Multi-Protocol label switching (MPLS):-

→ 1980 several vendors created router that implement switching technology.

→ In this standered, some conventional router in the internet can be replaced by MPLS, which can behave like a router and a switch.

→ When behaving like router, MPLS can forward the packet based on destination address

→ When behaving like switch, it can forward a packet based on the label.

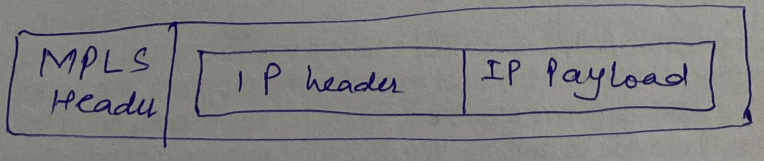
A new header

→ A new field is added to packet that carries label info. (Assume connection oriented switching using IP Protocol).

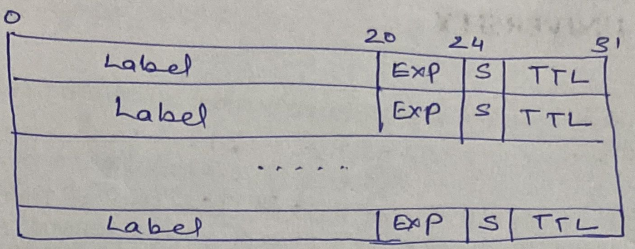
→ IPV4 does not allow this extension.

→ The solution is to encapsulate the IPV4 packet in an MPLS packet (as through MPLS layer between a DLL and N/w layer)

→ The whole IP packet is encapsulated as payload in an MPLS packet and MPLS header is added.



→ MPLS header is actually a stack of subheaders that is used for multilevel hierarchical switching.



4-byte long ~~multilabel~~ subheader

(i) Label: This 20 bit field defines the label that is used to index the forwarding table in the router.

(ii) Exp: This 3 bit field is reserved for experimental purpose.

(iii) S: The one-bit stack field defines the situation of the subheader in the stack. When the bit is 1, it means that the header is the last one in the stack.

(iv) TTL: 8 bit field similar to TTL in IP datagram.

Hierarchical switching

- A stack of label in MPLS allows hierarchical switching
- For example, a packet with two labels can use the top label to forward the packet through switches outside an organisation, the bottom can be used to route the packet inside the organization to reach the destination.

(it is similar to conventional hierarchical routing)

RARP (Reverse address resolution Protocol)

↳ it used to map Physical address to IP address.

→ it is reverse of ARP.

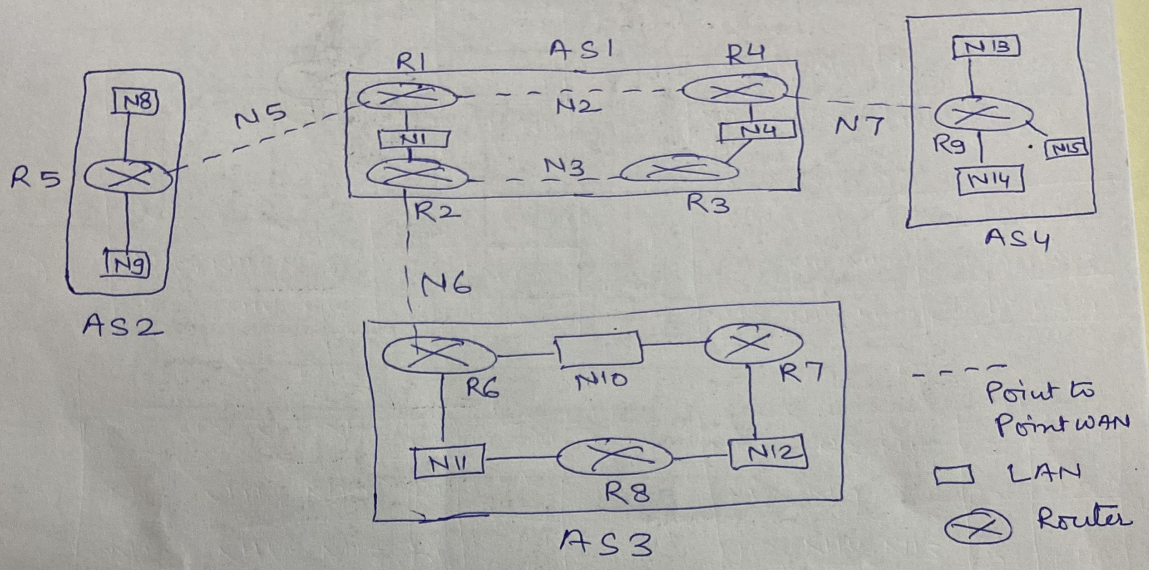
→ RARP was developed in early days of computer networking as a way to provide IP addresses to diskless workstation or other device that could not store their own IP address.

→ With RARP, the device would broadcast its MAC (Physical) address and request an IP address. and RARP server on the n/w would respond with corresponding IP address.

→ RARP used in past, it is replaced by DHCP.

Border Gateway Protocol (BGP) :-

↳ used for interdomain routing



→ Above example is internet with four autonomous system. AS2, AS3 and AS4 are stub autonomous system, AS1 is transient one. (only one connection to other AS)

→ Data exchange between AS2, AS3 and AS4 should pass through AS1.

→ Each autonomous system run OSPF or RIP in AS

→ Each router know how to reach a n/w that is in its own AS, but it does not know how to reach a n/w in another AS.

→ to enable route a packet to any n/w install a variation of BGP called External BGP (eBGP) on border router.

install second variation of BGP called internal BGP (iBGP) on all routers.

→ which means ~~on~~ all ~~internal~~ boarder routes install three routing Protocol (eBGP, iBGP, OSPF/RIP).

→ All internal run two (iBGP, OSPF/RIP).

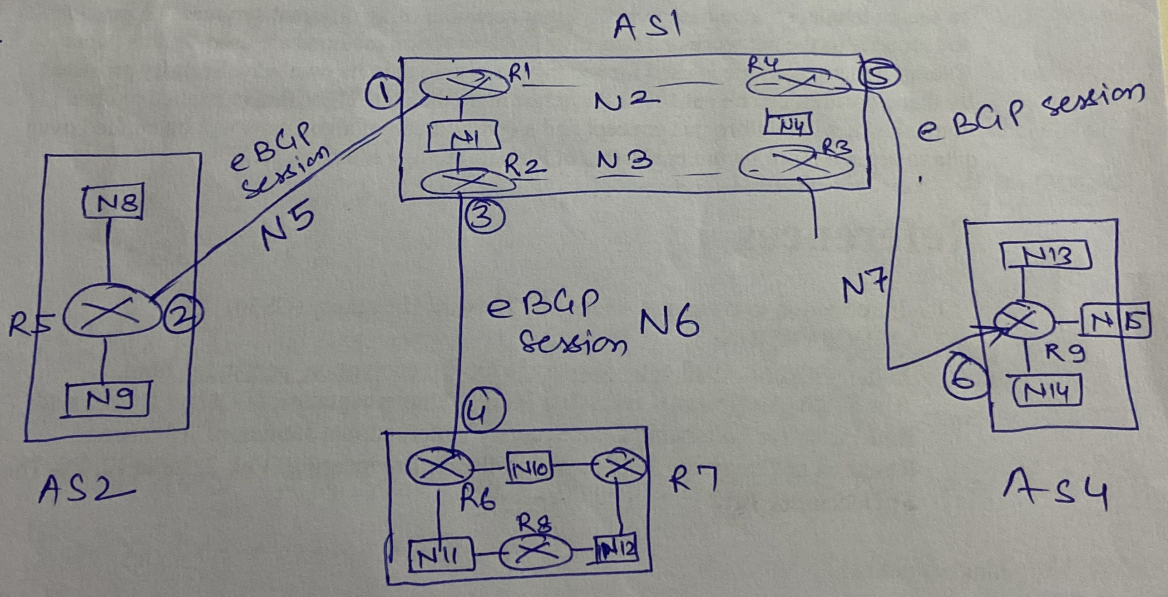
Operation of External BGP

it is kind of Point to Point protocol. uses TCP connection using well known Port no - 179.

→ in other words pair of Client and server processes.

→ Two routes that run BGP Process called BGP Speakers or Peers.

Ex.



	Network	Next	AS
①	N1, N2, N3, N4	R1	AS1
②	N8, N9	R5	AS2

⑤	N1, N2, N3, N4	R4	AS1
⑥	N13, N14, N15	R9	AS4

③	N1, N2, N3, N4	R2	AS1
④	N10, N11, N12	R6	AS3

In this example, three pairs R1-R5, R2-R6, and R4-R9.

→ The connection between these pairs is established over three Physical WAN (N5, N6, N7).

→ TCP logical connection to be established, three three session will be created for exchanging the information.

→ The circle no. represents sending router in each case.

→ for example msg no. 1 is sent by router R1 and tells router R5 that N1, N2, N3 and N4 can be reached through router R1 (R1 gets this info^n from the corresponding intradomain forwarding table).

→ Router R5 can now add these pieces of info^n at the end of its forwarding table. When R5 recieve any packet destinied for these four n/w, it can use its forwarding table and find that the next router is R1.

issue ① R5 does not known how to route packets destinied for n/w in AS3 and AS4, same for R6 and R9 are in same situation as R5.
R6 does not known AS4 and R9 does not know in AS3.

② non-border route does not known to route a packet destinied for any n/w in AS.

Sol^n ⇒ To address we need to allow all router need to run iBGP.

Operation of internal BGP (iBGP):- (4)

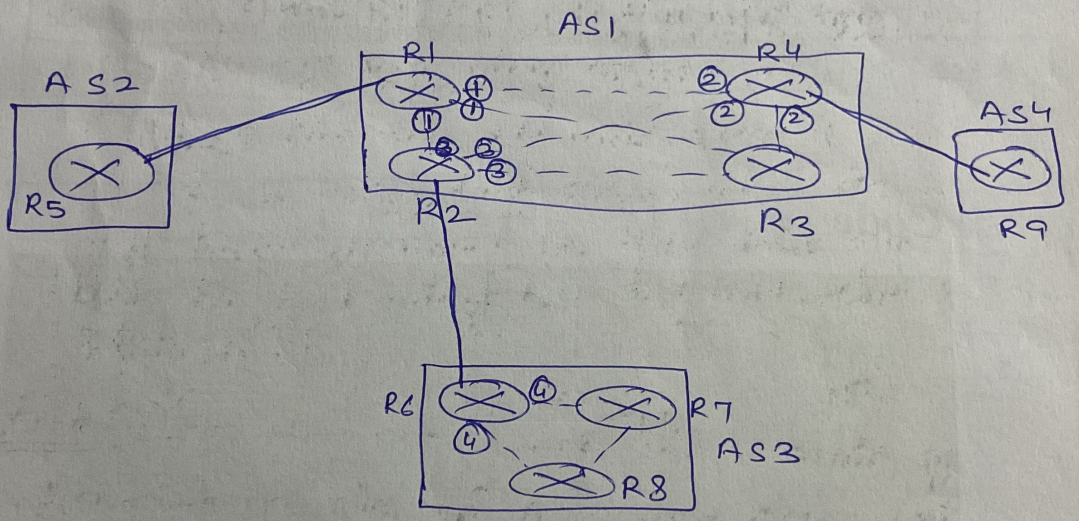
→ Same as eBGP for TCP connection and Port no.

→ but it create a session bet^n any Possible pair of routers inside an AS.

→ if AS has only one router, there cannot be an iBGP session.

→ for example we cannot create iBGP session in AS2 or AS4.

→ if there are n- routers in AS then there should be $(n \times (n-1)/2)$ iBGP session in AS fully connected Mesh to prevent loops in AS.



①

N/W	Next	AS
N8, N9	R1	AS1, AS2

②

N/W	Next	AS
N13, N14, N15	R4	AS1, AS4

③

N/W	Next	AS
N10, N11, N12	R2	AS1, AS3

④

N/W	Next	AS
N1, N2, N3, N4	R6	AS3, AS1

digit.

table

Path table for R1

Network	Next	Path
N8, N9	R5	AS1, AS2
N10, N11, N12	R2	AS1, AS3
N13, N14, N15	R4	AS1, AS4

R2

N8, N9	R1	AS1, AS2
N10, N11, N12	R6	AS1, AS3
N13, N14, N15	R1	AS1, AS4

R3

N8, N9	R2	AS1, AS2
N10, N11, N12	R2	AS1, AS3
N13, N14, N15	R4	AS1, AS4

R4

N8, N9	R1	AS1, AS2
N10, N11, N12	R1	AS1, AS3
N13, N14, N15	R9	AS1, AS4

R5

N1, N2, N3, N4	R1	AS2, AS1
N10, N11, N12	R1	AS1, AS2 AS3
N13, N14, N15	R1	AS2, AS1 AS4

R6

N1, N2, N3, N4	R2	AS3, AS1
N8, N9	R2	AS1, 2, 3
N13, N14, N15	R2	3, 1, 4

R7

1, 2, 3, 4	R6	3, 1
8, 9	R6	3, 1, 2
13, 14, 15	R6	3, 1, 4

R8

1, 2, 3, 4	R6	3, 1
8, 9	R6	3, 1, 2
13, 14, 15	R6	3, 1, 4

R9

1, 2, 3, 4	R4	4, 1
8, 9	R4	4, 1, 2
10, 11, 12	R4	4, 1, 3

Interdomain forwarding Tables

for simplicity it is assumed that RIP as the interdomain routing protocol.

→ default destinations are indicated as zero.

→ Cost value :- set the cost to the foriegn networks at the same cost value as to reach the first AS in Path.

→ Ex. the cost for R5 to reach all n/w in other AS is the cost to reach N5.

Table for R1

Dest.	Next	cost
N1	—	1
N4	R4	2
N8	R5	1
N9	R5	1
N10	R2	2
N11	R2	2
N12	R2	2
N13	R4	2
N14	R4	2
N15	R4	2

Table for R2

N1	—	1
N4	R3	2
N8	R1	2
N9	R1	2
N10	R6	2
N11	R6	1
N12	R6	1
N13	R3	3
N14	R3	3
N15	R3	3

Table for R3

N1	R2	2
N4	—	1
N8	R2	3
N9	R2	3
N10	R2	2
N11	R2	2
N12	R2	2
N13	R4	2
N14	R4	2
N15	R4	2

R4

N1	R1	2
N4	—	1
N8	R1	2
N9	R1	2
N10	R3	3
N11	R3	3
N12	R3	3
N13	R9	1
N14	R9	1
N15	R9	1

R5

N8	—	1
N9	—	1
0	R1	1

R6

N10	—	1
N11	—	1
N12	R7	2
0	R2	1

R7

N10	—	1
N11	R6	2
N12	—	1
0	R6	2

R8

N10	R6	2
N11	—	1
N12	—	1
0	R6	1

R9

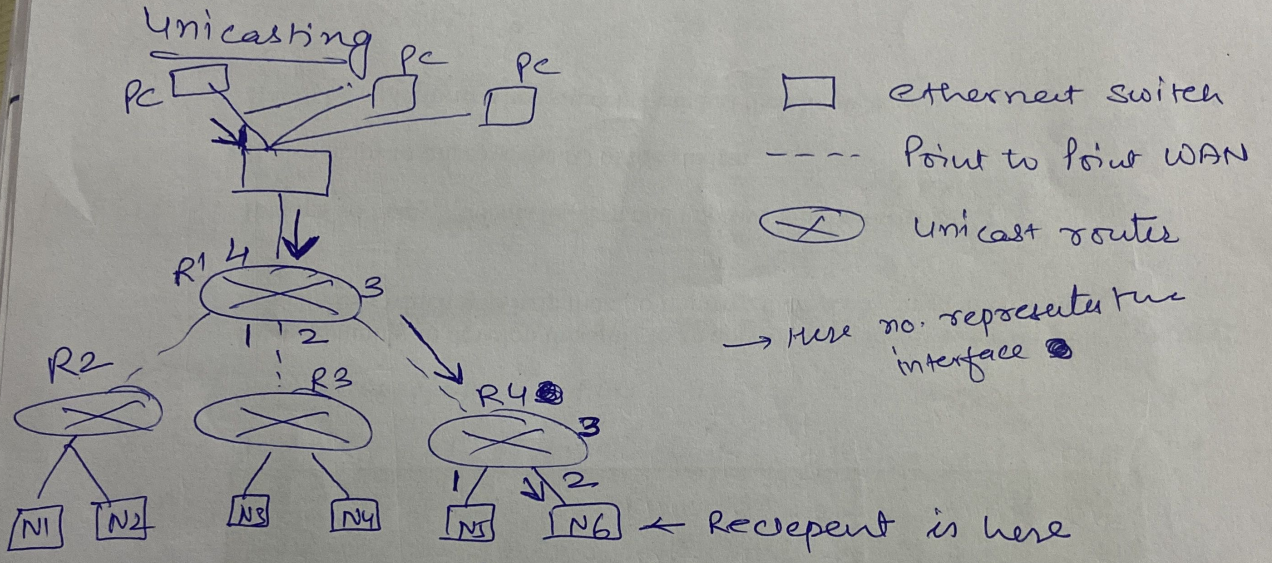
N13	—	1
N14	—	1
N15	—	1
0	R4	1

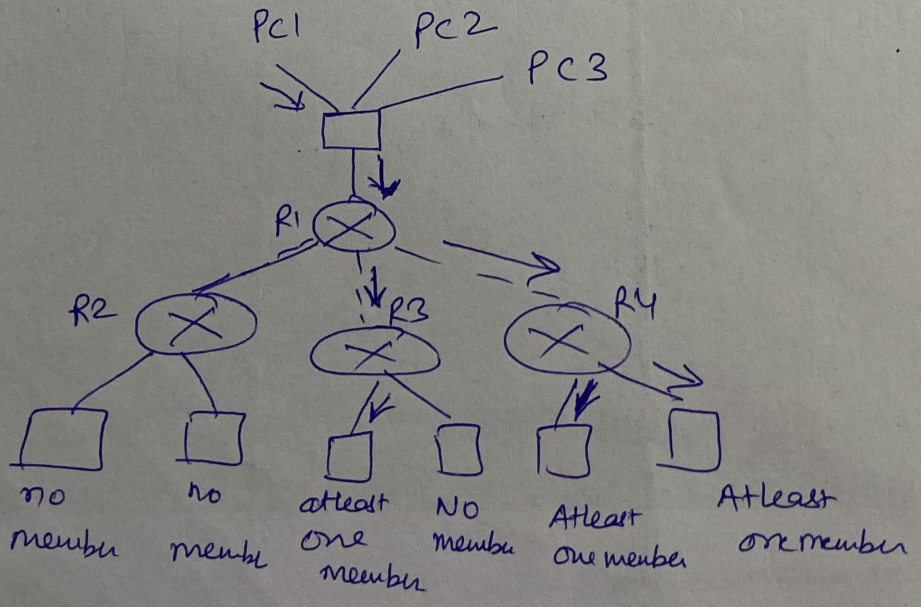
Multicasting

→ in unicasting one source and one destination

→ multicasting one source and group of destination.

→ in multicasting source address is a unicast address, but the destination is a group address, a group of one or more n/w in which there is at least one number of the group that is interested in recieving the multicast datagram.





Multicasting → one packet which is duplicated by router

Multiple unicasting → several packets starts from the source.

Broad casting → one to all relation

~~Internet group management protocol (IGMP):-~~

Application of multicasting

1. Access to Distributed databases
2. information Dissemination
3. Teleconferencing
4. Distance Learning

IGMP (internet group management protocol):-

The protocol which is used for collecting info about group membership is the IGMP. it is defined at n/w layer, it is one of the auxilary protocol, like ICMP, which is considered part of IP.

→ IGMP encapsulated in an IP datagram.

→ IGMP have two types of message → 1. query 2. ~~resp~~ report.

Query msg → Periodically msg sent by a router to all hosts attached to it to ask them to report their interest about membership in groups.

ery msg can be take one of three forms (3)

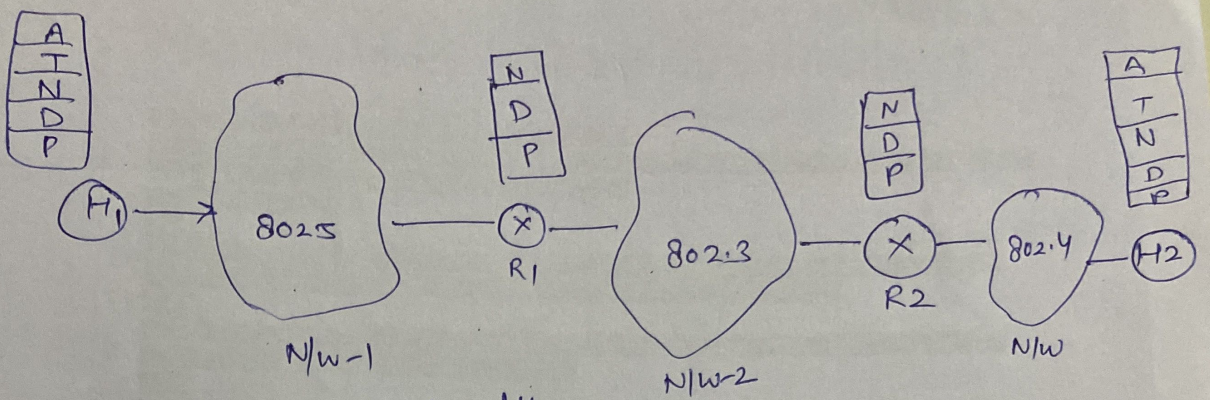
(a) General ~~msg~~ query msg:- sent about membership in any group.

(b) A group specific query msg is sent from a router to ask about the membership related to a specific group.

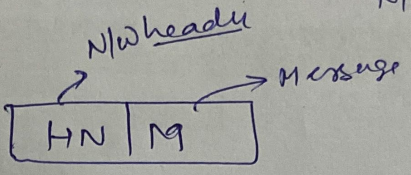
(c) source and group specific query msg is sent from a router to ask about the membership related to specific group when msg comes from a specific source or sources.

(2) Report Message:- A report msg is sent by a host as a response to a query message.

... when it reverse.

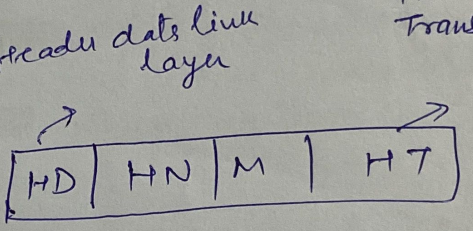


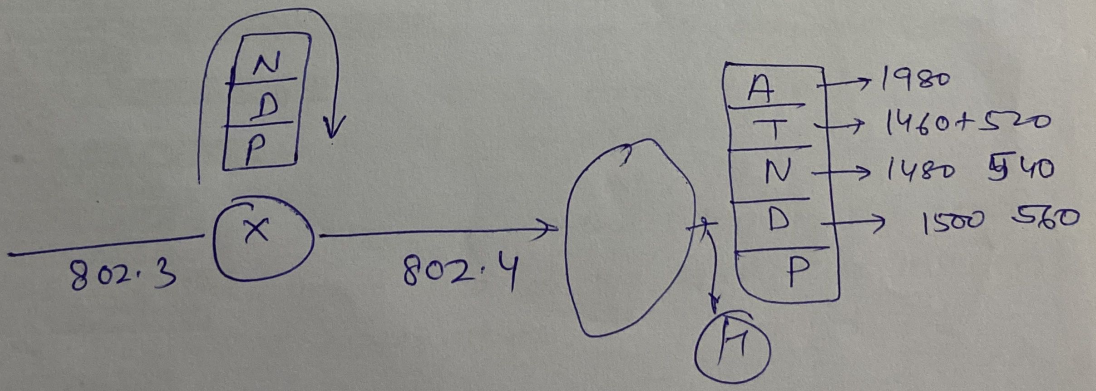
Packet



⇒ M Contains application data + Application Header + Transport header.

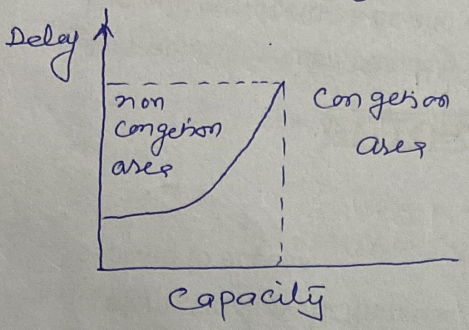
At data link layer frams

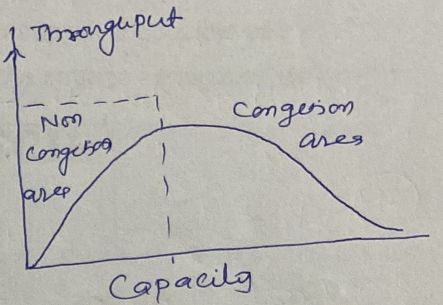




Congestion Control

Too many Packets in any Part of the network can ultimately introduced packet delay and loss that degrade the Performance. This situation is called congestion.





Congestion Prevention

1. Retransmission Policy: some times it should be avoided. if sender feels that a sent Packet is lost or corrupted, the Packet needs to be retransmitted, which may increase congestion in n/w.

2. Acknowledgement Policy:- The acknowledgement ~~Policy may also affect Congestion~~. imposed by the reciver may ~~slow down the sender~~ affect congestion. if reciever does not ack to every Packet then it may be control of congestion.

3. Discarding Policy: A good discarding Policy by the router may Prevent the congestion and at the same time may not harm the integrity of transmission.

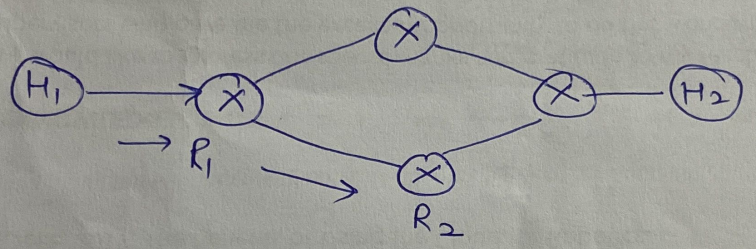
4. Admission Policy: A admission Policy, which is a quality of service mechanism, can also prevent congestion in virtual - circuit n/w.

ngestion control in virtual circuit:-

in VC subnet the congestion can be controlled by a procedure called as "Admission control".

→ once congestion has been signaled, no more virtual circuit are set up until the problem has gone away

→ ex. in telephone system, when a switch gets overloaded, it also practices admission control by not giving dial tones.



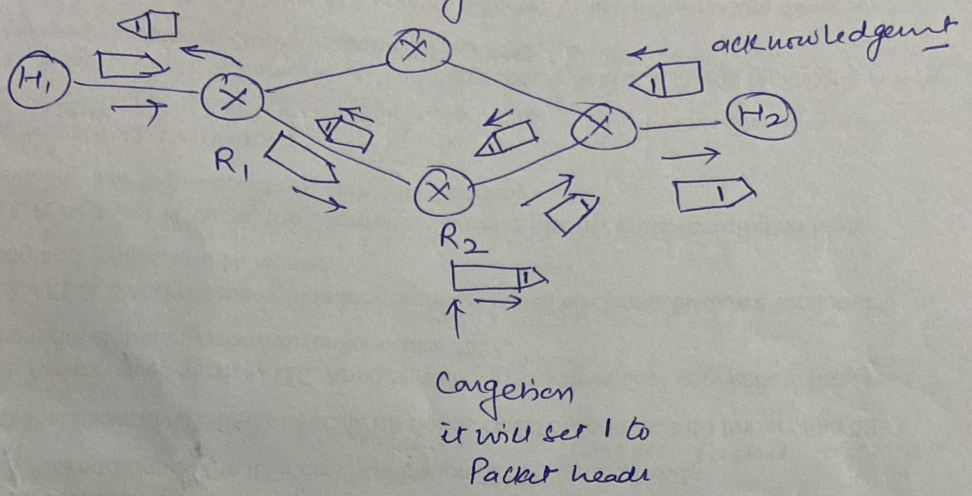
VC is not formed, if R_2 is congested.

Congestion control in data gram subnet

1. warning bit
2. Chock packet
3. Hop by Hop Chock packet
4. load shedding
5. RED (Random early detection)

Warning bit

The Idea is to reduce the speed of transmission of Packet in the n/w by sender

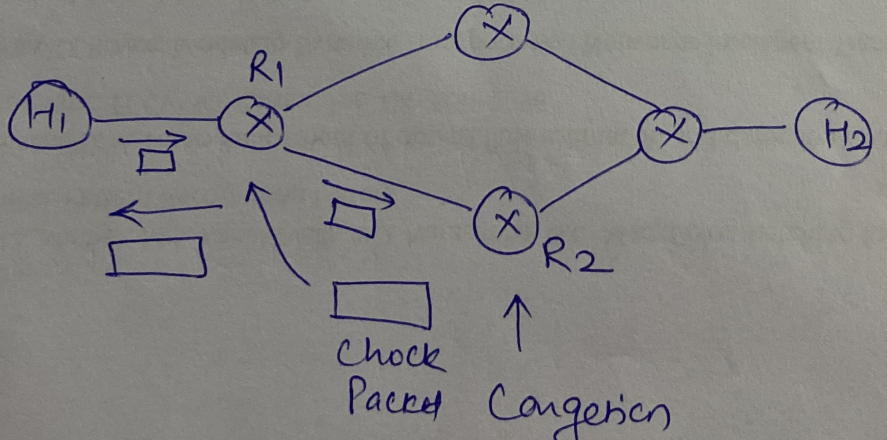


* if warning bit = 1 in reply, the sender reduce its speed of transmitting data.

Drawback ⇒ delay between warning is max.

(2) Chock Packet

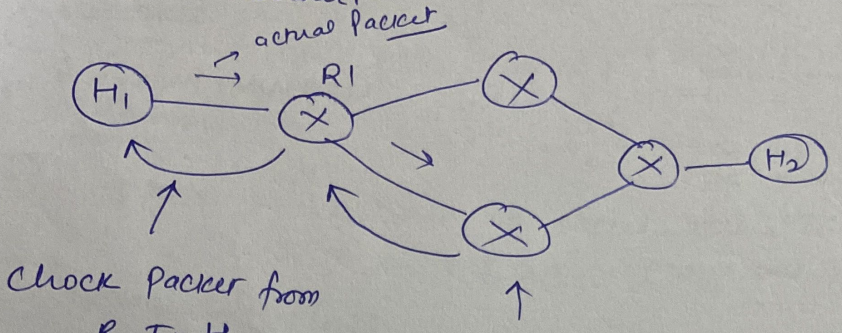
* Chock Packet is a Packet sent by a node to the Source inform it of Congestion.



due to less delay, it is better in comparsion to warning bit

Hop by hop Choke Packet

send the Choke Packet to Previous router only rather than sender.



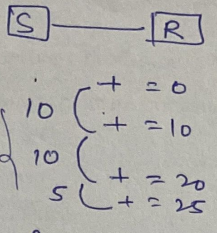
Delay is less in comparision to Choke Packet method.

(4) Load Shadding :- Discard the Packet based on Priority

(5) RED (Random Early detection) :- Before the congestion occurs, take the necessary steps so congestion does not occur. (Congestion Prevention).

QoS (Quality of service Parameter):→ (5)

1. Delay
2. Throughput
3. Bandwidth
4. Jitter :- Variation in Packet arrival time or delay in arrival time. (Difference of arrival time of two successive Packet
5. Reliability / loss



QoS depends on application

	Delay	throughput	Reliability	Jitter
File transfer	M	M	H	M
Mail transfer	M	M	H	M
Audio service	L	H	M	L
Video service	L	H	M	L

if the delay is varying fast then more jitter

Method of Achieving QoS

1. over provisioning
2. Buffering
3. Traffic shapping — Leaky Bucket / Token Bucket
4. Resource reservation Protocol.

(5)

Over provisioning:- Allocate sufficient resources like memory, CPU etc.

so it is built a network with enough capacity for whatever traffic will be thrown at it.

like telephone n/w system.

Problem :- Lot of cost (expensive)

(2) **Buffering**

↳ Packet scheduling

FIFO or FCFS

one queue

once a packet in first it will out first

Fair queuing

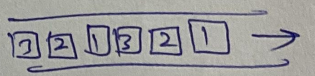
weighted fair queuing

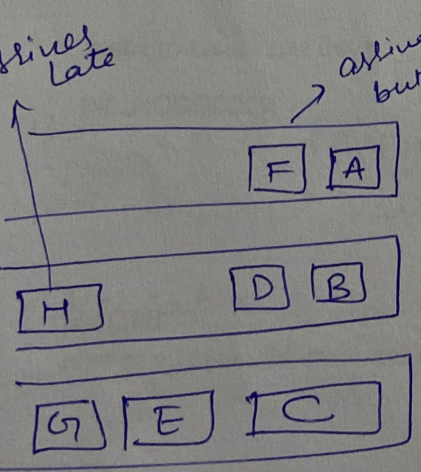
no. of byte is weight for WFQ

1 2 3

Round Robin service

input queue





fair queuing

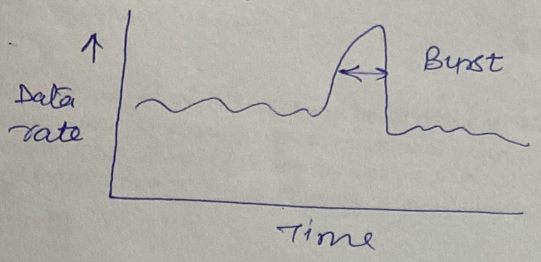
Packet	arrival time	length	FT	output order
A	0	8	8	1
B	5	6	11	3
C	5	10	10	2
D	8	9	20	7
E	8	8	14	4
F	10	6	16	5
G	11	10	19	6
H	20	8	28	8

finish time ↑ output order ↑

A_i → arrival time L_i → length weight is 2
F_i → finish time W → weight

in weighted $F_i = \max(A_i, F_{i-1}) + L_i/W$

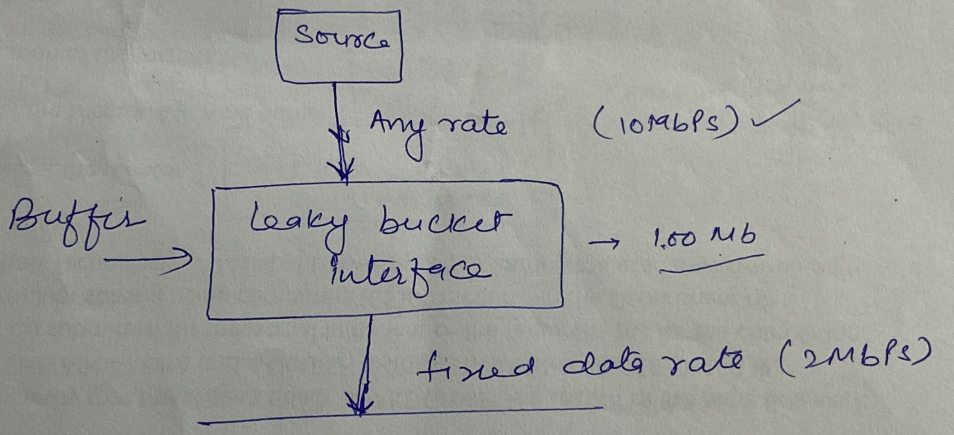
Traffic shapping



Burst (large amount of data in short time reason for congestion)

To avoid congestion due to burst we shape the transmission rate.

(1) Leaky Bucket



The idea of leaky bucket is that it sends the data with constant rate to the n/w by using buffer.

Calculation of time t which after bucket will full:

$10 \swarrow^{in}$ $2 \rightarrow^{out}$ = ~~Data transfer to leaky bucket + data stored in leaky bucket~~

$(10-2) = 8$

$8 \times 10^6 \times t = 100 \times 10^6$ ⇒ ~~10×10^6 bits/sec $\times t = 100 \times 10^6 + 2 \times 10^6 \times t$~~

$t = 100/8$ sec.

Token Bucket

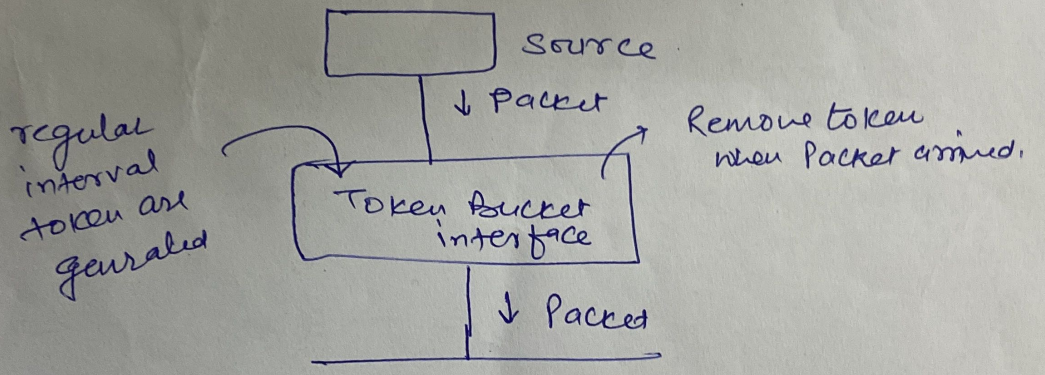
In this tokens are generated.

Step-1 in regular interval tokens are thrown into bucket f.

Step-2 The bucket has max capacity f

Step-3 if Packet is ready, then a token is removed from bucket and Packet is sent

Step-4 if there is no token in the bucket, the Packet cannot be sent.



Ex. Lets 5 tokens/sec. are generated

Data is transfered by capacity of token.

Let Suppose 1 kbits data transfered to n/w by capacity of 1 token.

Data rate = 1 × 5 kbps = Token generation rate

= 5 kbps

when the system is idle, tokens are keep generated by token bucket interface

10 sec. no. of token = 50

Token Bucket capacity = 50 token × 1 kbps
= 50 kbps.

Assume that the high speed of token bucket is M kbps.

The time for which token bucket send the data with high speed (Burst time)

Capacity of token bucket (c) + Token generation rate (e) × t

= Max data rate of token bucket (M) × t

= c * e × t = M × t

= $t = \frac{c}{M-e}$

Q. Communication on 6 Mbps is regulated by token bucket. Token bucket is filled with 1 Mbps rate. Initially it is filled with capacity 8 MB. How long can the computer transmit at the full 6 Mbps.

e = 1 Mbps , c = 8 Mbps

M = 6 Mbps $\Rightarrow t = \frac{8}{6-1} = \frac{8}{5} = 1.6$ sec.

(10)

Imagin a flow specification that has max. packet size 1000 byte. Token bucket rate of 10 MbPS. Token bucket size 1 MB and the max. transfer rate = 50 mbps. How long a burst can be at max. speed.

C =

$$t = \frac{1 \times 10^6}{(50-10) \times 10^6} = \frac{1}{40} = 25 \text{ msec.}$$

Packet Fragmentation :→

Each n/w or link imposes some max. size on its Packets. These limits have various causes among them

1. Hardware (e.g. the size of an Ethernet frame)
2. Operating system (all buffers are 512 bytes)
3. Protocols (e.g. the no. of bits in the packet length field)
4. Compliance with some (inter) national standered.
5. Desire to reduce error-induced retransmissions to some level.
6. Desire to prevent one packet from occupying the channel too long.

Max. Payload for some technologies are

Ethernet = 1500 bytes

802.11 = 2272 bytes

IP = 65,515 bytes.

* Host usually wants to send large Packets for reducing Packet overhead such as bandwidth wastages on header bytes.

→ A problem occur when Packet wants to travel through n/w whose max. Packet size is too small.

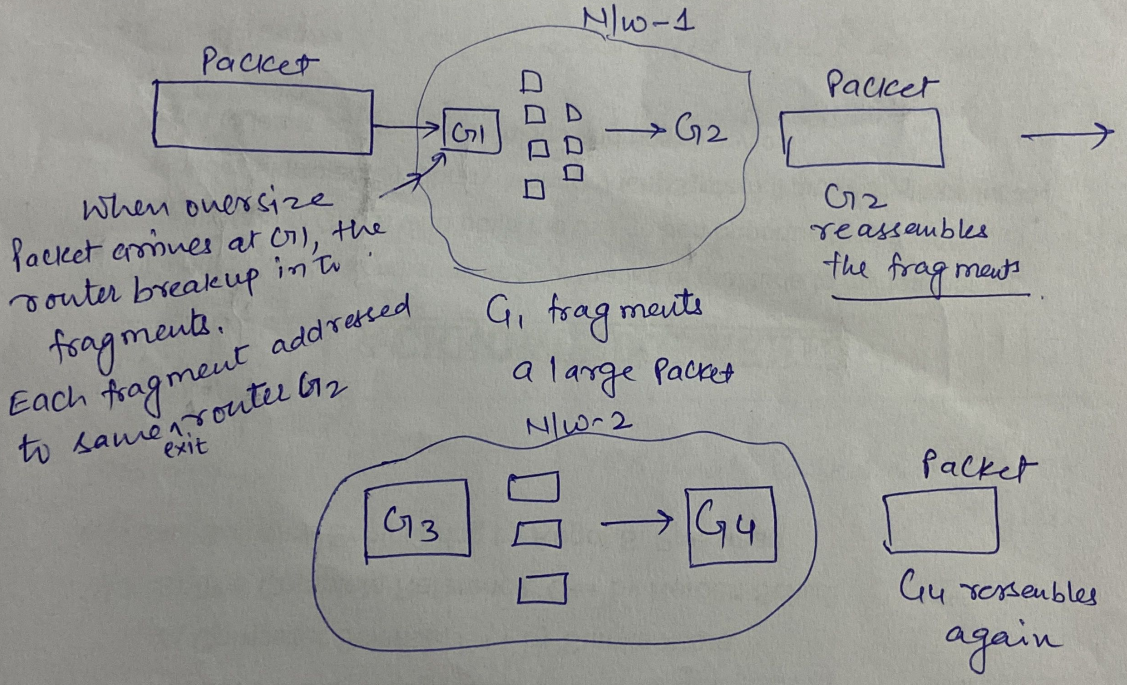
→ The solution is breakup the Packets in to fragments, Sending each fragment as a separate network layer Packet.

→ Converting a large object in small ~~objects~~ fragment is considerably easy but complex when it reverse.

There are two strategies exist for recombining the fragments back into the original packet.

- Transperent fragmentation
- Non transperent fragmentation

make all the fragmentation caused by "small packet" n/w transperent to any subsequent n/w through which the packet must pass on its way to ultimate destination.



Problems

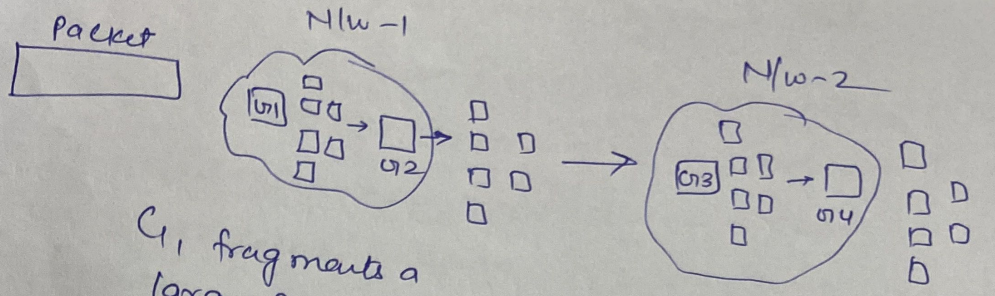
→ Exit router must know when it will recieve full information.

→ all packets must be exit from same router so they can be reassembled, the routes are constrained

→ Performance loose when routes are constained.

→ Sperately fragment and reassembled at all small packet n/w will not be worthful.

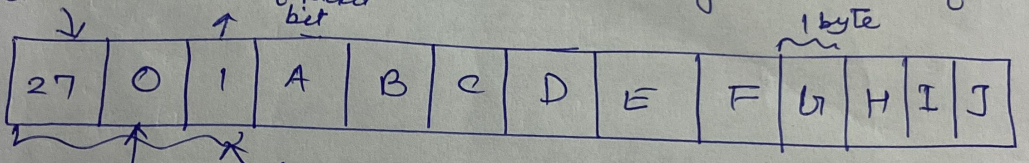
Non transperent fragmentation:-



G1 fragments a large Packet

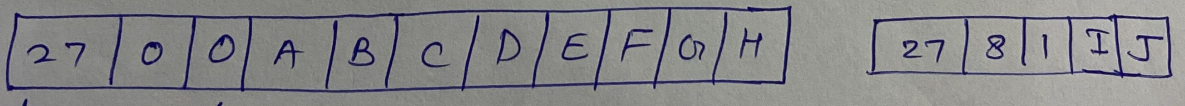
The fragments are not reassembled until the final destination (a host) is reached.

→ The Designe used by IP is to give every fragmented Packet no, an absolute byte offset with in the Packet. and a flag indicating it is end of Packet.

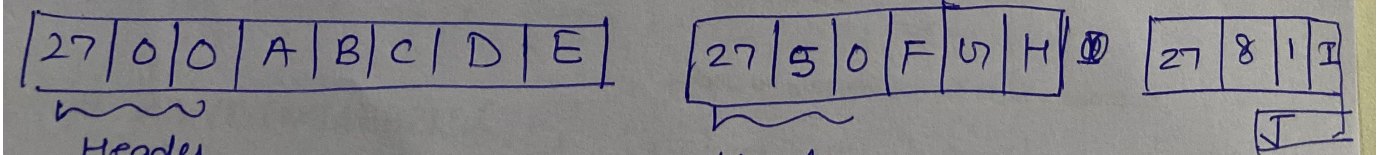


no. of first elimentary fragment in this Packet

Original Packet Containing 10 data bytes



Fragments after Passing through a n/w max. Packet size of 8 Payload bytes + header



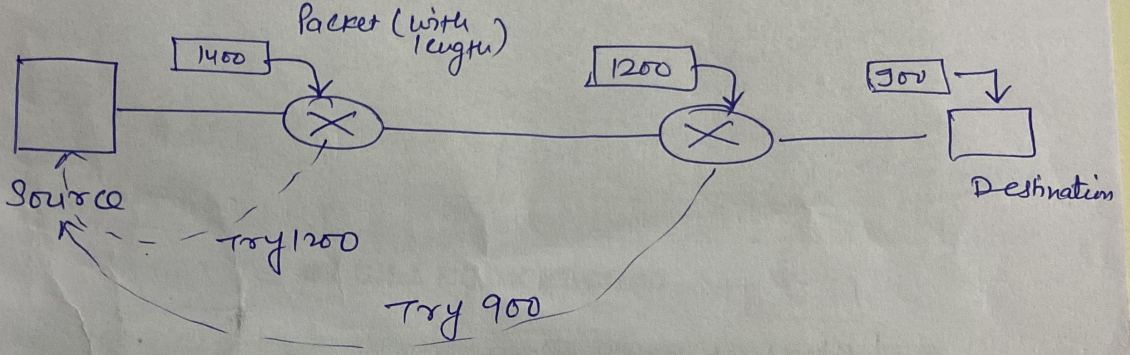
fragments after Passing through a size 5 gateway.

(4)

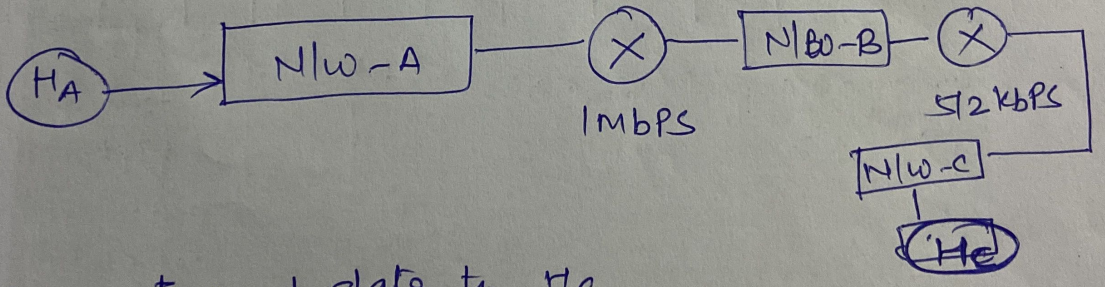
Modern solution used in internet is Path MTU discovery. In this strategy fragmentation is not allowed.

→ Each IP Packet is sent with its header bits set to indicate that no fragmentation is allowed to be performed.

→ if router recieves a packet that is too large, it generate an error packet, return it to the source and drop the packet.



Q.



→ H_A wants send data to H_C

→ Message containing 180 bytes of data. TCP layer prifix 20 bytes header. IP head is 20 byte and MTU size for N/W A, B and C are 1000 bytes, 100 bytes and 1000 bytes respectively.

(A) How many bytes including header are

delivered to the IP layer at the destination for 1- application message. (5)

Ans.

Message = 180 bytes

↓ 20 + 20
(TCP) (IP)

220 byte from Network-A

MTU N/W-A ⇒ 1000byte
220 < 1000byte

N/W layer header 60 60 60

220 − 20 = 200 (80+80+40)

200 bytes of (TCP + 180 byte data)
20

80 + 20	80 + 20	40 + 20

N/W layer header

So three packet will generate
2 are of 100, 1 of 60

⇒ Total 260 byte for each message.

(B) What is the rate through application data is transfered to host Hc

$$= \frac{180}{260} \times 512$$

$$= \frac{9}{13} \times 512 = 354.5 \text{ kbps}$$

TCP message consisting of 2100 bytes.
it is Pass to IP for delivery across the n/w

MTU for 1st N/w = 1200 bytes / frame

2nd = 400 bytes / frame

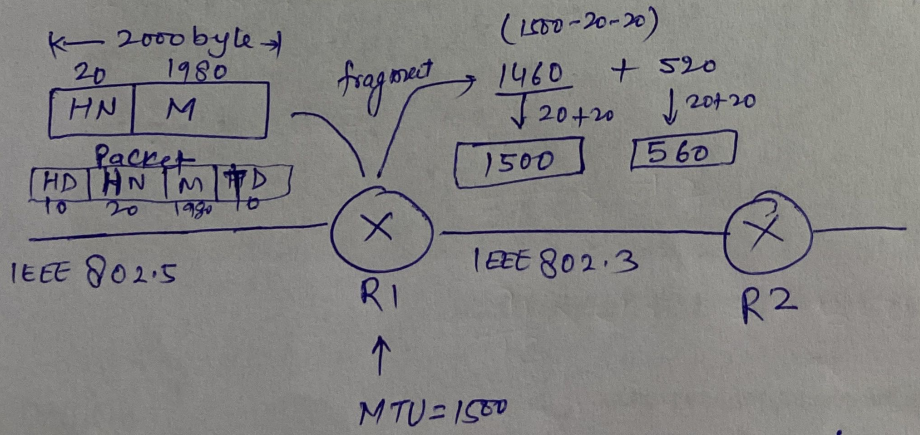
Ans. excluding n/w overhead.
↓
means header inclusion

2100 bytes = 1200 + 900
↓+20 ↓+20

N/w layer — (1) 1220 920
↓-20 ↓-20

N/w layer (2) 400+400+400 400+400+100
↓+20 each ↓+20 each
420+420+420 420+420+120

Total overhead = 6 × 20 = 120 bytes

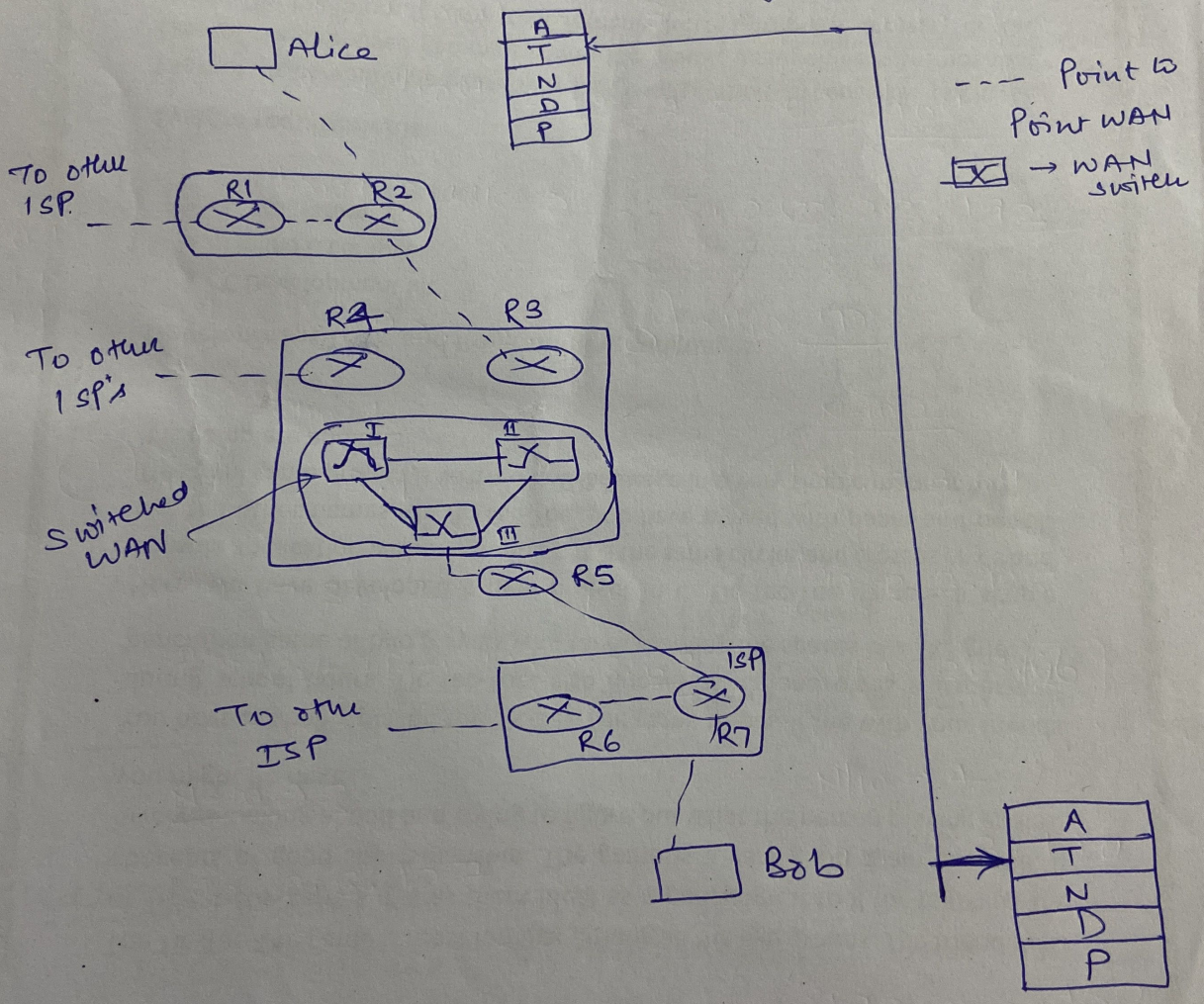


Overhead at R1 = 20 byte N/w layer + 20 byte DLL frame = 40 byte
R2 = 40 + 40 = 80 bytes for two frames

Transport Layer :-

it provides process to process communication between two application layer, one at local host and other at remote host. This is also called logical connection, which means two application layer, which can be located in different part of the globe.

Logical connection at the Transport layer :-



* Alice and Bob two end system use the service of transport layer, all ~~oth~~ intermediate route use only the first three layers.

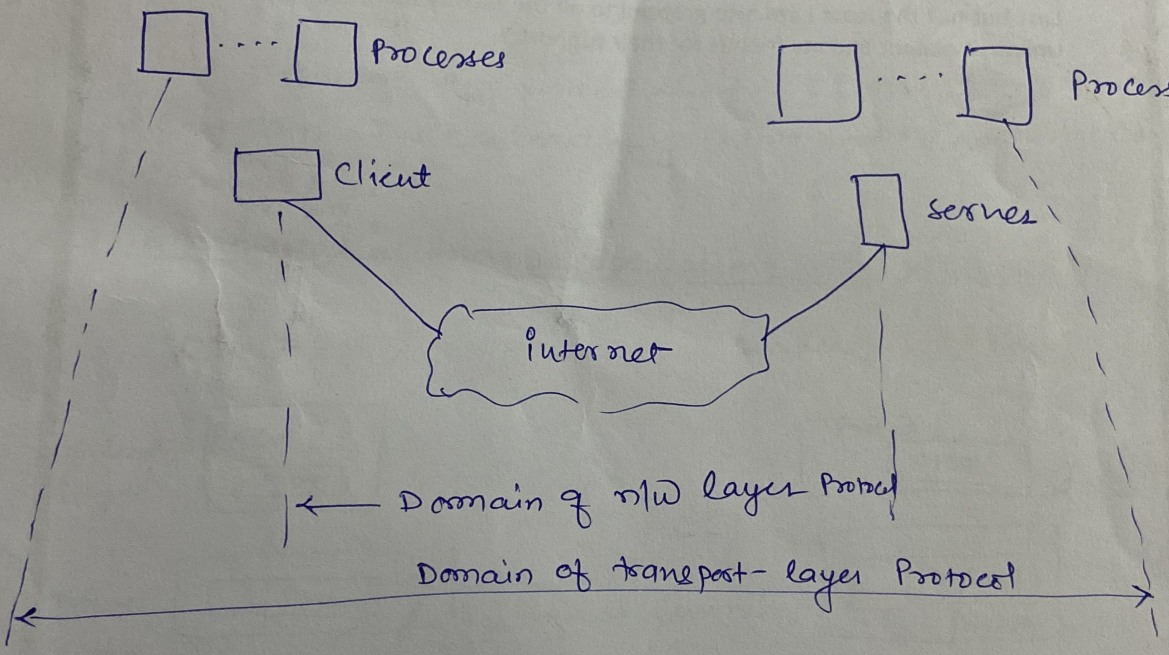
Transport layer services:-

① Process to Process communication

→ Process is an application layer entity (running program) that uses the services of the transport layer.

Network layer ⇒ host to host comm^n.

↳ can deliver the msg to destination, however it is the incomplete delivery, handling to the correct Process at destination, is working of Transport layer.



② Addressing Port no.

For communication in, multiprograming and multiuser environment we need to define local host, local Process, remote host and remote Process.

→ local host and Remote host have IP (defined by)

→ But remote Process and local Process defined by TCP have (0 to 65,535) Port no. Port no.

ICANN Ranges

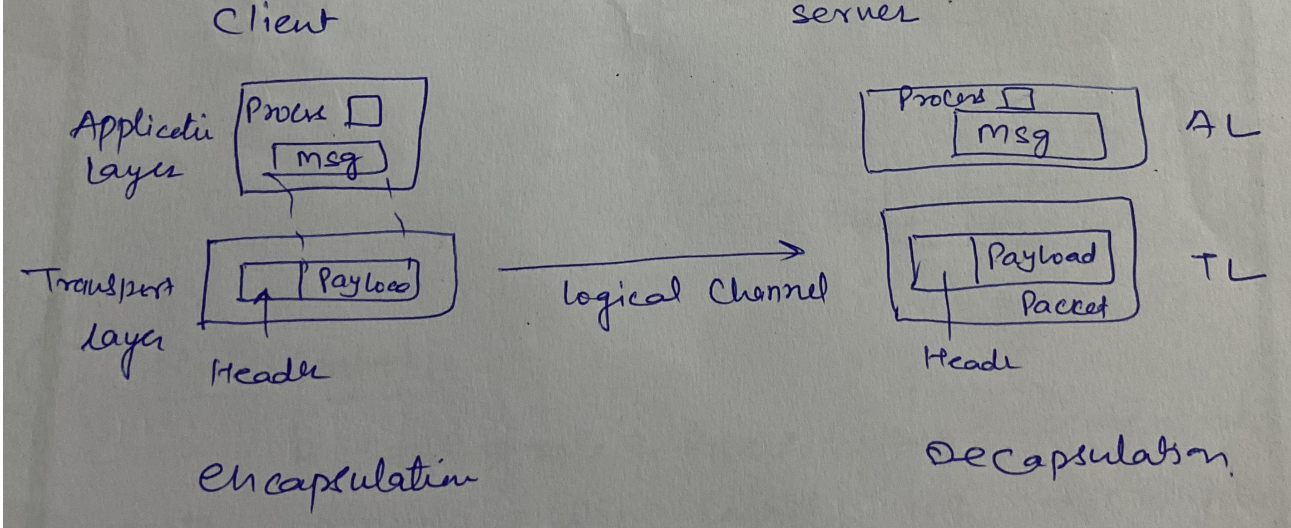
divided into three ranges

- **Well-known** (0 – 1023)
  - Controlled by ICANN
  - (Well known port)
- **Registered** (1024 – 49151)
  - Are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication
- **Dynamic or Private** (49152 – 65535)
  - are neigther controlled nor registered. They can be used as temporary or Private Port numbers.

④ Socket address

A Transport layer protocol needs IP and Port no. to make a connection. The combination of Port no. and IP address called Socket address

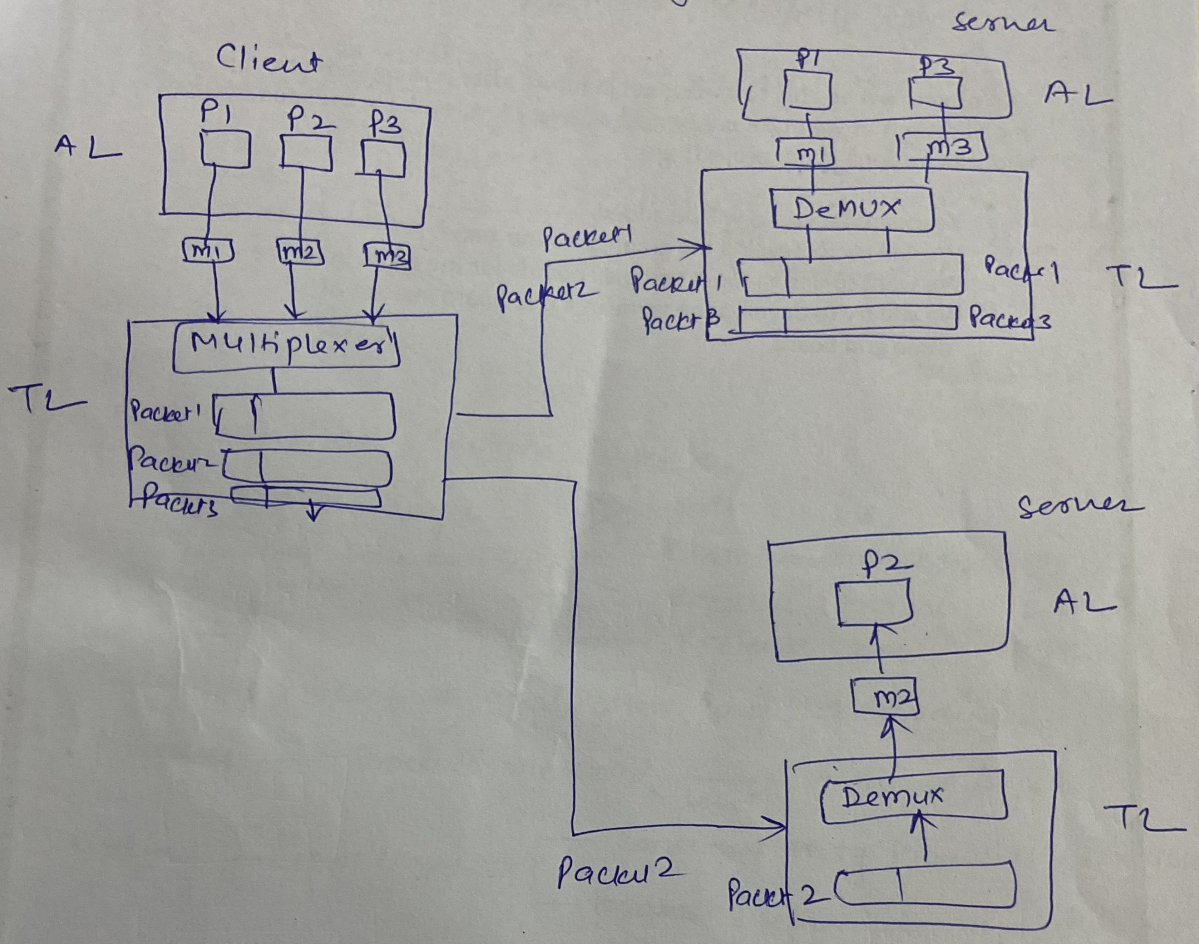
⑤ Encapsulation and Decapsulation



(6) Multiplexing and Demultiplexing :→

Many to one

one to many



(7) flow control :-

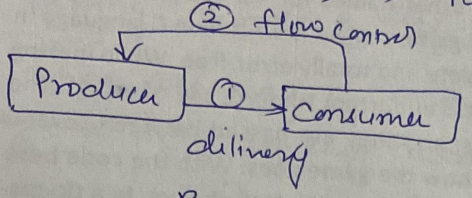
if sending rate of packet higher than transmission rate. → need of flow control., we need to prevent the data items at the consumer site

Pushing or Pulling | flow control at transport layer | Buffer | sequence no. | Acknowledgment

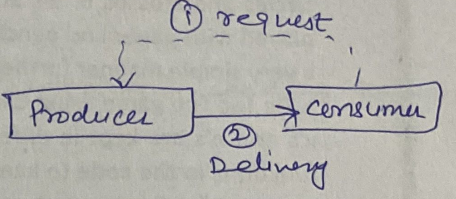
Pushing or Pulling

→ if sender delivers items whenever they are produced, without a prior request from consumer ⇒ Pushing.

→ if Producer delivers the items after the consumer has requested them, ⇒ Pulling.



Pushing



Pulling

(b) flow control at transport layer :-

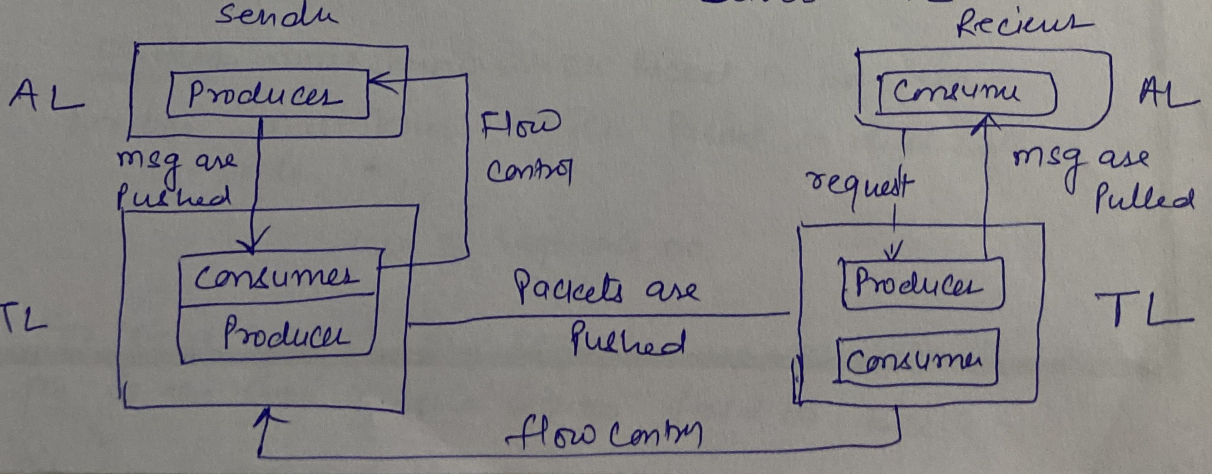
Transport layer dealing with four entities
- sender process
- sender transport layer
- Reciever process
- Reciever transport layer

⇒ Sending process at application layer ⇒ Producer

⇒ Producer → Produce message → send to → transport layer

⇒ Sending transport layer
- Consumed msg Produced by Producer
- encapsulate msg in Packet and send to reciever TL.

⇒ reciever transport layer
- Decapsulate msg
- Deliver to TL



(7) Buffer ⇒ flow control can be implemented by two buffer one at sender transport layer and another at receiver transport layer.

⇒ Producer - Consumer Problem

→ When producer buffer full, it inform to AL to stop the Passing Chunks of msg.

→ When Recieving TL is full, it info° the sending transport layer to stop sending Packet.

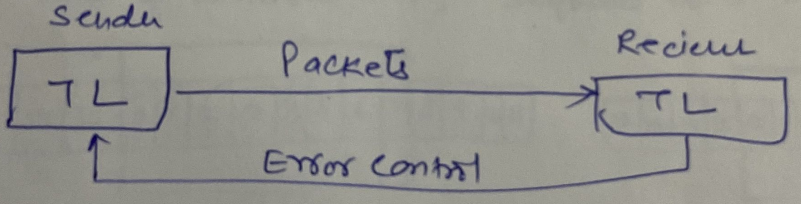
(8) Error control:- Reliability can be achieved to add Error control service to TL. it is responsible for

(a) Detecting and discarding corrupted Packets.

(b) Keeping track of lost and discarded Packets and resending them.

(c) Recognizing duplicate Packets and discarding them.

(d) Buffering out of order Packets until the missing Packets arrive.



(i) Sequence Number

Sender must know which Packet to be resent

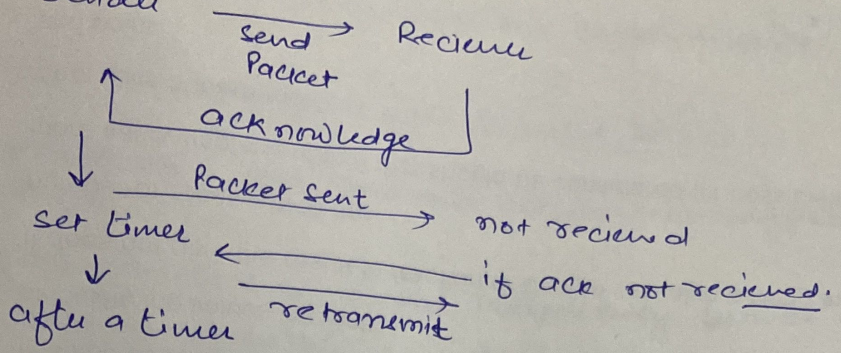
Reciem must know which Packet is duplicate or out-of-order

⇕

use of sequence no.

For error control, the seq. no. are modulo 2^m, where m is the size of the seq. no field in bits.

Acknowledgment :-



⑨ Combination of flow and Error Control :→

flow control requires → Two buffer

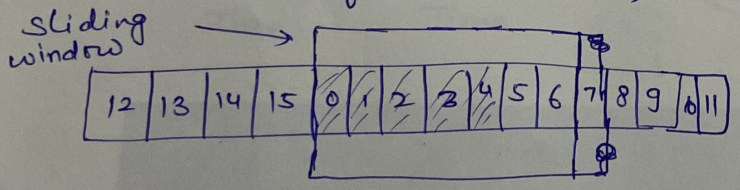
Error control requires → sequence no.

⇓

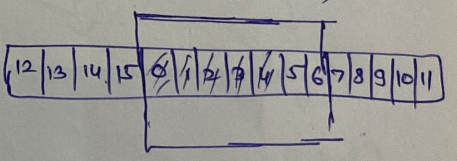
Make combine to both

⑨ Sliding window

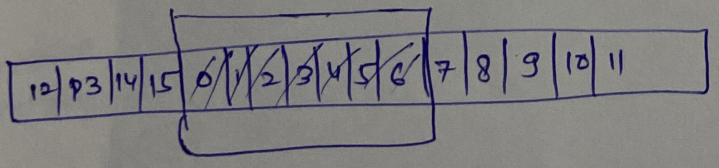
Ex. Size of window = 7, Sequence no. = module 16 (m=4)



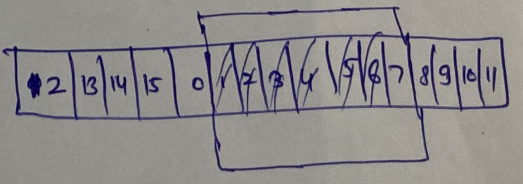
4 - Packet send



5 - Packet sent



7 - Packet sent



Packet-0 has recieved ack.

Congestion Control

TCP also performs the Congestion Control

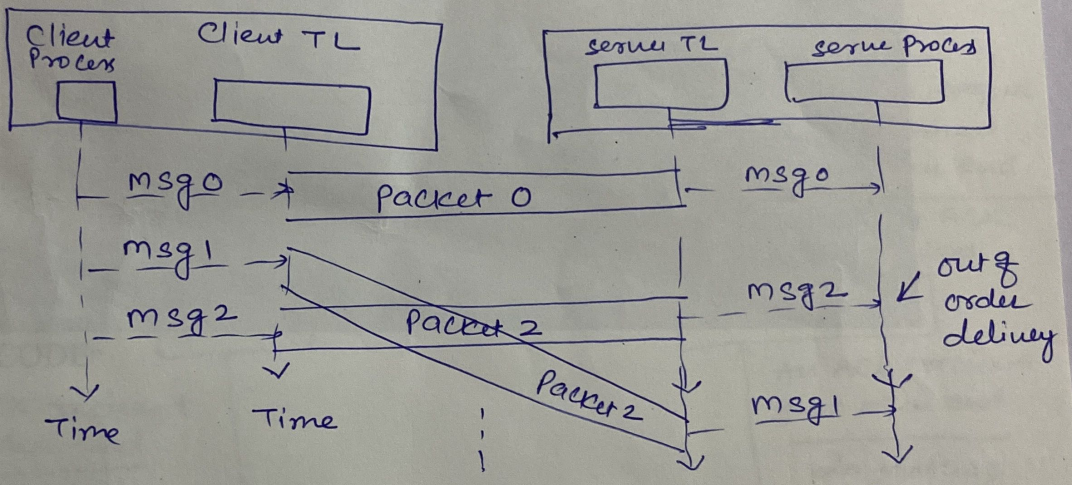
(ii) Connectionless and Connection-oriented service:-

Connectionless and Connection oriented have different Perception at TL.

→ Connectionless ⇒ means independency between Packets

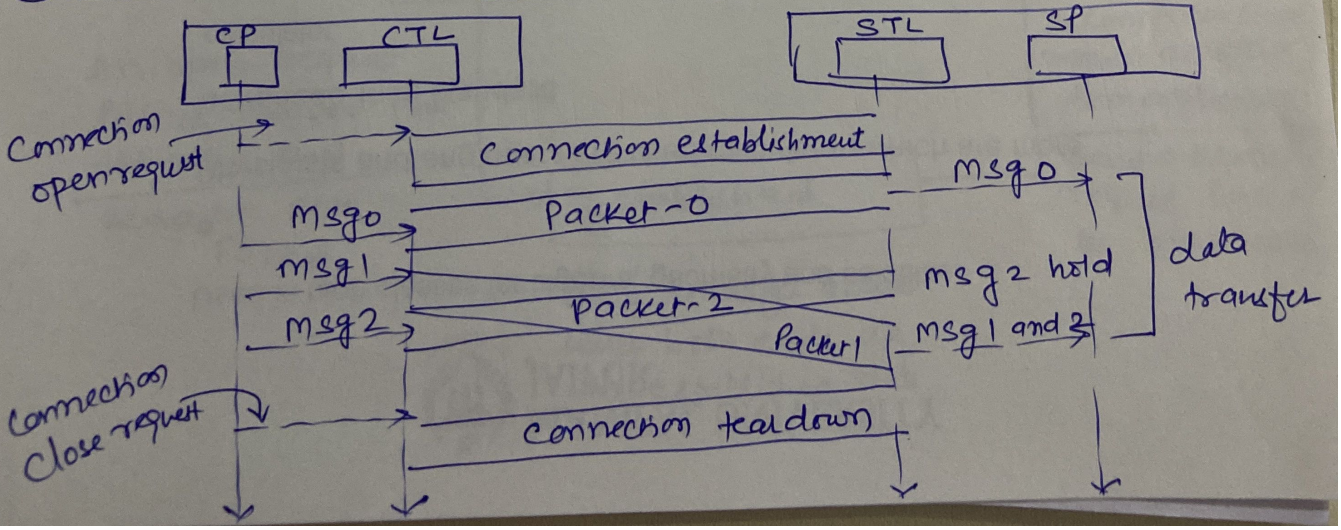
→ Connection oriented ⇒ dependency

(a) Connection less service



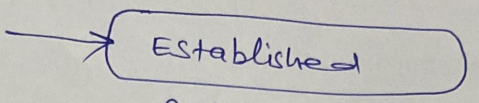
no dependency of Packets at the transport layer.

(b) Connection oriented service (logical connection establishment)



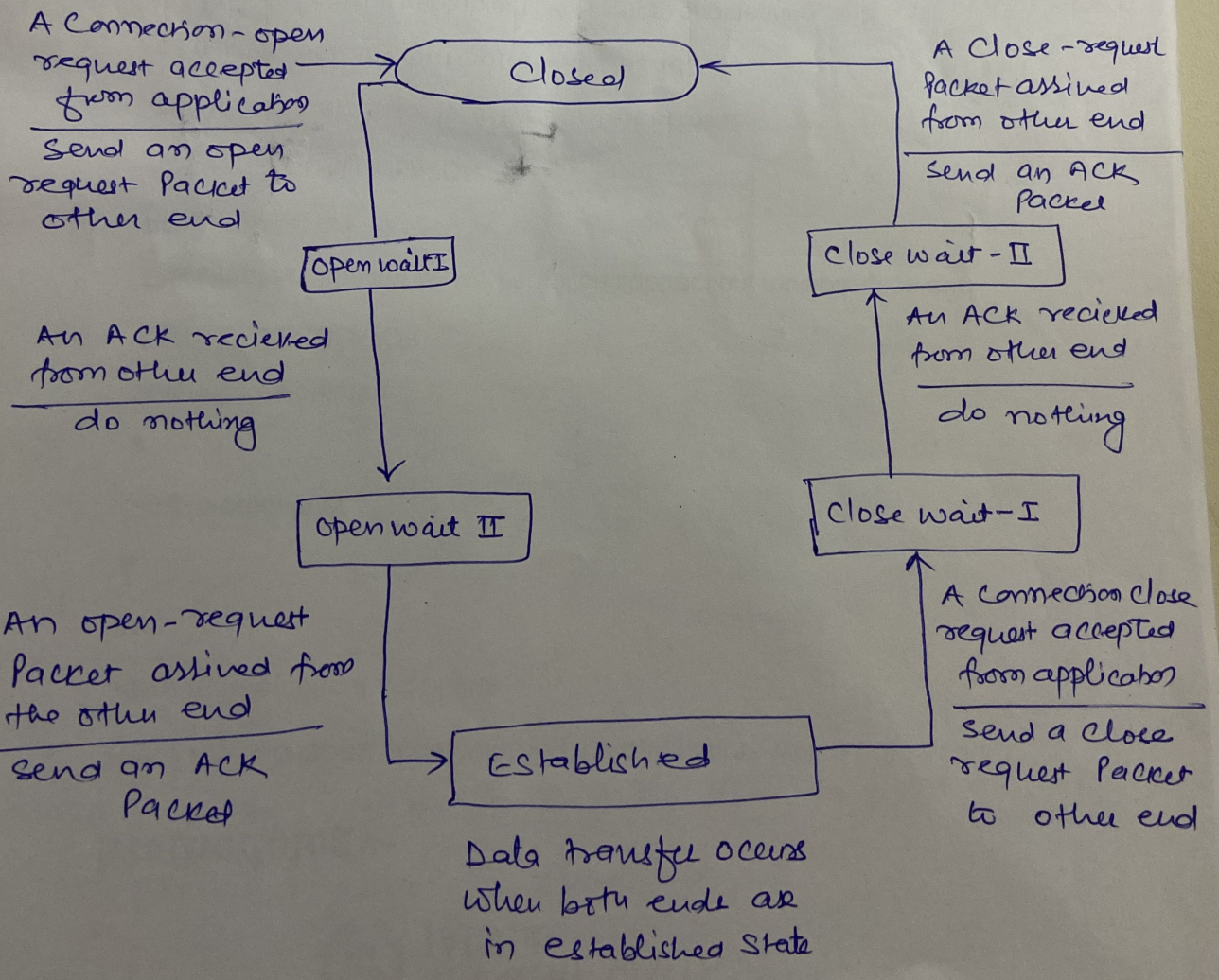
Finite-state machine

FSM for connectionless transport layer



Both ends are always in the Established state

FSM for connection oriented TL



Data transfer occurs when both ends are in established state