Computer Network: A collection of devices interconnected together to exchange information.

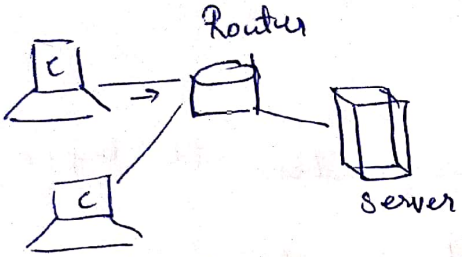
Internet: network of network → largest

Uses:-

1) Resource Sharing → file, data, information etc.

Client → machine that request resources/services

Server → machine that provides requested resources/services



Request - Response model.

2. Communication (email, video conferencing, placing business order)
3. Electronic Commerce → B2B/C, G2C, C2C, P2P (Government, peer)
4. Financial Services → Bank, paytm, UPI
5. Ubiquitous (everywhere) Computing → IOT, IOE, Smart device
6. Mobile/wireless Computing → Hotspot
7. Satellite Communication → GPS
8. Wearable Computers.

Network Hardware:- The basic Computer hardware components that are needed to set up a network as follow:

1) Network Cables:

→ Network Cables are the transmission media to transfer data from One device to another.

→ Commonly Used Cable is Category 5 cable with RJ-45 Connector.

2. Routers:

→ A Connecting device that transfer data packet between different Computer network.

They are used to connect a PC (or) an Organization's LAN to a broadband Internet Connection.

3. Repeaters, Hubs and Switches:

They Connect network devices together so that they function as a single segment.

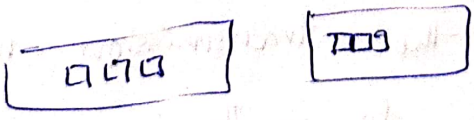
→ A repeater receives a signal and regenerates it before re-transmitting so that it can travel longer distance

→ A hub is a multiport repeater having several having input & Output ports, so that input at any port is available at every other port.

→ A Switch receives data from a port, uses packet Switching to resolve the destination device and then forwards the data to the particular destination

4) Bridges:

A Bridge Connects two seperate ethernet network segment It forwards packets from the Source network to the destined network



5. Gateways:

→ A Gateway connects entirely different networks that work upon different protocols.

→ It is the entry and the exit of the point in network & control access to other networks.

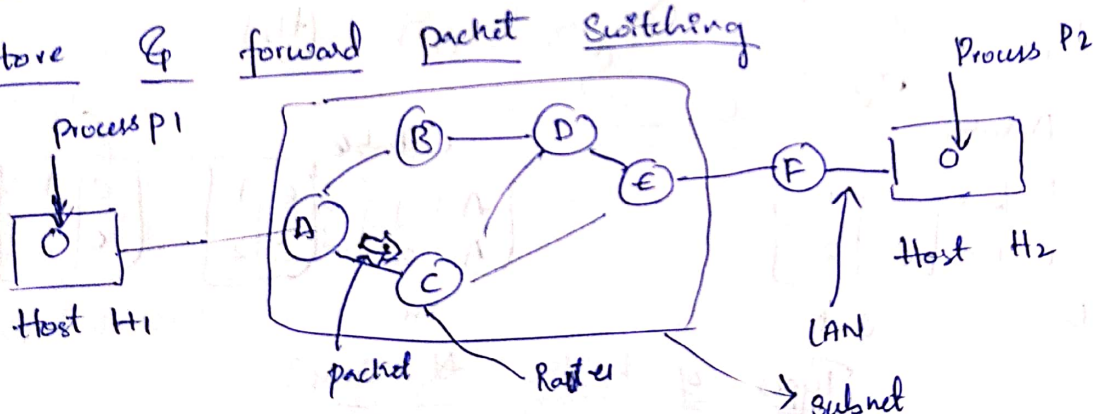
6. Network Interface Cards:

→ NIC is a component of the computer to connect it to a network.

→ Network card are two types
  1) Internal network card
  2) External network card.

Network layer Design Issues:

1. Store & forward packet Switching



2. Services provided to transport layer

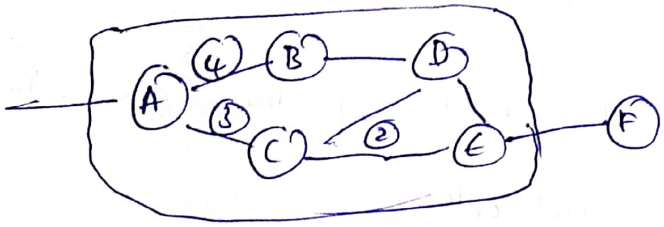
1. The Service should be Independents of router technology.
2. The transport layer should be shielded from the no, type & topology of routers present
3. The n/w addresses made available to transport layer should be a Uniform number plan, even across LAN & WAN.

3. Implementation of Connection less Service:

(Large packet split into small packet)

→ Routering table are updated periodically.

Datagram:



Router A initial

A	–
B	B
C	C
D	B
E	C
F	C

Router A table later

A	–
B	B
C	C
D	D
E	D
F	B

C

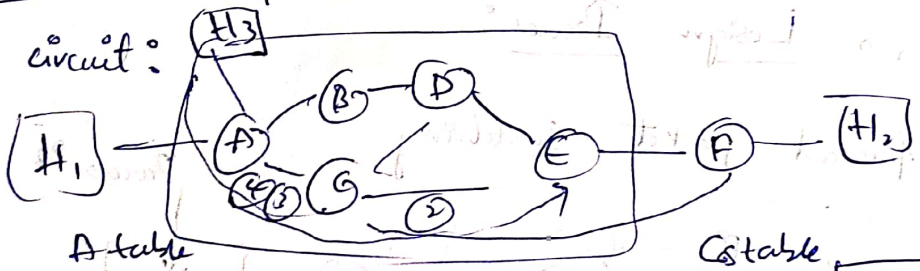
A	A
B	A
C	–
D	E
F	E
E	E

E

A	C
B	D
C	C
D	D
E	–
F	E

4. Implementation of Connection Oriented Service:-

Virtual circuit:



A table

In		Out	
H1	1	C	1
H3	1	C	2

C table

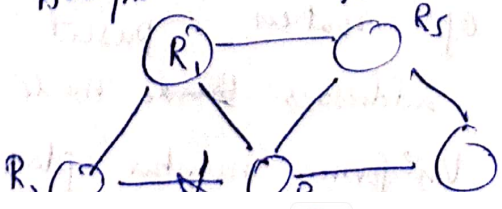
In		Out	
A	1	E	1
A	2	E	2

E's

In		Out	
C	1	F	1
C	2	F	2

Types of Routing Algorithms:-

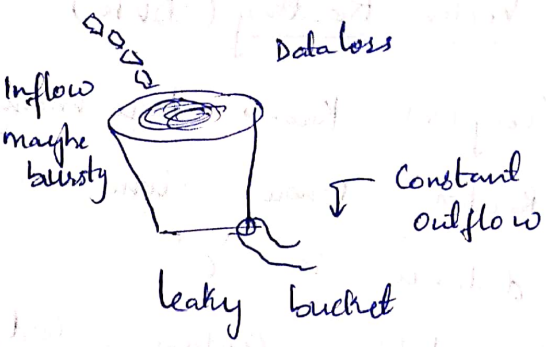
Non Adaptive Routing Alg. (Static)	Adaptive routing Alg (Dynamic)
→ Routing decision is always same	→ Routing decision changes
→ Constant rate	→ no Constant rate
→ preloaded	→ Not preloaded
→ Don't adapts to traffic	→ Adapts to traffic

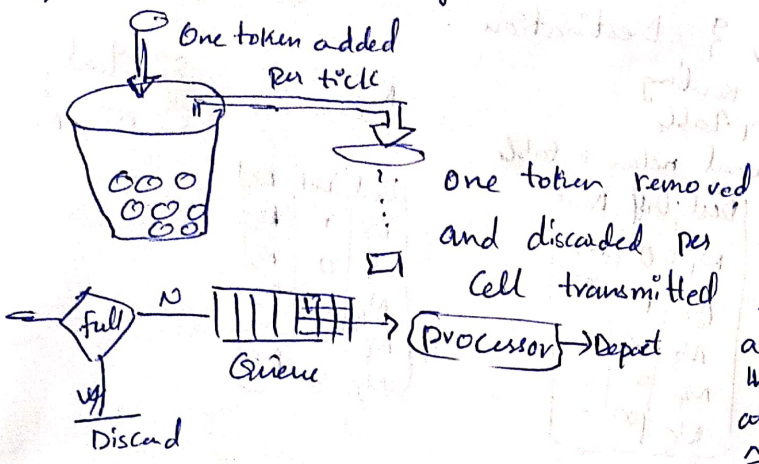


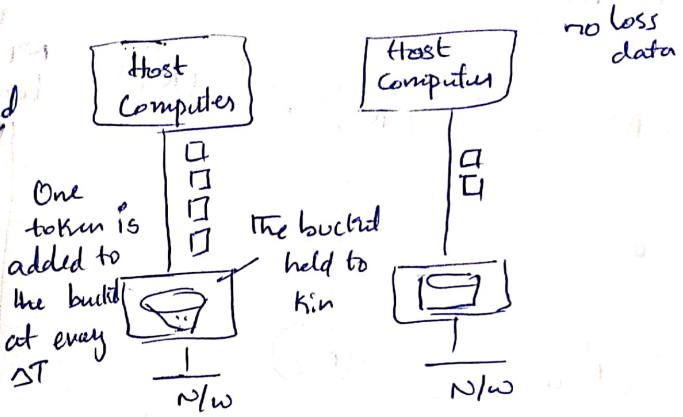
Congestion Control: (Jam)

a) leaky bucket algorithm

b) Token bucket algorithm







→ leaky Bucket discard packet

→ Token Bucket does not, it discards tokens.

→ with token Bucket, a packet can only be transmitted if there are enough tokens to cover its length in bytes.

→ Token Bucket allows for large bursts to be sent faster by speeding up the output.

→ Token Bucket allows saving up tokens (permissions) to send large.

→ leaky Bucket sends packet at an avg rate.

→ leaky Bucket doesn't not allow saving.

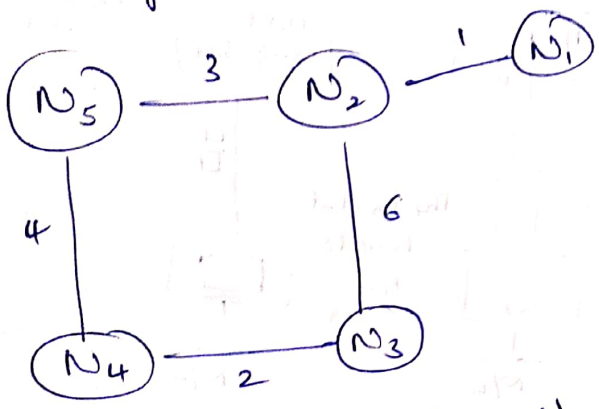
Distance Vector Routing (DVR)

→ Router Every (r) knows how many routers in the network

→ Each Router knows who is his neighboor

→ Self distance is '0'

→ Routing table Contain Cost, & Destination.



Routing table
N_1 local network table

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

N_2

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

Similarly N_3, N_4, N_5

1) Only neighbour (shared)

2) Only Distance vector ($N_1 \rightarrow N_2$)

At N_1

N_2

1
0
6
∞
3

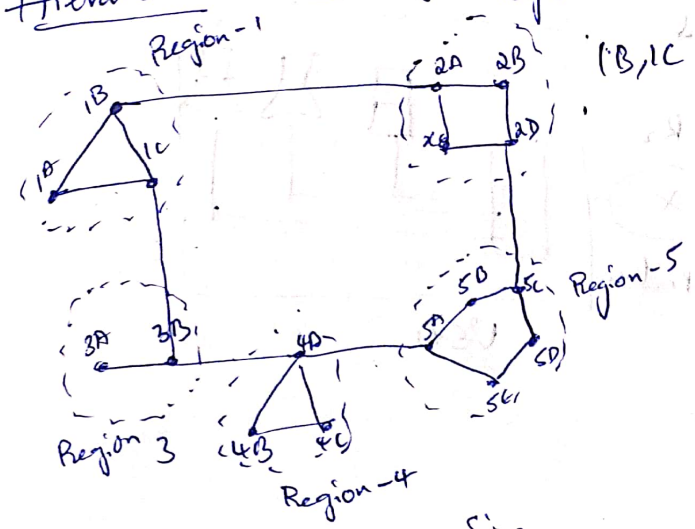
N_1 new RT

Dist	Dist	Next
N_1	0	N_1
N_2	1	N_2
N_3	7	N_2, N_3
N_4	∞	–
N_5	4	N_5

Iterative Process

→ Always update.

Hierarchical Routing :



1B, 1C is gateway Router

Full table for 1A

Dest	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

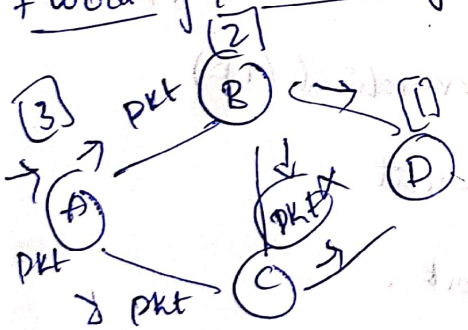
Hierarchical table-A

Dest	line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4.

→ To Reduce memory size we are dividing Router into Region.

→ Each Router knows the internal Router node but doesn't know the another Region Router Information.

Flooding / Broadcasting :



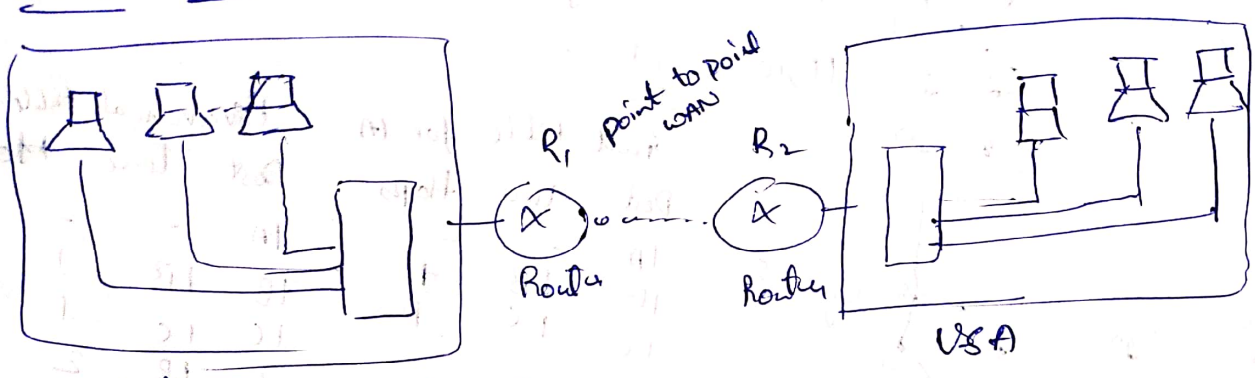
→ transmitting the packet to all its neighboring router except source router from which packet is arrived.

→ Vast no. of duplicate generate.

→ Sequence no (for duplicate)

→ Hop count / router count

Internet works:



Connection. ~~Oriented~~

Internetworking:

Inter networking is the process or technique of Connecting different networks by using intermediary devices such as router, Switches, gateways etc.

how network Differ:

i) Services Offered: Virtual circuit vs Datagram (Types)

ii) Protocol Used: Some protocals are IP, CLNP, DEC, Apple Talk etc

iii) Addressing: It can be flat (802) (or) heerarchical (IP)

iv) Multicasting: Can be present or absent.

v) packet Size: It depend on the network.

vi) Error handling: we can have reliable Ordered (or) Unordered delivery.

vii) flow Control: we can get sliding window, rate control etc.

viii) Congestion control: Different algo such as leaky bucket, choke packet are available.

Ipv4 Header:

→ Connection less

→ Datagram Service

Datagram = Header Size = 20 – 60 bytes + Payload = 0 – 6515 bytes

13 field + 12 mand

Version 4	HLEN 4	Types of Service (DSCP) 8	Total Length 16
Identification bits 16		Flag 3	Fragment offset 13
Time to live 8	Protocol TCP/UDP 8	Header checksum (error detection) 16	
Source Ip address 32 bits			
Destination Ip address 32 bits			
→ Options & padding.			

avoid loop congestion

3 fragmentation part

160 bits
20 byte

Ver: 0100 (4), 0101 (6)

Hlen: header length

Type of service: Differentiated Services Code point (DSCP)

P	P	P	D	T	R	C	0

Cost future

Precedence — Delay — Throughput — Reliability

DSCP	ECN
0 – 6	7

Explicit Congestion notification.

Flag 3

	DF	MF

frag	0	0
	0	1
No frag	1	0
	1	1

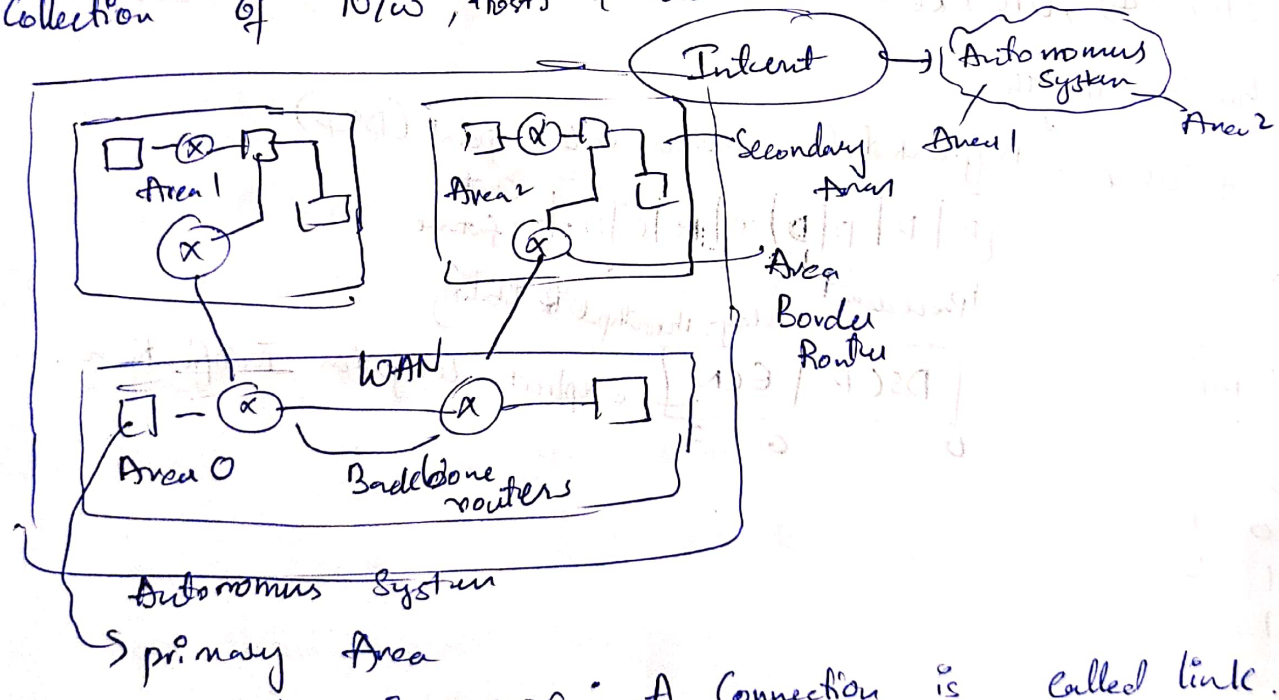
Routing protocols.

- Intra domain
  - Distance vector (RIP) — Real life ppt
  - Link state (OSPF) — Open shortest path first.
- Inter domain → path vector. (BGP)

Open Shortest path first Protocol.

→ It is an intra domain Routing protocol & is based on link state protocol.

→ It divides an autonomous system into Areas which is a collection of N/w, Hosts & routers.



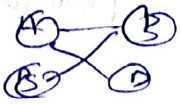
Types of links in OSPF: A Connection is called link.

i) Point to point: Connects two routers without any host in between.

(A) —— (B).

ii) Transient link: It is a n/w with several routers attached to it

→ Unrealistic

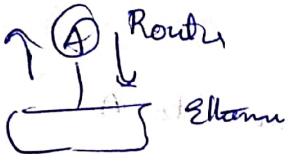


→ realistic

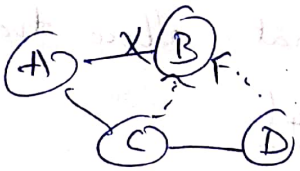
iii) Stub link:

It is a n/w that is connected to only one Router

Data entry & leave through single router



iv) Virtual link: when the link b/w two routers is broken, the administrator may create virtual link b/w them using a longer path.



OSPF:

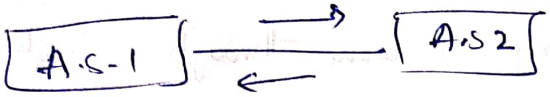
→ Hello (Establish conn)
→ Database Description (Create links)
→ link state Request
→ link state update
→ " " Ack.

Border Gateway Protocal (BGP):

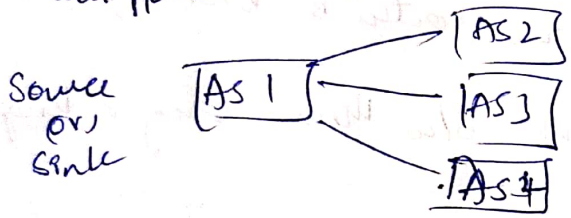
It is an inter domain routing protocal that uses path vector routing

Types of Autonomous Systems:

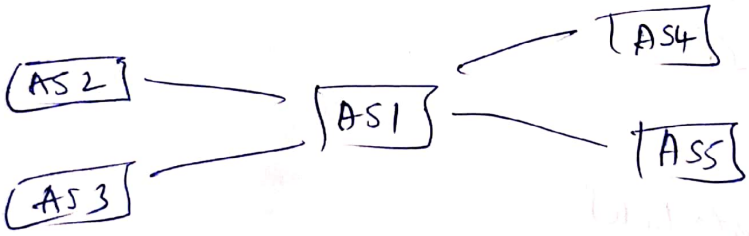
i) Stub As: A Stub As has only one connection to another As. Data traffic can't pass through a Stub As



ii) Multihomed AS: It has more than one conn to As.



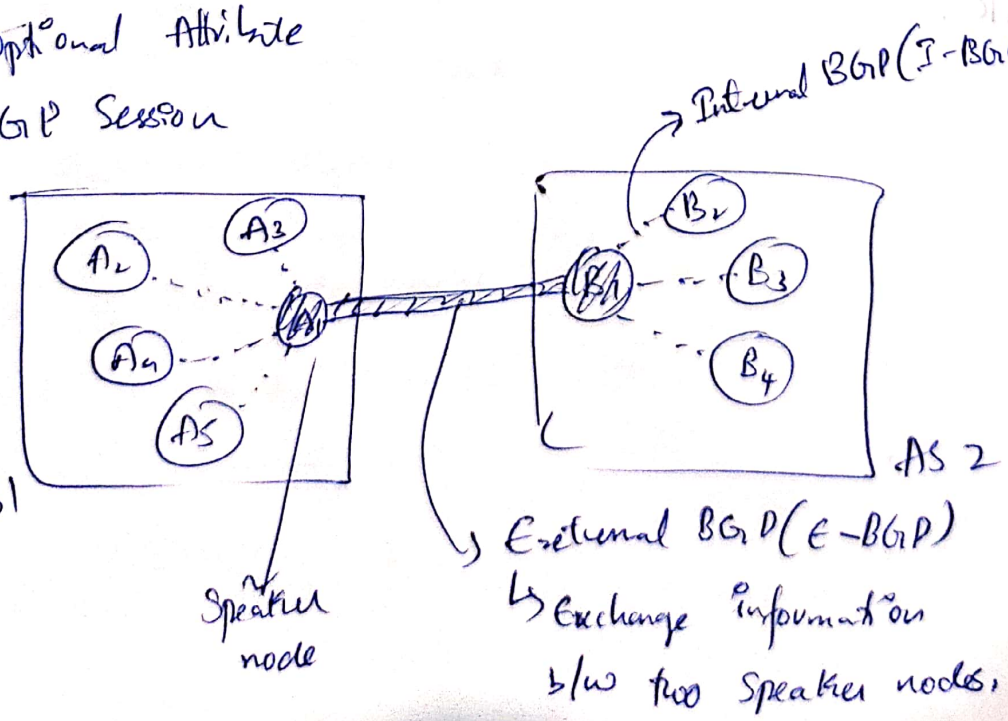
iii) Transit AS: It is a multihomed As that allow transit traffic



path attributes:

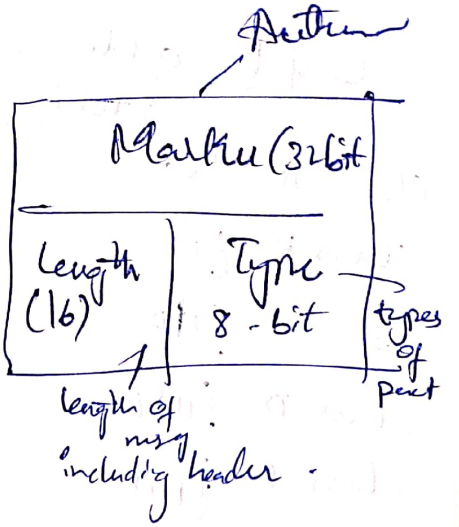
1) well know Attributes : → origin, path, need hop.
2) Optional Attribute

BGP Session



Types of packet

1) Open: Create an neighbourhood Relation
2) Update: withdraw destination
3) Keep alive: alive (or) not packet
4) Notification: Close connection reqⁿ packet



Fragmentation in CN (nodes).

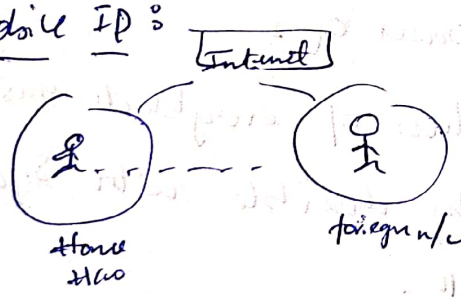
Identification (16)	Flags (3)	Fragmentation (13) offset

bit 0 → Reserved Always set to 0
bit 1 → DF (Don't fragment forget)
bit 2 → MF (more fragment

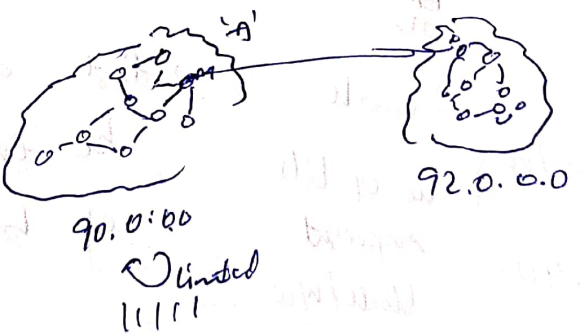
NAT – Network Address translation
CIDR – Classless Addressing (CIDR) & Interdomain Routing
ARP – Address Resolution Protocal.

Tunelling → encapsulate & decapsolate the data b/w two router.

mobile IP:



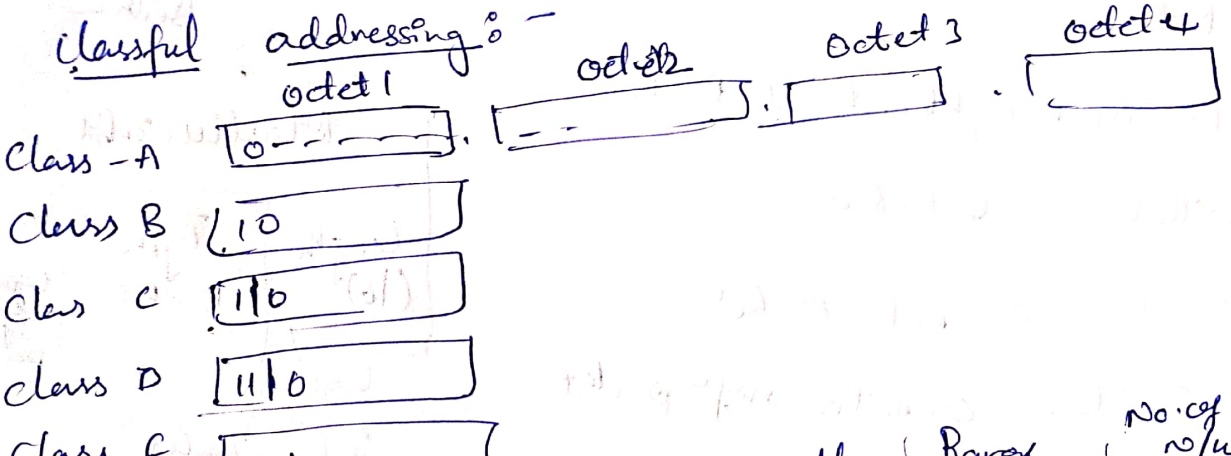
Unicast, Broadcast, multicast (one to one)

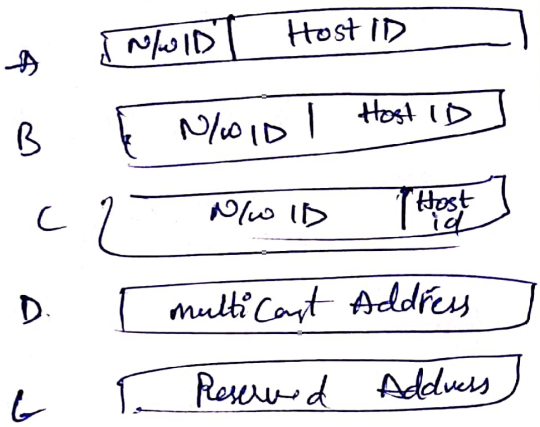


(Intra)
→ limited broadcast
→ Direct broadcast (inter)

Limited
11111

Classful addressing :-





	no. of I/P Addrs	Range	No. of n/w	No. of Hosts
A	2^{31} (50%)	0-127	2^7	2^{24}
B	2^{30} (25%)	128-191	2^{14}	2^{16}
C	2^{29} (12.5%)	192-223	2^{21}	2^8
D	2^{28}	224-239	Not defined	ND
E	2^{28}	240-255	ND	ND

Classless Addressing :-

→ No classes

→ Only Blocks

→ Notation

x.y.z.w/n

n → mask

w → no. of bits represent block/n/w

200.10.20.40.

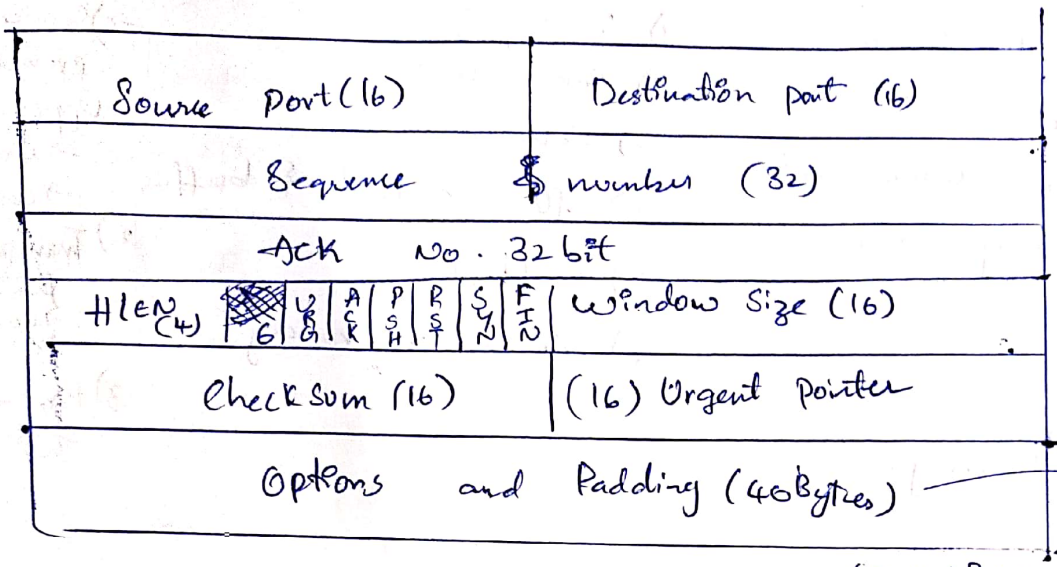
Rules :-

→ Addresses should be Contiguous

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

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

TCP Header (Transmission Control protocol)



Segment is a collection of bytes.

(20-60) Bytes

0 - 1023 - well know port

5000 - 5050

5051 + ACK

TCP

→ Byte Streaming
→ Connection Oriented
→ Full Duplex
→ Piggybacking
→ Error Control
→ flow Control
→ Congestion Control.

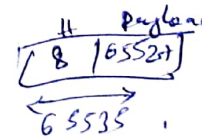
URG - Urgent flag
Ack - If sending 1 flag notification
PSH - push (no wait for Buffer full)
RST - Reset (three way handshaking)
Syn - Synchronization flag '1' to connect the server
FIN - terminate to process '1'
window size: Receiving window size (mm - capacity to receive)
Urgent pointer: which data is urgent

UDP header :-

Source Port (16)	Destination Port (16)
length (16)	Checksum (16)

(8B fixed)

→ Conn less protocal (Unreliable)
→ NO Order
Checksum = UDP Header + UDP Data + Pseudo header of IP
→ payload ⟶ $.



Transport Service

- → full duplex communication
- → Connection Oriented Service
- → Reliable Service
- → process to process communication
- → Stream Delivery service
- → Segments
- → flow control
- → Error control
- → Guarantee Delivery.

NSAP - Network Service Access point.

Transport Service Element

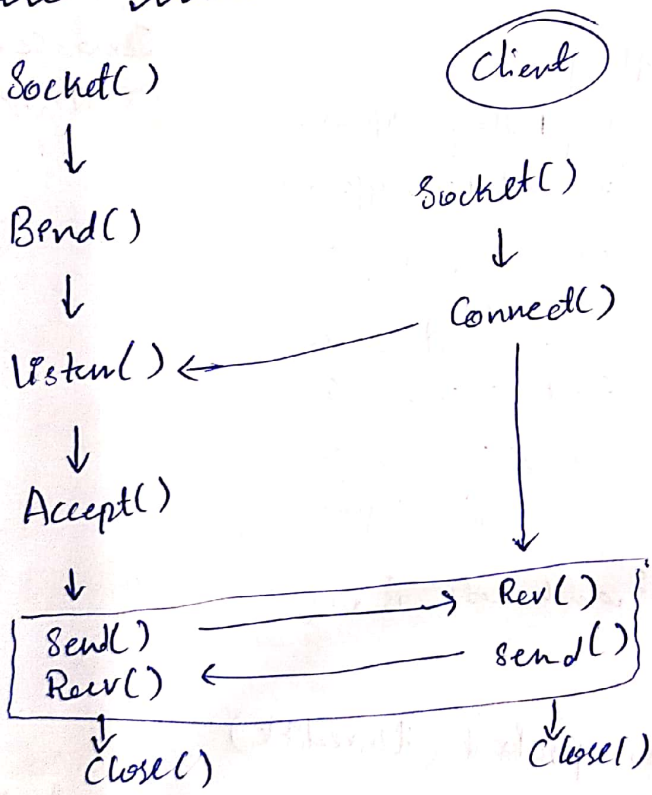
1) Addressing
2) Conn est
3) Conn release
4) flow control & buffer
5) multiplexing
6) Crash recovery

Trans Services

1) Service provide to upper layer
   - → Conn
   - → Conn
2) Transport
   - Primitive
   - → Co
   - →
3) Brac Soc

TCP fou

Socket programming :



→ Socket (Domain, Type, Protocal)

TCP Vs UDP

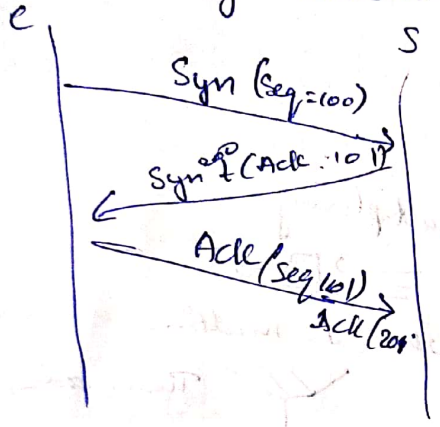
TCP	UDP
1) Connection Oriented	1) Connection less
2) Reliable	2) Less Reliable
3) Error control is mandatory	3) is optional
4) Slow transmission	4) fast
5) More Overhead	5) less Overhead
6) flow control, congestion control	6) No FC, CC

TCP Connection Management :

1. TCP Connection Establishment
2. Data transfer
3. TCP Connection termination

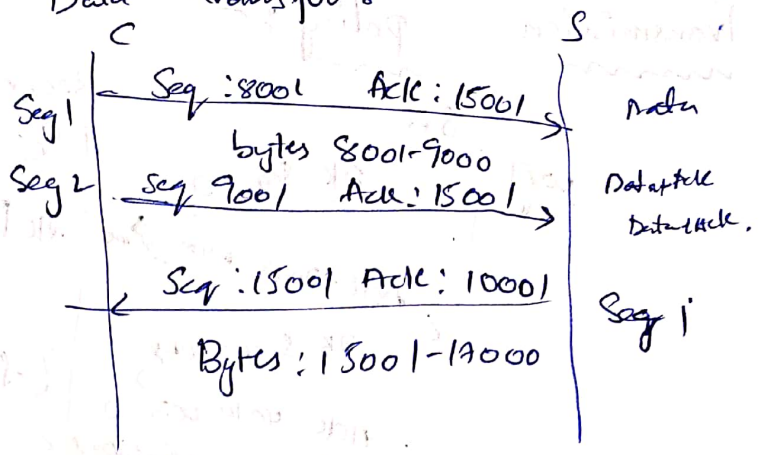
1. Establishment

Three-way handshaking



1. Client Sends Syn Segment to Server. I want to Establish a Connection with you.
2. Server Acknowledge the client Segment & Send Syn Segment want to establish Connection with you.
3. Client Acknowledg the Server I am ready to have A Connection with you.

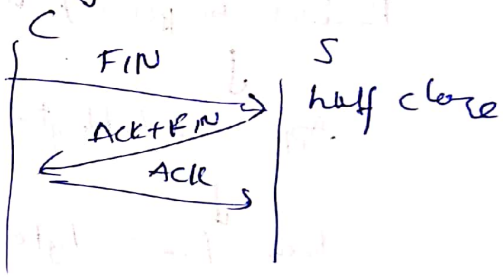
Data transfer :



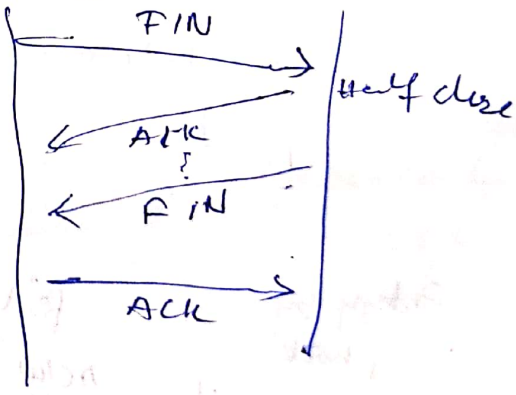
Piggybacking : along with the Server data sends Ack previous of it.

TCP termination :

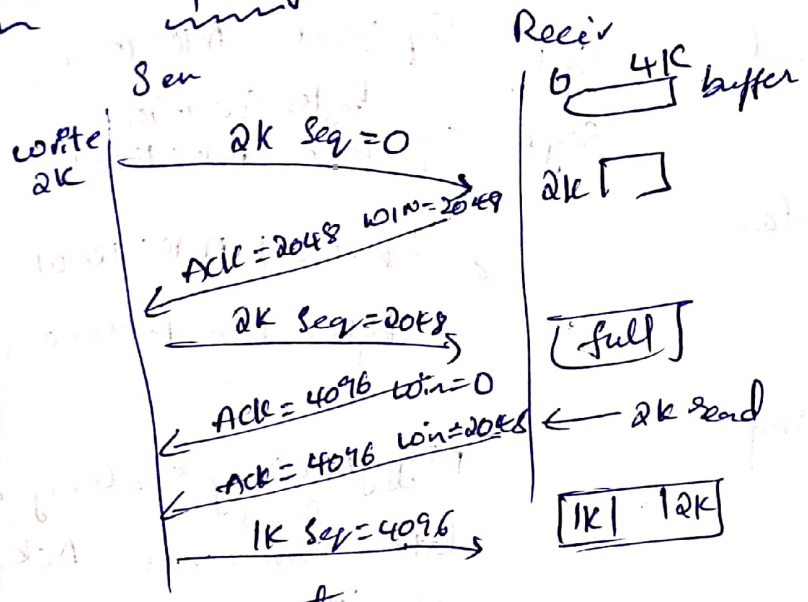
Three-way handshake



four way handshake

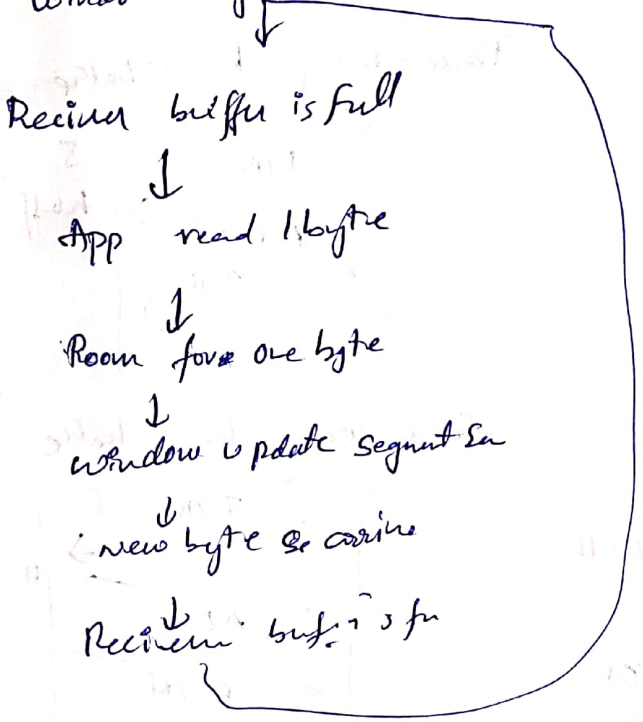


Transmission policy :-

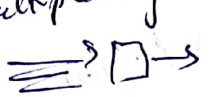


window management

Silly window Syndrome

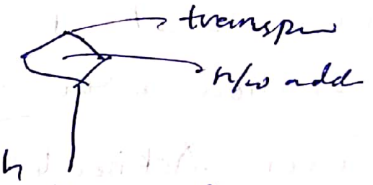


→ multiplexing



1) Upward multiplexing

2) Downward m



→ Crash Recovery :

→ Crash blw Server(OR) Client

→ host & router.

TPDU

So : no outstanding TPDU

S1 : One TPDU outstanding

Strategy by Sending host

Always Retransmit

never "

Retransmit in S0

" S1

"

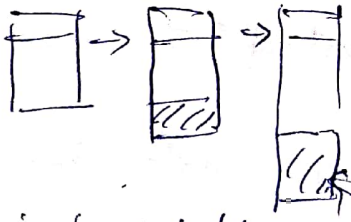
first Ack then write		first write then Ack		
ACK(W) OK	AWC DUP	C(WA) OK	WAC DUP	WC(A) DUP
Lost	OK	Lost	Lost	OK	OK
OK	DUP	Lost	Lost	DUP	DUP
Lost	OK	OK	OK	OK	DUP.

Buffering :-

a)

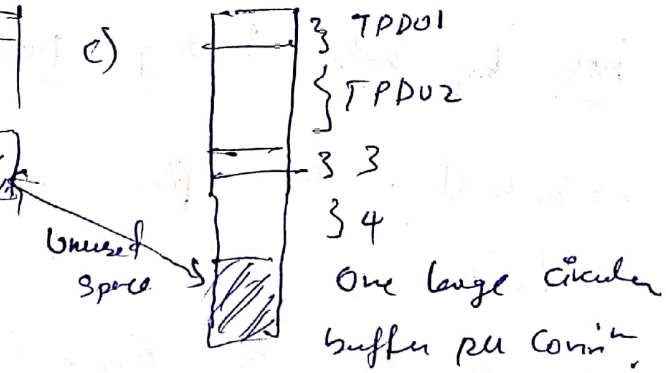
Chain fixed size buffer

b)



Chained variable sized buffer

c)



One large circular buffer per conn.

Data link Control

-> flow control (stop & wait, Sliding window)

=> error control. (CRC, parity check, Checksum)

(Hamming Distance.

TCP Congestion Control:

-> Congestion occurs, if the load offered to any n/w is more than its capability

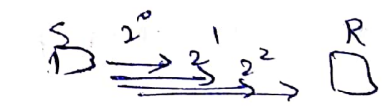
-> TCP control Congestion by means of windows mechanism.

-> TCP set a window size telling the other end how much data segment to send.

3 algo. (1) slow start algo

(2) congestion avoidance algo (to slowdown the exponentially growth) by using additive Increase

(3) Congestion detection algo.



Threashold set to half.

-> (decrease the congestion window size) -> 1) Connection timeout
2) Reception of 3 ack.

Real Time protocal : (multimedia).

-> To handle real time traffic like audio, video over the internet is known as RTP.

Source → Encoder → packetize → Transport control network

Display ← decoder ← Reassembly ← Trans

QOS
Quality of Service

Mixer :-
= one stream.

hob by hob Routing protocal :-

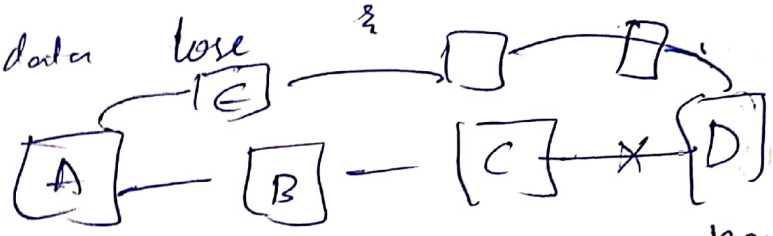
-> Controlling the flow of data in n/w

-> Chunk of data are forwarded from node to node in a store & forward manner.

-> not only source & destination node, All the intermediate nodes as well

-> No data lose

->



nexthop :	B	C	D
B	C	B	
E	A	B	

normal

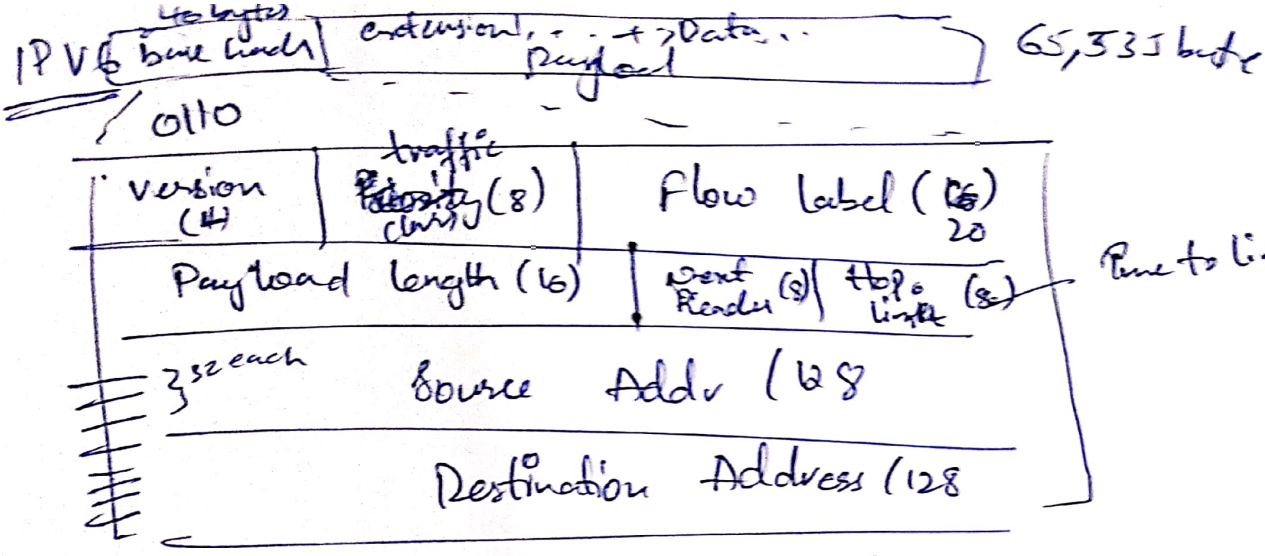
After further, before convergence

After convergence

-> multicasting is a available

-> Useful for packet transfer & data cut lose

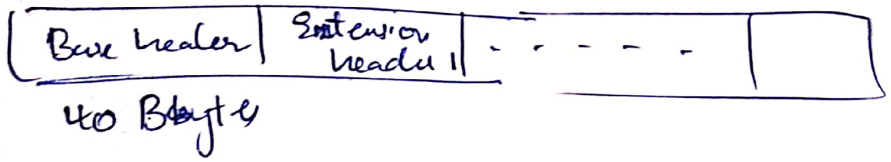
-> hops have packet in it



Base Header = 40 bytes (320 bits)

Extension Headers:

1) Routing Header (43)
2) hop by hop option (0)
3) Fragment Header (44)
4) Authentication (51)
5) Destin option (60)
6) Encapsulating Security payload (50).



Scalability :-

=> Web host.
→ go daddy
→ VPSes (fast pc)
→ AWS EC2 EC2.

Vertical Scaling
→ Core / CPU.
→ Disk
→ RAM

horizontal Scaling
→ move machine
→ multiple Server
then DNS will give request to whom Server.
(Dns = load Balancing)
IP address get by DNS. Server.

→ load Balancing. decide the which Server to choose & Send request to Server.

Client → load balancing → Backend Server.

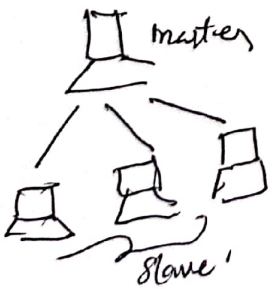
→ round robin
→ caching is use to get IP addr.
→ Static will work.
→ login again & again
→ data inconsistency.
Soln dedicated php Server, HTml " " db
→ dedicated Hard drive for session
→ but if hard drive serve is die
→ how to fix the problem

→ RAID
Redundancy Array Inexpensive
DISK
RAID-0 - Performance
RAID-1 - mirroring the data, 1/2 50%.
RAID-5 - 3,4,5 drive, One is redundancy
RAID-6 - , too die redundancy
RAID-10 + performance
Down time decrease
up time Increase

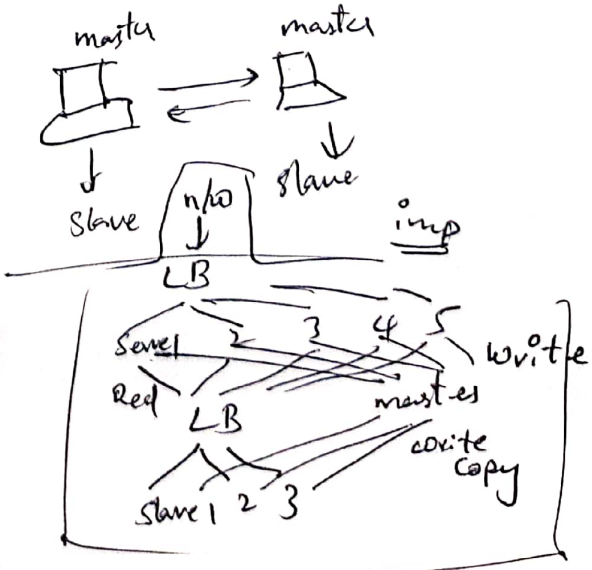
→ Some One remove power cable
→ Sticky Session
→ shared storage FC, ISCSI, mysql, NFS etc
→ cookies ?

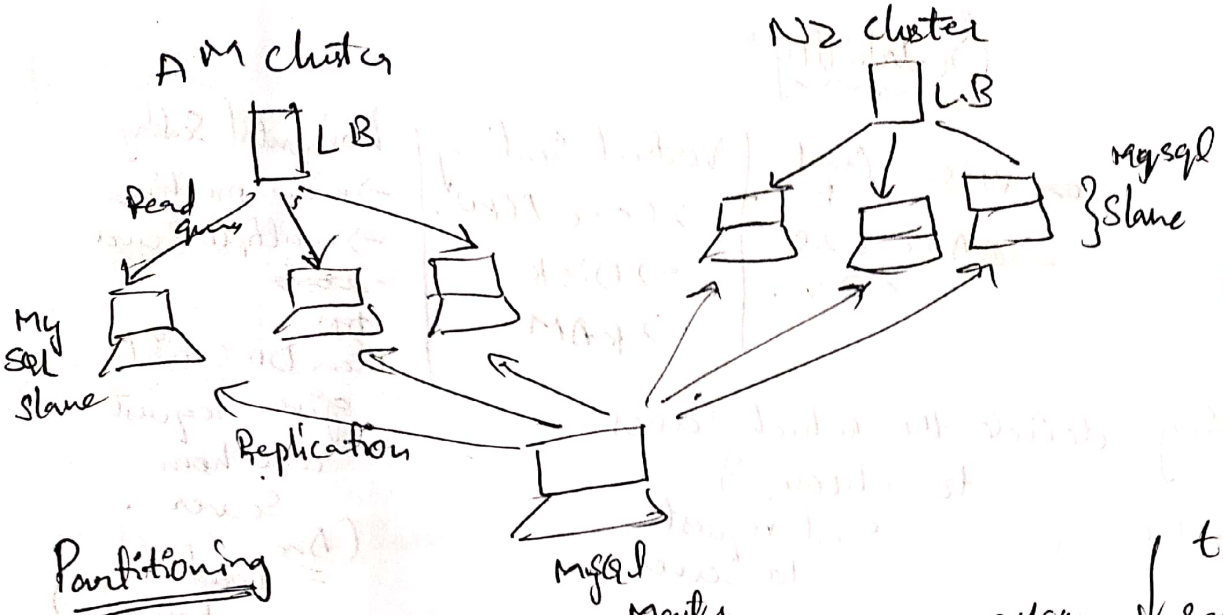
$20000 for LB min 100K basic

memcached
Key-value storing info.



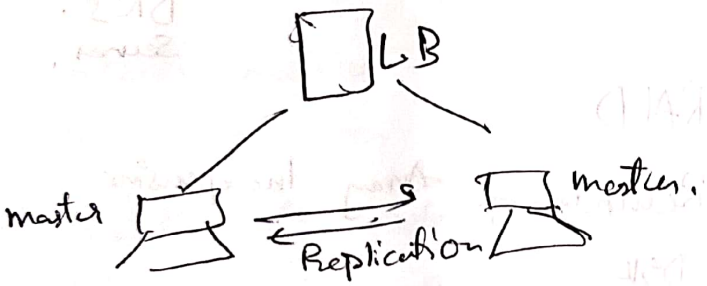
read heavily problem
we can read from master and slave but for write use master only and slave have to copy master.





Partitioning

High Availability



Security.

tcp 80, 443

Sticky session: SSL HTTPS