4. Network Layer

Page No :
Date :

Network layer

i) Network layer is responsible for the source to destination delivery of packet across multiple network, it ensures that each packet gets from it's point of origin to it's final destination.

ii) It selects & manages the best logical path for data transfer between nodes.

iii) The routing information contained within a packet includes source of the sending host & eventual destn of remote host.

iv) This information is contained within the network layer header that encapsulate network frams at the data link layer.

v) Primary function of the network layer is to permit different n/w to be interconnected

IP address

i) An internet protocol address is a logical numeric address that is assigned to every single computer printer, switch, router or any other device that is part of TCP/IP based network.

ii) The IP address is the core components on which networking architecture is built, no network exists without it.

iii) An IP address is a logical address that is used to uniquely identify every node in the network. because IP addresses are logical address that is used to uniquely identify every node in the network they can change.

iv) They are simillar to addresses in town/city because the IP address gives the n/w node an address. so that it can communicate with other nodes/n/w.

IPv4

i) The identifier used in the IP layer of the TCP/IP protocol suite to identify each device connected to the Internet address or IP address.

ii) An IPv4 address is a 32-bit address that uniquely & universally defines the connection of host or routes to the Internet.

iii) IPv4 addresses are unique. They are unique in the sense that each address defines one & only one, connection to the Internet.

iv) Two devices on the Internet can never have the same address at the same time. if a device has two connection to the Internet via two networks, it has two IPv4 addresses.

v) IPV4 addresses are unique & universal.

Address space

i) Address space is total no. of addresses used by the protocol.

ii) If a protocol uses b bits to define an address, the address space is 2^b because each bit can have two different values (0 & 1)

iii) IPV4 uses 32-bit addresses, which means that the address space is 2^{32} / 4,294,967,296.

Notation

There are 3 common notations to show an IPv4 address, binary notation (base 2), dotted decimal notation (base 256) & heradecimal notation (base 16)

1) Binary Notation (Base 2)

i) In binary notation an IPv4 address is displayed as 32 bits.

ii) IPV4 address referred to as a 32-bit address, 4 octet address or 4 byte address.

e.g →

01110101 10010101 00011101 11101010

2) Dotted-Decimal Notation (Base 256)

i) In that each byte (octet) is only 8 bits, each number in the dotted decimal notation is between 0 & 255.

Page No :
Date :

Bindry 10000000 00001011 00000011 00011111

128 . 11 . 8 . 31 Dotted decimal

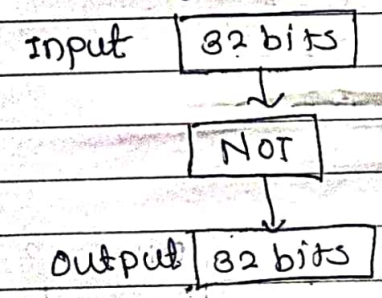
Operations

3 operations

1) NOT
2) AND
3) OR

1) Bitwise Not operation

i) It is a unary operation
ii) It takes one input
iii) In Not operation every 0 bit is changed to a 1 bit, every 1 bit is changed to 0 bit.

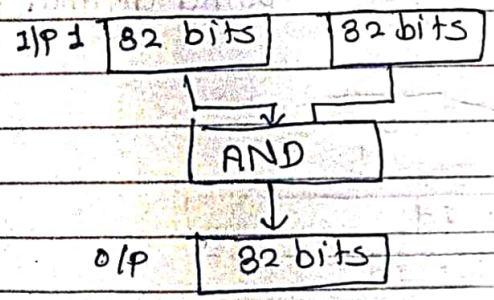


NOT operation

Input	Output
0	1
1	0

2) Bitwise AND operation

i) It is a binary operation, it takes two input.
ii) It compares two corresponding bits in two inputs & selects the smaller bit from the two.

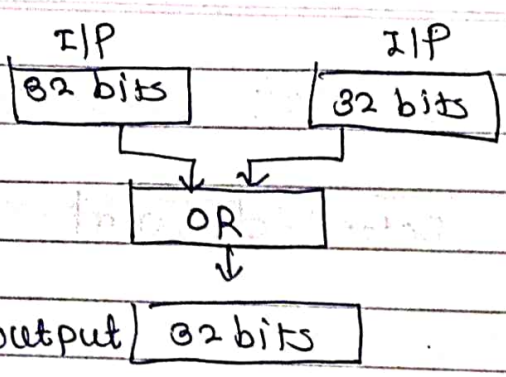


AND

I/P 1	I/P 2	O/P
0	0	0
0	1	0
1	0	0
1	1	1

3) Bitwise OR operation

i) It is a binary operations, it takes two no. & select larger bit from two



OR

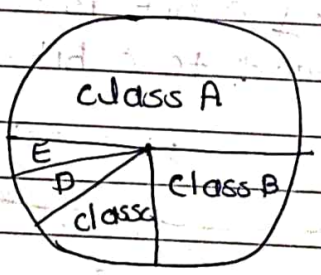
I/P	I/P	O/P
0	0	0
0	1	1
1	0	1
1	1	1

* Classful Addressing

classful Addressing contain 5 classes such as A, B, C, D, E

classes

In classful addressing, the IP address space is divided into 5 classes, A, B, C, D & E



class A = 2^{31}

B = 2^{30}

C = 2^{29}

D = 2^{28}

E = 2^{28}

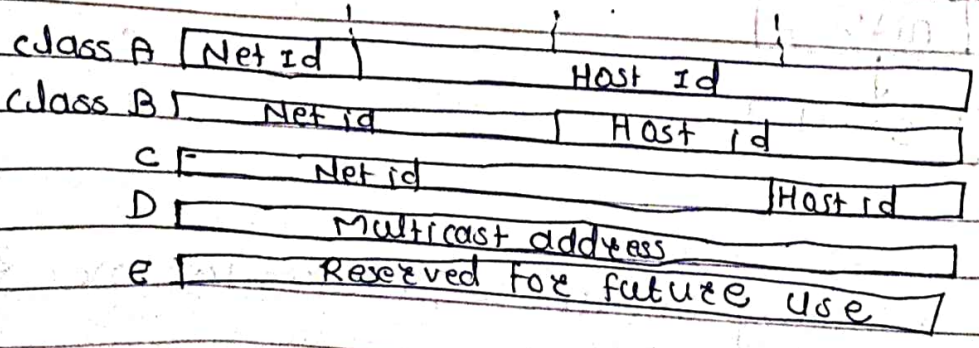
classes & Blocks

	octet 1	2	3	4	Byte 1	2	3	4
class A	0------				0-127			
B	10 ----				128-191			
C	110 ---				192-223			
D	1110 ---				224-239			
E	1111				240-255			

Binary Notation

Dotted decimal Notation

Netid & hostid



Page No:
Date:

i) In classful addressing, an IP address is classes A, B, C is divided into netid & hostid.

ii) fig. shows netid & hostid bytes, classes D & E are not divided into netid & hostid.

iii) In class A 1 byte defines the netid & 3 bytes define hostid. In class B 2 bytes define netid & 2 bytes define the hostid, In class C 3 bytes define the netid & 1 byte defines the hostid.

① Class A

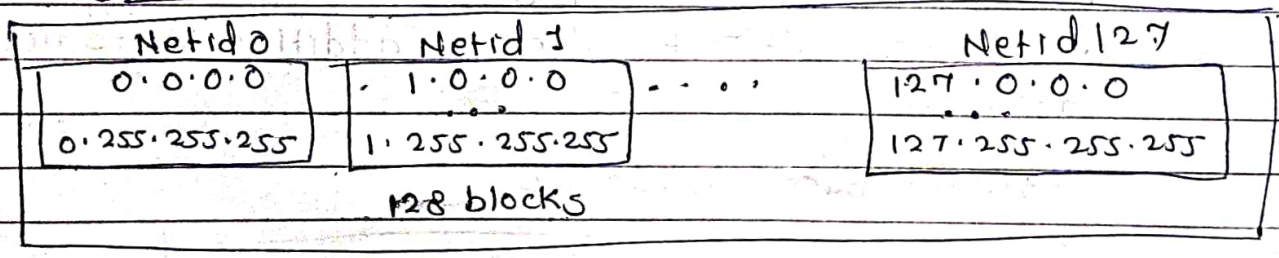
i) The 1st octect denotes the network address & last three octets are the host portion.

ii) Any IP address whose 1st octet is between 1 & 126 is a class A address.

iii) 0 is reserved as part of the default address & 127 is reserved for internal loopback testing.

iv) class A is divided into $2^7 = 128$ blocks that can be assigned to 128 organizations

Blocks in class A



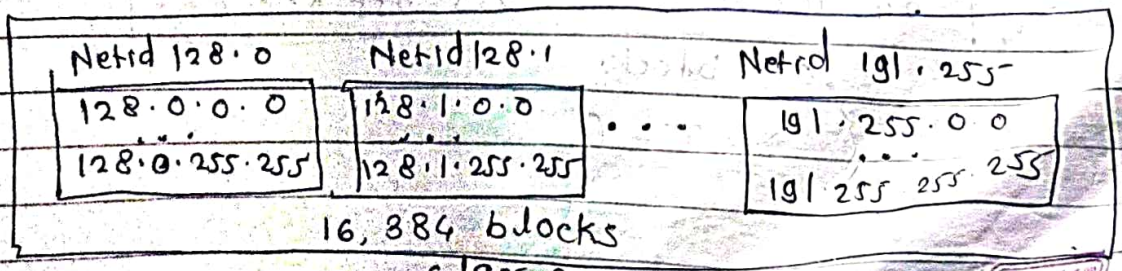
Class A

2) Class B

i) 2 bytes in class B ~~the~~ define netid ~~class~~ & two leftmost bit should be to (fixed), next 14 bits can be changed to find the no. of blocks in this class.

ii) Class B is divided into $2^{14} = 16,384$ blocks.

Blocks in class B



Class B

Sulekha

Class C

Netid

i) 3 bytes in class C define the ~~class~~ & 3 leftmost bit should be 110(fixed), the next 21 bits can be changed to find the no. of blocks in this class.

ii) Class C is divided into $2^{21} = 2,097,152$ blocks

class C

Netid 192.0.0	Netid 192.0.1	...	Netid 223.255.255
192.0.0.0 ... 192.0.0.255	192.0.1.0 ... 192.0.1.255	...	223.255.255.0 ... 223.255.255.255

class D

i) Used for Multicast

ii) Multicast IP addresses have their 1st octet in range 224 to 239

iii) There is one block of class D addresses

iv) Each address in this class is used to define one group of hosts on Internet, when group is assigned an address in this class, every host i.e member of this group will have multicast address in addition to its normal address.

single block in class D

224.0.0.0 ... 239.255.255.255
one block

class E

i) There is just one block of class E addresses.

ii) It was designed for use as reserved addresses.

240.0.0.0 ... 255.255.255.255
one block

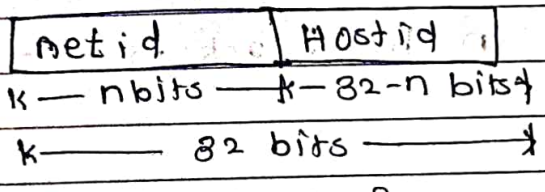
class E

Page No :
Date :

- Two level Addressing

i) The range of addresses allocated to an organization in classful addressing was a block of addresses in class A, B or C.

ii) Each address in classful addressing contains two parts netid & hostid, the netid defines networks, hostid defines



class A = n = 8

B : n = 16

C : n = 24

Example 1)

An address block is given as 180.8.17.9 · find the no. of addresses in the block, the 1st address & last address.

→ 180 is between 128 – 191

so class B

value of n for class B is 16

so i) No. of addresses in this block is $N = 2^{32-n}$

$$N = 2^{32-n}$$
$$= 2^{32-16}$$
$$= 2^{16}$$
$$\boxed{N = 66,536}$$

ii) To find 1st address, we keep leftmost 16 bits ~~& 1~~ set rightmost 16 bits all to 0s. The 1st address is 180.8.0.0/16

iii) To find last address we kept leftmost 16 & set rightmost 16 bits all to 1s.
The last address is 180.8.255.255

(2) 200.11.8.45

(3) 78.22.17.25

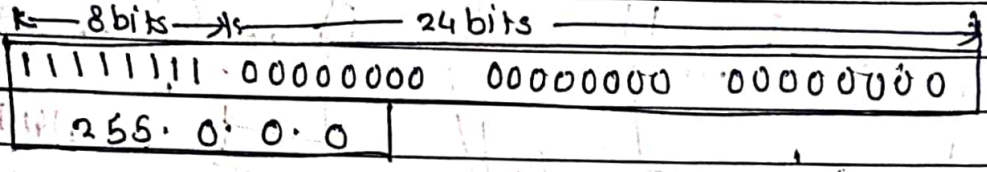
TEJ MY BRAIN
DATE / /

Network Mask:

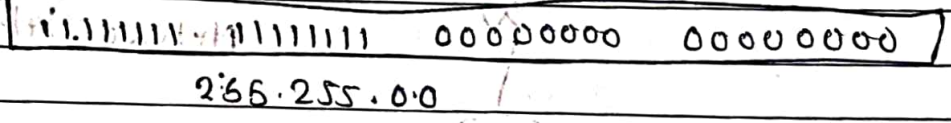
i) The routers in the internet normally use an algo. to extract the network address from the dest. address of a packet, to do this we need network Mask

ii) The network mask or default mask in classful addressing is a 32 bit no. with leftmost bits all set to 1s & 32-n rightmost bits all set to 0s

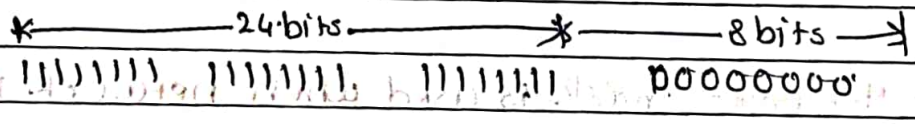
Mask for class A



Mask for class B



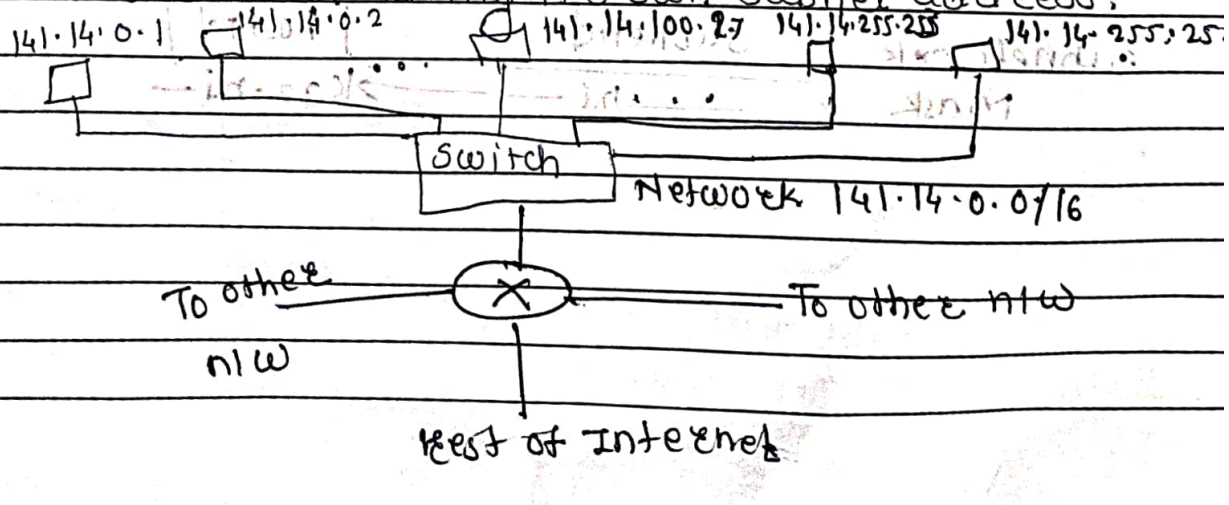
Mask for class C



Subnetting & Supernetting

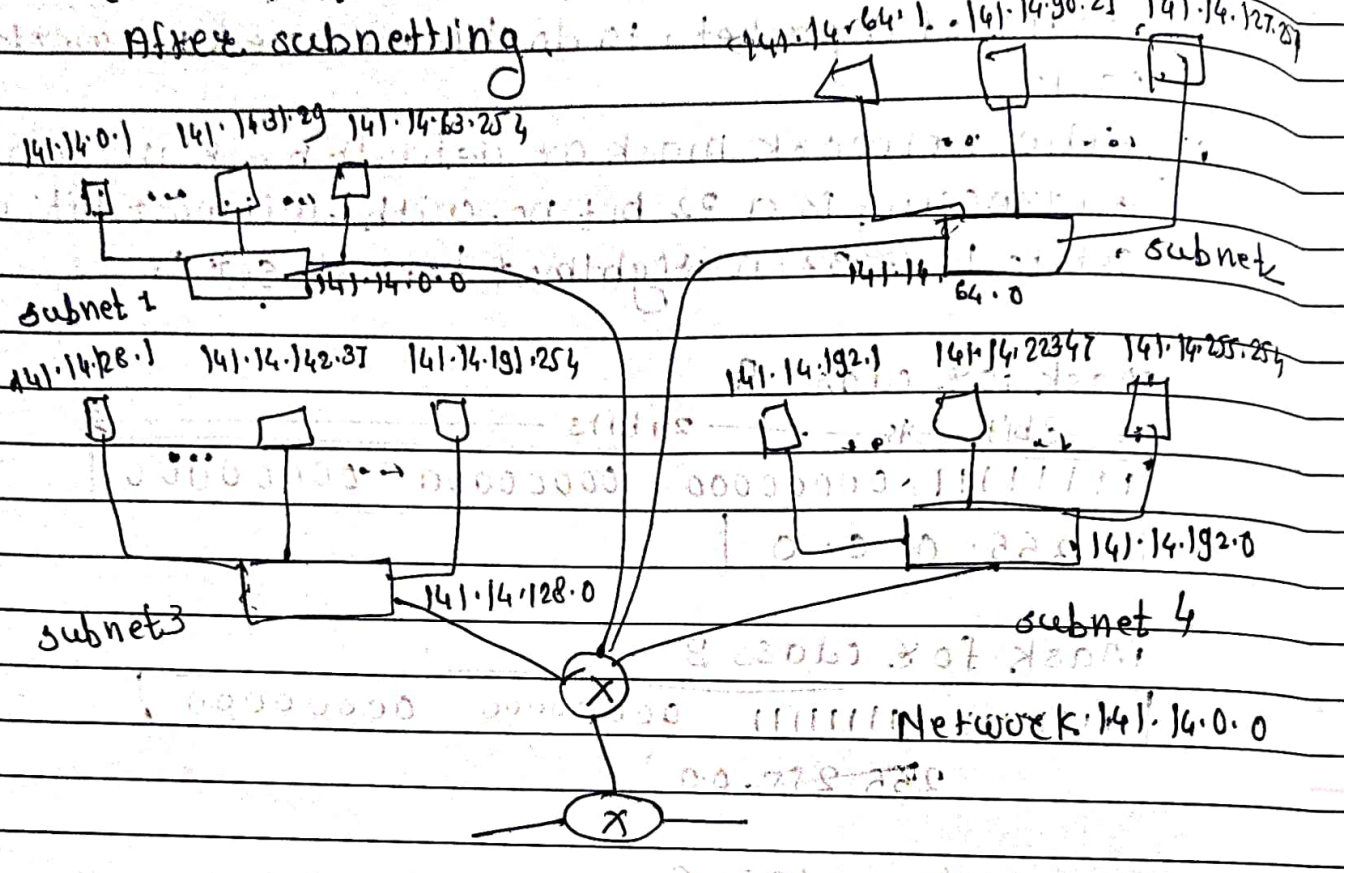
Subnetting

In subnetting, network is divided into several smaller subnetworks (subnets) with each subnetwork having it's own subnet address.



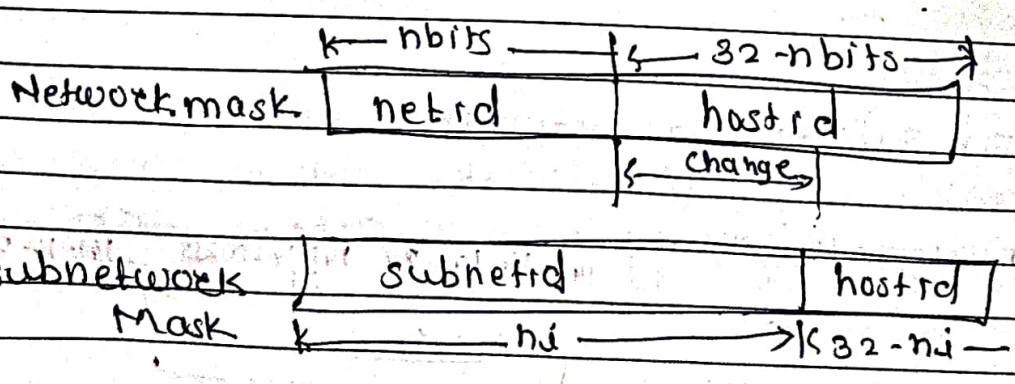
In last fig network using class B before subnetting The whole nw is connected through one single connection to one of the routers in internet.

After subnetting



Subnet Mask

i) Network mask is used when network is not subnetted. when we divide network to several subnetworks we need to create subnetwork mask for each subnetwork.



TEJ MY BRAIN
DATE / /

Subnet Address

when a network is subnetted, the 1st address in the subnet is the identifier of the subnet & is used by router to router packet destined for the network.

Supernetting

i) In supernetting an organization can combine several networks to create supernetwork.

Supernet Mask:

A supernet mask is the reverse of subnet mask

~~A subnet mask for class C has mo~~

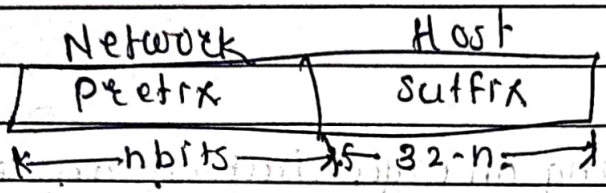
comparison of subnet, default & supernet Mask for class C

Subnet Mask:	11111111	11111111	11111111	11100000	nsub = 24+3 = 27
Default mask	11111111	11111111	11111111	00000000	n = 24
Supernet Mask	11111111	11111111	11111000	00000000	nsuper = 24-3 = 21

Classless Addressing

i) In classless the whole address space is divided into variable length block.

ii) In classless addressing the prefix defines the network & suffix defines the host



iii) In classful addressing length of net id depends on the class of address it can be only 8, 16, 24.

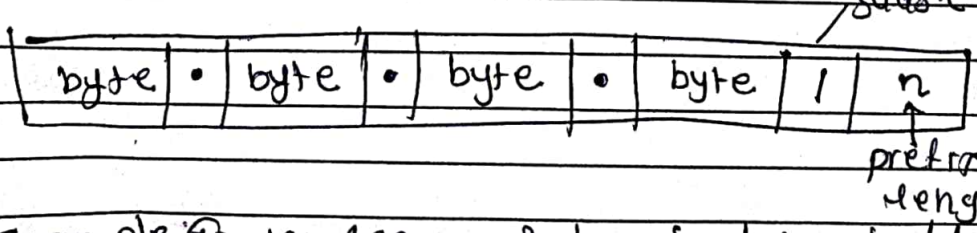
iv) In classless addressing the length of suffix of the prefix n depends on the size of block, it can be 0, 1, 2, 3 ... 32

v) In classless addressing, the value of n is referred to as prefix length, the value of 32-n referred to as suffix length.

vi) The prefix length in classless addressing can be 1 to 32.

Slash notation.

In classless addressing, we need to include prefix length to each address if we to find the block of the address. in this case, prefix length n is added to the address separated by slash.



Example ① 167.199.170.82/27 find no. of addresse in nlw, 1st address & last address.

② 17.63.110.114/24

③ 110.23.120.14

Page No :
Date :

Delivery & Forwarding of IP packets

1) Delivery

The delivery of packet to its destination is accomplished using two different methods of delivery

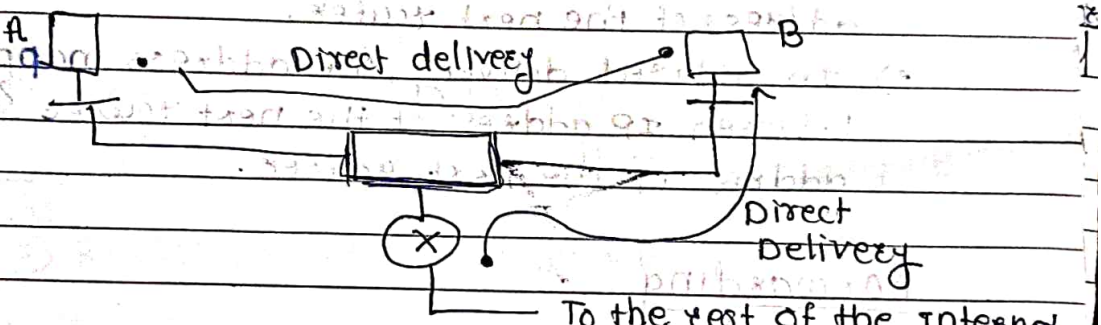
i) direct

ii) Indirect

i) Direct Delivery

- In direct delivery, final destination of the packet is host connected to the same physical network as the deliverer

- Direct delivery occurs when source & destination of the packet are located on the same physical network or if delivery is between last router & the destination host.



- The sender can easily determine if the delivery is direct, it can extract network address of the destination & compare this address with address of the networks to which it is connected, if match is found the delivery is direct.

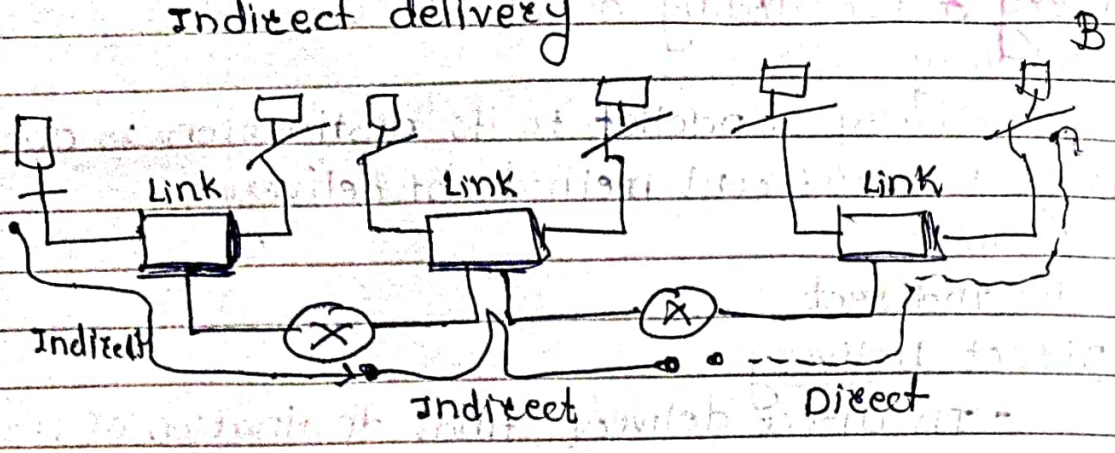
- In direct method, sender uses the destination IP address to find the destination physical address. so that reason we use the ARP because it mapping IP address to the physical address.

ii) Indirect delivery

a) If the destination host is not on the same network as a deliverer, the packet is delivered indirectly.

b) In indirect delivery, the packet goes from router to router until it reaches one connected to the same physical network as it's final destination

Indirect delivery



c) In an indirect delivery, the sender uses the destination IP address & routing table to find the IP address of the next router to which the packet should be delivered.

d) The sender then uses ARP to find the physical address of the next router.

e) In indirect delivery, the address mapping is between IP address of the next router & physical address of the next router.

Forwarding

i) forwarding means to place packet in it's route to it's destination

ii) when IP used a connectionless protocol, forwarding is based on the destination address of IP datagram when the IP used connection oriented protocol, forwarding is based on the label attached to an IP datagram.

iii) forwarding requires host or router to have routing table, when host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.

Page No :
Date :

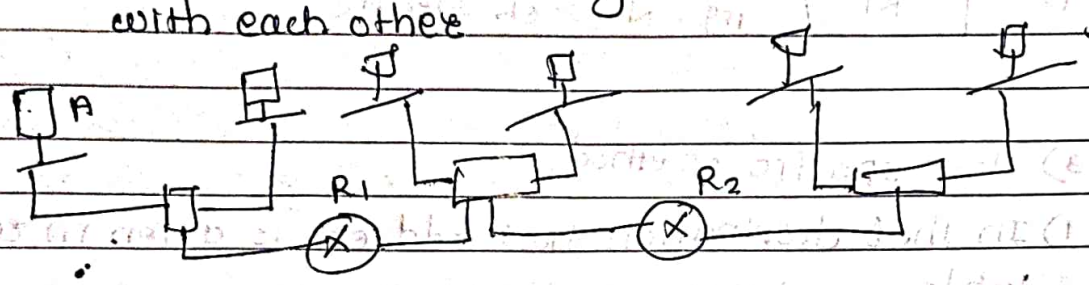
Forwarding Techniques

1) Next hop method

i) To reduce the contents of the routing table is called the next hop method.

ii) In this routing table holds only address of the next hop instead of information about complete route.

iii) The entries of routing table must be consistent with each other



A

Destination	Route
Host B	R1, R2, B

R1

Dest.	Route
Host B	R2, Host B

R2

Dest	Route
Host B	B

a) Routing table based on route

A

Destination	Next Hop
Host B	R1

R1

Dest	Next Hop
B	R2

R2

Dest.	Next hop
B	—

b.) Routing table based on next hop.

2) Network specific Method

i) To reduce the routing table & simplify the searching process is called network specific method.

ii) Here instead of having entry for every destination host connected to the same physical network, we have only one entry that defines the address of dest. network itself.

iii) We treat all hosts connected to the same ~~physical~~ network as one single entity

Network specific routing table for host S

Dest.	Next hop
N2	R1

Host specific routing table for host S

Dest.	Next hop
A	R1
B	R1
C	R1
D	R1

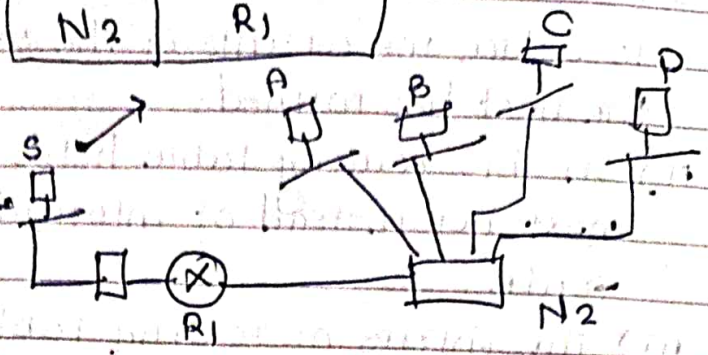


fig - Network specific

3) Host specific Method.

i) In that destination host address is given in routing table.

ii) It is inverse of network specific method.

iii) It is not efficient to put the host address in the routing table, there are occasions in which administrator wants to have more control over routing

iv) In fig. if the admin wants to all packets arriving for host B delivered to router R3 instead of R1, one single entry in the routing table of host A can explicitly define route.

Routing table for host A

Dest	Next hop
B	R3
N2	R1
N3	R3
⋮	⋮

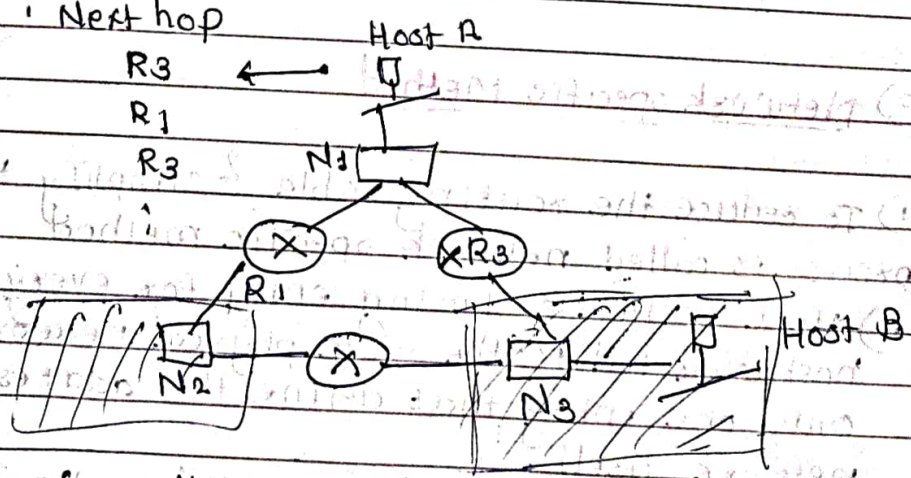


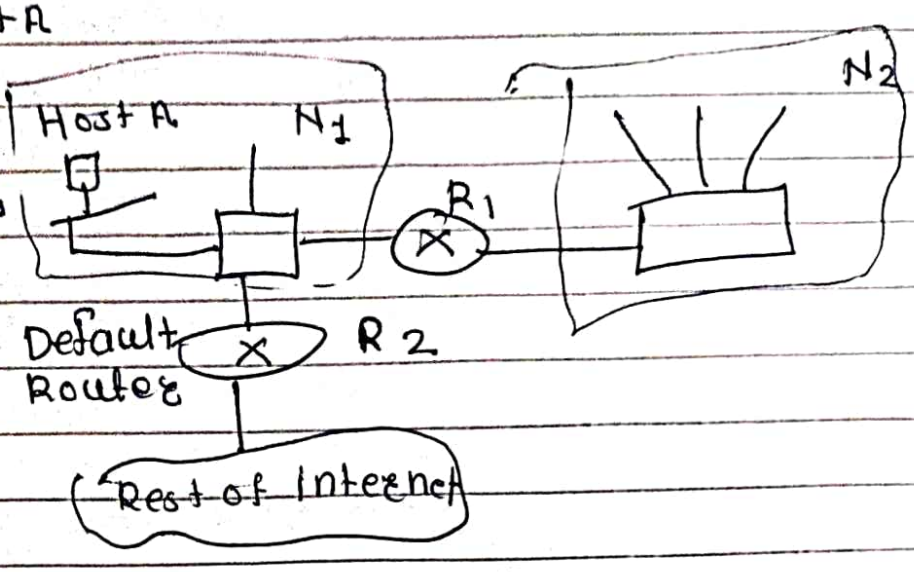
fig :- Host specific routing

Page No :
Date :

4) Default Routing.

Routing table for host A

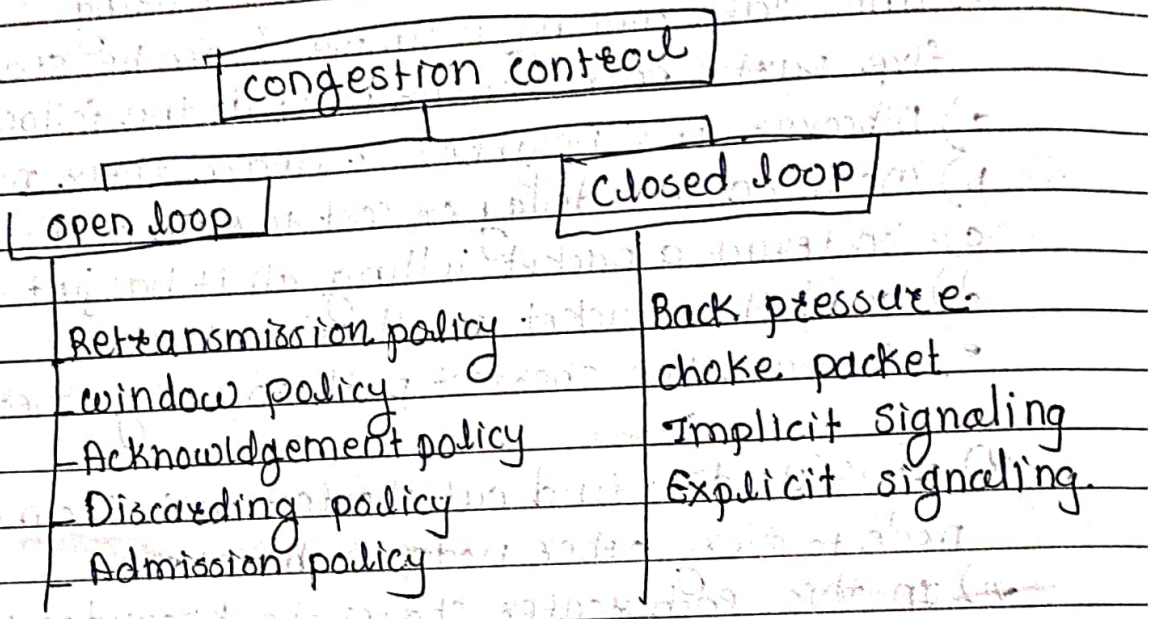
Dest.	Next hop
N2	R1
⋮	⋮
Default	R2



i) In above fig. host A is connected to a network with two routers. Router R1 routes the packets to hosts connected to a network N2.
- For the rest of internet, router R2 is used.
- So instead of listing all networks in the entire internet, host A can just have one entry called the default router.

Congestion control

i) It refers to techniques & mechanisms that can either prevent congestion before it happen or remove congestion after it has happened.
It is divided into two categories
a) Open loop (before)
b) Closed loop (after)



Open loop congestion control

i) In open loop congestion control, policies are applied to prevent congenstion before it happen
ii) It is handled by either source or destination

1) Retransmission policy
i) Retransmission is sometimes unavoidable.
ii) If the sender feels that sent packet is lost or corrupted, the packet needs to be retransmitted
iii) Retransmission increase congestion in the network so, good retransmission policy can prevent congestion.
iv) Retransmission policy & retransmission timers must be designed to optimize efficiency & at the same time prevent congestion.
v) Used in TCP

2) Window policy
i) The type of window at the sender may also affect congestion
ii) The selective repeat window is better than the Go-back-N window for congestion control.
iii) Go-back-N window, when the timer for packet times out, several packets may be resent although some may have arrived safe & sound at receiver.
iv) This duplication may make congestion worse
v) Selective repeat window on other hand tries to send specific ~~imposing less loo~~ packets that have been lost or corrupted.

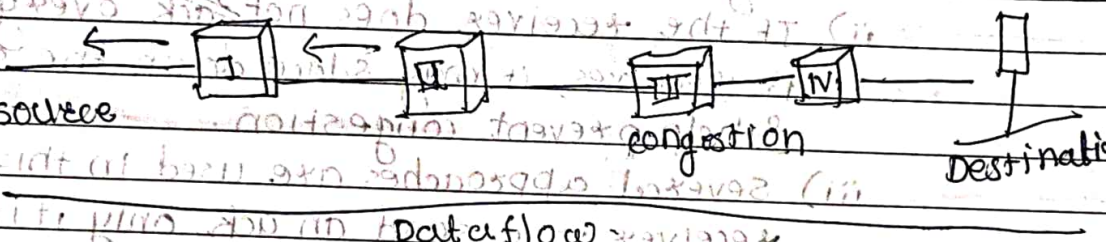
3) ~~Windo~~ Acknowledgment policy.
i) It imposed by the receiver may also affect congestion.
ii) If the receiver does not ~~ack~~ every packet it receives, it may slow down the sender & help prevent congestion.
iii) Several approaches are used in this case. receiver may send an ack. only if it has a packet to be sent or special timer expires.

4) Discarding policy
i) A good discarding policy by the routers may prevent congestion & at the same time may not harm integrity of the transmission.

5) Admission policy
i) An admission policy, which is quality of service mechanism, can also prevent congestion in virtual circuit network.
ii) switches in flow 1st check resource requirem of a flow before admitting to the network.
iii) A router can deny establishing virtual circuit connection if there is congestion in the network.

Closed loop congestion control
- congestion after it happens.

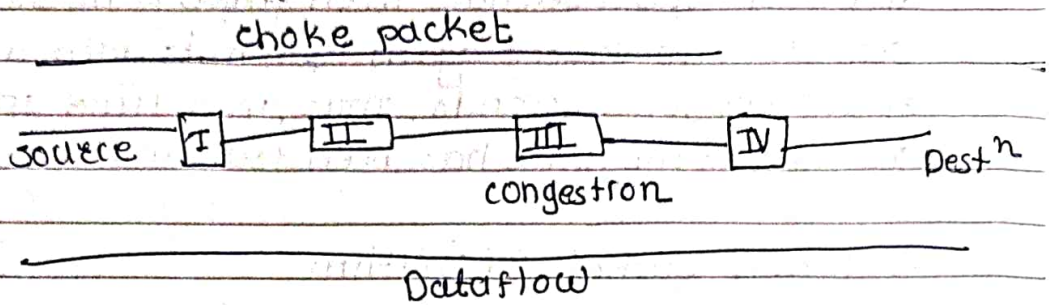
1) Backpressure
i) The technique of backpressure refers to a congestion control mechanism in which congested node stops receiving data from the immediate upstream node & nodes.
ii) Backpressure is node to node congestion control that start with a node & propogates, in the opposite direction of data flow, to the source.
iii) This techniques can be applied only to virtual circuit networks, in which each node knows the upstream node from which a flow of data is coming



iv) In above fig node III in the fig. has more input data that it can handle. it drops some packets in it's input buffer & informs node II to slow down. Node II in turn may be congested because it is slowing down the output flow of data. If node II is congested, it informs node I to slow down, which it turn may create congestion If so, node I informs the source of data to slow down.

2) Choke Packet
i) A choke packet is packet sent by node to the source to inform it of congestion
ii) In backpressure, the warning is form one node to it's upstream node, although the warning may eventually reach source dest.

ii) In the choke packet method, warning is from the router, which has encountered congestion, to the source station directly.



* Congestion control Algo.

① Leaky Bucket Algorithm

i) It is traffic shaping mechanism that controls the amount & rate of the traffic sent to network.
ii) A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate
iii) Imagine a bucket with small hole at the bottom
iv) The rate at which the water is poured into the bucket is not fixed & can vary but it leaks from the bucket at a constant rate.
v) Thus the rate at which water leaks does not depend on the rate at which water is input to the bucket.
vi) When bucket is full, any additional water that enters into the bucket spills over sides & is lost

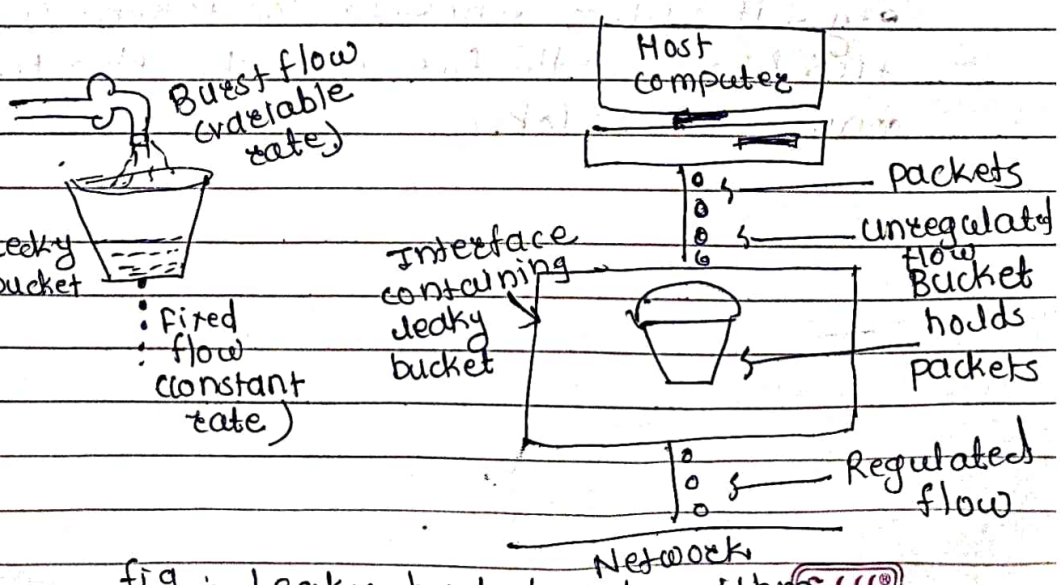


fig: Leaky bucket Algorithm

The same concept can be applied to packets in the network. Consider that data is coming from the source at variable speeds. Suppose that source sends data at 12 Mbps for 4 seconds, then there is no data for 3 seconds. The source again transmits data at a rate of 10 Mbps for 2 seconds. Thus, in a time span of seconds, 68 Mb data has been transmitted.

2) Token bucket Algorithm

i) The leaky bucket algo. does not considers the idle time of the host.
e.g. - if the host was idle for 10 seconds & now it willing to send data at a very high speed for another 10 seconds, total data transmission will be divided into 20 seconds & average data rate will be maintained

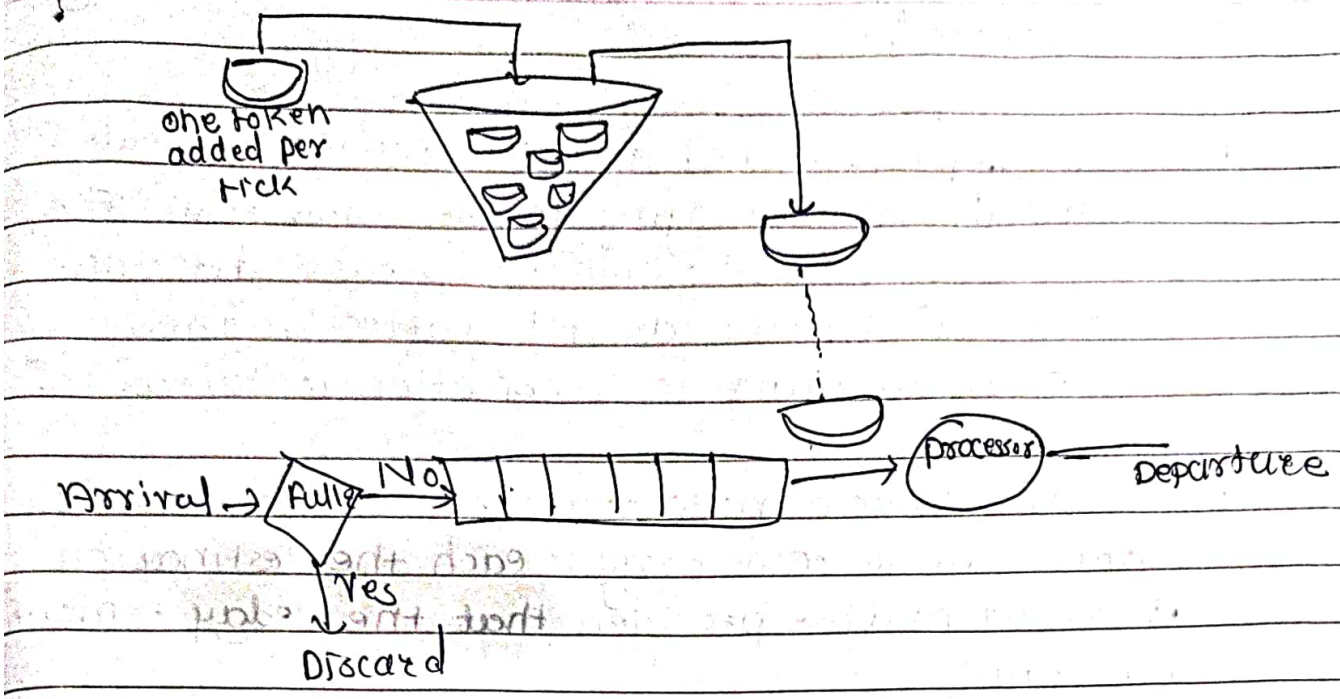
- To overcome this problem, a token bucket algorithm is used. A token bucket algo. allows bursty data transfers.

- A token bucket algorithm is modification of leaky bucket in which leaky bucket contains tokens.

- In this algo. a tokens are generated at every clock tick, for packet to be transmitted, system must remove tokens from the bucket.

- Thus token bucket algo. allows idle host to accumulate credit for future in form of tokens

e.g → if system generates 100 tokens in one clock tick & host is idle for 100 ticks, the bucket will contain 10,000 tokens.



Eg. Token bucket

Load shedding

i) Load shedding will use dropping the old packet than new to avoid congestion.

ii) Dropping packets that are part of the difference is preferable because future packet depends on full frame

iii) The policy for dropping packets depends on the type of packet, for file transfer, old packet is more important than new packet. In contrast, for multimedia new packet is more important than old one so the policy for file transfer called wine (old > new) & that for multimedia is called milk. (new > old)

Jitter control

i) Jitter may be defined as the variation in delay for the packet belonging to the same flow. The real time audio & video cannot tolerate jitter on the other hand jitter doesn't matter, if the packets are carrying an information contained in file.

ii) For the audio & video transmission, if packets take 20 ms to 30ms delay to each the destination it doesn't matter provided that the delay remains constant.

iii) when packet arrives at a router, the router will check to see whether packet is behind or ahead & by what time.

iv) This info. is stored in the packet & updated at every hop. If packet is ahead of the schedule then router will hold it for slight longer time & if the packet is behind schedule, then the router will try to send it out as quickly as possible.