}{8} = 60$

	P_7	P_6	P_5	P_4	P_3	P_2	P_1
MF	0	1	1	1	1	1	1
Offset	360	300	240	180	120	60	0.

- **Options (0-40B)**: • Record Route



- Source Routing (Path will be previously defined)
  - Strict Routing
  - Loose Routing
- Padding (Header length of IPV4 will always be the order of 4)

1 Router = 4B
Total Max = 40B
Total Router = $\frac{40}{4}$
= 10

IPV6 Header: Total 128 bit is there. So, possible IP addresses are 2^{128}.

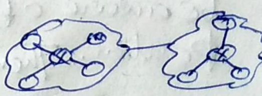
• **Extension Headers**:
1) Routing Header (43)
2) Hop by Hop Opt. (0)
3) Fragment Header (44)
4) Authentication Header (51)
5) Destination Opt. (60)
6) Encapsulating Security Payload (50)

Version (4)	Priority (8)	Flow Label (20)	
Payload Length (16)		Next Header (8)	Hop Limit (8)
Source Address (128)			
Destination Address (128)			

Base Header = 40 Bytes (320 bits) Fixed

Base Header	Extension Header 1	...	Ext Header N	Data
40B				

Autonomous System: Networks those are controlled by one network administrator are known as Autonomous System.



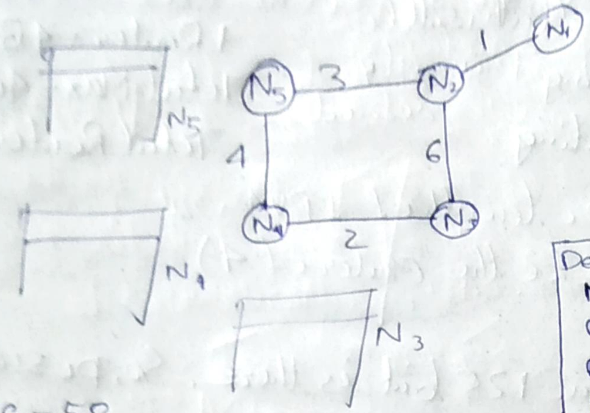
Routing Protocols

Intradomain [Diff networks can communicate with each other in one autonomous system]
- Distance Vector (RIP)
- Link State (OSPF)

Interdomain (Different autonomous systems communicate with each other)
- Path Vector (BGP)

They all are working under unicasting system.

Distance Vector Routing: (DVR)



Routing table

Dest.	Dist.	Next
N_1	0	N_1
N_2	1	N_2
N_3	∞	—
N_4	∞	—
N_5	∞	—

N_1

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

N_2

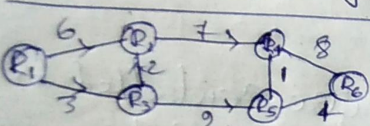
Lec-58

- Count to infinity problem in DVR:

C → A → B → Internet [This will works normally]

But, If the connection with the internet is disconnected there can be a problem of infinite count in each iteration for every nodes. This problem is solved using Link State routing.

- Link State Routing: Flooding is used. Step 1



Dijkastra algorithm is used. Step 2

After flooding all the nodes will be aware of its positions and all the other nodes position. Then Dijkstra will appear on that diagram. [Lec 60]

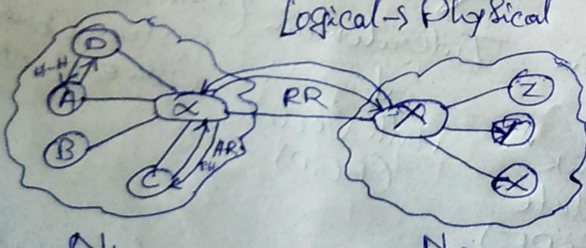
- ARP protocol: IP → Mac

Logical → Physical

4 Conditions are there

H → H R → H

H → R R → R



We need to find IP as well as mac addresses.

- NAT (Network Address Protocol):

Used to translate private IP to Public IP and Public IP to private IP.