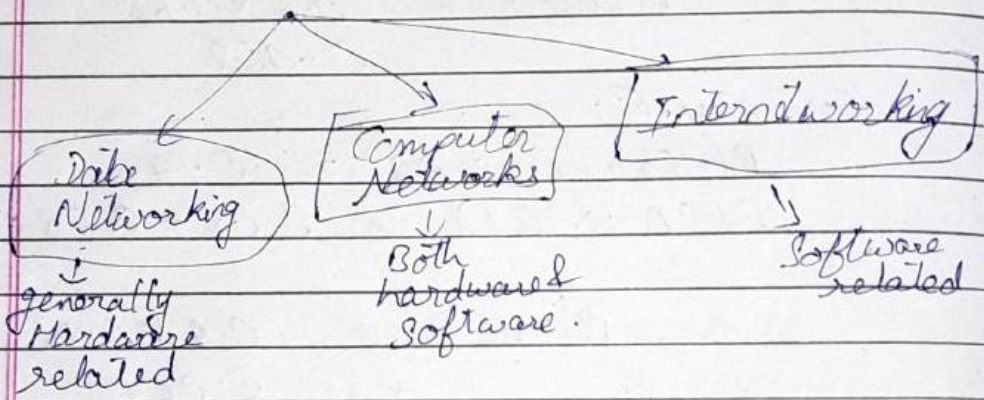
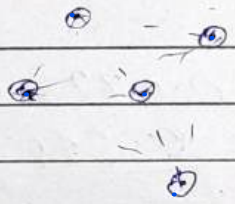
Computer Networks

(2) Connection related problems
(1) Communication "
(2) Identification

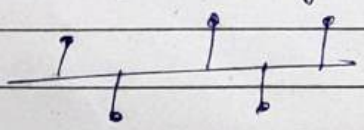


Network

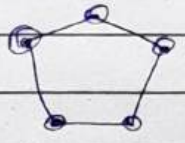


The nodes and their connections together are called network.

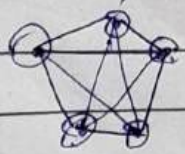
Network Topologies



(Bus topo)

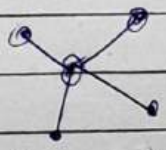


(Ring top)



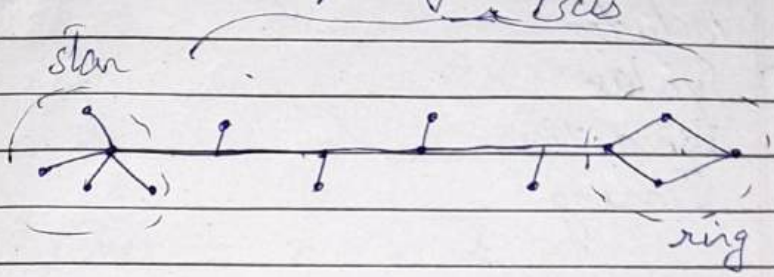
$^5C_2$ connections $= 10$

(Mesh topology)



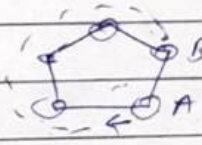
(Star topology)

Hybrid topology: It has a bus and other topologies



Bus uses a common communication route for all nodes. It has poor privacy, but is very simple to implement.
If there is a breakage in the main path, all communication would break

Ring topology the other nodes will receive get the data



for A to B all nodes recieve data.

use Star topology where devices can be divided based on their priorities.
The issue is that low priority devices can't have direct communication. If the central node is disturbed, all comm is affected.

In Mesh topology all nodes are interconn. It is complex to create and difficult to maintain.

Q) who standardises Internet protocols?

~~Ans:~~

For any protocol we must have fixed and unambiguous set of rules that includes

1. Syntax
2. Semantics
3. Timing

Creating a completely new protocol is called Vertical Development.

Horizontal Development is addition of new features (creating new versions).

Software Engineering: Braessman.

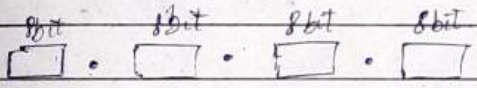
PAGE NO.:
DATE:

Addressing system in Computer Networks:

Logical address → IP address → IPV4 (32 bit)
(virtual address) → IPV6 (

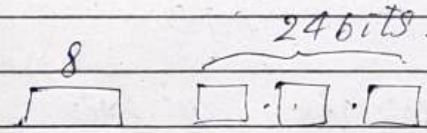
IPV4 (32 bit)
divided into 4 octets of 8

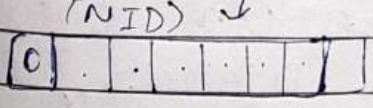
It has: Network ID (NID)
Host ID (HID)
combine to give IP address



This IP address is divided into 5 classes:
class A, B, C, D, E.

* class A





NID cannot be all 0s (0000000 is not an all 1s is not allowed. (111111 x)

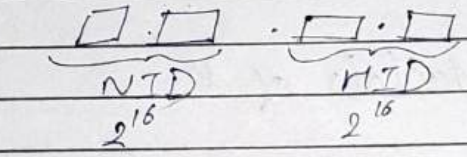
∴ Effective address: $2^{7}-2$ Network IDs.

Similarly for Host ID

$2^{24} - 2$ HID

(All 0s and all 1s not allowed)

Class B:



↓

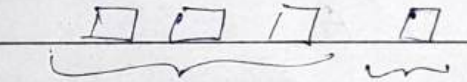
first two bits are reserved as 10

reserved

$\therefore 2^{14}$ Network IDs

2^{16} HIDs

Class C



2^{24} Networks 2^{8} Hosts

3 MSBs are reserved as 110

$\therefore$ effective no. of NIDs → 2^{21}

Class D

PAGE NO.:
DATE: / /

Class D
used for Multicasting.

First 4 bits are reserved as

1110 - - - .

Class E.

First 4 bits reserved as

1111 - - - -

for future / research purposes.

* Class A IP addresses are used by large organisations that have huge no. of hosts on same networks.

* Class C: used by small organization.

For the first Octet

1. Class A → '0' →, 1 to 126
2. class B → '10' → 128 to 191
3. class C → '110' → 192 to 223
4. class D → '1110' → 224 to 239
5. class E → '1111' → 240 to 255

~~Special address~~ Specify the class of each of the following IPs

(1) 0.191.25.0 (special)
(2) 1.1.1.1 (class A)
(3) 10.10.10.0 (class A)
(4) 127.1.1..1 (special)
(5) 255.255.255.255 (E)
(6) 255.255.258.1 (invalid)
(7) 127.0.0.0 (special)
(8) 0.0.0.0 (special)
(9) 239.0.1.255 (D)
(10) 241.255.10.0 (E)
(11) 11011010.--- (C)
(12) 11100000.--- (E)
(13) 10101010.--- (B)
(14) 1110 1111 .--- (D)
(15) 010 10101 .--- (A)
(16)
=

The IP addresses are assined by the IANA (Internet Assigned Number Authority)

∴ The IANA assignes the addresses to the ISPs, who provide us the IP addresses.

Public IPs	Private IPs
For networks that wish to interact with other compaters over the internet through an ISP.	for local networks in small clusters or groups
class A class B Class C are used for Public IPs.	Private A → 10.0.0.0 to 10.255.255.255 B → 172.16.0.0 to 179.31.255.255 C → 192.168.0.0 to 192.168.255.255

Subnetting and Supernetting

In subnetting we divide a single IP address into multiple groups, where each group is called a subnet.

~~Supernetting~~

Types of Communication in Computer Networks

1. Unicasting (1 source; 1 destination. Eg: 1 phone call)
2. Multicasting (1: many; email with multiple recievers)
3. Broadcasting (1: All; radios, etc)
4. Anycasting (1:1 and 1: All)

Limited Broadcasting → ~~Network~~ The broadcaster will send the data to all recievers on the same network. (Same network ID, but varying Host ID)

Directed broadcasting → The network ID and host ID both can vary.

OSI Model
(Open Systems Interconnection)

Application Presentation Session	} software oriented layer.
Transport	→ Interface
Network Data link Physical	} Network oriented layer

OSI is used for reference, however for practical purposes we use TCP/IP

Application layer
Transport layer
Network layer
Data link layer
Physical layer

Transport layer is the thickest layer.
Session layer is thinnest
Network layer is the most complex layer.

Physical address is represented in an alphanumeric format in 48 bits.

Data link layer does:
- Flow control
- Error Control
- Access Control.

Error detection:
Error Correction

CRC & Hamming codes are used in Error Control.

For downloads, if the download continues from the last interrupted point, the protocol being used is DAP (Download Accelerator Protocol)

Out of the 7 functionalities of the OSI protocol, they are divided into 7 layers, of which some are compulsory and some are optional.

Presentation layer (layer 6)
- Encryption
- Decryption
- Encoding
- Translation

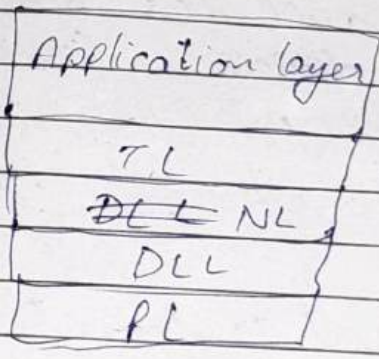
Plain text —(Encryption)→ Cypher text (Encrypted text) —(decryption)→ plain text

Application layer
- provides GUI (UI)
- Harmony among the protocols / layers.

(TCP/IP) → model
TCP → protocol
IP → protocol.

TCP/IP

5 layers.

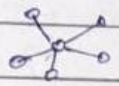


Multicasting is defined by this model

Lots of flexibility.

Practical rules / protocols

Networking devices

Hub → broadcasting device 

Switch

Bridge

Router

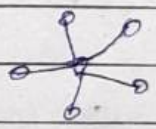
Brouter

Gateway

Web Server / Work Station

Repeater.

① Hub → broadcasting device with only a hardware component. It is a physical and passive device.



② Repeater : It regenerates the signals at different distances increasing the effective range. (It does not amplify the signal in any way)

(2) Switch

It maintains a look up table for all devices, and has both hardware and software devices. (Connects devices on the same network).

Active device :

(4) Bridge

It is used to connect two different networks. (Two LANs only).

Uses Physical address.

(Bridge is more expensive than switch)

It can't connect (WAN's)

(6) Router (connects LAN and WAN)

Complex devices

Costly.

Routing tables

Has all functionalities of Network layer.

(5) Brouter : ~~Has both the~~

It has functionalities of both the Routers and bridge

(8) Gateway:

Also known as Protocol conversion

Connects networks of different types (that use different protocols).

All 7 layers of OSI are involved

Complex and costly device.

① Web Server / Workstation
used for large networks and huge data.

Four Different types of Delay

① Queue Delay → could be 0 to inf.
② Processing Delay
③ Transmission Delay
④ Propagation Delay.

① In the presence of multiple packets of varying priorities, some of the packets would have to wait in the queue for a long time causing a delay.

② The input recieved is not sent as is, the encryption, modulation, compression of the input data requires some time, called the processing delay.

③ The data is transmitted through specific bandwidth. The data has to be bought to that network bandwidth before propagation. This is called Transmission delay.

$$T_d = \frac{L}{B}$$

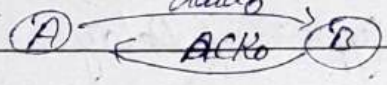
L → size of packet
B → bandwidth of channel

④ Propagation delay is the delay in sending the data from source to destination.

$$\text{Line utilisation} = \frac{\text{Transmission delay}}{\text{Total delay.}}$$

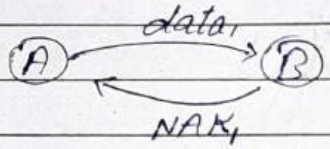
Acknowledgements

Used to signify that the data packet has been successfully accept.



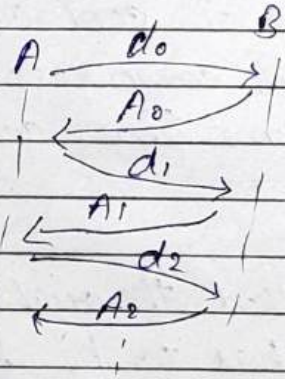
(+ve ack)

if the data is not recieved, the reciever sends NAK (negative acknowledgement).



Apart from the positive and negative classification, another classification is used:

① Independent acknowledgment
② Cumulative acknowledgement.

① 

② 

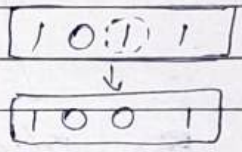
PAGE NO.:
DATE: / /

Piggybacking acknowledgement:

If some data is to be sent back, then the acknowledgement is packed and sent along with the data.

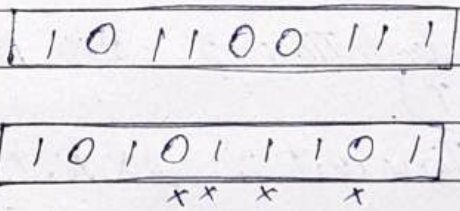
Error

1. Single bit error:



2. Multibit error:

Burst length: The first bit that is flipped to the last bit that is flipped.



Total delay = Transmission delay + Propagation delay

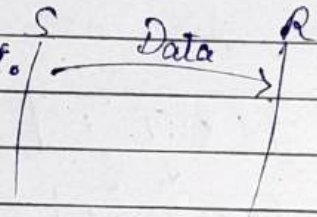
2x Propagation delay = Round trip time

unit testing is part of coding

- Integration and system Testing are a different part from coding.

Sliding Window Protocol (SWP)

Deals with packet level errors.



$t_p \rightarrow$ transmission time

- Ideally the sender has to wait $2t_p$ units of time before recieving acknowledgment from the reciever.

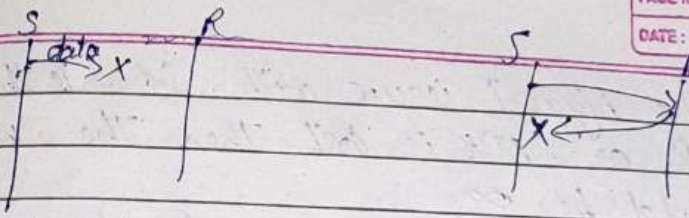
However considering all the delays and possible buffers, we generally consider the

Round Trip Time = 2 × Propagation Delay (RTT).

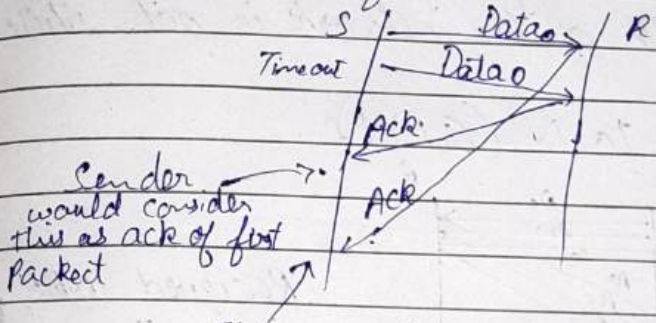
∴ Time out = 2 × R.T.T.

The following cases are also possible:

1. The data is sent by the sender, but gets lost so reciever must wait.
2. The data gets recieved but the acknowledgement gets lost.



One consequence of this is:



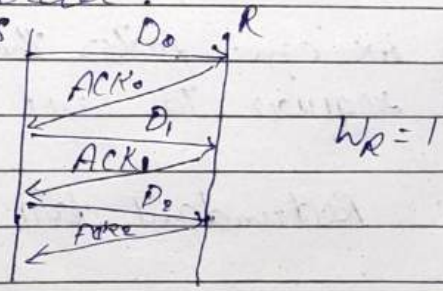
Skipping the D_0 and sending D_2.

Stop & Wait

Used to eliminate above cases.

1. Send only 1 data packet at a time
2. Wait for ACK of prev Data Packet before sending next one.

(In this case both the data and the ACK are numbered in order).



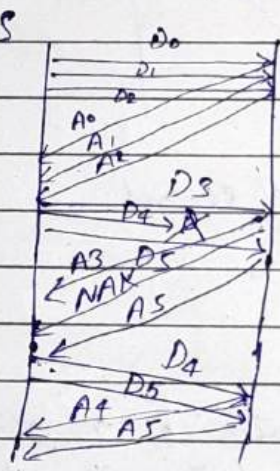
Since next DP is sent only after previous ACK, there is no need to acknowledge the number the data and ACK.

However, if Cumulative acknowledgement is used (multiple data packs at a time), then numbering is required.

The biggest issue with S&W is that if a D.P. or ACK is lost then the wait time would be ∞.

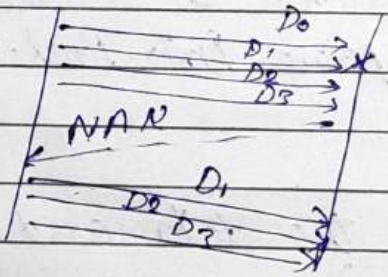
Even if everything works ideally, the entire bandwidth of the network is not utilised.

Go back to N (GBN)



Recieved NAK for D_4, then it would send all packets in that group starting from D_4.

Eg.



Adv → ~~we can~~ faster than S & W as we don't require to send each packet separately

Dis Adv: Redundant data packets.

* Sender has a window size = W_S
reciever has window size = 1.

DATE: / /

Selective Repeat (SR)

In this case, we do not send all packets from lost packets to all the further packets, but only the one lost would be resent.

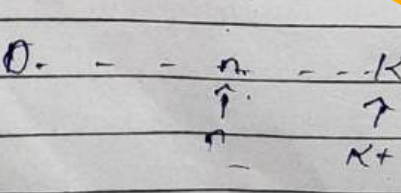
On reciever side we would need to implement a sorting technique to organize the data packets. On Senders side, searching must be done, in order to find the NAK (or lost packets.)

Q The GBN sender must respond to
(i) Receipt of an acknowledgement
(ii) A timeout event
(iii) Invokation from above
(iv) All the above ✓

Q In what protocol a cumulative ackn becomes an ordinary ackn
(i) Selective Repeat (iii) S&W ✓
(ii) GBN (iv) None of the ab

Q In what protocol/protocols it is possible for the sender to recieve an acknowl for a packet that falls outsid its current window?
(i) S&W (ii) SR ✓
(iii) GBN (iv) All of the ab

Q If the current sequence number is K, and the last NAK was for packet N, then how many unacknowledged packet are in the pipe?
(i) K-(N+1) (ii) N+(K-1)
(iii) N-(K-1) (iv) K-(N-1) ✓



The nth packet gets NAK, but it still inside the pipeline, so it is also considered

K+1-n → K-(n-1)

0 . . . 1 . . . K

K+1-n → K-(n-1)

K+1-n

K+1:

DATE: / /

Q. If K = no. of bits in sequence no field, In SR protocol both sending and reciever windows have a size

(i) $2^K - 1$ (ii) 2^K

(iii) 2^{K-1} ✓ (d) K.

Total no. of bits → 2^K

then half for sender and half for reciever, which gives 2^{K-1} per window.

Q. In S & W of flow control, if 100 good data frames are sent and recieved, how many acknowledgement frames have been sent by the recievers.

(i) 99 (ii) 100 ✓

(iii) 101 (iv) 200

Q. In Sliding window method of flow control, if 100 good DFs are sent and recieved. How many ack frs are recieved.

(i) 99 (ii) 100

(iii) 101 (iv) $n \leq 100$

Since other protocols under sliding window send cumulative acknowledgements. Then $n \leq 100$

Size 15

Q. A sender has a sliding window of 000. Th first 15 are sent. The first ackno recieved is AK no.15. What frame/fra has the reciever accepted?

(i) 15 (ii) 14

(iii) 0-15. (iv). 0-14 ✓

It is expecting frame 15 a above

Expected frame : 15.

Accepted frame : 0-14.

Q. K is the total sequence no. available then what is the relationship between sliding window size (W) and K in S.R. protokocol.

(i) $W \leq \frac{K+1}{2}$.

(ii) $K \geq W/2$

(iii) $K/2 \geq W$ ✓

(iv) $K > 2W$ ✓

LAN

Purpose:
- → Resource sharing
- → Information or Data sharing

Types of LAN
1. Dedicated Server LAN
2. Peer to Peer LAN
3. Zero-Slot LAN.

Components of LAN
- → NOS (Network operating system) used to handle all the data on the network)
- → Cables (for physical connection (used in all types of LANs)
- → Network Interface Card (NIC). Used to interface all ports (USB, HDMI etc) to the computers.

1. Dedicated Server LAN.

Three levels of security are provided in this LAN:
1. Network level security → connection to the network itself.
2. User level security → diff types of access to diff users
3. Application level security → permissions given to the applications to use network.

The no. of nodes are devices are fixed in this LAN.

(ii) P2P.

There is no central server or such. (Also called a workgroup). All devices are connected together with same priority. It is highly flexible.

(iii) Oslot:

less security, high flexibility. There is no fixed slot for connections. Any device can access the network at any time.

old standards.

IEE 802.1 are the standard for LAN.

802.2

802.3 → for ethernet

802.4 → token bus

802.5 → token ring

802.11 → Wireless LAN

802.16 → Wireless MAN

PAGE NO.:
DATE: / /

Q If the bandwidth of a line is 1.5 Mbps, RTT is 45 ms, and packet sizes are 1 KB. Then find the line utilisation in S & W protocol.

Total time

$$T_d = \frac{L}{B} = \frac{1\,Kb}{1.5\,Mbps} = \frac{1\,KB}{\frac{1024}{128} \times 1.5}$$

$$= \frac{1\,KB}{192\,KB}\,s.$$

line utilisation = $\frac{\text{Transmission delay}}{\text{Total delay}}$

RTT + T_d = Total delay

Q A channel has a bit rate of 4 Kbps, and a propagation delay = 20 ms. For what range of frame size, does S & W give an efficiency of at least 50%.

$$\frac{L}{4} = T_d$$

$$\text{Lin} \Rightarrow \frac{T_d}{T_d + 40}$$

$$0.5 = \frac{\frac{L}{4}}{\frac{L}{4} + 0.04} \Rightarrow 0.5 = \frac{\frac{L}{4}}{\frac{L}{4} + 40}$$

$$0.5 = \frac{L}{L + 0.16} \qquad (L+40)\,0.5 = L$$

$$20 = 0.5L$$

$$L = 40$$

$$\Rightarrow L = B.R$$

$$= 4\,Kbps \times 40$$

$$\Rightarrow 4 \times 1024 \times 0.04 = 164.$$

IEEE 802.3 (Ethernet)

LAN

generally uses two layers:

(i) Physical layer

(ii) Data link layer

- Logical link control (LLC) → framing
- Media Access Control (MAC) → physical address, Error control, flow control, Access control.

Cables

the cables are differentiated based on their bandwidths. Eg:

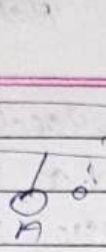
10 Mbps
- 10 base 2 → 200 metre
- 10 base 5 → 500 metre

100 Mbps
- 100base T
- 10 base T → twisted pair (100 m range)
- 100 base F → Fibre optic (2000 m)

Ethernet characteristics

1. Connectionless Communication
2. CSMA/CD (Access Control mechanism)
3. Bus topology

(Carrier sense multiple access / collision detection)



B must wait for some time before sending some data to A.

When A sends the data and then receives back the acknowledgement, only then B can send new data.

During that time B can stage that data and bring it onto the channel. This time for the staging is called Transmission delay

$$\therefore \text{Transmission delay} \geq RTT$$

$$\Rightarrow \boxed{\frac{L}{B} \geq \frac{2 \times d}{v}}$$

Suppose you are designing a sliding window protocol for a 1 Mbps, p2p link to moon, which has a one way latency of 1.25s. Assuming that each frame carries 1 KB of data. What is the minimum no. of bits for the sequence number?

$L = 1KB$; $B \rightarrow 1$ Mbps

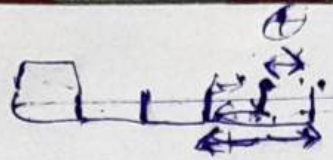
$RTT = 2.5s$

1 Mbits $\rightarrow$ 1s

for 2.5s $\rightarrow$ data $\Rightarrow$ $1.25 \times 1024 \rightarrow 1280$ (8Kb)

data $= 2.5 \times B = 2.5$ Mb

no. of p $= \frac{2.5 \times 1024}{8}$ Kb $\Rightarrow$ 320 bits



GATE

PAGE NO.:
DATE: / /

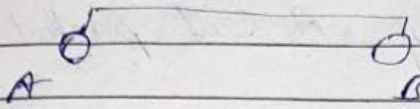
Q Consider the GBN protocol with a sender window size of 'n'. And a sequence no. range of 1024. Suppose that at time t, the next inorder packet that the receiver is expecting has a sequence no. of k. Assume that the medium does not reorder messages. What are the possible sets of sequence no. inside of sender's window at time t? Assume the sender already received ack.

~~Ans: (k%n) + n - 1~~

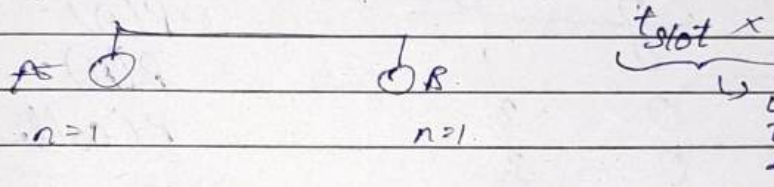
(k%n) + n - (k%n)

PAGE NO.:
DATE: / /

Back Off Algorithm:



if A & B start transmitting data, there will be collision. In this case both will be notified of the collision. and we would resolve this issue by waiting for some time before Retransmitting.



$K_A = (0 \text{ to } 2^n - 1)$ $\quad K_B = (0 \text{ to } 2^{n-1})$

* Here, n is the no. of times a packet has participated in a collision

∴ for first packet (n=1) → K = 0 to 1;

Eg: 0 1 means

$t_{slot} \times 0$ wait for stn A

$t_{slot} \times 1$ wait time for station B.

for the above two values of K, the possible combinations of wait times are:

Collision ← 0 0

0 1 → A transmits in

1 0 → B transmits in

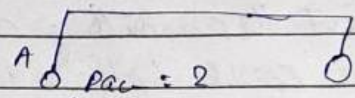
Collision ← 1 1

∴ Probability of winning of A = 1/4

" " " B = 1/4

Probability of collision = 1/2

- Now let's say A sent packet



for packet 2 ← n = 1

↳ for pac 1 coll = 1 ⇒ n = 1

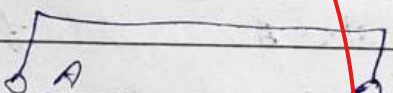
∴ K = (0 to 1)

K = (0 to 3)

0	0
0	1
0	2
0	3
1	0
1	1
1	2
1	3

P(A) = 5/8
P(B) = 1/8
P(collo) = 2/8

for next step :



K = (0 to 1)

(0 to 7)

0
0
0
1
1
1
1

∴ P(collo) = 1/8

P(A) = 11/16

P(B) = 4/16

The above method reduces the probability of collision, but gives rise to an effect called capture effect, where one station overtakes the transmission line.

Q. Ethernet adapters recieve all frames and accepts:
(i) frame address to its own address
(ii) frame address to multicast (if it has been instructed) or broadcast address
(iii) frame if it has been placed in promiscuous mode
(iv) All of the above. ✓

Q. After the Kth consecutive collision, each colliding station waits for a random time chosen from the interval
(a) (0 to 2^{K-1}) × RTT
(b) (0 to $2^{K}-1$) × Maximum propagation delay
(c) (0 to $2^{K}-1$) × RTT ✓
(d) (0 to 2^{K-1}) × Maximum propagation delay

for RTT, we need the time from A to B and then B to A, so total time is RTT. not T_d.

for 2^K → probability of collision each time becomes $\frac{1}{2}$. ∴ after Kth $\frac{1}{2^K}$.

Q Consider a CSMA/CD network running at 1 Gbps over a 1 km cable with no repeaters. The signal speed in the cable is 2×10^5 km/s. What is the min frame size

$$\frac{L}{1\text{Gbps}} \geq \frac{2 \times 1}{2 \times 10^5}$$

$$L \geq 1\text{Gbps} \times 10^{-5}$$

$$L \geq 1024 \times 1024 \times \text{Kbps} \times 10^{-5}$$

$$L \geq 10.4576 \text{ Kb}$$

$$L \simeq 1.3 \text{ KB}$$

Ans. Suppose 2 nodes A & B are attached to opposite ends of a cable with $t_d = 12.5\mu s$. Both nodes attempt to transmit at $t = 0$, frames collide and after first collision A draws $K = 0$, and B draws $K = 1$ in the exponential backoff protocol. Ignore the jam signal. At what time, is packet completely delivered at B, if $B = 10$ Mbps, $L = 1000$ bits

Wait $\Rightarrow$ 25 μs

$$t_{in} = \frac{L}{B} = \frac{1000}{10 \times 10^6} \Rightarrow 10^{-4} s = 100\mu s$$

$$\Rightarrow 125\mu s$$

DATE: / /

Ethernet 802.3 frame format with all diagram and all fields.

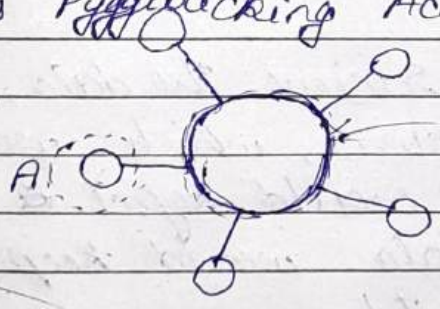
Ethernet

Adv: Reliable, high bandwidth, cost-effective.

Disadv: slow, there is no priority system (all devices), it is non-deterministic.

Token Ring (IEEE 802.5)

- Connectionless communication.
- Deterministic services
- Ring topology is used
- It has a priority system.
- There is no collision
- It uses Piggybacking Acknowledgement system.



a token system is used to access the main communication channel.

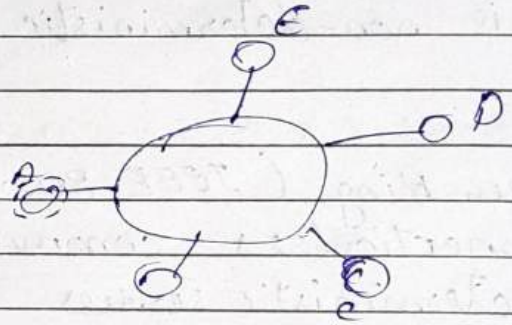
The system has 1 token, and the sender must have that token for it to send the data. Once all data is sent, and ACK recieved, then the token is released by the initial station for others to use.

The token is then assigned to the next station based on some priority.

One of the issues is managing the token. Who would monitor the token, and manage who gets the token, etc. For this we elect a monitor from within the token ring for manging token.

Problems:

① Source Related



~~Once~~ D say A is source, D is destination. let's say that A sends the data and ~~once~~ after that it disconnects in...

Now D will recieve the data, and check for the source, which would be missing. So D would reject it and the entire data would keep on circling the ring infinitely

Such Data packet is called Orphan Packet.

If the source disconnects after sending partial data, it is called Stray packet.

PAGE NO.:
DATE: / /

② Destination ~~packet~~ problem

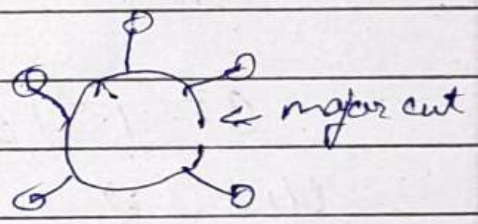
Could be busy, disconnected or recieves the data halfway and disconnects.

③ Token ~~Ring~~ problem

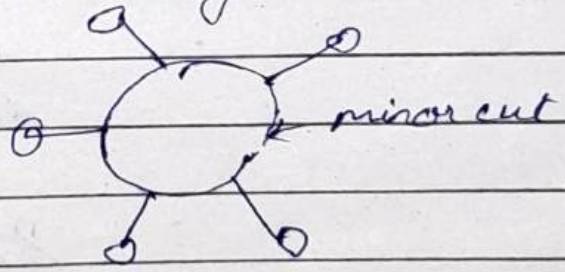
Token gets corrupted, or vanishes.

④ Ring Related.

Major cut → Some part of the ring is completely disconnected.



Minor cut : The ring is not completely disc but that part of the ring results in data loss etc.



⑤ Monitor related

Monitor doesn't pass the token, alters the token, is biased etc.

Q Consider an 802.3 LAN with 500 stations connected to 500 m segments. The data rate is 10 Mbps, and the time slot is 51.2 μs. If all the stations transmit with equal probability, what is the channel utilization using $L = 512$ bytes. Assume no. of contention slots are 1.716.

$F = 512 \times 8 = 4096$ bits.

$R \rightarrow 10$ Mbps

$F/R = \frac{4096}{10} = 409.6\ \mu s$

$C = 1.716$

$\therefore U = \frac{409.6}{409.6 + 51.2 \times 1.716}$

$\frac{409.6}{409.6 + 87.8592} = 0.823$

$= 82.3\%$

Contention slots $= \left(1 - \frac{1}{N}\right)^{1-N} - 1$

$N \rightarrow$ no. of channels

PAGE NO.:
DATE: / /

Solutions:

Orphan Packets / Stray Packets:

The monitor will validate all the packets and remove any stray or orphan packets.

We maintain a special frame with the data to ensure that the source exists.

Destination Related

Avail (A)	Copy (C)	
0	0	← initially
1	1	← safe option (available & copied the data)
1	0	← (destination is busy)
0	1	← (some other channel than the intended copied the data)

Ring related

Major cut: A beacon is sent to identify the cut.

Minor cut: The monitor identifies the cut.

Monitor related

Maximum holding time is fixed, after which the station must release the token irrespective of its priority.

Ring latency = Prop-delay + N x Min delay at each station

Max Ring Latency = Prop-delay + N x Token Holding Time (THT)

Q. Find the ring latency of the ring where R = 4Mbps, N = 20 stations separated by 100m, and bit delay at each station is 2.5 bits. Recalculate the latency for R = 16 Mbps N = 80, bit delay = 2.5 bits.

Rate = 4×10^6 bits/s

∴ Propagation delay = $\frac{\text{bit delay}}{R}$

= 0.625 μs

Assume prop delay = Trans delay

∴ R_{la} = 0.625 + 20 x 0.625.

= 13.125 μs

PAGE NO.:
DATE: / /

Minimum size of ring

(Transmission delay = Propagation delay) *

Delayed Token Ring and Early token ring strategy

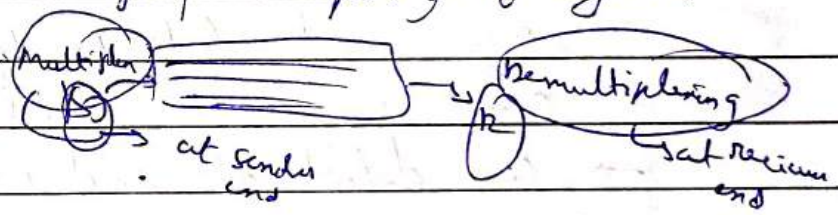
- The token is released only after verifying the delivery of the data.
- The token is released immediately after sending all the data.

$\frac{L}{1 \times 8} \geq$

Physical layer

- cables & connectors
- → physical topology
- → Hardwares (Repeaters, Hubs)
- → Transmission → (simplex, half duplex, full duplex)
- → Multiplexing → using existing channel logically for more than one S-R pair by changing frequency of signals
- → Encoding (digital ⟷ analog)

(converts bits to signal for propagation through guided or unguided media)



Efficiencies

S&W

$$\eta = \left(\frac{1}{1+2a}\right), \quad a = \frac{T_p}{T_t}$$

GBN

$$\eta = (2^k - 1) \times \frac{1}{1+2a}$$

SR

$$\eta = (2^{k-1}) \times \left(\frac{1}{1+2a}\right)$$

Framing

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

(A) ——— 1 Gbps ——— (B)

10^9 bits – 1 sec

1 bit – $\frac{1}{10^9}$ sec

This will cause single bit error

If error lasts for → $\frac{1}{100}$ sec, then bits corrupted

$= \frac{1}{100} \times 10^9 = 10^6$ bits corrupted.

Lec - 28

Error Detection -

① Simple parity (even, odd)
② 2D parity check
③ checksum
④ CRC (Cyclic Redundancy check)

Error correction
Hamming code

Single parity (lec-28)

If given Hamming distance is d, then detect (d-1) bit errors.

Hamming distance

0001
1101 } XOR
0010 → one
so H.D = 1

Lec-29 Cyclic Redundancy check (CRC)

→ Based on binary divisions
→ total bits = (n+k) n → no. of bits in original message
k → no. of redundant bits sent to detect error
→ polynomial shall be divisible by x
→ also not with (x+1)
→ can detect all odd errors, single bit burst error of length equal to polynomial degree.

e.g. $x^4 + x^3 + 1$
↳ polynomial
∴ 4 = no. of redundant bits.
$1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 1 \cdot x^0$
↳ 11001 → divisor

1010101010

So append four bits.

10101010 0000
↳ dividend.

XOR → same → 0
diff → 1

5 bits, so appended 4 bits

11001) 10101010 0000

11001
01100
11001
00010 0
11001
00011000
11001
00001 0

Start from 1 from

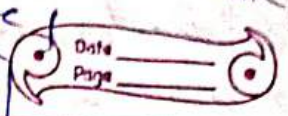
→ last four bits

1010 1010 0010

↳ Now receiver will divide it using same divisor. If remainder = 0 no error, if any 1, then error.

DLL → LLC + MAC

Multiple Access Control (MAC)



Access protocol

- Aloha
  - Pure
  - Slotted
- CSMA
- CSMA/CD (Collision detection)
- CSMA/CA (Coll. Avoidance)

Control Access

- Polling
- Token Passing (Token ring)

Channelization protocol

- FDMA (Frequency Division Multiple Access)
- TDMA (Time Division multiple Access)

CSMA → senses/checks if the carrier/transmission line is empty (for data sending or not).

- 1-persistant → Ethernet
  - Senses continously for empty transmission line (high chance of collision)
- 0-persistant
  - Wait for random amount of time for sensing again & again (low chance of collision)
- p-persistant (with probability)
  - Checks only at connection point of node with main line.
  - Checks here & not in full line
  - Check for free line but if found free then may release data with p probability.

Acknowledgement data not used together to -

CSMA/CD

→ no acknowledge to prevent extra load on line.

→ $TT \geq 2 * PD \Rightarrow \frac{L}{BW} \geq 2 * PD$

→ can detect that its data has undergone collision if it recieves collision signal when its transmitting.

→ $\eta = \frac{1}{1 + 6.44a} \Rightarrow a = \frac{PD}{TT}$

Transmission time (for how much time it should transmit data).

Eg: $\frac{1250 \times 8}{10^8} = \frac{2 \times 1}{n} \Rightarrow n = \frac{2 \times 10^8 \times 1}{1250 \times 8}$

$\Rightarrow n =$ 2000 (bps)

Frame size = 1250 bytes
Length = 1 km
Signal speed = ??
Transmi. rate = 100 Mbps (10^8 bits/s)

Lec-40 Token Ring (IEEE 802.5)

→ Ring topology is used.
→ Access control method used is token passing.
→ Token ring is unidirectional.
→ Piggy backing ack. is used.
→ Monitor station is used.
→ ~~multiple~~ variable size framing.

Early & delayed release of token (to reduce traffic congestion.) — immediate, connected to itself.

Lec-41 Network Layer → uses IP

Roles

Transport Layer
[Network Layer]
DLL

→ Host to Host delivery / source to dest. del. / Machine to machine deliv.
→ Helps establish communication b/w two host in different networks.
→ uses Logical (IP) Address for data transfer. to identify reciever & sender.
→ Fragmentation
→ Congestion control.

→ Routing (Router is used to decide the next path which data packet should follow to reach destination.)
→ Router has intelligence.

Every router has → NL, DLL, PL, Bridge → DLL, PL

Transport Layer → TCP & UDP (user data protocol) → process to process delivery

Roles

1. End to End delivery (port to port delivery of data). It means that if a machine A has different running application, then data from a particular app'n of Machine A is sent to a particular app'n of machine B in different net using port address (simply app'n add.). One level above network layer.
2. uses TCP for reliability (means if n message sent, then recieving to reciever is n msg)
3. follows in order of messages. ↳ connection oriented.
4. Error control (checksum).
5. Congestion control
6. Flow control (GBN, S&W, SR)

(7) Segmentation (divides continuous data coming from application layer into segments by applying ~~header~~ and it to network layer forward)

(8) ~~Multiplexing~~ & Demultiplexing

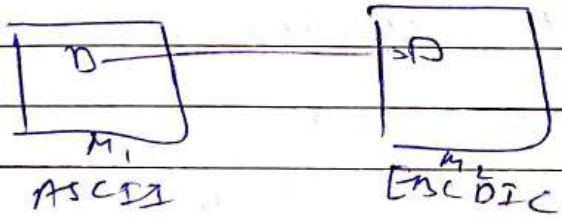
Ex sends messages from different application together the channel.

73, 80, 25, 91, 27,

Session Layer (not responsibility of OS)

→ creating a session.
→ checks for authentication of request to the server and then assign authorization.
– session restoration (checkpoints the last state of our interaction/activity)
→ uses session beams
→ creates checkpoints (if downloading video ---)
→ helps in webinar/web conferencing by doing synchronization.
• and flow control.

Presentation layer (not responsibility of OS)

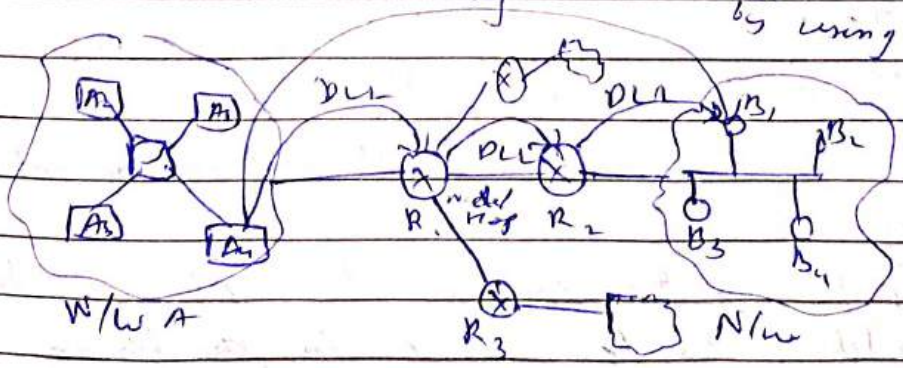


1) Code conversion (formatting)
2) Encryption/Decryption
3) Compression of data (by removing redundant data)

Data Link layer

Network layer → data → DLL → data → PL

Roles
1) Node to Node delivery
2) Is sufficient for data transfer within a network by using MAC & physical address
3)



→ Flow control → Stop & wait
→ GBN
→ SR.

→ In transport layer, flow control takes care of destination (here B,) capacity to decide what should be the flow in order to prevent buffer overflow.

→ In DLL, flow control takes care of next node's (on which data is to be sent) capacity to decide
↳ controls flow at each node.
control's flow b/w source & destination

→ Error control
DLL does errors control hop to hop or node to node where as transport layer does error control from source to destination

→ DLL error control (CRC, Checksum, parity)
DLL TL.

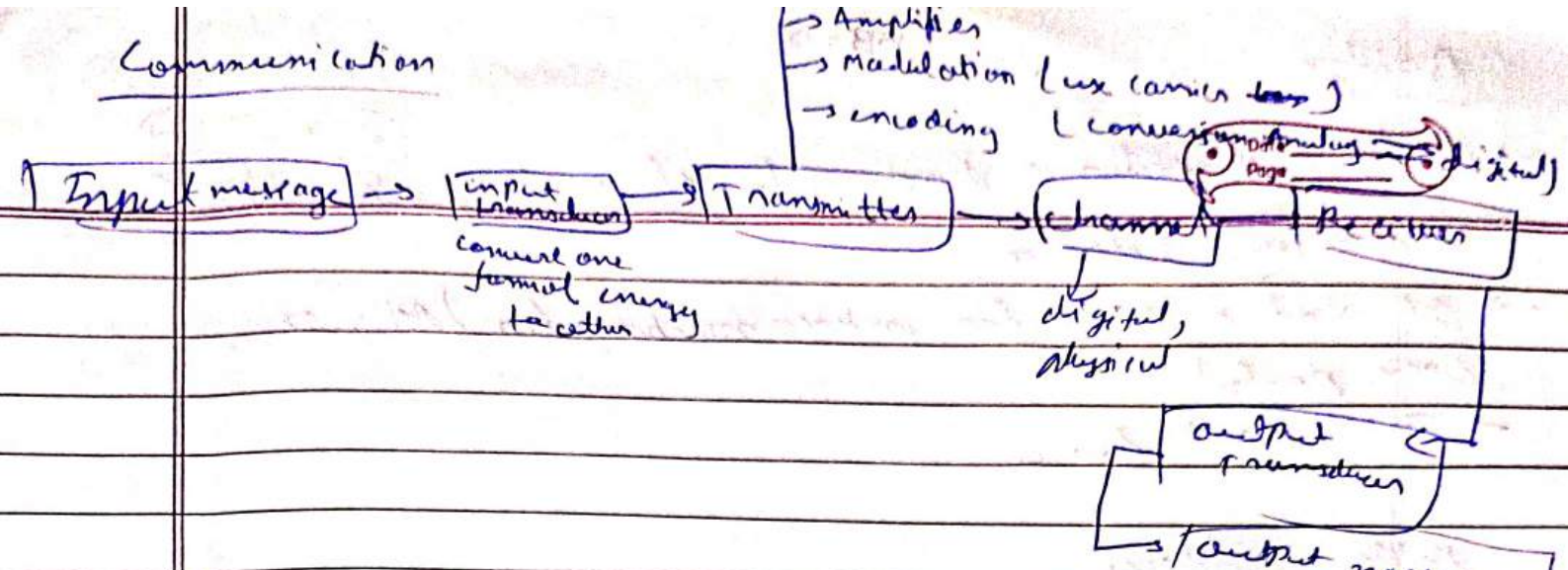
→ Error detection is DLL is more efficient in terms of time & network utilization.

→ Access control (CSMA/CD, Aloha, Token Ring)
↳ to prevent collision of data.

→ Physical Address (MAC) [48 bits]
↳ constant / fixed address
can use MAC addr. to contact different nodes within same network but not in inter network

→ Framing
Divides data into frames by splitting data and adding headers & trail to them to help in proper further transmission of data.

Communication



→ A CN is a telecommunications networks, which allows autonomous digital devices (nodes) to exchange data b/w each other using either wired or wireless connections to share resources (h/w or s/w) interconnected by a single technology eg. Internet.

→ Goals of CN :-

① Facilitating communication ② Resource sharing.
③ Data storage & Access ④ cost efficiency ⑤ Reliability & Redundancy.

Backoff Algo

Used in Ethernet to schedule retransmission of data after collision. Here waiting time is given to each station to wait for some time, then again retransmit. This waiting time is b/a backoff time.

Binary B/o Algo (on only two station).

$$WT = \text{R} \times T_{slot}$$

R → R.T.

T_{slot} → $2 \times t$ (t → max propagation delay)

Capture effect.

Router → has memory (and stores Routing table in its memory)
A networking device that forwards data packets between Computer Networks.

Switch → has memory & stores MAC addressing table.

Switch operates in DL & Router " in NL.

Bridge

→ Bridge = Repeater + functionality of reading MAC address.
→ It is a layer 2 device.
→ It is also used for interconnecting two LAN's on same protocol.
→ Two port device.

MAC Address

→ MAC = media access control
→ Every node in the LAN is identified with the help of MAC address.
IP address = Location of a person
MAC address = Name of the person
→ Switch uses MAC address & Router uses IP address.
→ Unique → physical address or hardware address in world
→ cannot be changed → Assigned by manufacturers.
→ Represented in hexadecimal (eg → 70-20-84-00-EA-0A (48 bits))
→ Separator: hyphen(-), period(.), and colon(:).

Flow control

→ Speed matching mechanism
→ Flow control coordinates the amount of data that can be sent before receiving an acknowledgement.
→ Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.

Ex: Bandwidth - Delay product = Bandwidth × Delay
Delay = 80 ms
Bandwidth = 128 kbps
Packet size = 32 bytes.

Bandwidth delay product = 128 kbps × 80 ms

$= 128 \times 1024 \times 80 \times 10^{-3}$ bits

$= \frac{128 \times 1024 \times 80 \times 10^{-3}}{8}$ bytes

Optimal window size = $\frac{128 \times 1024 \times 80 \times 10^{-3}}{8 \times 32}$

Subnetting

→ A subnetwork or subnet is a logical subdivision of an IP network.

→ The practise of dividing a network into two or more networks is called subnetting.

→ Computers that belong to a subnet are addressed with an identical most-significant bit-group in their IP addresses.

Network software

→ Check for the protocol heirarchies (layered structure)

→ It checks about design issues of layers

→ It has to check whether it is connection oriented or connectionless service b/w the layers.

→ It checks the service primitives b/w the layers.

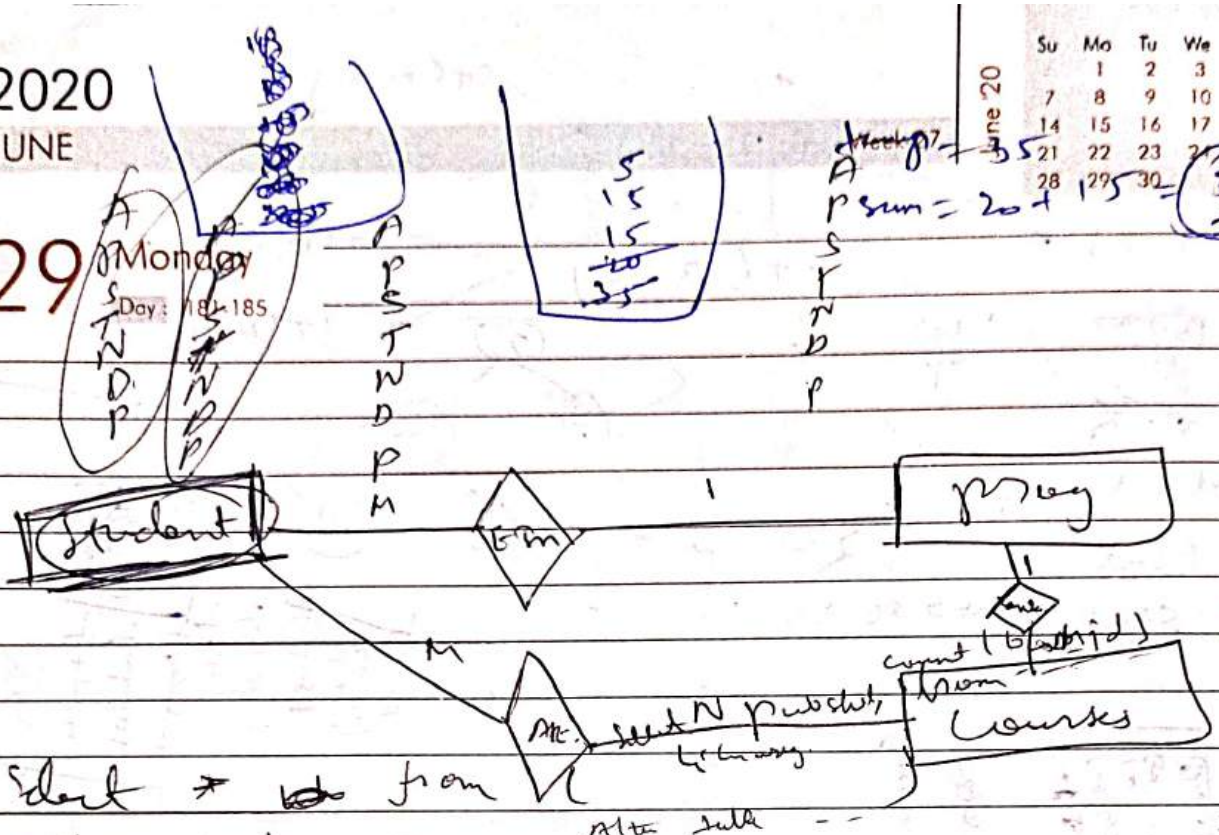
→ It studies the relationship of services to protocols.

within layers physical communication b/w two hosts

virtual communication

2020
JUNE

29 Monday
Day: 181-185



Select * from where pubs+ -

CN

Connection + protocol = Communication

30 Tuesday
Day: 182-184

Data is transmitted, formatted & processed.

MAN → Fiber distributed Data Interface, Copper

WAN → Leased line, Dial-up, (internet)

Devices in CN

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

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

7) Gateway
8) IDS
9) Firewall
} Security

10) Modem → modulator & demodulator to convert.

Analog ⇌ digital

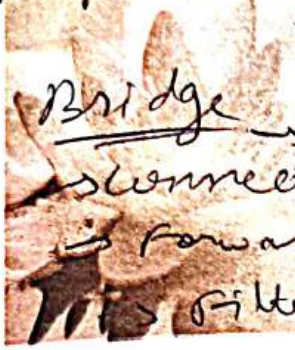
Hub (only H/W) → used to connect devices within same network.

MONTH AT A GLANCE 2020 JULY

→ multiport Repeater → collision domain possible

→ No filtering

→ forwarding



नम्रता में रहने वाला ऊंचाई को पाता है।
मिलता है सम्मान उसको, जहां जहां भी जाता है।

- A 'Humble' being is exalted in life and accepted by all

Bridge → Two port device / Layer 2 device
connects two or more LAN.
→ forwarding.
→ filtering } on the basis of Mac address (maintains of table).

Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Lec 2

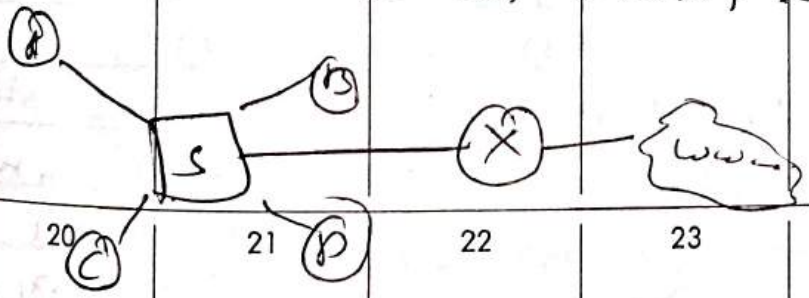
1 → collision not possible due to its own buffer which uses store & forward technique.
→ Bridge uses spanning tree to prevent data from getting stuck in loop.

2 3 4 5 6 11 12

Switch

Layer 2 Device, multiport bridge, full duplex link, collision domain is zero, traffic is minimal.

13 15 16 17 18 19



20 21 22 23 24 25 26

Routers (Physical, Data link, Network Layer)
→ can check mac as well as IP address.
→ connects & separates distinct networks, operating at IP address level and provides advanced features like security and routing.

27 28 29 30 31

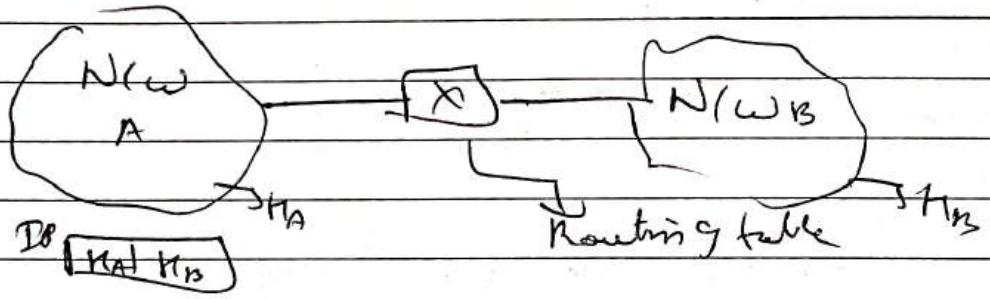
2020 JULY — Week-27 — July

Su Mo Tu We Th Fr Sa
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31

Bridge suitable for extending / Connecting within the same broadcast domain, the MAC address level.

01 Wednesday
Day : 183-183

→ Routes maintains Routing table to forward or filter the data.



Router → Forwarding, filtering, collision domain
Store & forward method using buffer.
Routing, Flooding (broadcasting).

Unicast → sending message one to one.

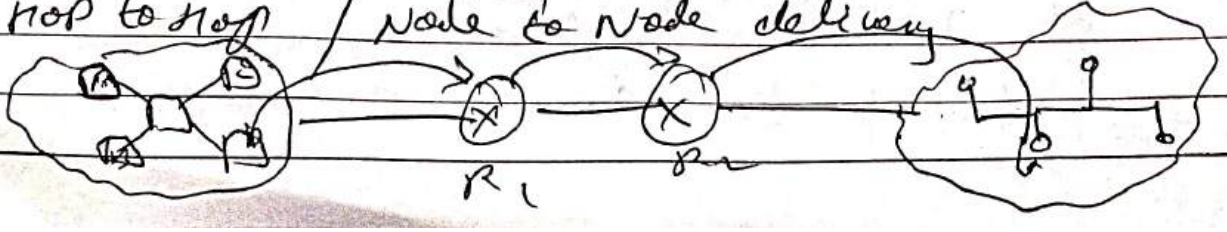
02 Thursday
Day : 184-182

Broadcast → Limited Broadcast
Sending message to all device within same network
255.255.255.255

→ Direct Broadcast
Send msg from device in net. A to all devices in network B.
92.255.255.255 → Destiny network ID of B.

Multicast
used to send msg to group like mails to a particular group of research students (class 0).

Data link Layer
→ transfers data between two device in same network - Hop to Hop / Node to Node delivery



Su	Mo	Tu	We	Th	Fr	Sa
30	31					1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

Aug '20

→ DLL

Week-27

Friday 03

→ reliable delivery → Error control (CRC, checksum, parity)
↳ DLL ↳ T.L

→ flow control
↳ S/w ↳ GBN ↳ SR

→ Access control (CSMA/CD, CSMA/CA, pure Aloha, Token)
↳ prevent multiple nodes from sending message at a time to prevent collision.

→ physical address (MAC addr.)

→ Adds header & tail to the data received from network layer after ~~framing~~ organising data into frames.

Data link layer
- two layers
  - → Logical link control (LLC)
    - ↳ deals with data syn., error control, flow control, etc.
  - → Medium Access control (MAC)
    - ↳ used to avoid collision on data transfer through common communication link (eg: bus topology)

MAC
- Random Access protocol → no priority (anytime data transfer)
  - Aloha
  - CSMA
    - ↳ Carrier sense multiple access
  - CSMA/CD
  - CSMA/CA
- Control Access
  - polling
  - Token passing
- Channelization protocol
  - FDMA
    - ↳ Frequency division multiple access
  - TDMA
    - ↳ Time division multiplexing.

Saturday 04
186-180 Day:

Carrier sense multiple access (CSMA)

Sense whether any signal (data) is already in the channel. ~~and~~ we can check only at the point where node is connected to main line and if any signal detected, it can hold its data and wait for line to be empty.

Sunday 05

2020
JULY

Week 28

CSMA

→ p=1 ↓ → p=0

1-Mpersistent | 0-persistent | p-persistent

06 Monday
Day: 188-178

Check if main line is empty, if yes releases data immediately otherwise continuously keep checking for empty line. Chance of collision is very high.

If empty line/idle line, releases data immediately, else wait for particular amt. of time & then release data. line is not fully utilized but chance of collision is low.

Continuously check for empty line, if yes then have probability p to transmit data.

LAN (wired)

↖ CSMA/CD (collision detection)

→ No Acknowledgement is used as it will increase traffic on main line and cause more collision.

07 Tuesday
Day: 189-177

Collision is detection by a particular station iff it recieves collision signal at the time when it is transmitting its data. If it has stopped transmission, then even on recieving collision signal, it can't detect collision as it would not be sure that whether this is collision signal of its own data or some other station's transmission.

→ TT ≥ 2*PD ⇒ Transmission time ≥ 2*PD

$$\Rightarrow \boxed{\frac{L}{BW} \geq 2 * PD}$$

efficiency of CSMA/CD = $\eta = \frac{1}{1+6.44a}$ $\boxed{a = \frac{PD}{TT}}$

CSMA/CA (WLAN) → wireless LAN

1. A device listens to the channel for check if it is idle before transmitting data.
2. If channel is busy, device waits for a random backoff time before trying again.
3. This reduce chance of multiple devices transmitting simultaneously
4. After successfull data transmission, the receiver sends an acknowledgement to conform receipt.
5. Use in wireless networks, where collisions are harder to detect.

Wednesday 08
190-176 Day:

Ethernet frame format (IEEE 802.3) - 1983.

→ used in data link layer, its a LAN technology.
→ used CSMA/CD.

Types of Ethernet

→ 10 Base 2 → 10Mbps base 200 m (Thin)
→ 10 Base 5 → 10 Mbps, 500 m (Thick) → Coaxial cables used.
→ 10 base T (T → Twisted)
→ 100 Base FX - Fast
→ 10 G Base T → Gigabit ethernet.

Thursday 09
191-175 Day:

Topology → Bus, Star (→ mostly) · Bit Rate → 1 Mbps - 400 GB/sec.

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

Physical layer adds it ← → DLL add these

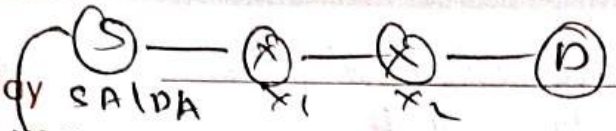
PREABLE → 56 bits (10101010 - - - 10) → Just to alert the receiver that msg is coming.
SFD → 8 bits (10101011)

2020 JULY

Week-28

10 Friday Day: 192-174

Destination Address (DA) → gets MAC address
Source address (SA) → " "



SA | DA | X1 (as we don't know D's address).

Length → 16 bits (0 - $2^{16}-1$ / 0 - 65535) frame can't have this length

Data must be atleast 46B for collision detection to work.

packet → NL
segment → TL
frame → DLL

DATA FORMAT

Token ring frame format

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

SD → start delimitator (1byte) used for alert & synchro.
DATA → size depends on token holding time (min. ⇒ 0)

11 Saturday Day: 193-173

AC → Access control (1byte)
FC → frame control (bits to check whether frame is data frame or control frame)
CRC → for error control (cyclic red. check).
ED → end delimitator, FS → frame status.

TOKEN FORMAT (3byte)

12 Sunday

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

→ one property of network layer is Routing → it has two different protocols
① RIP (Routing Information protocol)
② OSPF.
Routers decide where to send the msg/signal next to get it to destination through shortest paths. This intelligence of routes is due to algorithm like RIP & OSPF.

Lec → 46, 47, 48 (left).

Subnetting

→ Process of dividing a large network into smaller, managable subnetwork (subnet).
why its done?
→ Efficient IP address allocation (no wastage of IP addresses)
→ Improved network performance due to reduced Tuesday 14 196-170 Lecture
congestion.
→ Enhanced security by isolating different parts of networks, limiting the spread of security threats.
→ Simplified network management by allowing better organization & control of resources.
→ Support for multiple network while all networks still being part of same larger network.
→ Scalability by allowing network to grow in a controlled manner, accomodating more devices without redesigning the entire network.

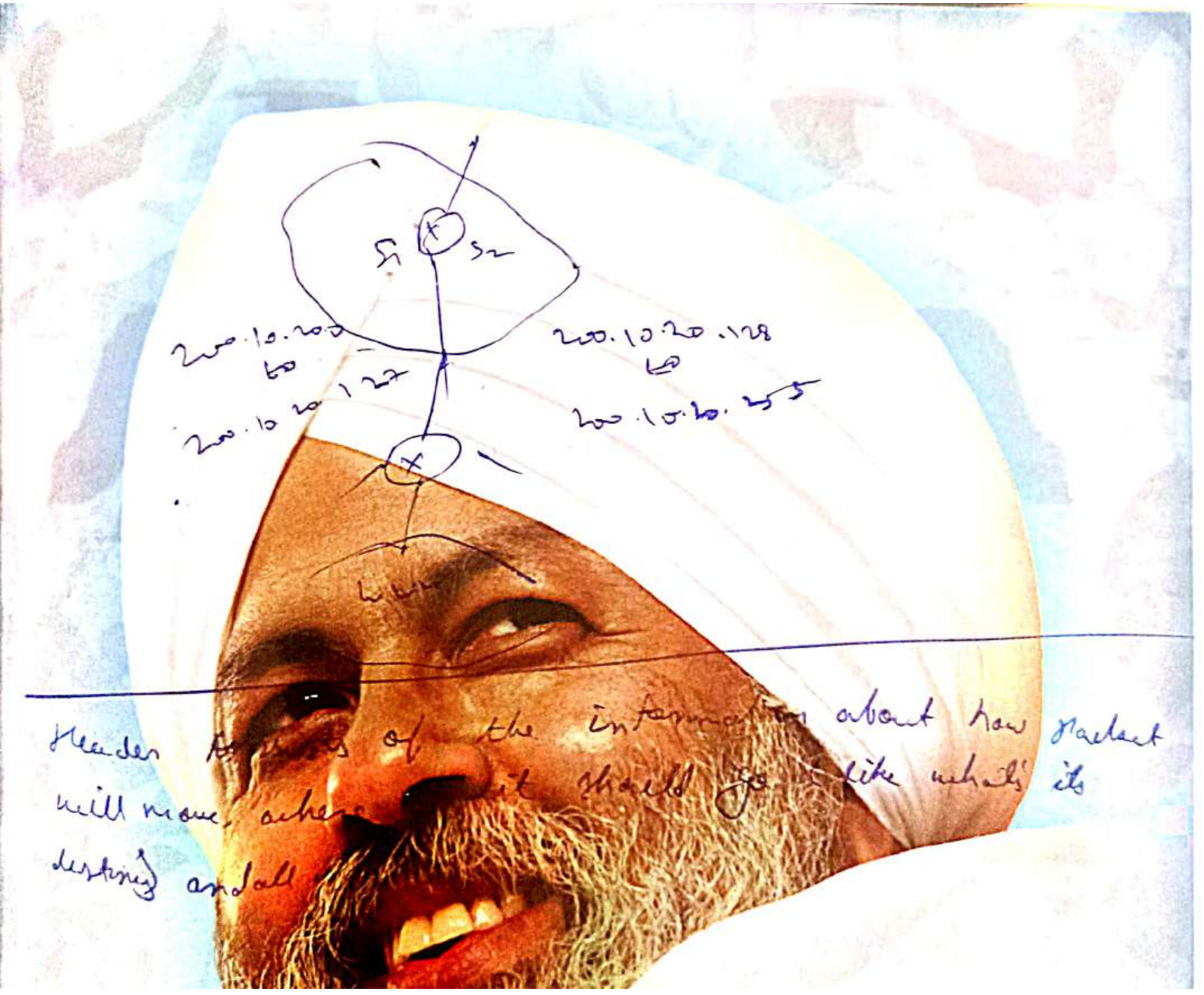
Check ss in CN folder of lec. 49.

CW

Subnet mask → 0s from starting the no. of bits reserved, Put 1.

IPV4 → Internetworking protocol.
→ connectionless
→ Datagram service

Low reliability as no connections established, so data packets may get lost, collided, etc.



Header bits of the information about how packet will move, where it should go, like what's its destiny and all

Differentiated service code point (DSCP)

Week 30

| P | P | P | D | T | R | C | 0 |

precedence.

Provides priority in packet, tells whether its sending packet or to send packet immediately.

D → delay (no delay → 1) R → Reliability (1 → max)

T → Throughput (max. → 1) ↳ no data lost etc.

C → cost (1 → low cost, shortest path).

0 → reserved for future purpose.

| DSCP | ECN |

0 5 7

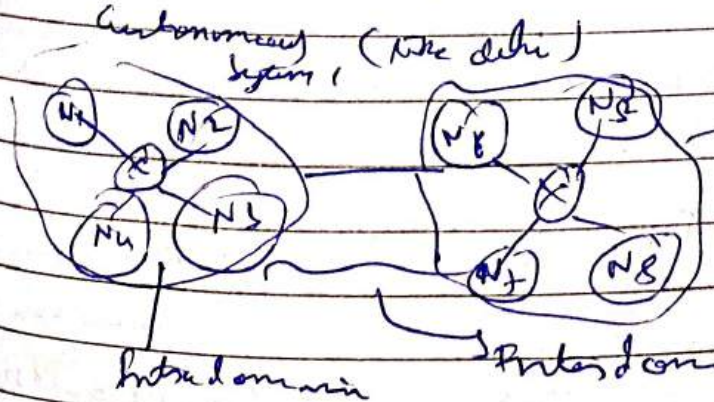
ECN → Explicit congestion notification (1 1 → congestion notification sent to sender to lower speed)

IPv6 → 128 bit addr.

Options & padding → used when we have to add packets, when original packet is not in the multiple of 32.

In IPv4, we divide packets into smaller fragments (datagrams) and send it to destination via different routes.

Identification bit used to tell that all fragments reaching destiny via different routes belong to same initial packet.



2020 JULY

Wednesday 22

204-162 Day

Thursday 23

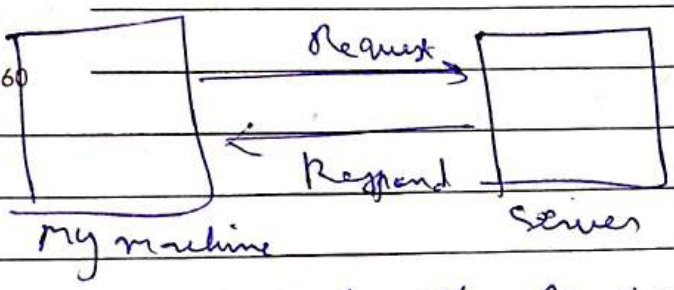
205-161 Days

July '20

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Session Layer

24 Friday
Day: 206-160



The responsibility of the session layer is to create the session. My machine would send request to that server. I would provide my credentials to get authentication and in return server would allow me to create a session with it while providing authorization like homepage login is session and various features there is authorization.

Session layer responsibilities :-
Authentication, Authorization, Session restoration (checkpoint) by using session beacons, helps in flow control and synchronization

25 Saturday
Day: 207-159

Session layer & presentation layer is not provided by OS but by the application which we are using.

Encrypted → Cypher text → Decrypted

presentation layer

26 Sunday

No vulnerability

ASCII
M_1

EBCDIC
M_2

1) Code format conversion
2) Encryption / Decryption
3) Compression by removing redundant info.

Application layer

assign 16 bits port no → 2^{16} → 0 - 65535

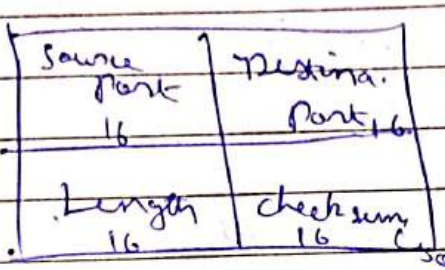
TCP → establishes dialup connection

↓

0 - 1023 → well defined port no.

User datagram protocol (UDP)

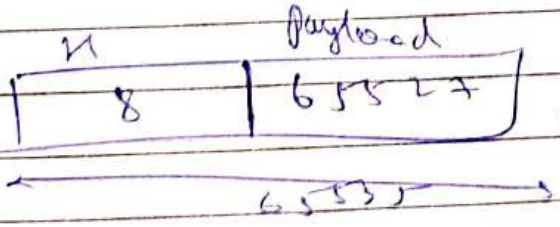
Header → (8 B fixed)



UDP header (8 B fixed)

→ connection less (unreliable)

It transfer data without establishing the connection with server. UDP just add header to Payload (user data) and sends it to server. If some packet is lost, then UDP don't cares about it and not even the sequence of the packets in the order in which they are sent



source IP, header IP

values which are fixed in IP (not for whole IP)

Checksum used for error control.

Checksum = UDP Header + UDP data + Pseudo header of IP.

It's like find unique hash value of data, and if anything changes in data, that hash value would also change.

We send this checksum with data and server will recalculate the hash value to check if both hash values are same or not.

2020
JULY

29 Wednesday
Day: 211-155

30 Thursday
Day: 212-154

UDP applications

1) One request one reply (DNS) Dynamic host control protocol DHCP

2) High speed is due to less overhead.
Online games, voice over IP

TCP low speed as if single packet is lost, it will retransmit it & Data applied congestion control.

3) Broadcasting / multicasting (RIP)
as TCP reserves buffers to share its routing table at every time period.

4) Continuous streaming (Skype, ~~Hotstar~~ Youtube)
Cs If some pixels get lost also, it will move on but not so at high definition.

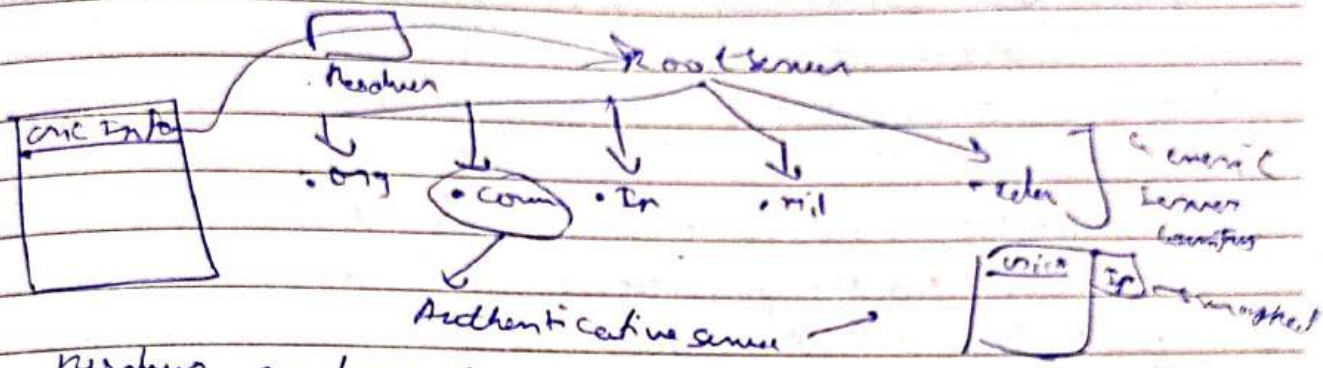
UDP is stateless (It doesn't save the value of the connection it makes).

Two types of protocols → Stateless & Stateful.

TCP	UDP
1) Connection oriented	1) connectionless
2) Reliable	2) less Reliable
3) Error control is mandatory	3) Error control is optional
4) Slow transmission	4) Fast transmission
5) More overhead	5) Less overhead
6) Flow control, congestion control	6) No FC, CC

Domain Name system (DNS)

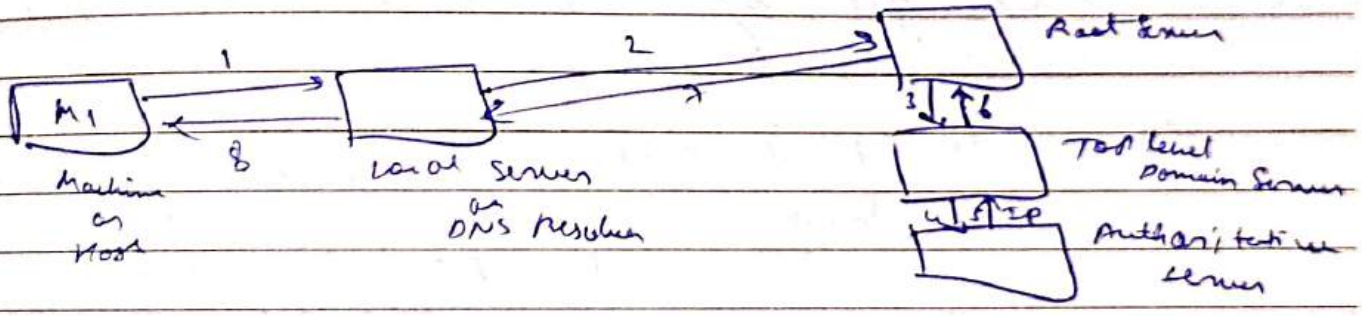
IP address may get changed but domain name remains the same. We remember by domain name and not IP add.



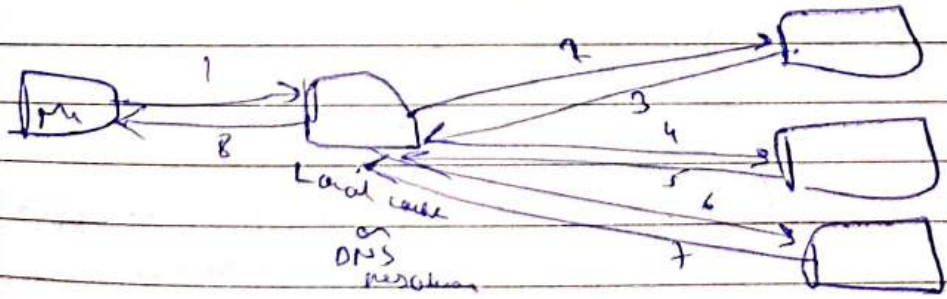
Resolver resolves domain name into IP add..

DNS query are solved either iteratively or recursively.

Recursive



Iterative



TCP/UDP (because its fast)

2020
NOTES

HTTP (Hyper Text Transfer protocol)

- Port no 80
- widely use to fetch the web pages on www.
- Itself not reliable but use TCP to achieve reliability
- Inband protocol (command & data travel from same port no.)

commands
data
→ 80

- Stateless (no information saved)
- HTTP 1.0 Non-persistent
- HTTP 1.1 persistent (eg → gmail)

Information may gets saved in cookies.

Connections are not persistent, as soon we we close tab all connection get lost. and again fill username & pass

eg → IRCTC.

mails get open directly without filling username and password.

- Commands (Head, Get, Post, Put, Delete, connect)
  - Head → to retrieve header
  - Get → accessing web page
  - Post → providing input to web page
  - Put → input
  - Delete → delete input

HTTPS → works on secured socket, i.e, at each connection username & password gets checked each time

SMTP (Simple mail Transfer Protocol)

→ SMTP is both synchronous & asynchronous

→ SMTP port no 25 for pushing the mail.

2020

MONTH AT A GLANCE

AUGUST

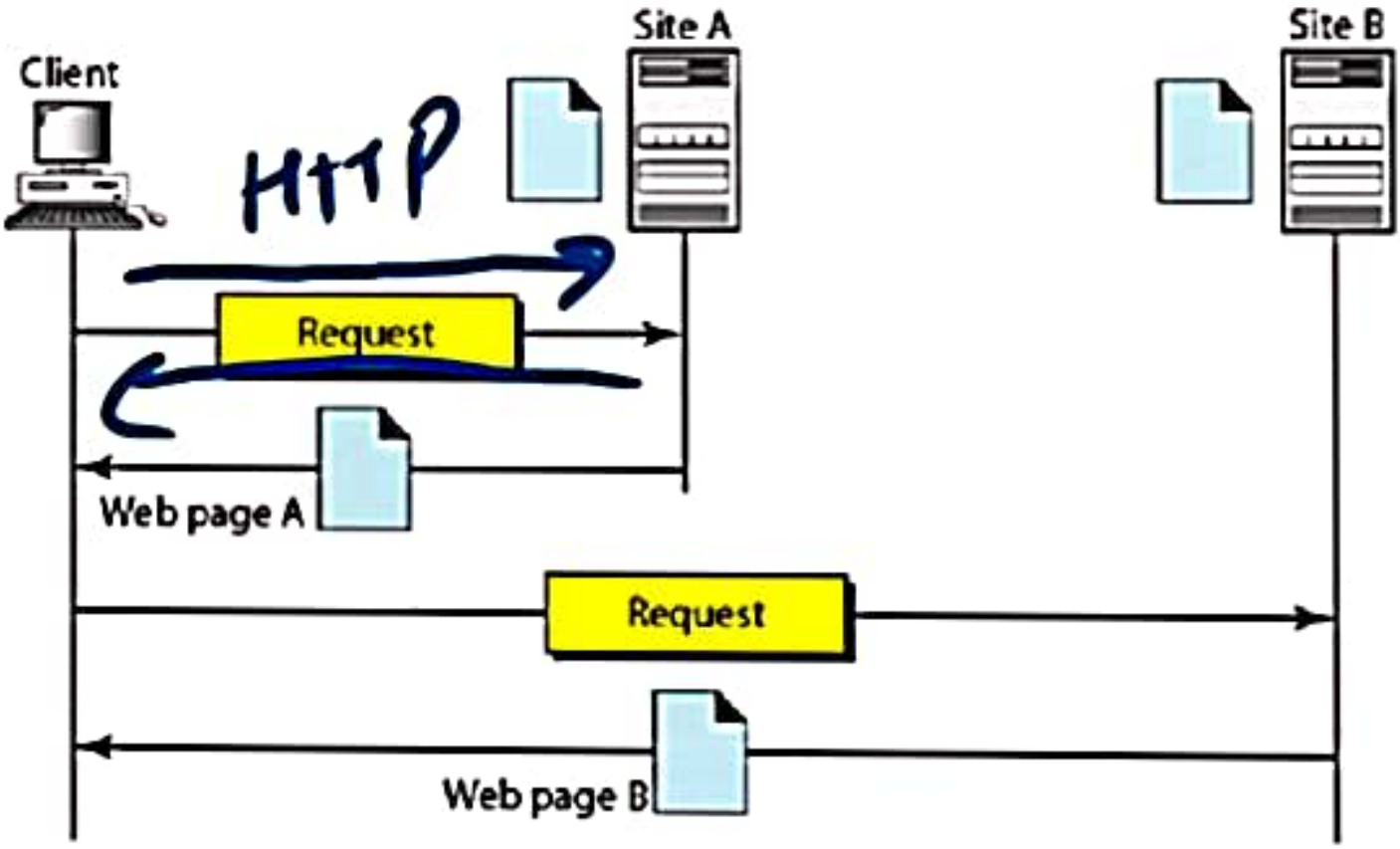
चित्त बसे यदि निरंकार तो अधरों पर खेले मुस्कान।
चित्त बसे यदि निरंकार तो दु:ख नहीं करते परेशान।

- सम्पूर्ण अवतार बाणी (शब्द संख्या 37)

- If Nirankar dwells in consciousness,
a devotee attains the ultimate 'Bliss'

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
31					1	2
3	4	5	6		8	
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

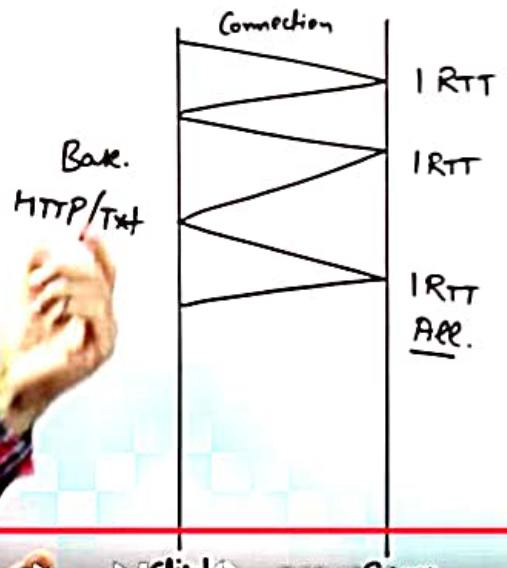
Protocol Name	Port No.	Transport Protocol
Echo	7	TCP / UDP
FTP	20/21	TCP
Secure Shell (SSH)	22	TCP
Telnet	23	TCP
SMTP	25	TCP
DNS	53	UDP
DHCP	67/68	UDP
TFTP	69	UDP
HTTP	80	TCP
POP	110	TCP
NTP	123	UDP
HTTPS	443	TCP
RIP	520	UDP


Site A
Site B
Client
HTTP
Request
Web page A
Request
Web page B

Method	*Action*
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
POST	Sends some information from the client to the server
PUT	Sends a document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Reserved
OPTION	Inquires about available options

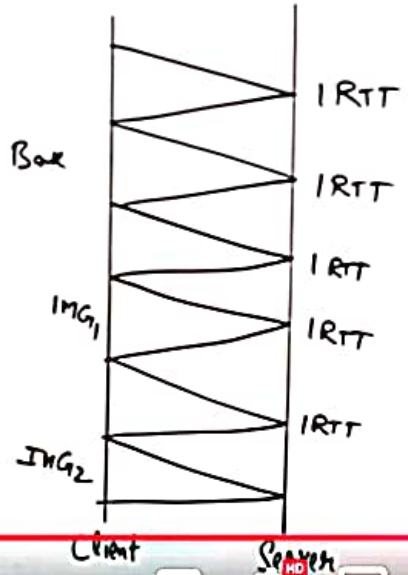
Persistant HTTP Connection (HTTP/1.1)

1) Server leaves Connection open after sending response
   1 RTT for all referenced object
2) Less overhead



Non persistant HTTP (HTTP/1.0)

1) It Requires 2 RTTs for object
2) More overhead



Why there is need of IPv6(IPng)

- Limitation in IPv4 addresses

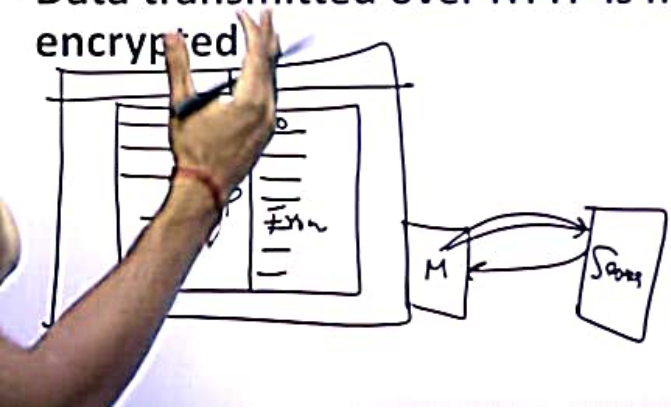
2^{32} = 4,294,967,296

2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456

- Realtime data transmission
- Authentication
- Encryption enabled
- Fast Processing at routers

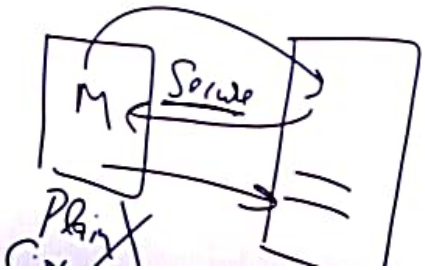
HTTP (Hypertext Transfer Protocol)

- HTTP is the standard protocol used for transmitting data over the web.
- It operates over port 80.
- Data transmitted over HTTP is not encrypted



HTTPS (Hypertext Transfer Protocol Secure)

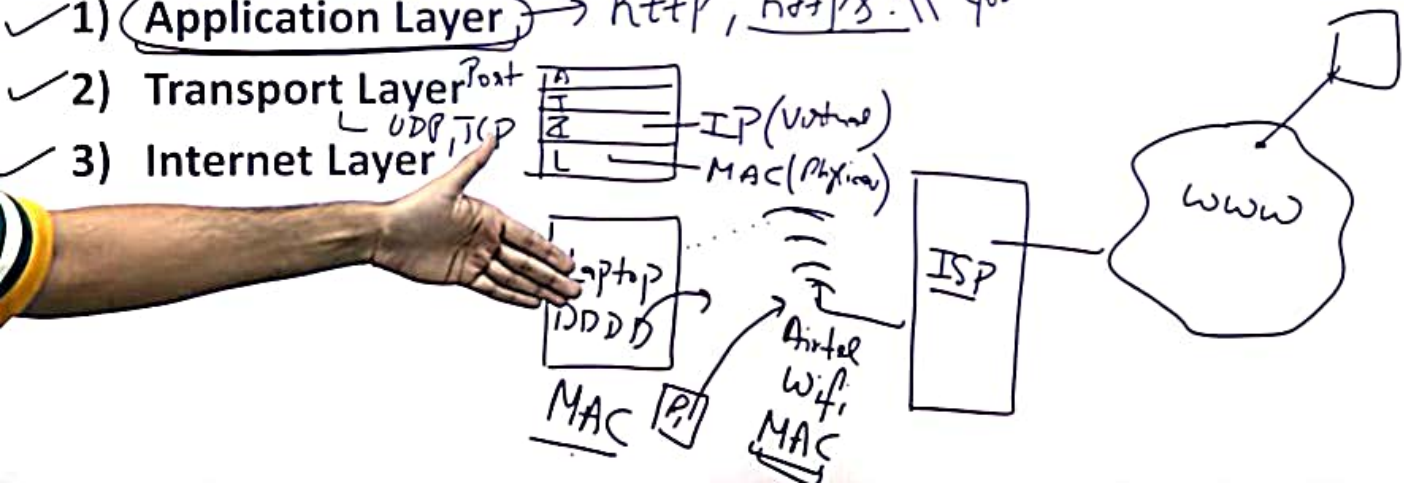
- HTTPS is a secure version of HTTP that uses encryption to protect data during transmission.
- It operates over port 443.
- HTTPS encrypts data using SSL (Secure Sockets Layer) or TLS (Transport Layer Security) protocols



TCP/IP Protocol Suite

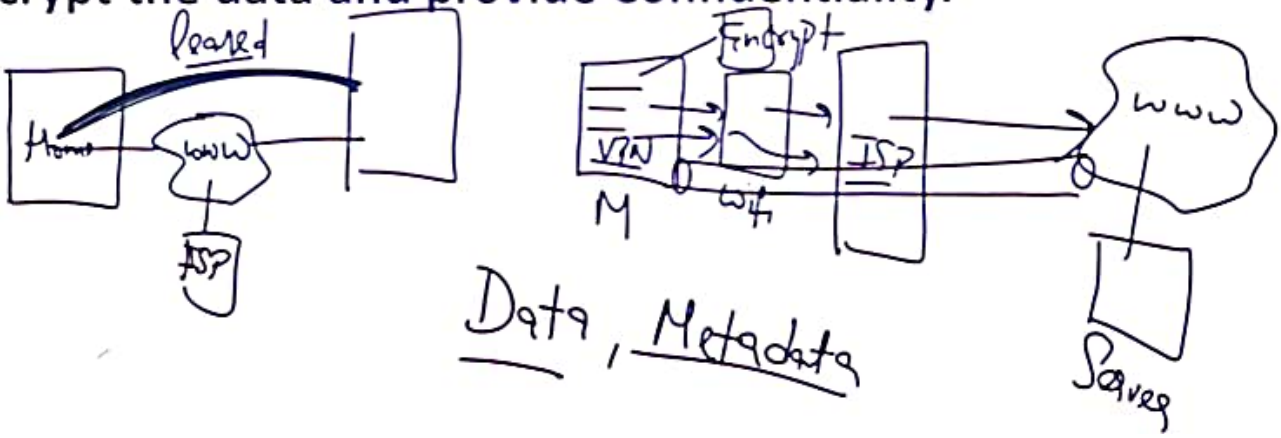
- The TCP/IP protocol suite is organized into four layers.

1) Application Layer → Http, https:\\ 90
2) Transport Layer (Port) — UDP, TCP
3) Internet Layer



VPN(Virtual Private Network)

- **It is used to Establish a secure & reliable connection over unsecure network(Internet).**
- **It will encrypt the data and provide Confidentiality.**



ethernet frame format :- (IEEE 802.3)

Preamble	SFD	DA	SA	length	Data	CRC
7 Byte	1 Byte	6B	6B	2B	46B-1500B	4B

Physical layer

Data Link layer

↳ we use CSMA/CD for collision detection.

thin ethernet 10Base2 → 10MBPS, 200m

10Base5 → 10MBPS, 500m } Thick ethernet (use coaxial cables)

↳ we use Bus topology

Bit rate → mbits/sec - 40GB Gbits/sec.

→ Preamble → 1010 ---- 10 } 56 bits

→ SFD → 10101011 → 8 bits } use this for alert or syncronization

→ DA (Destination address) [MAC address]

↳ SA (source address) → source address

↳ Data [0 to $2^{16}-1$] } pure data should be atleast 46B

↳ max^m data = 1500 byte

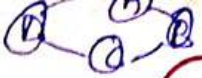
IP

S — X_1 — X_2 — D

SA/DA

S X_1 X_2 D

Token Ring (802.5)



↳ Ring topology is used
↳ Access Control method used is token passing.
~~↳ Token Ring is unidirectional.~~
↳ 4Mbps & 16Mbps.
↳ piggybank acknowledgement is used.

Frame format

Start Delimeter	Access control	Frame control	Destination address	Source address	Data (0 to MAX token holding time)	CRC	ED	FS
SD	AC	FC	DA	SA	Data	4	1	1
1	1	1	6	6				

CRC → Error Control
ED → end delimeter
FS → Frame Status

Token

Start Delimeter	Access control	End Delimeter
SD	AC	ED
1	1	1

→ Problem in Token Ring :- → Monitor Related
↳ Source Related & Orphan packet
↳ Destination Related → Down Ring (Buffer full) Loop Rd
↳ Token Related → token lost

Network layer :- Host to Host delivery.
source to destination delivery.
Machine to machine delivery.

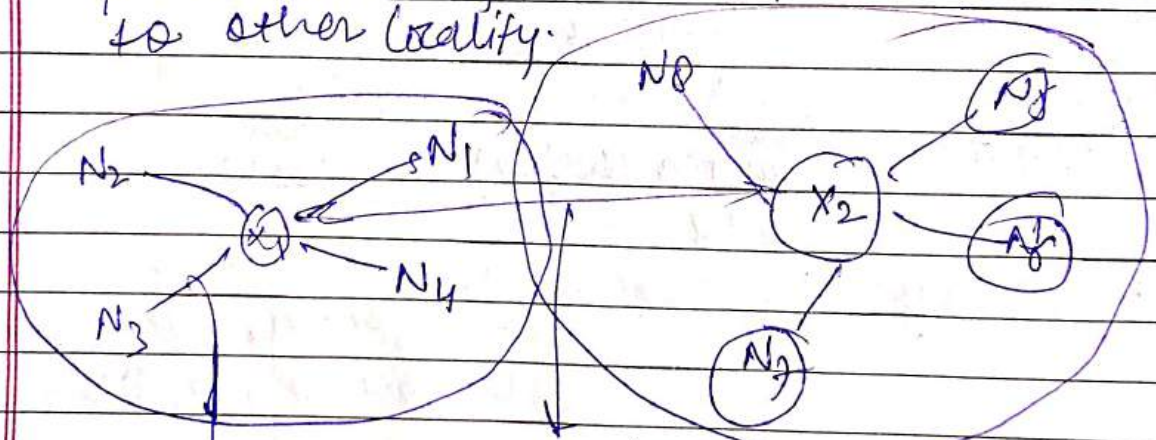
Routing protocol

Routing table { Collection of entries, which shows what is going on in any networks.

- Static (manually inserted data)
  - for small networks.
- Dynamic (routing table automatically share information & automatic updation)
  - for all type of networks.

Routing protocol

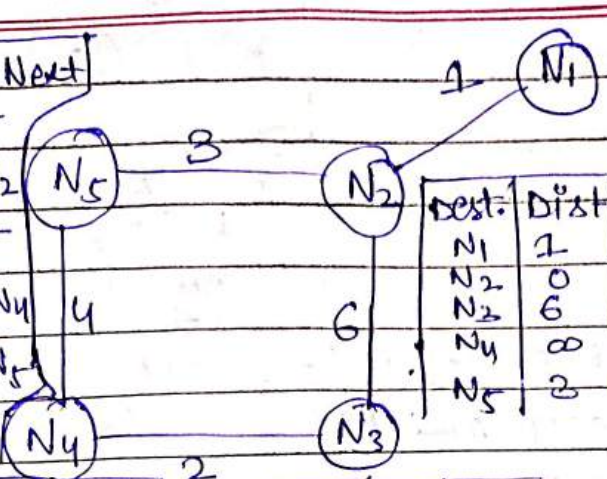
- Intra domain
  - Connection of modules within the system like in Delhi b/w one locality to other locality.
- Inter domain
  - → Connection b/w 2 autonomous system like Delhi network to Mumbai networks.



- Intra domain
  - ** Distance vector (RIP)
    - Routing information protocol
  - Link State (OSPF)
    - Open shortest path first
- Inter domain
  - path vector (BGP)
    - Border Gateway path vector

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	Next
N_1	1	N_1
N_2	7	N_2
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	∞	-

Rules :-

1. Share distance vector only with neighbours only.
2. Only share distance vector

at $N_1 \rightarrow N_2$

at $N_2 \rightarrow N_3$
$\rightarrow N_5$

at $N_3 \rightarrow N_2$
$\rightarrow N_4$

at $N_4 \rightarrow N_3$
$\rightarrow N_5$

at $N_5 \rightarrow N_4$
$\rightarrow N_2$

SB :-

After getting distance vector, we have to update the tables.

At N_1

1
0
6
∞
3

N_1 new RT

Dest	Dist	Next
N_4	0	N_1
N_2	1	N_2
N_3	7	N_3
N_4	∞	-
N_5	4	N_5

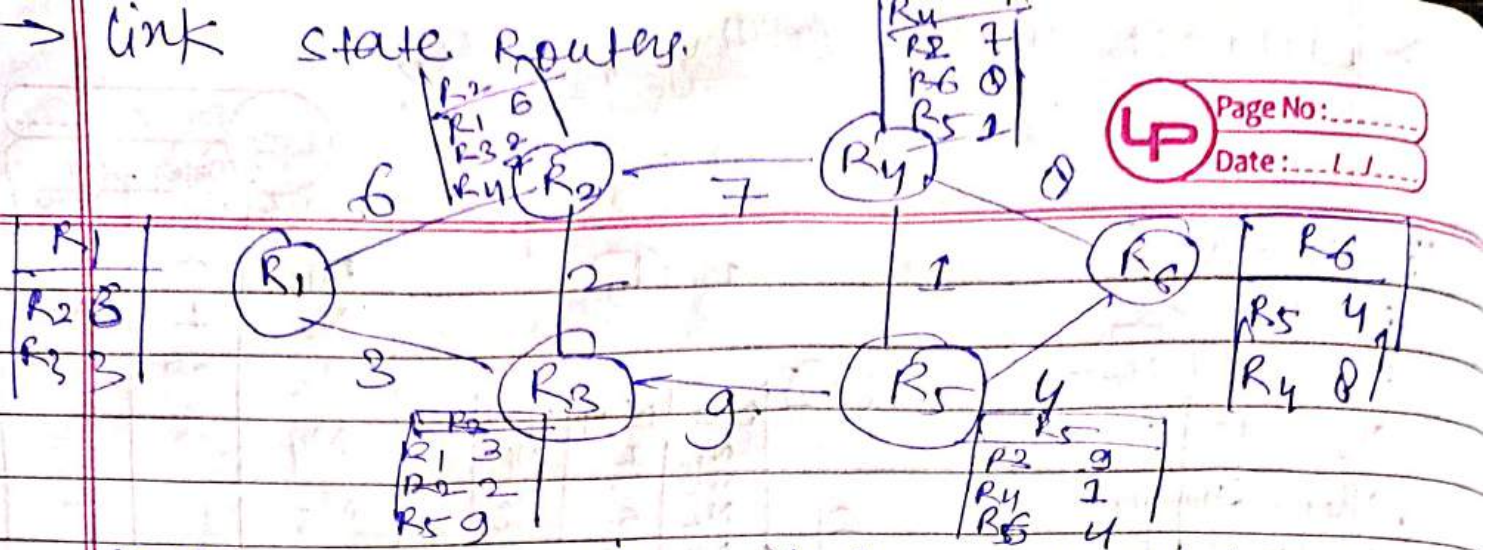
$N_1 \rightarrow N_2$
$\Rightarrow N_1 \rightarrow N_2$ AND $N_2 \rightarrow N_2$
$1 + 0$
$\Rightarrow 1$

$N_1 \rightarrow N_3$
$N_1 \rightarrow N_2 + N_2 \rightarrow N_3 + N_3 \rightarrow N_3$
$1 + 6 + 0$
$\Rightarrow 7$

$N_1 \rightarrow N_4$
$N_1 \rightarrow N_2$ & $N_2 \rightarrow N_4$
$1 + \infty \Rightarrow \infty$

$N_1 \rightarrow N_5$
$N_1 \rightarrow N_2$ AND $N_2 \rightarrow N_5 \Rightarrow 4$

→ Link state Routing.



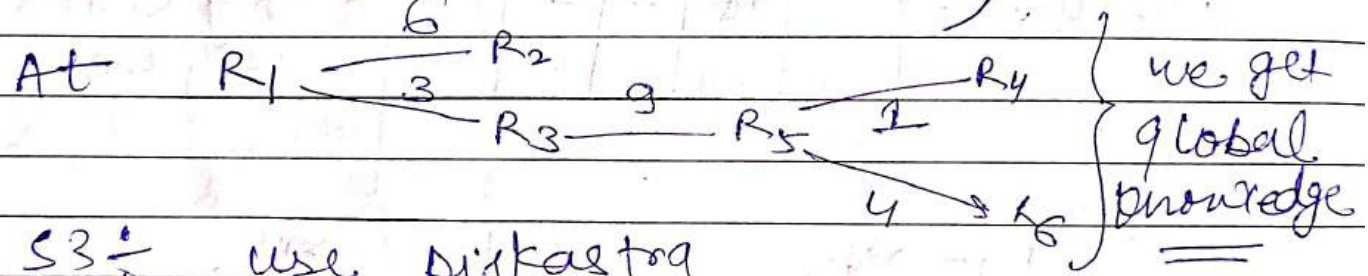
S1 :- create Routing table for all Network node

S2 :- Table sharing of data done through flooding

↓

(send packet (data) to all nodes, as any packet lost then that packet will be share by another link)

At



} we get global knowledge

S3 :- use Dijkastra algorithm

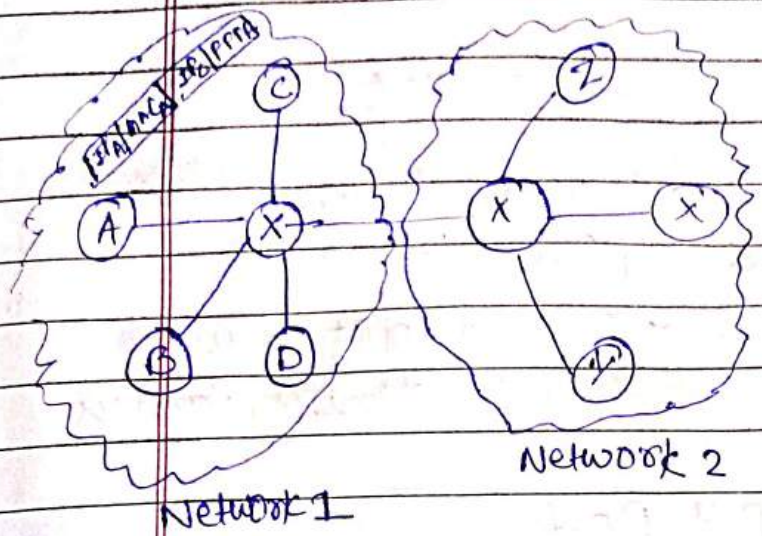
Source	R_2	R_3	R_4	R_5	R_6
R_1	6	3	∞	∞	∞
R_1R_3	(5)	(3)	∞	12	∞
$R_1R_3R_2$			(12)	12	∞
$R_1R_3R_2R_4$				(12)	21
$R_1R_3R_2R_4R_5$					16

R_1	0	R_1
R_2	5	R_1
R_3	3	R_1
R_4	12	R_3R_2
R_5	12	R_3
R_6	16	R_3R_5

Routing table

ARP :- (Address Resolution Protocol)

IP address (logical) → MAC address (Physical)



Hardware Type		Protocol Type
Hardware Length	Protocol Length	Operation Req-1, Rep-2
Sender Hardware Address 6B		
Sender Protocol Address 4B		
Target Hardware Address		
Target Protocol Address		

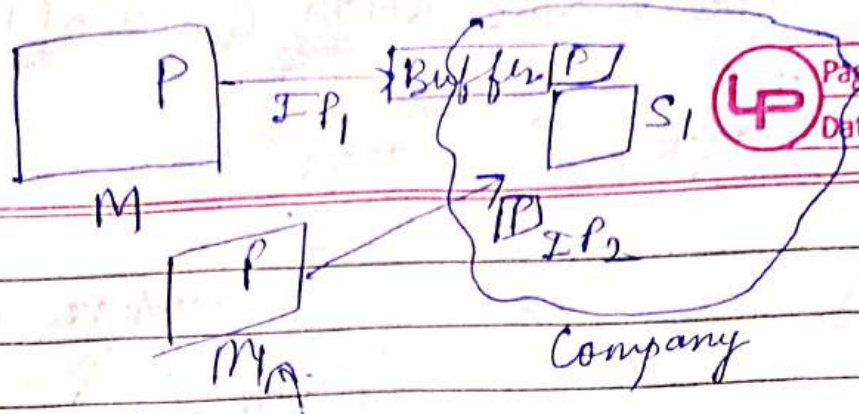
Request → Broadcast
Reply → unicast

NAT (Network Address Translation)

Private IP → public IP
AND
Public IP → Private IP

Transport Layer

- → end to end delivery (port to port)
- → Reliable delivery
- SMTP [simple mail transfer protocol]
- → follow inorder deliver of message
  - send A → B → C → D
  - Receive A → B → C → D
  - } order can't be changed so No loss of data
- → error control through checksum method (CRC)
- → Congestion Control
- → flow Control (pre send window size)
- → we use segmentation (0101010 ——) (header + data)
- → Multiplexing / Demux



machine will reserve resources of S1

portnumber (16 bit)
0-65535

Should have diffent port numbers
Should not have diffent IP address.

Socket address ⇒ IP + Port
32 + 16 ⇒ 48 bit
⇒ 6 byte

TCP (Transmission Control protocol)

- Byte streaming → Application layer to transport layer continuous data → make Bytes → segments
- Connection Oriented → Reliability → 3way (1) Req for Connection (2) target accept Req (3) sends data
- full duplex (A — B both transmitted at same time)
- Piggybacking (Acknowledgment) → GBN / selective Repeat
- Error control
- flow control
- Congestion Control.

TCP header = (20-60 Byte)

Source Port 16	Destination Port 16
Sequence Number 32	
Acknowledge NO 32	
HLEN | URG | ACK | PSH | RST | SYN | FIN | Window Size 16	
16 Check Sum	Padding | Urgent point 16.
Options & Padding 40 Byte	

TCP → process to process communication using port numbers

Page No.:
Date: 1.1.

Q) Basic Algo-

IRTT → Initial Round trip time
ARTT → Actual " " "
NRTT → New " " "

$$NRTT = \alpha \, IRTT + (1-\alpha) ARTT$$

α = Smoothing factor
Time out = 2 × NRTT

Q) IRTT = 10msec, $\alpha = 0.5$
for segment 2 → ARTT = 15msec

$$NRTT = 0.5 \times 10msec + (1-0.5) 15msec$$
$$\Rightarrow 5msec + 7.5msec$$
$$\Rightarrow 12.5msec$$

TO = $2 \times 12.5msec \Rightarrow 25msec$.

for segment 1 IRTT → 10msec
TO = $2 \times 10ms \Rightarrow 20msec$

for segment 3
NRTT = $\alpha IRTT + (1-\alpha) ARTT$
$0.5 \times 12.5 + 0.5 \times 20$
$\Rightarrow 6.25 + 10 \Rightarrow 16.25msec$
TO = $2 \times NRTT \Rightarrow 2 \times 16.25 \Rightarrow 32.50$

for segment 4
NRTT = $\alpha IRTT + (1-\alpha) ARTT$
$\Rightarrow 0.5 \times 32.5 + 0.5 \times 10$
$\Rightarrow 16.25 + 5 \Rightarrow 21.25$
TO = $2 \times 21.25 \Rightarrow 42.50$

Jacobson's Algo

S1 :- Assume IRTT + initial deviation = D

S2 :- TO = 4ID + IRTT

S3 :- NRTT = αIRTT + (1-α)ARTT

Actual deviation ← AD = |IRTT − ARTT|

New deviation ← ND = αID + (1-α)AD

(smoothing factor)

TO = 4ND + NRTT

Alg: IRTT = 10msec, ID = 5msec, α = 0.5

for segment 1

ARTT = 20msec.

TO = 4ID + IRTT

⇒ 4X5msec + 10msec ⇒ 30msec

(to avoid congestion)

Karn's algo if T_O < ARTT → DOUBLE RTO

for segment 2

NRTT = 0.5 × 10msec + (1−0.5)20msec

⇒ 15msec

~~for~~ ND = αID + (1−α)AD

0.5 X 5msec + 0.5X 10

AD = |IRTT − ARTT| ⇒ (20−10

⇒ 10

T_O = 4X 7.5+15 ⇒ 45msec.

UDP :- connectionless, unreliable communication

↳ min^m amount of mechanism

↳ Speed more

→ process to process comm.

→ use port numbers

→ Flow Control → NO flow Control

→ Error Control → NO

→ Congestion Control → NO

User Datagram

[header | Data]

header format

0	16	31
Source port NO	Dest port NO	
Header + data	Total length	Checksum (Check error)

TCP	UDP
full function, Data Reliable Transfer	simple & high speed with low function protocol
Connection oriented	Connection less
stream Based data is send	message based data is sent
reliable + Ack	not reliable + NO acknowledgement
yes Retransmission	NO Retransmission
flow Control (SWP)	No flow Control
high Overhead as more feature.	very low as low feature overhead
High but lower than UDP data transmission	Very high speed transmission
eg = FTP, telnet, SMTP, DNS, HTTP- etc.	eg DNS, BOOTP, SNMP = (multimedia based)

Special IP address.

(1) for IP testing 127.0.0.0 to 127.255.255.255
(2) private → class A, B, C
(3) multicast → 224.0.0.0 to 239.255.255.255
(4) broadcast → 255.255.255.255

Session layer :- creating session (connection source ↔ server)

↳ Authentication

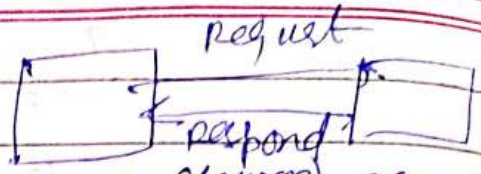
↳ Authorization

↳ Session Restoration (check point)

eg (Tab Restore in chrome)

↓

use session beans (save info)



↳ Webinar (web conferencing)

↳ logging problem / synchronization prbl } session layer manage synchronization

↳ flow control

Presentation layer → code conversion (formatting)

↳ encryption / decryption

↳ compression (can be lossy)

Application layer :- (topmost layer)

↳ enable communication

↳ Network services

↳ Authentication & Authorization

↳ web Browsing, Email, file Sharing,

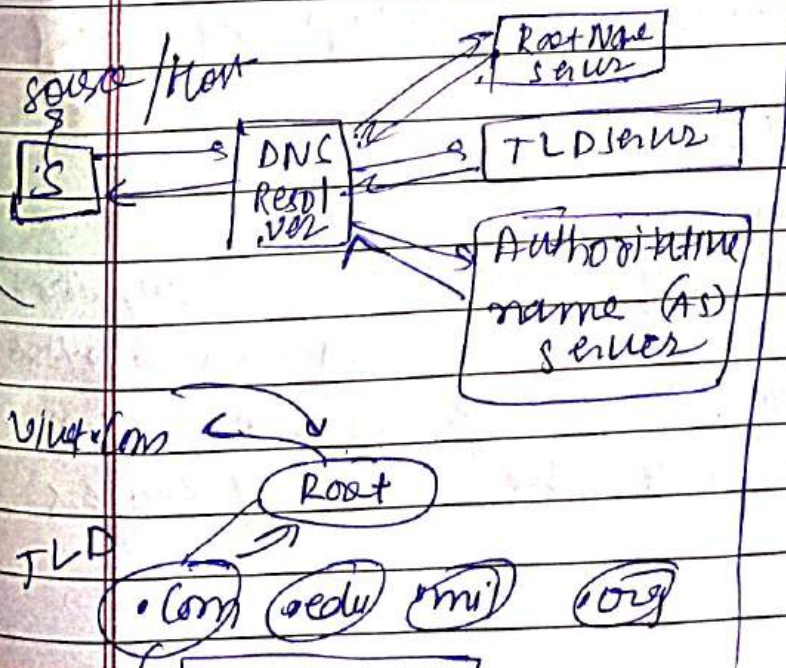
↳ Remote Access

↳ user friendly communication.

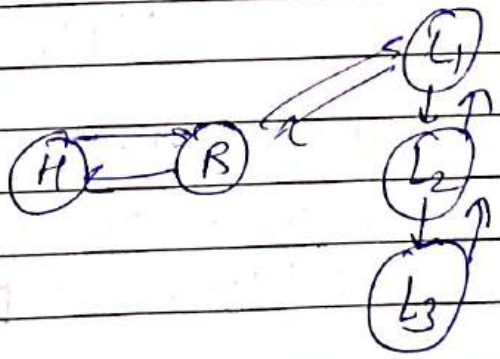
Protocol Name	Port No	Transport protocol
(RTT) Echo	7	TCP/UDP
FTP	20/21	TCP [File transfer]
(Secure Shell) SSH	22	TCP [security] *
Telnet	23	TCP
SMTP	25	TCP
DNS	53	UDP
DHCP	67/68	UDP
TFTP	69	UDP
HTTP	80	TCP
POP	110	TCP
NTP	123	UDP
HTTPS	443	TCP
RIP	520	UDP

DNS {Domain Name system}
- operate on Application Layer
- to map the Domain Name with IP address.
- IP addres are always dynamic not static that's why DNS comes in.
- works in 2 phase

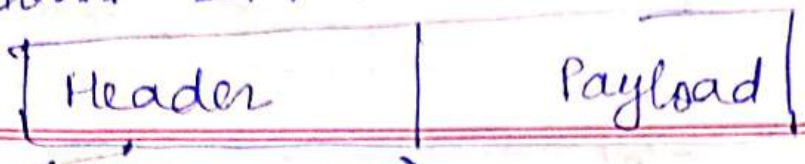
① Iterative



② recursive



IPv4



(20-60) byte

(20-65535) byte

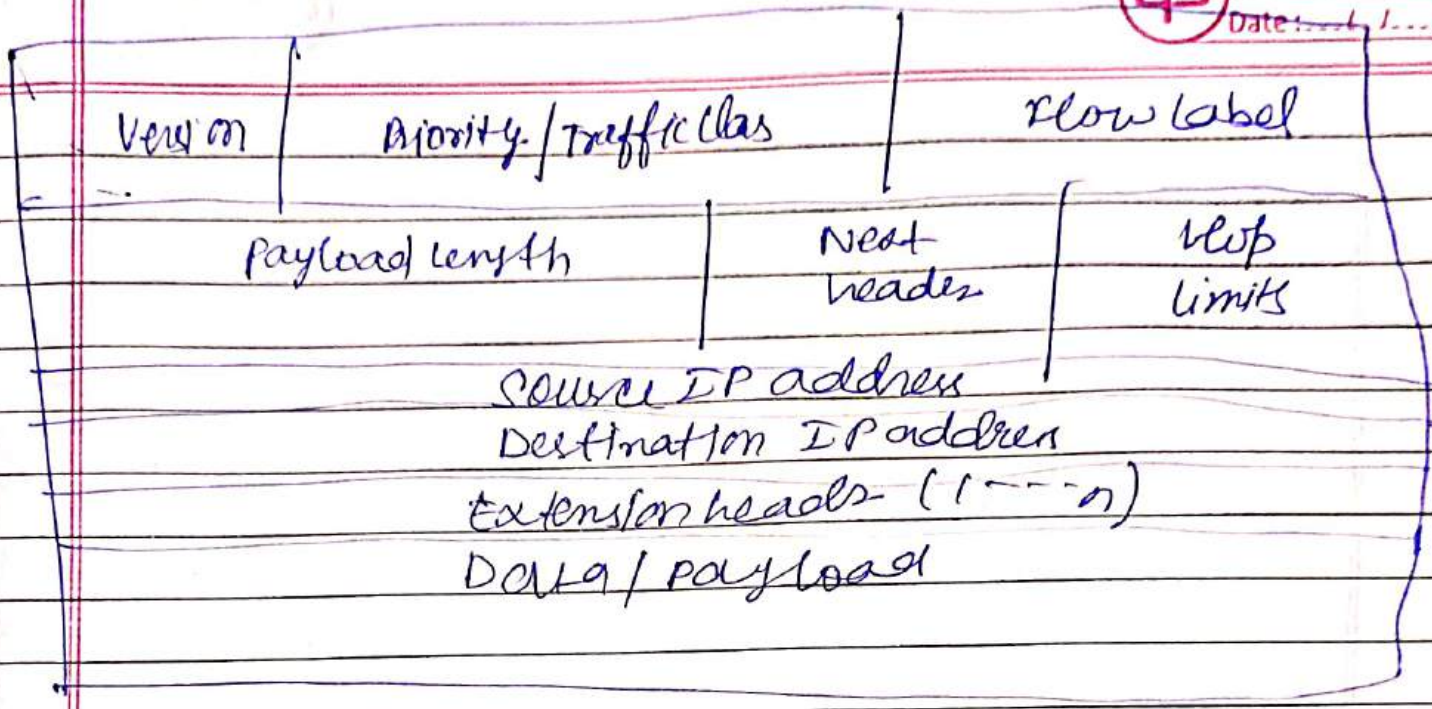
→ Header format

VER 4	HLEN 4	service type 8	Total length 16
Identification 16		flags 3	fragmentation offset 13
Time to live 8	protocol (TCP/IP UDP) 8	Header check sum 16	
source IP address 32			
Destination IP address 32			
Options + padding (0 to 40 bytes)			

→ unreliable connectionless datagram
→ less safety of packet
→ cost, delays
→ for safety IVPy should be coupled with TCP, forming TCP/IP psotocol

VER → Gives version → 4 or 6
Hlen → header length
Service type → priority check 000 → slow priority
111 → high priority
→ Time-to-live → max^m Number of hops / Round trip
(generally set twice the numb of Routers.

IPV6 (16 Bytes)



11-1 FRAMING

The data link layer needs to pack bits into frames, so that each frame is distinguishable from another. Our postal system practices a type of framing. The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter.

Figure 11.4 *Bit stuffing and unstuffing*

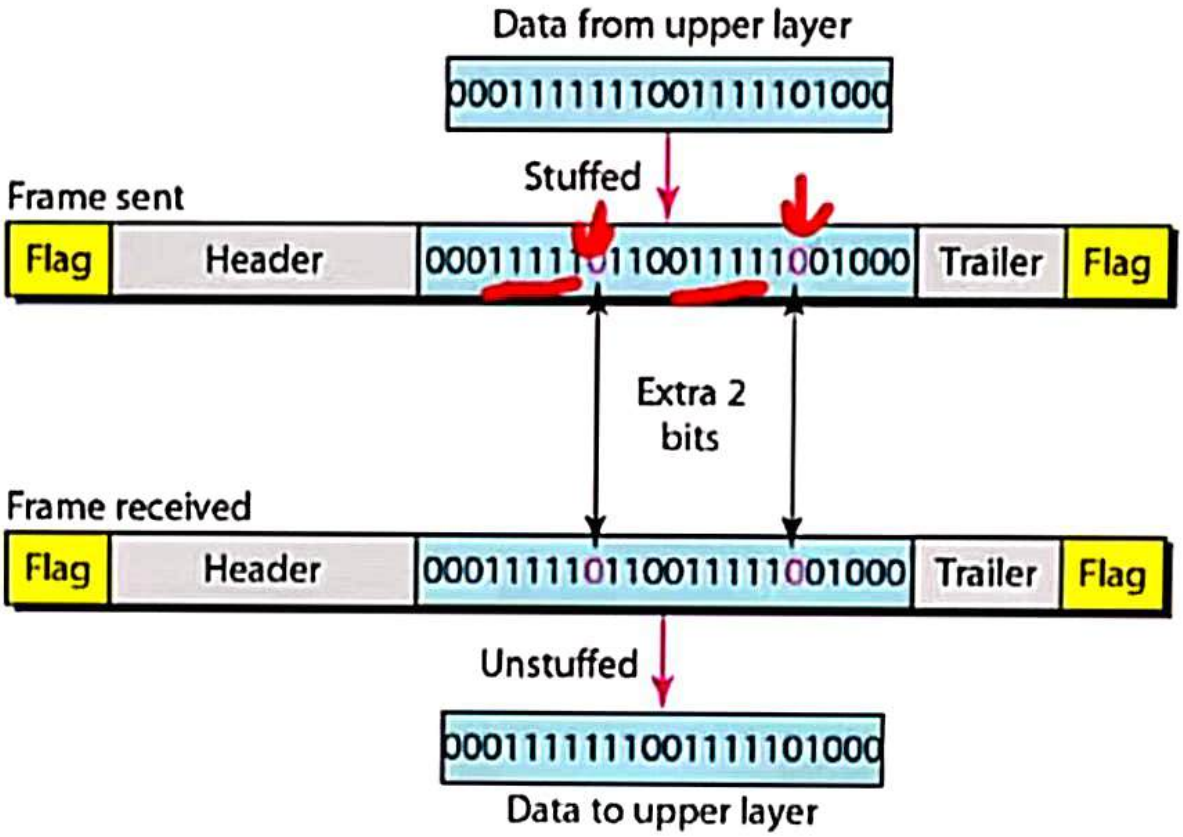


Figure 11.2 *Byte stuffing and unstuffing*

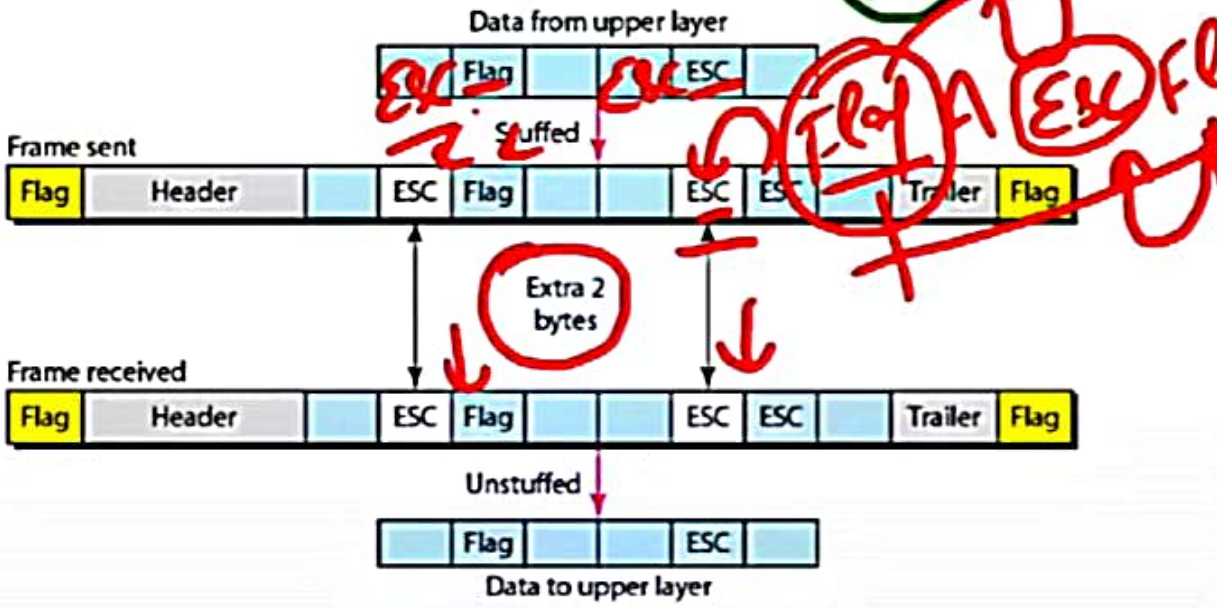
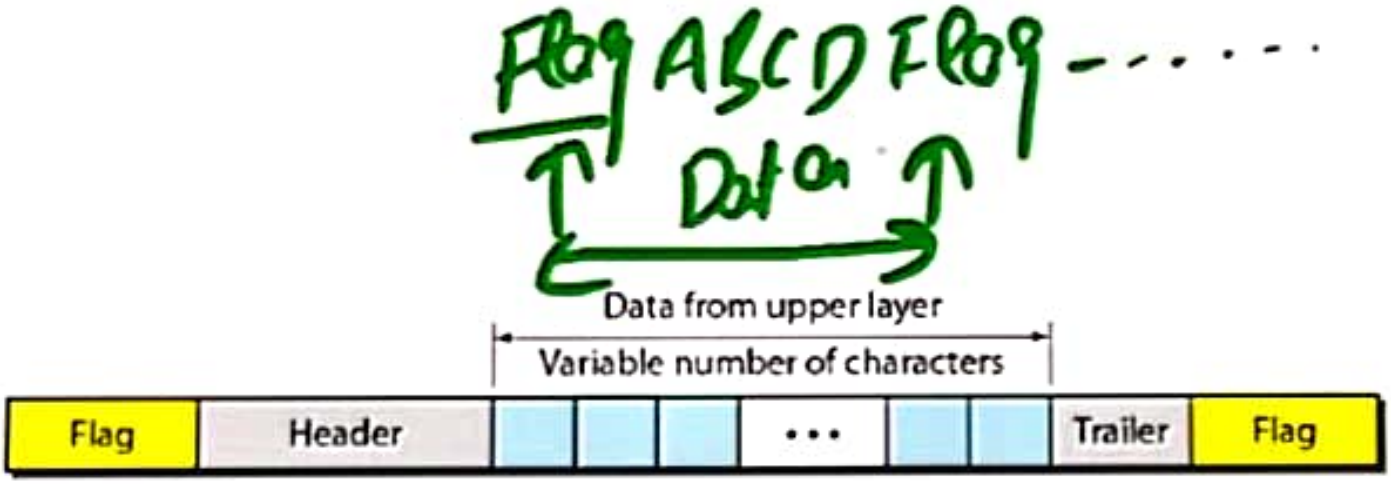


Figure 11.1 *A frame in a character-oriented protocol*

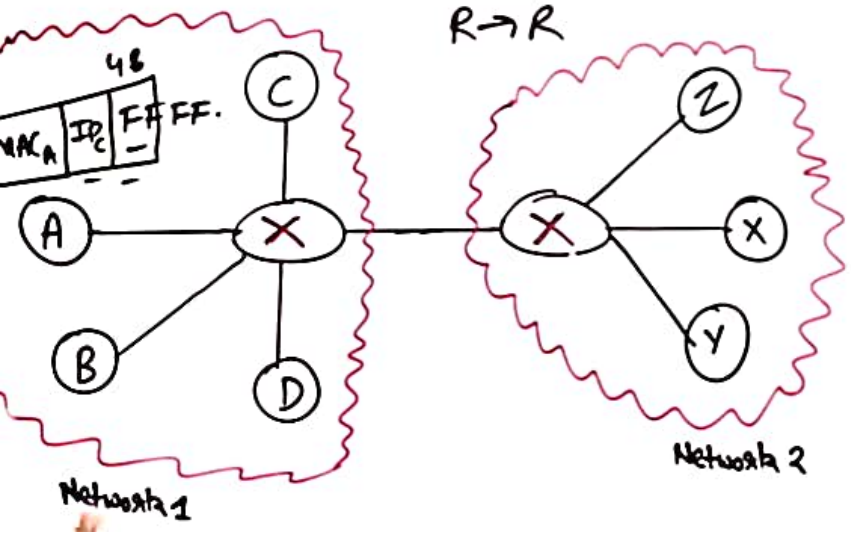


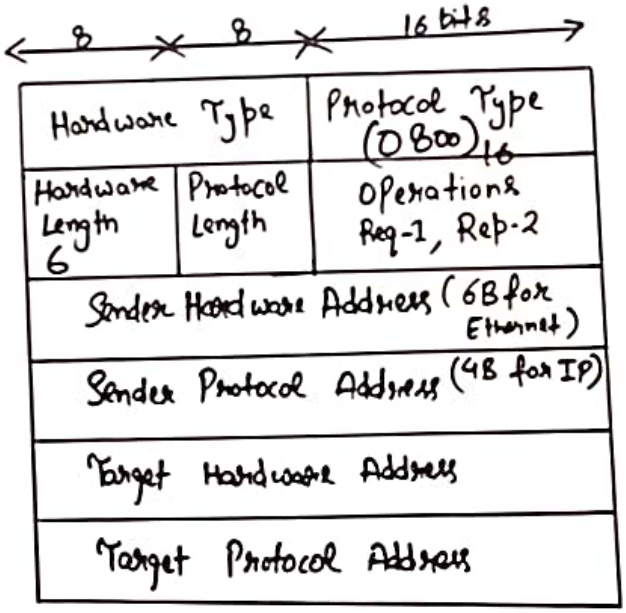
ARP (Address Resolution Protocol)"

IP → Mac

Logical → Physical

H → H
H → R
R → H
R → R





Single Parity
= message bits

→ (m+1) bits

→ Even Parity → no of '1' even

→ Can detect all single bit errors in code word

→ Can detect all odd no of errors also

1010 0 → 1110 1

1110 1 → 0110 1 → 0010

4 bit Data words = 2^4

Valid Codeword

0000 0
0001 1
0010 1
0011 0
0100 1
0101 0
0110 0
0111 1
1000 1
1001 0
1010 0
1011 1
1100 0
1101 1

11000
10000
= 2

d
d-1
detect
1

Hamming Distance

11101
↓
00001
Error

= 0000
1111
1111

0101
1000
1101
3

Error Detection and Correction

* → Single bit Error (1 → 0, 0 → 1) : 101 → 100 (5 → 4)

* → Burst Error : 5 bit, 100 → 101, 10101 → 11011, Length of error

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

1Gbps : 10^9 bits — 1sec

1 bit — $\frac{1}{10^9}$ sec = 1ns

$\frac{1}{1000}$ sec, $\frac{1}{1000} \times 10^9 = 10^6$ bits

Detection
- → Simple Parity (Even, ODD)
- → 2D Parity check
- → Checksum
- → CRC (Cyclic Redundancy check)

Correction
- → Hamming Codes

"IPv4 Header"

Differentiated Services Code Point (DSCP)

P	P	P	D	T	R	C	O
			1	1	1	1	

0 0 0 0

Explicit Congestion Notification

DSCP	ECN

0 6 5 6 7

11

2

256

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

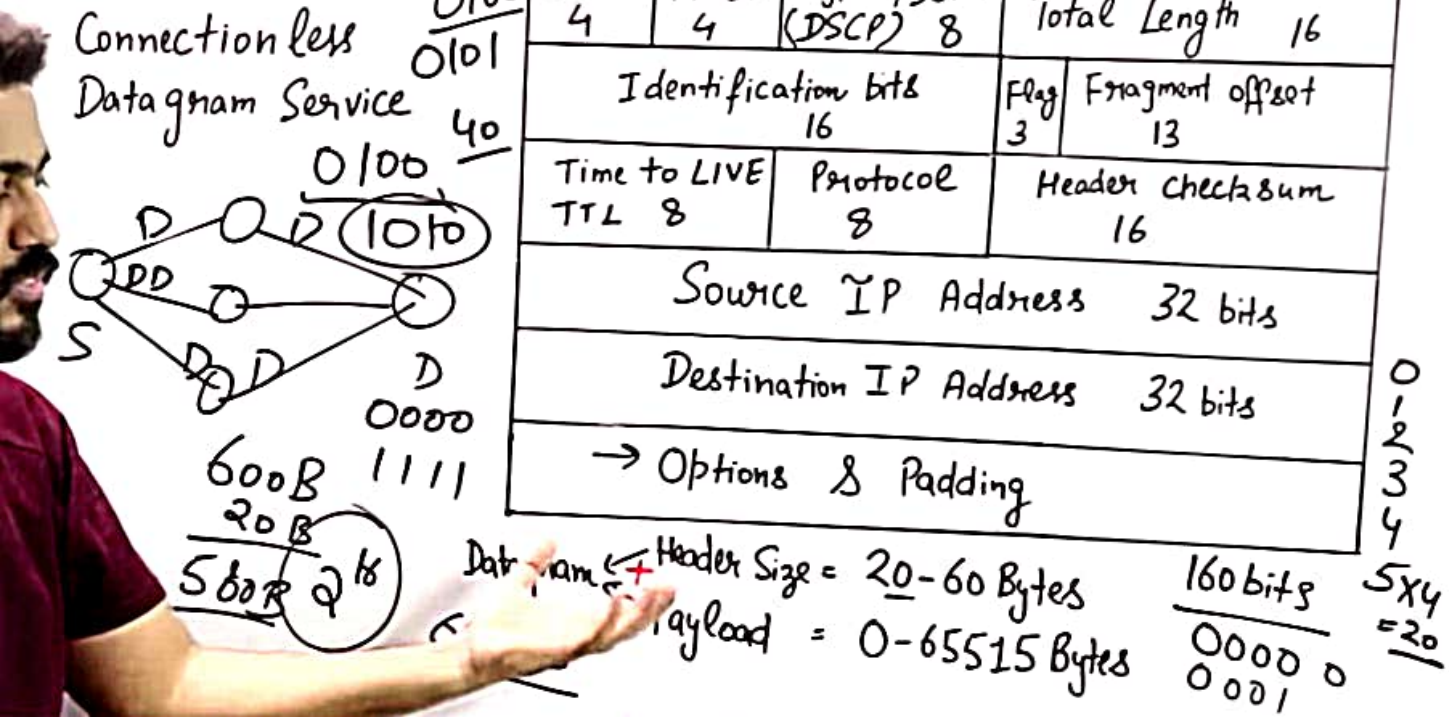
2^{16} 65535

$2^8 = 255$

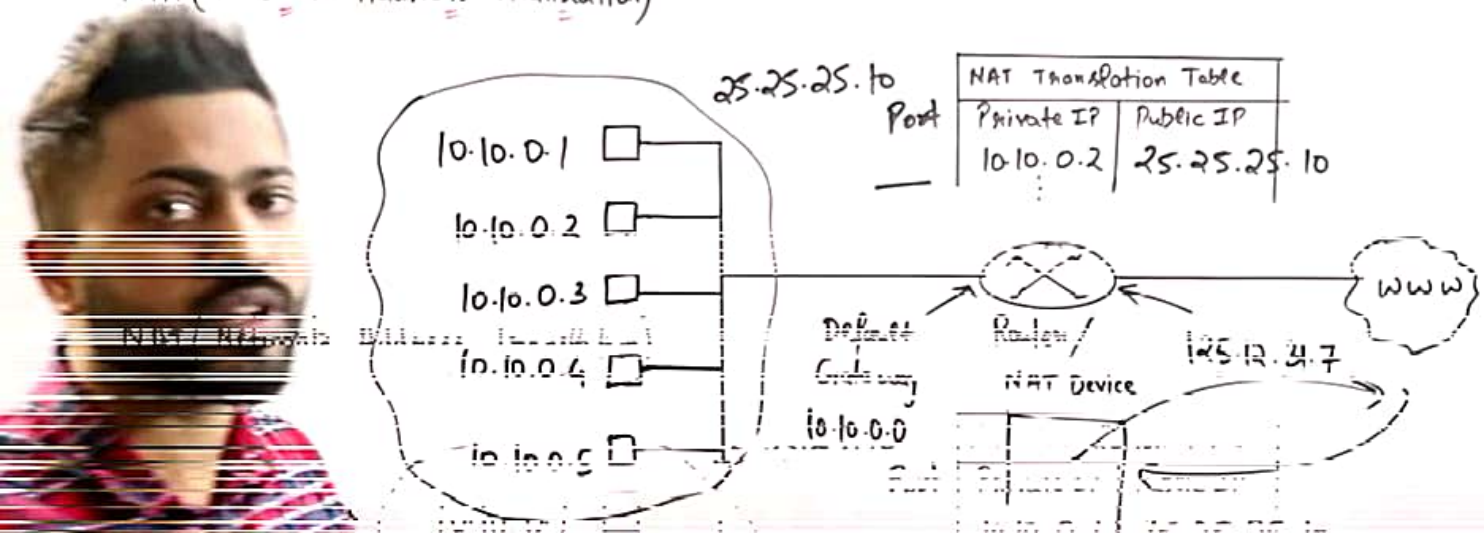
0-255

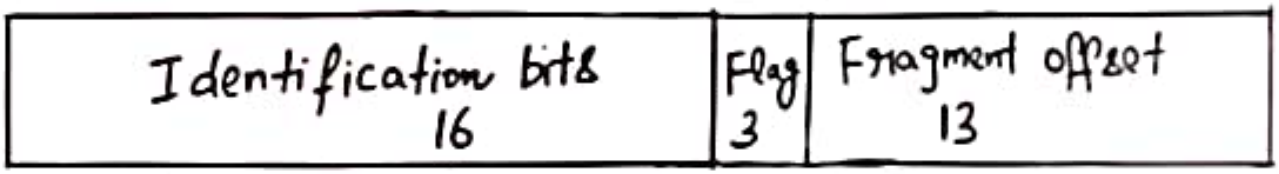
"IPv4 Header"

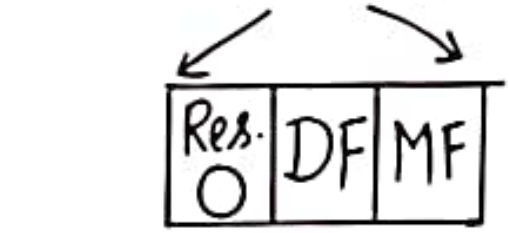
Connectionless Datagram Service

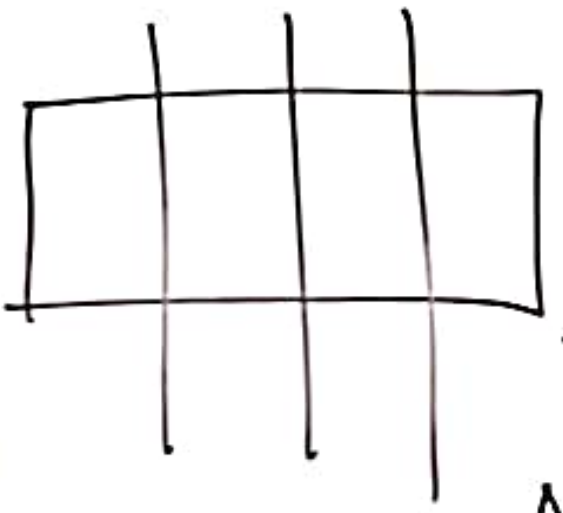


NAT (Network Address Translation)







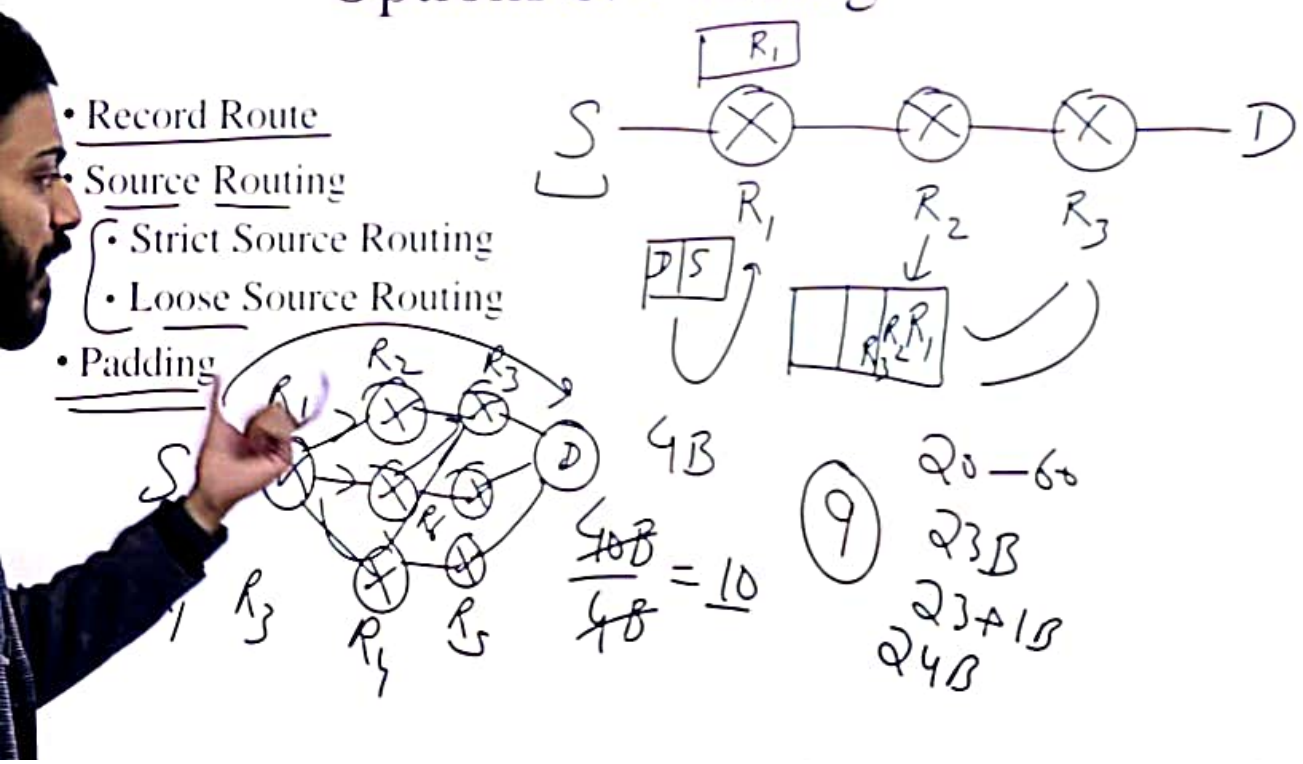


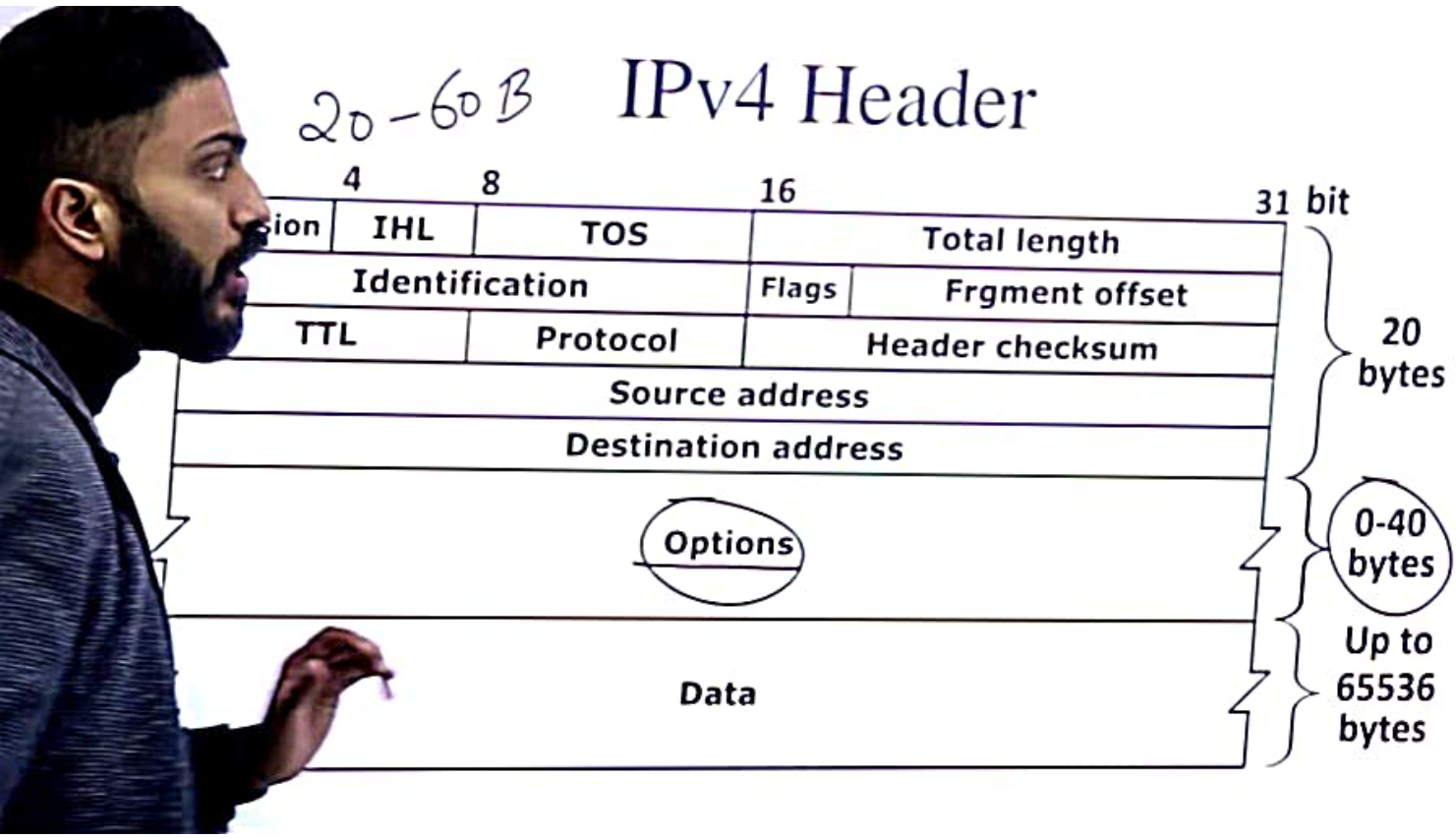
Frag. < 0 0 / 0 1

No frag. < 1 0 / 1 1

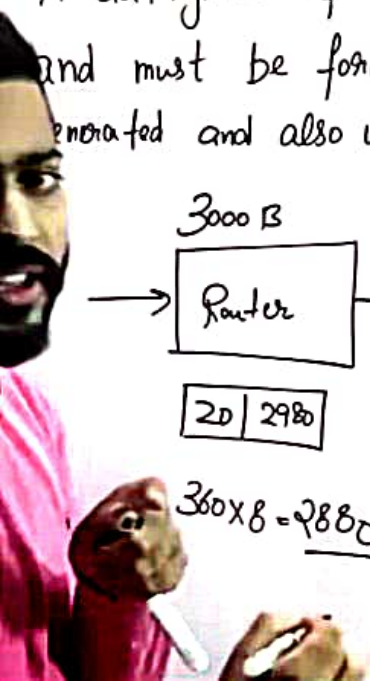
Options & Padding

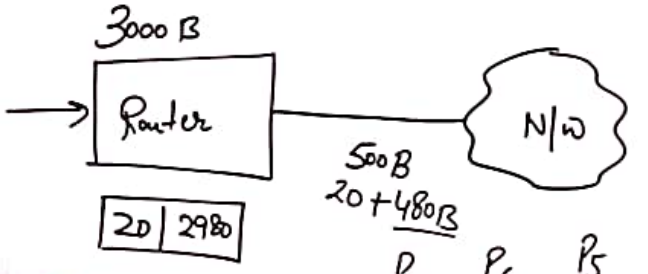
- Record Route
- Source Routing
  - Strict Source Routing
  - Loose Source Routing
- Padding




20-60B
IPv4 Header
4
8
16
31 bit
ion
IHL
TOS
Total length
Identification
Flags
Frgment offset
TTL
Protocol
Header checksum
Source address
Destination address
Options
Data
20 bytes
0-40 bytes
Up to 65536 bytes

A datagram of 3000 B (20 B 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.





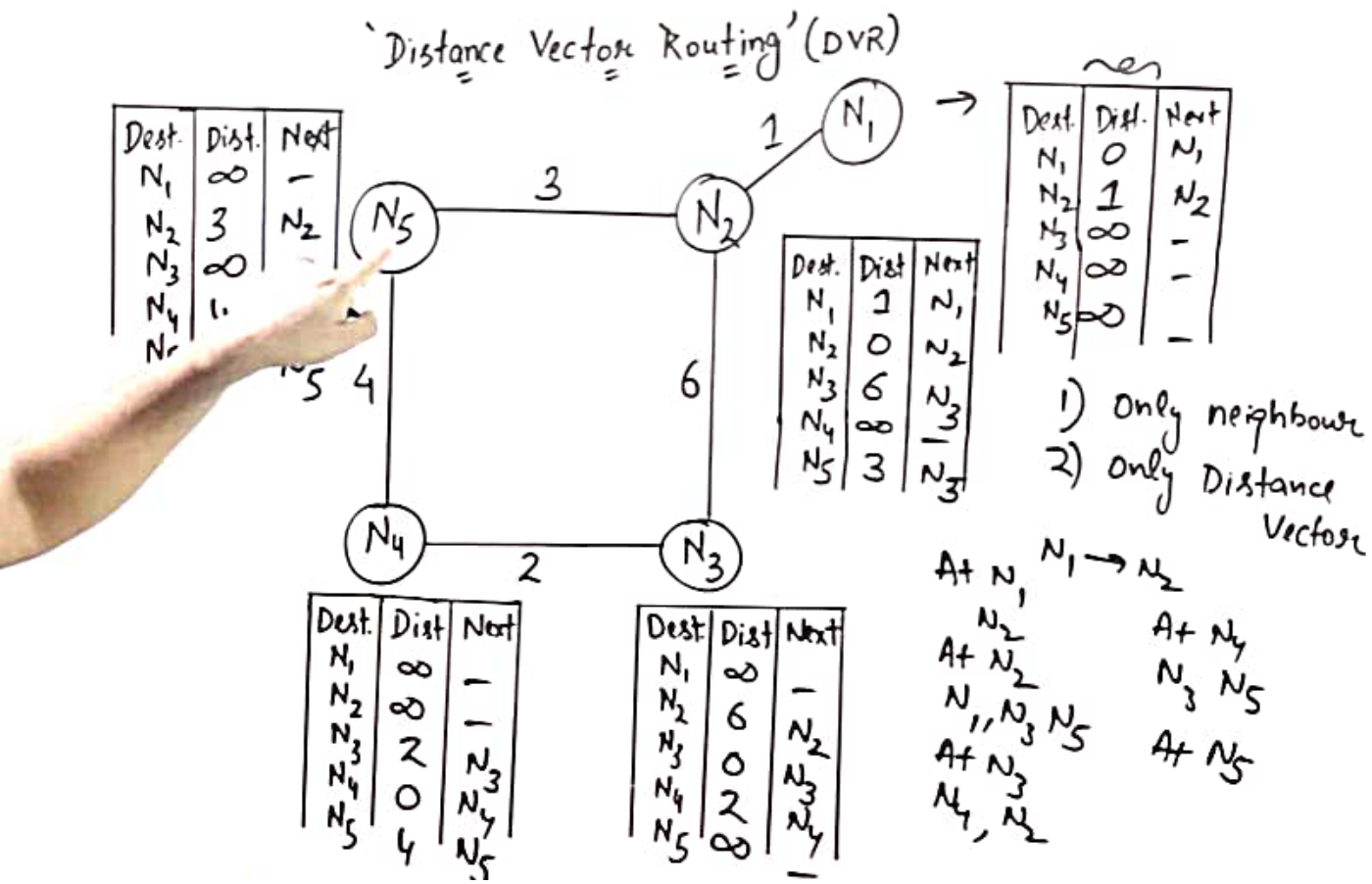
$\left\lceil \frac{2980\,B}{480\,B} \right\rceil = 7$ 480×6 = 2880

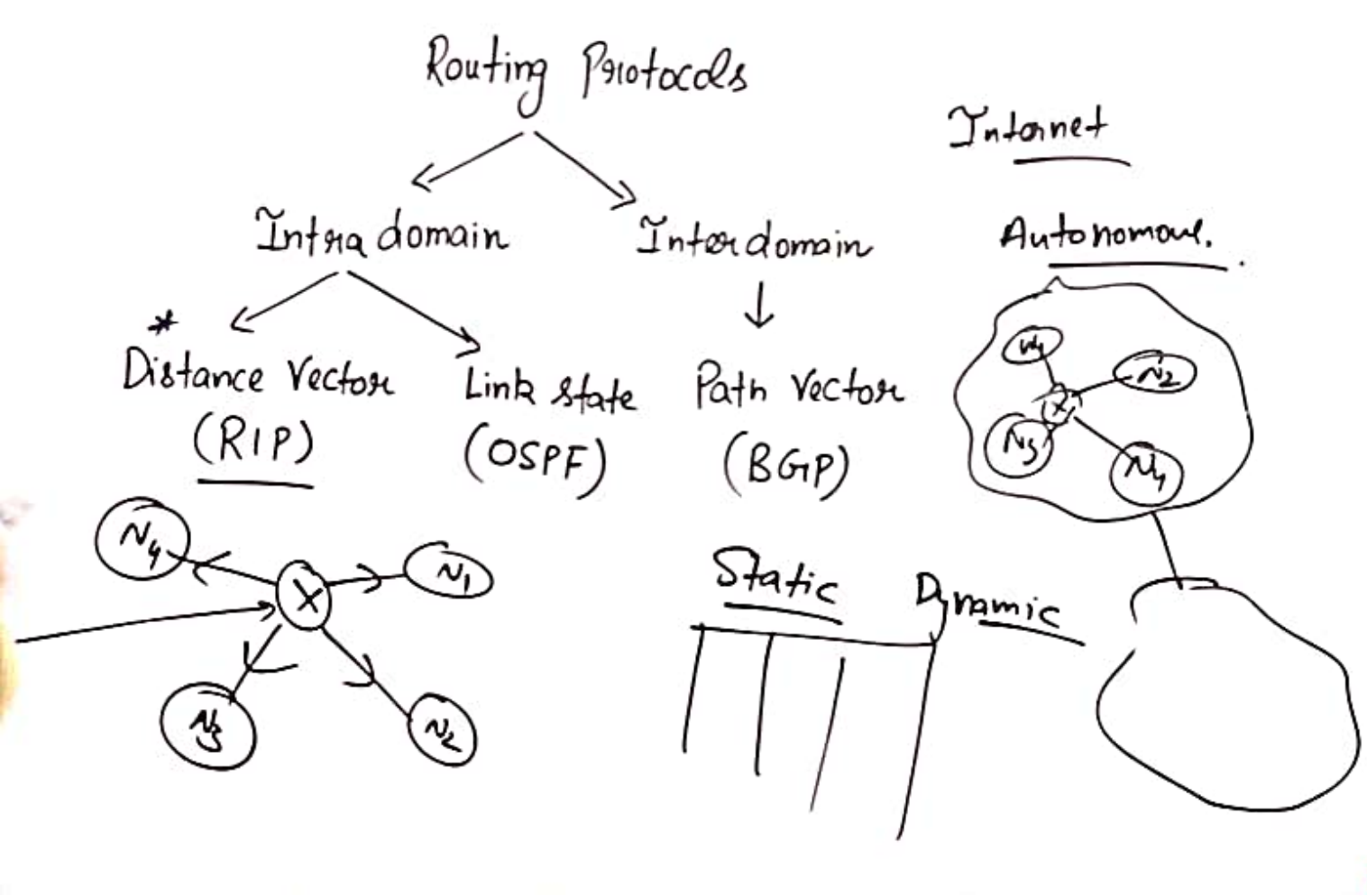
2

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

360×8 = 2880

	P_7	P_6	P_5	P_4	P_3	P_2	P_1	
	100+20	480	480	480	480	480+20	480+20	
	(120)	500	500	500	500	500	500	TL
	0	300	240	180	120	60	0	MF
	360							


'Distance Vector Routing' (DVR)
N1
N2
N3
N4
N5
1
3
4
6
2
Dest. Dist. Next
N1 ∞ –
N2 3 N2
N3 ∞
N4 1.
Nr
5
Dest. Dist Next
N1 1 N1
N2 0 N2
N3 6 N3
N4 ∞ –
N5 3 N3
Dest. Dist. Next
N1 0 N1
N2 1 N2
N3 ∞ –
N4 ∞ –
N5 ∞ –
1) only neighbour
2) only Distance Vector
Dest. Dist Next
N1 ∞ –
N2 ∞ –
N3 2 N3
N4 0 N4
N5 4 N5
Dest Dist Next
N1 ∞ –
N2 6 N2
N3 0 N3
N4 2 N4
N5 ∞ –
At N1 N1 → N2
N2
At N2
N1, N3 N5
At N3
N4, N2
At N4
N3 N5
At N5


Routing Protocols
Intra domain
Inter domain
Distance Vector
(RIP)
Link state
(OSPF)
Path Vector
(BGP)
Internet
Autonomous.
Static
Dynamic

"IPv6 Header"

128

32

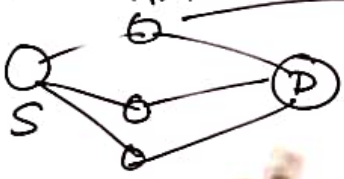
2^{32}

0110

65535 B

2^{128}

Virtual circuit

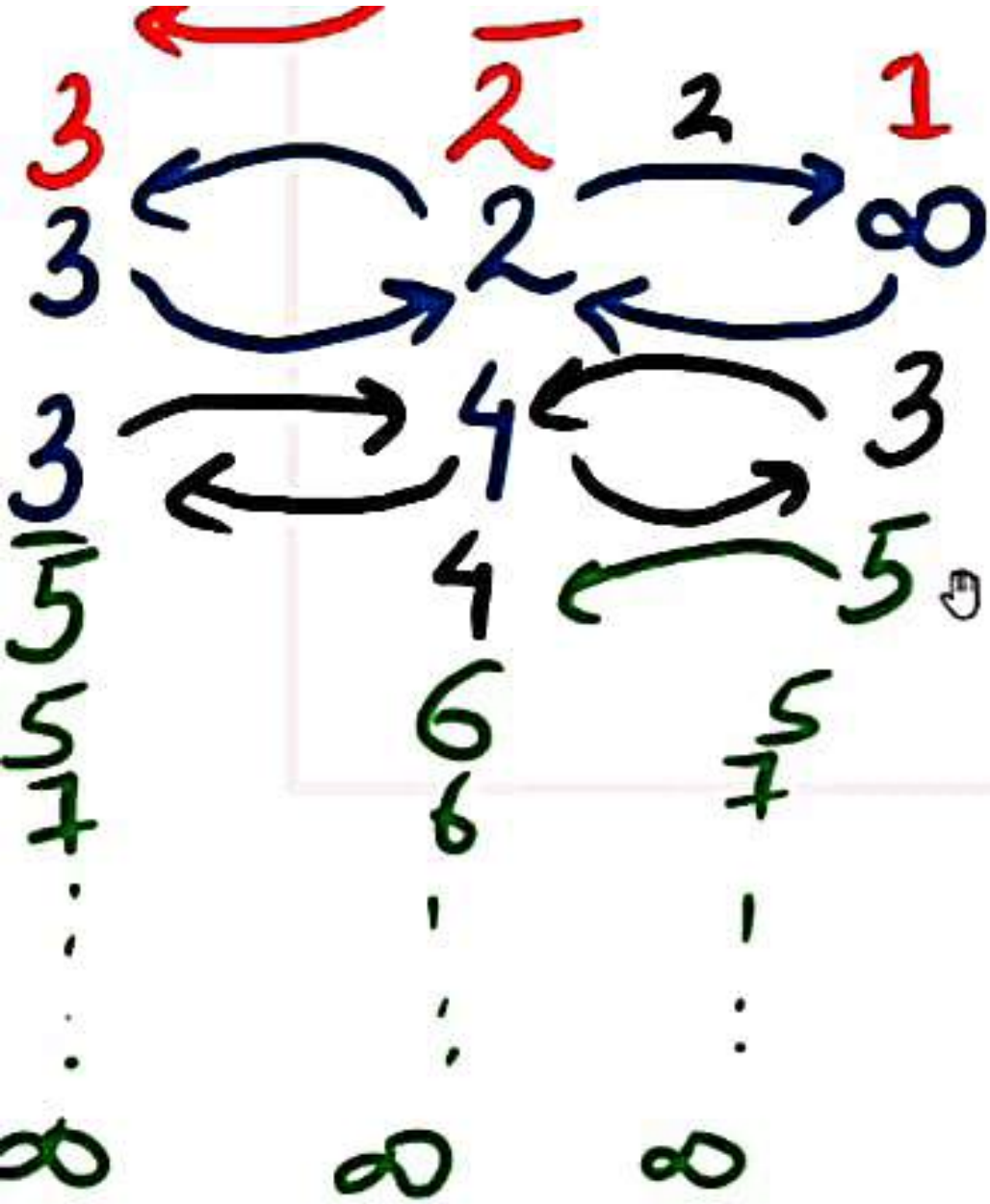


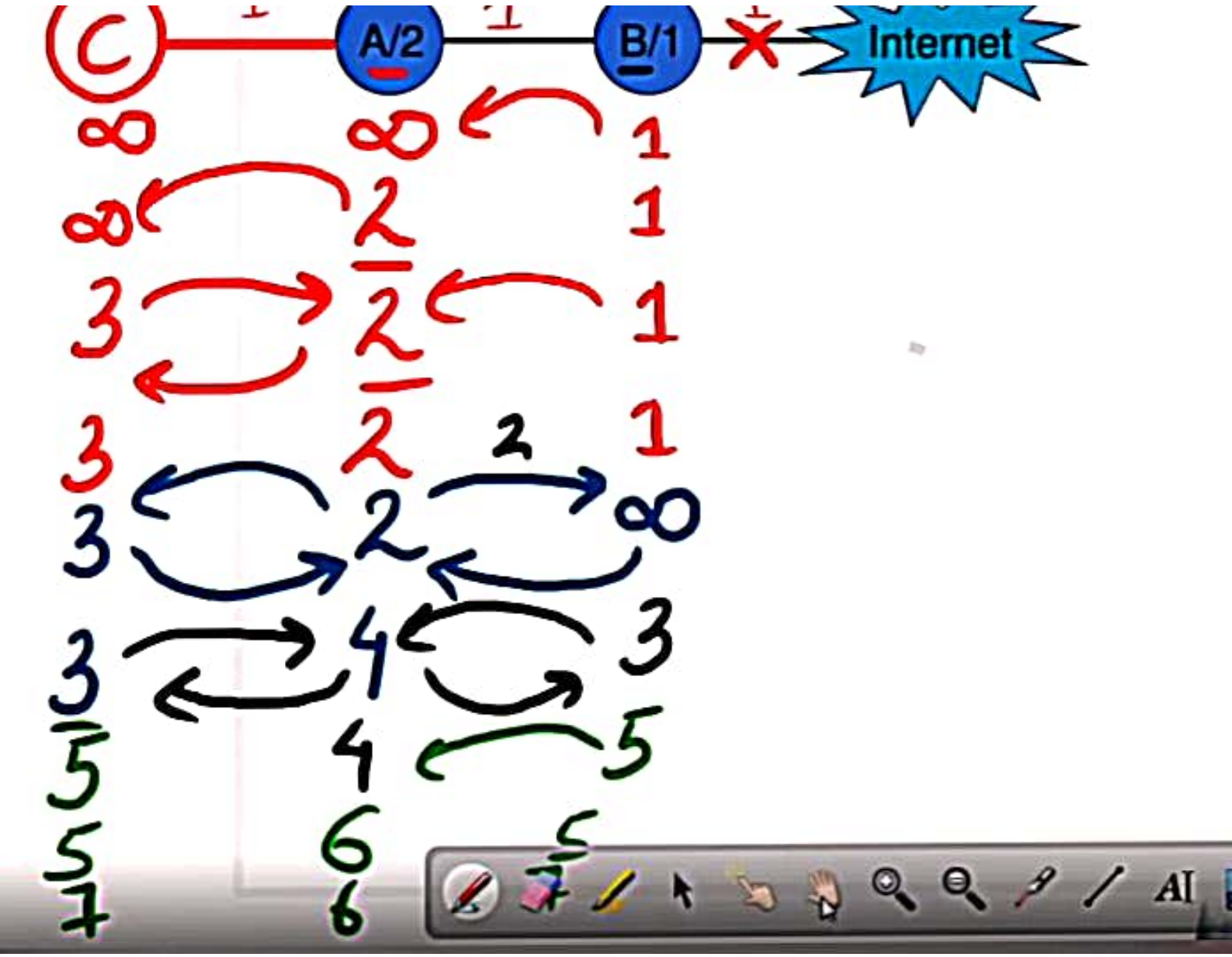
VERSION (4)	Priority (8) Traffic type	Flow Label (20)
Payload Length (16)	Next Header (8)	Hop (8) Limit
Source Address (128)		
Destination Address (128)		

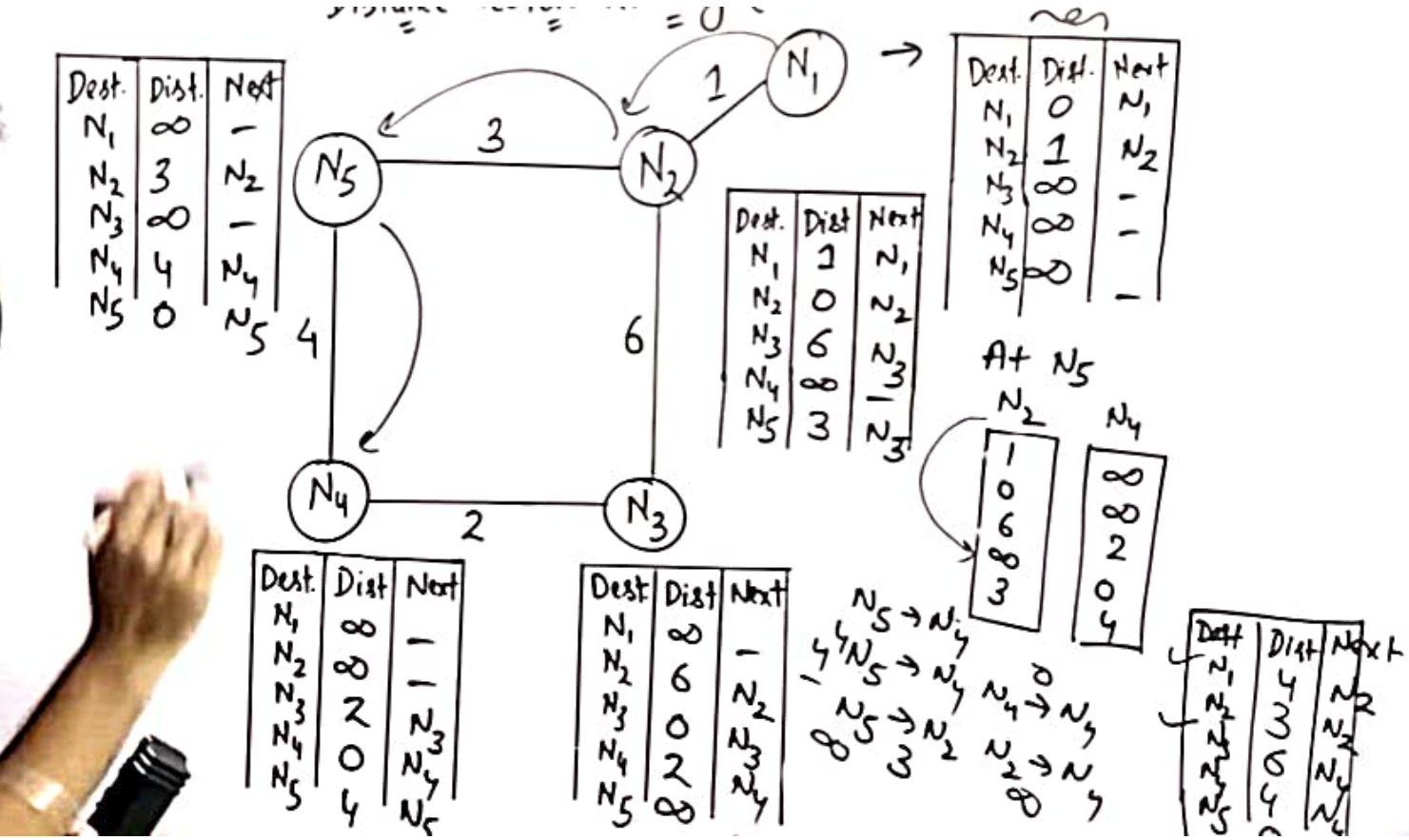
Base Header = 40 Bytes (320 bits) Fixed

Extension Headers:

1) Routing Header (43)
2) Hop by Hop option (0)
3) Fragment Header (44)
4) Authentication Header (51)
5) Destination Options (60)
6) Encapsulating Security Payload (50)


3
2
2
1
3
2
∞
3
4
3
3
4
5
5
6
5
5
7
6
7
1
1
∞
∞
∞


C
A/2
B/1
Internet


N1
N2
N3
N4
N5
1
3
4
6
2
Dest. Dist. Next
N1 ∞ –
N2 3 N2
N3 ∞ –
N4 4 N4
N5 0 N5
Dest. Dist Next
N1 1 N1
N2 0 N2
N3 6 N3
N4 ∞ –
N5 3 N5
Dest. Dist. Next
N1 0 N1
N2 1 N2
N3 ∞ –
N4 ∞ –
N5 ∞ –
At N5
N2
N4
1 ∞
0 ∞
6 2
∞ 0
3 4
Dest. Dist Next
N1 ∞ –
N2 ∞ –
N3 2 N3
N4 0 N4
N5 4 N5
Dest. Dist Next
N1 ∞ –
N2 6 N2
N3 0 N3
N4 2 N4
N5 ∞ N4
N5 → N4
N4 → N5
N5 → N2
N4 → N3
N2 → N4
0
∞
3
∞

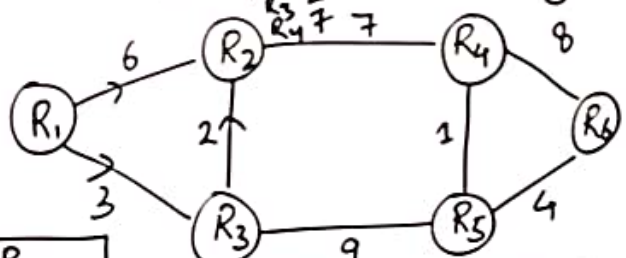
Jacobson's Algorithm for Timeout Timer in TCP

- Jacobson's Algorithm for Timeout Timer in TCP
  - Step – 1: Assume Initial Round Trip Time (IRTT) & Initial Deviation ID
  - Step – 2: Timeout Timer, To = 4 ID + IRTT
  - Step – 3: See the Actual Round Trip Time (ARTT) and find the New Round Trip Time (NRTT) & Actual Deviation AD.
    - NRTT = $\alpha\ \mathrm{IRTT} + (1 - \alpha)\mathrm{ARTT}$
    - AD = |IRTT – ARTT|
    - ND = $\alpha\ \mathrm{ID} + (1 - \alpha)\mathrm{AD}$
    - Here, α is smoothing factor.
    - To = 4 ND + NRTT
  - Step – 4: Repeat Step 3, to get To.

Silly Window Syndrome & Solutions in TCP

- Silly Window Syndromes are associated with ineffective utilization of bandwidth and resources.
  - Window size is full.
  - Slower Sender.
  - Slower Receiver.

Link State Routing — global knowledge: Flooding, Dijkastra



R_1	
SEQ No	
TTL	
R_2	6
R_3	3

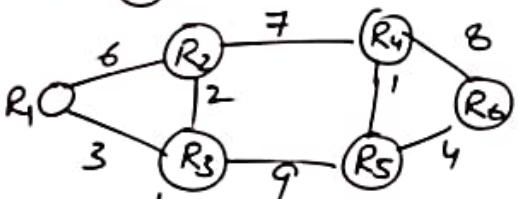
R_3	
R_1	3
R_2	2
R_5	9

R_5	
R_3	9
R_4	1
R_6	4

R_6	
R_5	4
R_4	8

	d	v.a
R_1	0	R_1
R_2	5	R_1
R_3	3	R_1
R_4	12	R_3 R_2
R_5	12	R_3
R_6	16	R_5 R_4

At R_1



	R_1	R_2	R_3	R_4	R_5	R_6
		6	(3)	∞	∞	∞
R_1 R_3		(5)	(3)	∞	12	∞
R_1 R_3 R_2				(12)	12	∞
R_1 R_3 R_2 R_4					(12)	21
R_1 R_3 R_2 R_4 R_5						16

Basic Algorithm for Timeout Timer in TCP

- Basic Algorithm for Timeout Timer in TCP
  - Step – 1: Assume Initial Round Trip Time (IRTT)
  - Step – 2: Timeout Timer, To = 2 IRTT
  - Step – 3: See the Actual Round Trip Time (ARTT) and find the New Round Trip Time (NRTT).
    - NRTT = $\alpha\,\mathrm{IRTT} + (1 - \alpha)\mathrm{ARTT}$
    - Here, α is smoothing factor.
    - To = 2 NRTT
  - Step – 4: Repeat Step 3, to get To.

Lec-46: Disadvantages of Classful Addressing | IP addressing | Computer Networks

Ne

Problems with classful Addressing

- Wastage of IP addresses
- Maintenance is time Consuming
- More prone to Errors

Flexibility

CA — 126

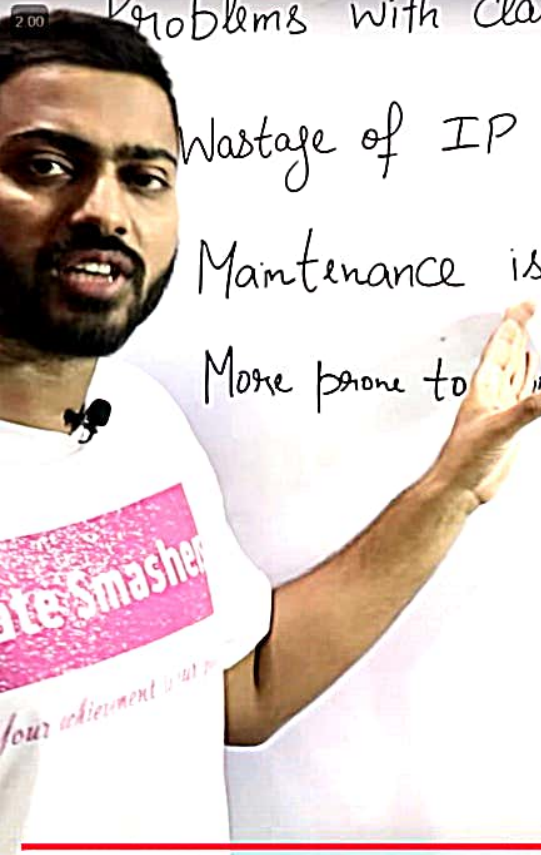
2^{24} = 1 Crore

CB = 2^{16} = 65K

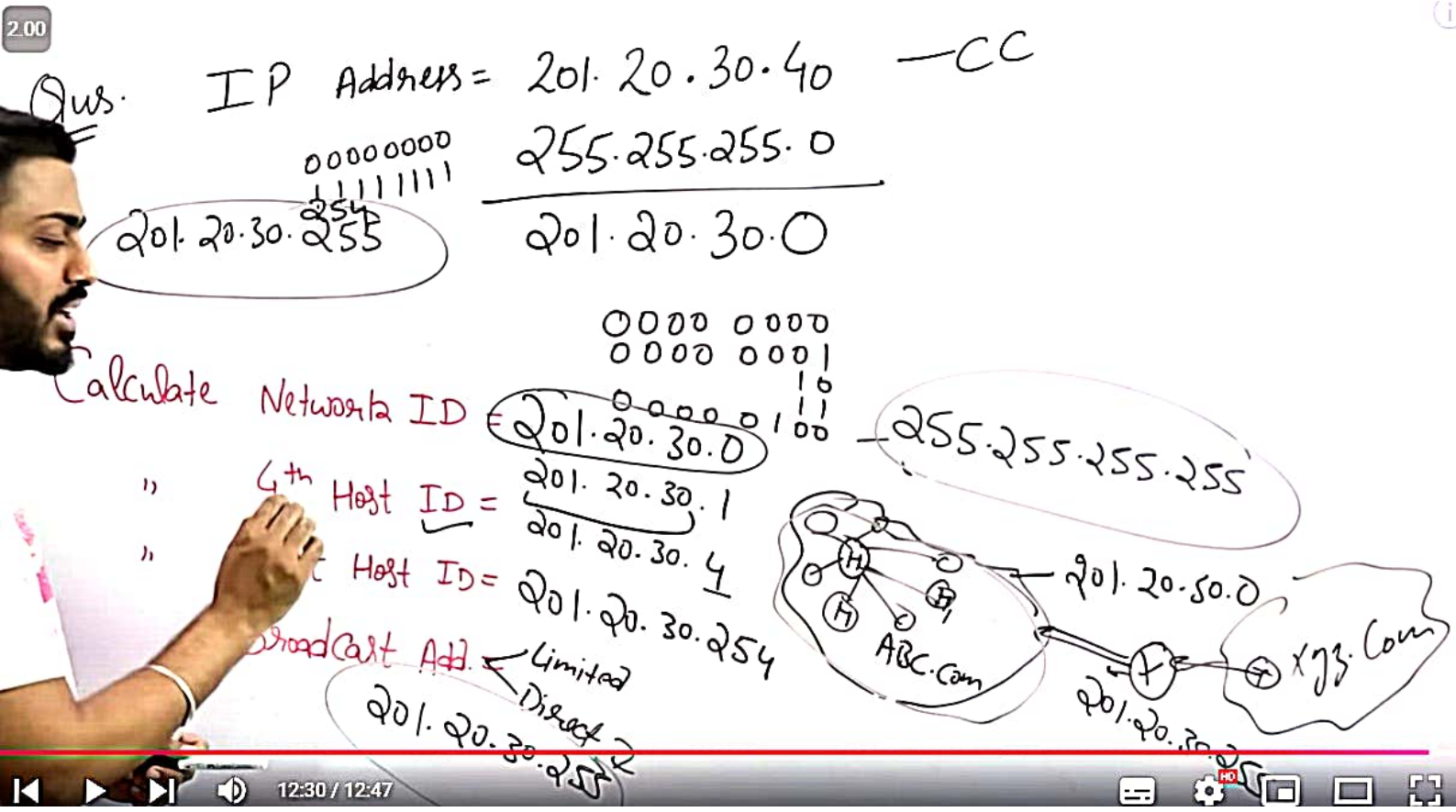
CC = 2^8 = 256

1024

CD, CE



5:19 / 6:11 • More prone to Errors >


2.00
Qus. IP Address = 201.20.30.40 —CC
00000000
11111111
255
201.20.30.255
255.255.255.0
201.20.30.0
0000 0000
0000 0001
0000 0010
0000 0011
Calculate Network ID = 201.20.30.0
" 4th Host ID = 201.20.30.1
201.20.30.4
" Host ID = 201.20.30.254
Broadcast Add. ← Limited
Direct
201.20.30.255
255.255.255.255
201.20.50.0
ABC.com
xyz.com
201.20.30.2
12:30 / 12:47