UNIT - 2

IPV4 A

- IPV4 address is a 32-bit address that uniquely and universally defines the connection of a device to the internet

- The address space of IPV4 is 2^{32} (4,294,967,296)

Dotted ~~Deci~~ Decimal → Binary Notation for IPV4

It can be determined by using bits

128	64	32	16	8	4	2	1

If the number is 252

1	1	1	1	1	1	0	0

128 + 64 + 32 + 16 + 8 + 4 + 0 + 0 = 252

1. Change the following IP4 address from binary notation to dotted decimal notation

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

a) 129.11.11.239

b) 193.131.27.255

2. Change the following IPV4 address from Decimal notation to Binary notation

a) 111 .56 .45.78

b) 221.34.7.82

Solution

a. 01101111 00111000 00101101 01001110

b. 11011101 0100010 00000111 01010010

3. Find the error if any in the following IPV4 address

~~Sol~~ a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.2.3.14.67

Solution

a. Zero should not be ther in IPV4 address

b. It must have only 4 numbers and not 5 numbers

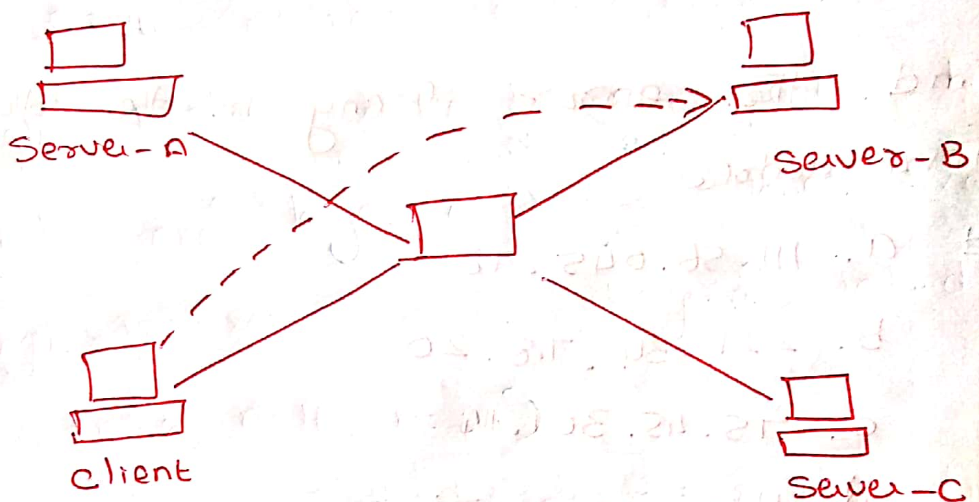
c. The value in IPV4 address should not exceed 255 (ie) ≤ 255 but here it has 301

d. IPV4 address should not be the mixture of Decimal + Binary. also there is 5 numbers.

IPV4 Addressing Modes

(i) Unicast Addressing Mode

* Data is sent only to one destination host
* The destination address feild contains 32-bit IP address of the destination host

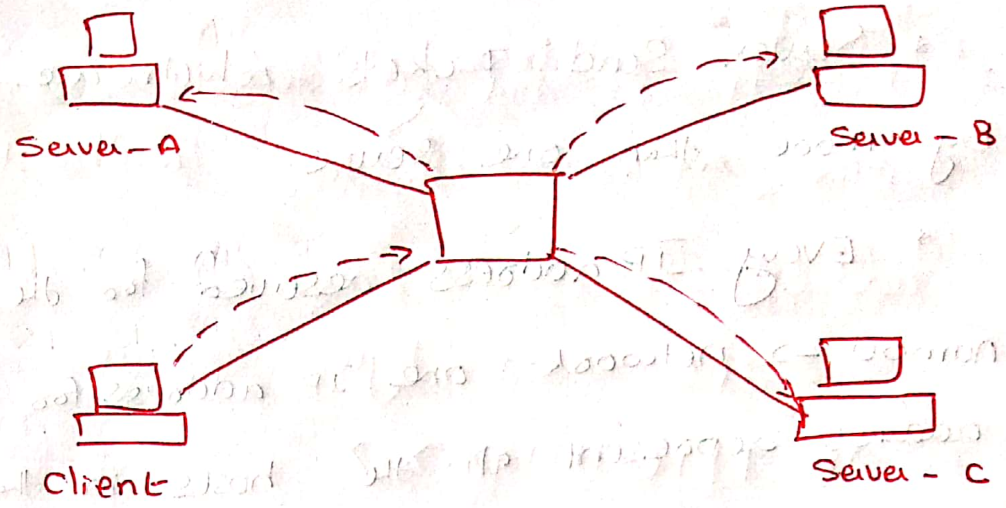


* Client sent data to the target Servers

(ii) Broadcast Addressing Mode:-

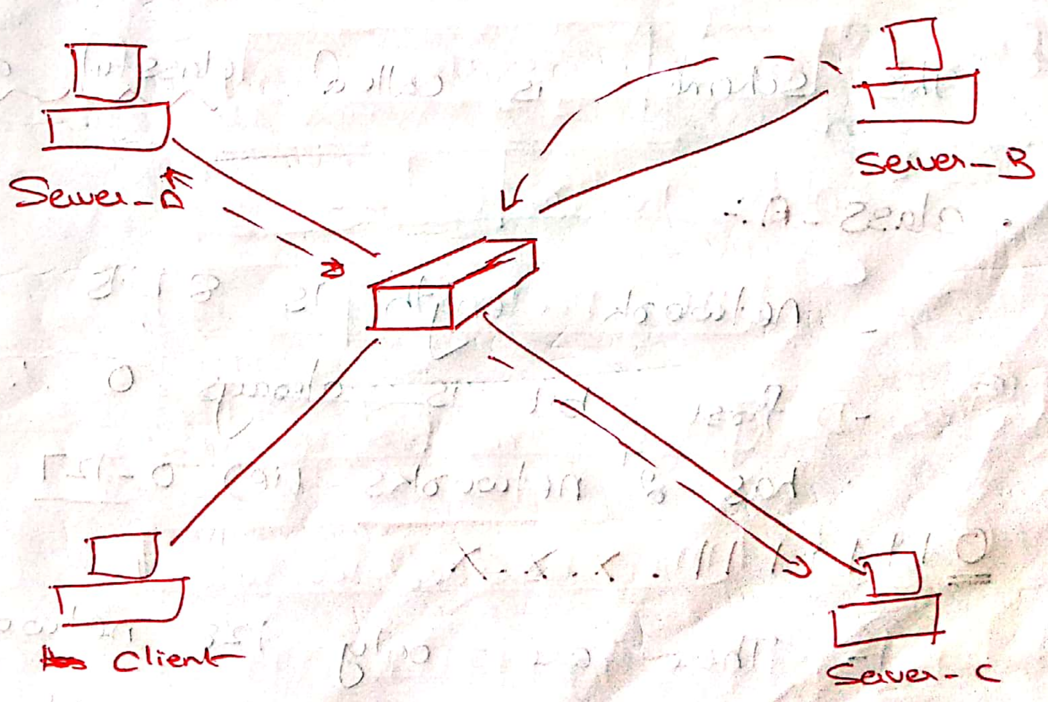
* In this mode, the packet is addressed to all the hosts in a network segment
* The destination Address feild contains a special broadcast address (ie) 255.255.255.255
* when a host sees this packet on the network it is bound to process it.
* Here the client sends a packet, which receivs by all the Servers.

Scanned by CamScanner



Multicast Addressing Mode:-

* This mode is a mix of the previous two modes (ie) Packet sent is neither destined to a single host nor all the hosts on the segment
* In this Packet the destination address contains a special address which starts with 224.X.X.X and can be entertained by more than one host



Scanned by CamScanner

* Server Send Packets which are entertained by more than one Servers

* Every IP address reserved for the network number → network one IP address for Broadcast address represent all the hosts in that network.

CLASSFUL ADDRESSING:-

- IPV4 address was designed with a fixed length prefix but to accomodate both Small and large networks, three fixed length Prefixes were designed instead of one (n=8, n=16, n=24)

- The whole address space was divided into 5 classes (class A, B, C, D + E) This Scheme is called classful addressing

• class - A:-

- network length is 8 bits
- first bit is always 0 ∴ it has 2^7 networks (ie) 0 - 127

0 1111111 . x . x . x

- There are only 128 networks in the world that can have Class A address.

Class B :-

— Network length is 16 bit

— first two bits are always $(10)_2$ we can have 14 bits as n/w identifier

10 111111.x.x.x

— First byte ranges from 128 to 191

— It can have $2^{14} = 16384$ networks in the world.

class C :-

— Network length is 24 bit

— first 3 bits are always $(110)_2$ we can have 21 bits as network identifier

— $2^{21} = 20,97,152$ networks in the world that can have class C address

110 11111.x.x.x

— First byte changes from 192 to 223.

Class D :-

- It is not divided into Prefix & Suffix. It is used for multicast addresses

- Its first byte always starts with 1110 1111 . x . x . x

Class E :-

- It starts with 1111 1111 . x . x . x

- It is not divided into Prefix and Suffix

- It is used as reserve

A	B	C	D	E
50 %	25 %	12.5 %	6.25 %	6.25 %

Class A	0 Prefix	Suffix
Class B	10 Prefix	
Class C	110 Prefix	
Class D	1110 multicast addresses	
Class E	1111 Reserved for future	

Subnet Mask :- [or] [Network Mask]

- In an IP Address has two components, the network address and host address

- It seperates the IP address into the network and Host

- Subnetting further divides the Host address of an IP into Subnet and host address if additional Subnetwork is used.

- A Subnet Mask is a 32-bit number that masks an IP address and divides the IP into network address and host address

- it is made by setting network bits to all 1s and setting host bits to all 0s

- within the given network two host addresses are reserved for special purpose, cannot be assigned for hosts

- The '0' address is assigned a n/w address

- 255 is assigned to broadcast address

⇒ classless Interdomain Routing

- It is invented to keep the internet from running out of IP addresses.

- In CIDR, a network of IP address is allocated in 1-bit increments as opposed to 8-bits in classful network

eg:

216.3.128.12 / 25 ⇒ 25 bits for network

for Class - A
0 - 127 | CIDR = 8 bcs of n/w id

for Class - B, CIDR = 16 bsc of n/w id

Class - C, CIDR = 24 bcs of n/w id

1. Find the first & last Address for the Given IP (or) N/w Id & Broadcast ID

i) 172.10.85.60 / 22

Soln:-

Subnet Mask by giving 1s to n/w bit & 0s to host id

11111111 . 11111111 . 11111100 . 00000000

	128	64	32	16	8	4	2	1
85 =>	0	1	0	1	0	1	0	1
And (3rd byte of subnet mask)	1	1	1	1	1	1	0	0
	0	1	0	1	0	1	0	0

2 | 85
2 | 42 - 1
2 | 21 - 0
2 | 10 - 1
2 | 5 - 0
2 | 2 - 1
1 - 0

Resultant decimal value

$64 + 16 + 4 = 84$

Starting address :- 172.10.84.0

To find Ending Address

(i) find the value of last 1 from subnet mask (ie) 4

Starting Number

least number

$\boxed{84 + 4 - 1} = 87$

formula

Ending Address :- 172.10.87.255

2. For the given IP find number of network + Host devices connected.

192.168.10.0 / 26

Given:-

IP: 192.168.10.0 /26

Subnet Mask: 11111111.11111111.11111111.11000000

Total number of 1's is 2 (ie) $N_1 = 2$

Total number of 0's is 6 (ie) $N_2 = 6$

∴ Number of Network: $2^{N_1} = 2^2 = 4$

Number of $\boxed{\text{Host}}$: $2^{N_2} - 2 = 2^6 - 2$

$= 64 - 2$

$= 62$ devices

3. An Organization is granted block of address with beginning address 14.24.74.0/24. The organization need to have 3 subblock to use in its 3 Subnet. Sub block of 10, 60 + 120 address. Design Subblock.

Given number of addresses in network = 24

$\therefore$ Total number of address $N = 2^{32-n}$; $n \to 24$

$= 2^{32-24} = 2^8$

$= 256$ address

$\therefore$ First address = 14.24.74.0/24

Last address = 14.24.74.255/24

Not:- Address must be assigned to sublock starting with largest and ending to smallest

(a) 120 address [Not a Power of 2 $\therefore$ find the number with nearest value which is greater than 120]

$\therefore$ $N_{sub1} = 128$ $[2^7]$

$n_{sub1} = 32 - \log_2 128$

$= 32 - 7$

$= 25$

First address :- 14.24.74.0/25

Last address : 14.24.74.127/25

(b) 60 address

Nearest power of 2 = $2^6 = 64$

$\therefore$ $N_{sub2} = 64$

$n_{sub2} = 32 - \log_2 64$

$= 32 - 6$

$= 26$

$\therefore$ first address: 14.24.74.128/26

Last address: 14.24.74.191/26

(c) 10 address

Nearest power of 2 = $2^4 = 16$

$N_{sub3} = 16$

$n_{sub3} = 32 - \log_2 16$

$= 32 - 4$

$= 28$

first address: 14.24.74.192/28

Last address: 14.24.74.207/28

(d) Reserve

$256 - 208 = 48$

$\therefore$ first address: 14.24.74.208

Last address: 14.24.74.255

4. Find the first, Last address + Number of Network + Host devices connected to the given ip 167.199.170.82/27.

Given:

167.199.170.82/27

Subnet mask

11111111.11111111.11111111.11100000

Number of Network $= 2^3 = 8$ Networks

Number of Host $= 2^5 = 32$ Devices

4^{th} Segement

	128	64	32	16	8	4	2	1
	1	1	1	0	0	0	0	0
82 =>	0	1	0	1	0	0	1	0
And Operation	0	1	0	0	0	0	0	0

Equivalent Decimal = 64

∴ First address = 167.199.170.64/27

To find Ending address

Subnet Mask = 32

Value of last 1 is

$64 + 32 - 1 = 95$

∴ Last address = 167.199.170.95/27

Classless Addressing

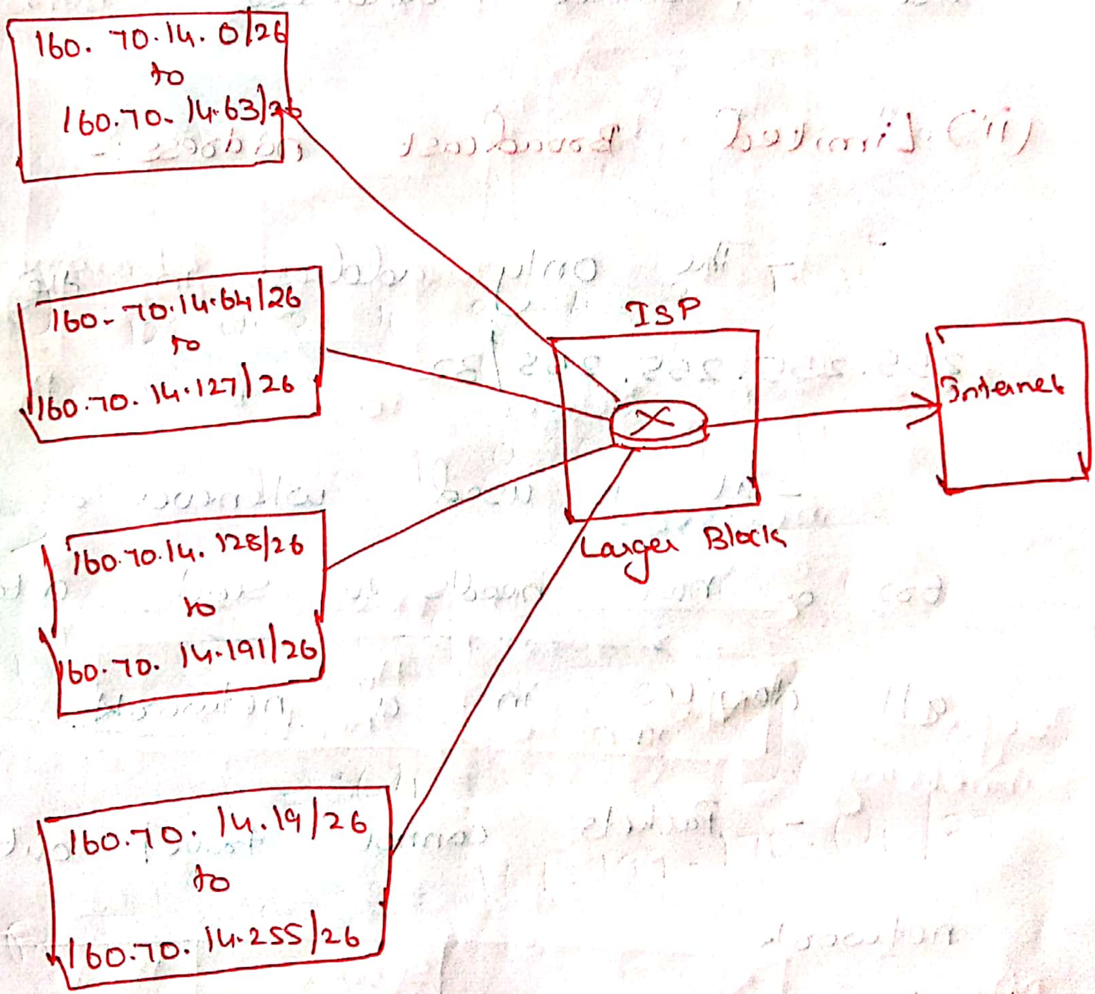
- In class A addressing it han have a total of 8 bits out of 32 for network Id and 2^{24} for Host devices which means in the entire world ony 0 - 127 organizations can have class - A addressing. If any other organization requires class - A addressing it can't be provided
- Similarly ~~foor~~ for class B + class C to overcome that classless addressing is introduced
- In classless addressing the prefix length is varied unlike to classful addressing (i.e) (class A, B, C)

Scanned by CamScanner

Address Aggregation:-

- Smaller Block addresses are combined to create a larger block

- ISP will be given with these larger blocks which was (or) can be divided into somany smaller box and - it grants the small sub blocks to its customers.



Special Addresses :-

(i) This - Host Address :-

- The only address in the block is called 0.0.0.0/32
- It is used whenever a host needs to send an IP datagram but it doesn't know its own address to use as source address

(ii) Limited Broadcast Address :-

- The only address in the block is 255.255.255.255/32
- It is used whenever a router or a host needs to send datagram to all devices in a network.
- Packets cannot travel outside the network

(iii) Loopback Address.

- The only address in the block is 127.0.0.0/8
- A packet with one of the address in this block as destination never

leaves the host; it will remain in the host.

- This block is used to test a piece of software in the machine

(iv) Private Addresses

Four Blocks are assigned as private address: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 169.254.0.0/16

- These addresses are not routed on the Internet and no traffic cannot be sent to ~~them~~ + from the Internet they are supposed to work within local network.

(v) Multicast Address:-

- The address block is 127.0.0.0/8
- Datagrams with this addresses are simultaneously transmitted to one (or) more multicast host groups (or) networked computers.

Subnetting :-

It is the process of dividing the network into sub-networks

- It is done by borrowing a bit from host (ie) network size is increased

Supernetting :-

- It is a process of combining small networks in to a large space

- It is done by borrowing a bit from Network id thus Host size is increased.

⟵ IP Address ⟶

Before Subnetting

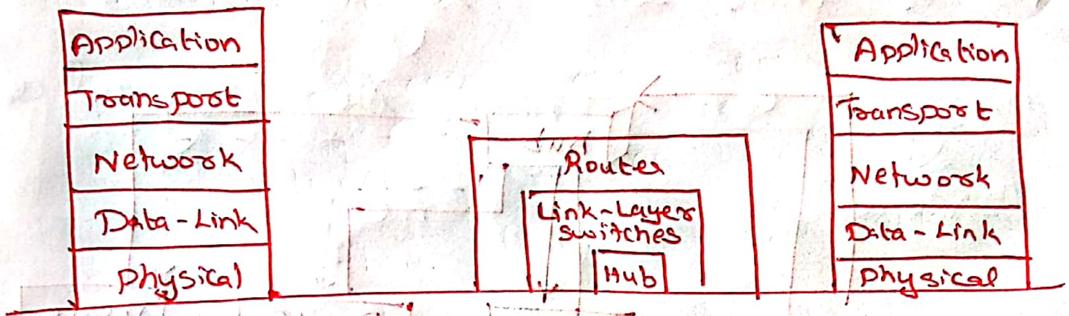
N/w identifier	Host Identifier

After Subnetting

N/w identifier	subnet identifier	Host identifier

Connecting Devices:-

It is used to connect hosts together to make a network or connect network together to make an internet.

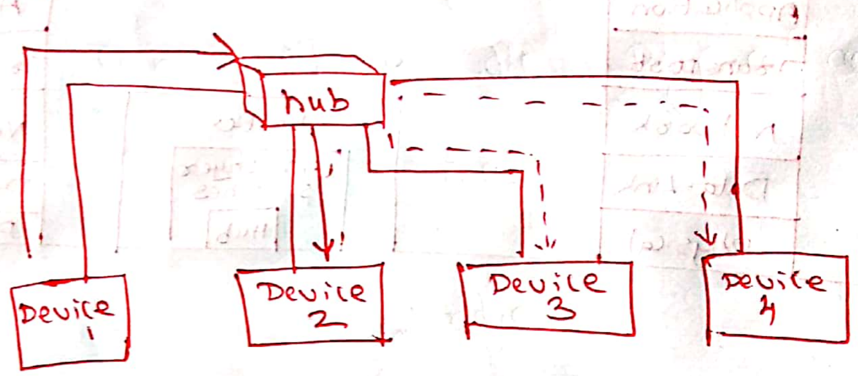


(i) HUB:-

- It operates only in physical layer.
- It can be used to serve as connecting point
- when packet from one Device to another at the hub the signal representing the frame is generated to remove any possible corrupt noise but hub

forwards the packet from all outgoing ports except the One from which the Signal was received.

- All device in the LAN Receives the packets / frame by only one Station which requires keeps it.



(ii) Repeater:-

- It Receives a Signal before it becomes too weak or Corrupted, regenerates and retimes the original bit pattern

- It then sends the refreshed Signal

- It works on physical Layer.

LINK- LAYER SWITCHES:-

- It operates in both physical and data Link Layers
  - physical layer device regenerates the signal which it receives
  - link layer Device can check the MAC addresses (source & destination) contained in the frame

* **Filtering:-**

Link layer switch check the destination of a frame and can decide from which outgoing port the frame should be sent

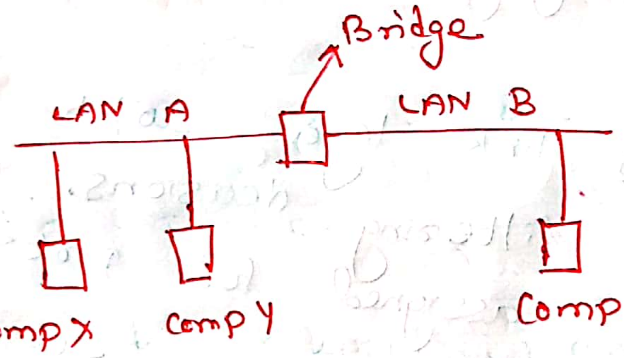
- A link layer switch has a table (ie) Addresses used in filtering decisions. for ports connected will be assigned switch when a message is received switch decides depending on the table which port has to be choosed.

Scanned by CamScanner

BRIDGE:-

* A bridge operates in both the physical and the data link layer and connect two different LAN

* It generates the signal it receives from the physical layer device. As a data link layer device, the bridge can check the physical addresses contained in the frame.



* A bridge has filtering capability It can check the destination address of a frame and decide if the frame should be forwarded or dropped

Router:-

- A router is a three layer device that routes packets based on their logical addresses
- Router normally connets LAN and WANs in the internet and has a routing table that is used for making decisions about the route
- Routing tables are normally dynamic and are updated using routing protocols
- Routers use header and forwarding tables to determine the best path for forwarding the packets and they use protocol such as ICMP to communicate with each other and configure the best route between any two host
- Primary function of a router is to connect network together and keep certain kind of broadcast traffic under control.

* NETWORK ADDRESS TRANSLATION (NAT)

⇒ Problem Statement

– Any device that connects directly into Internet must have a Public unique IP address.

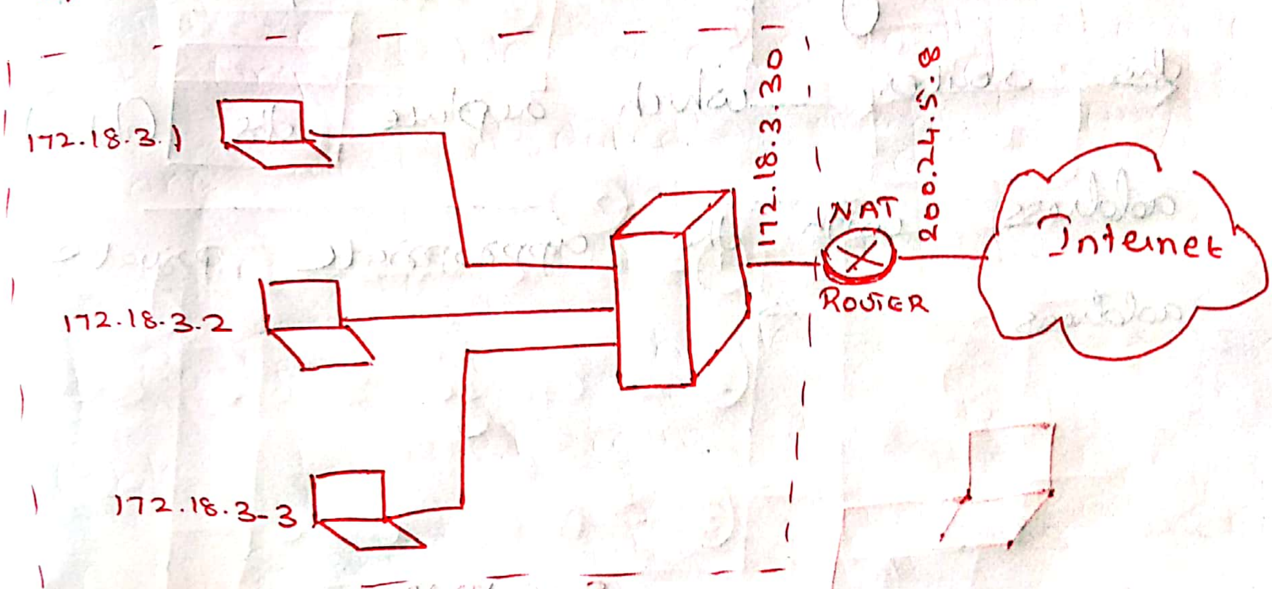
– There is a shortage of Public IPV4 address.

– Suppose if ISP grants a small range of addresses to a small business unit and after a course of time if more IP is needed ISP cannot provide IP in the nearing range.

– Only a portion of a small network access to a Internet simultaneously (ie) If a company has 50 computers and out of which only 10 computers directly access Internet then only 10 IP is used remaining is wasted.

∴ To overcome that a technology that can provide the ~~b~~ mapping between the Private and universal addresses and at the same time support virtual private networks. is called Network Address Translation.

⇒ IMPLEMENTATION OF NAT:-



Site using Private addresses

Private network uses private addresses.

- Router that connects the network ~~to~~ global address uses one private address and one global address

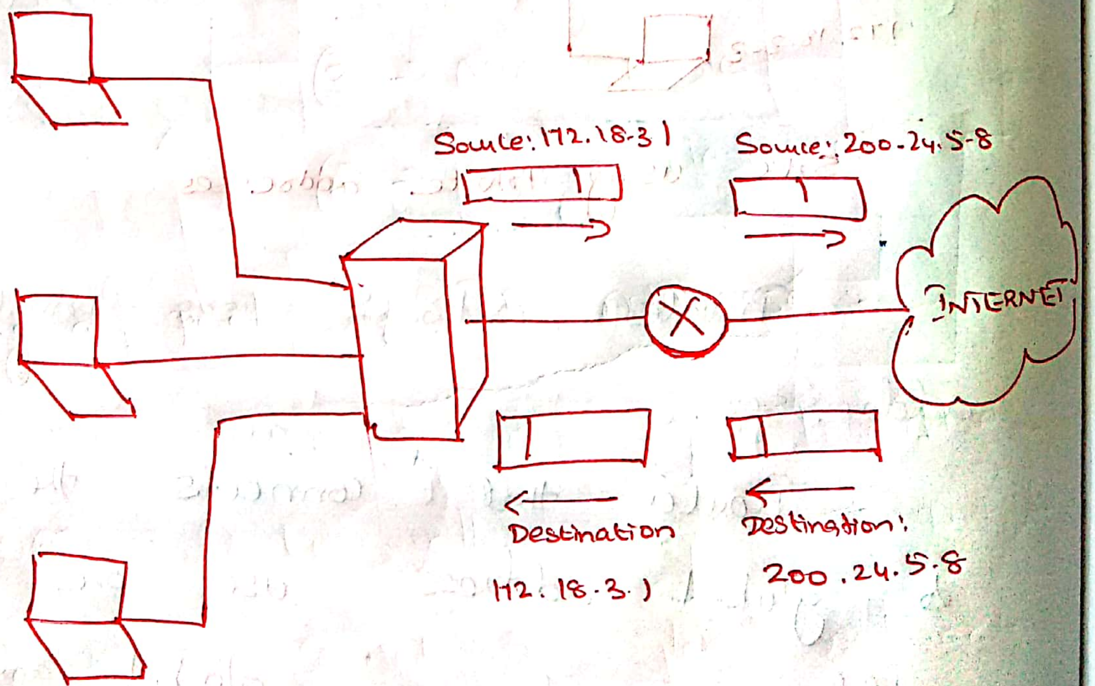
~~Private address uses one~~

⇒ Address Translation:-

- All outgoing messages go through NAT router.

- which replace the Source address (ie) Private address with global address

- Incoming packets also passes through this router which replace the Global address with the appropriate private address



⇒ Translation Table :-

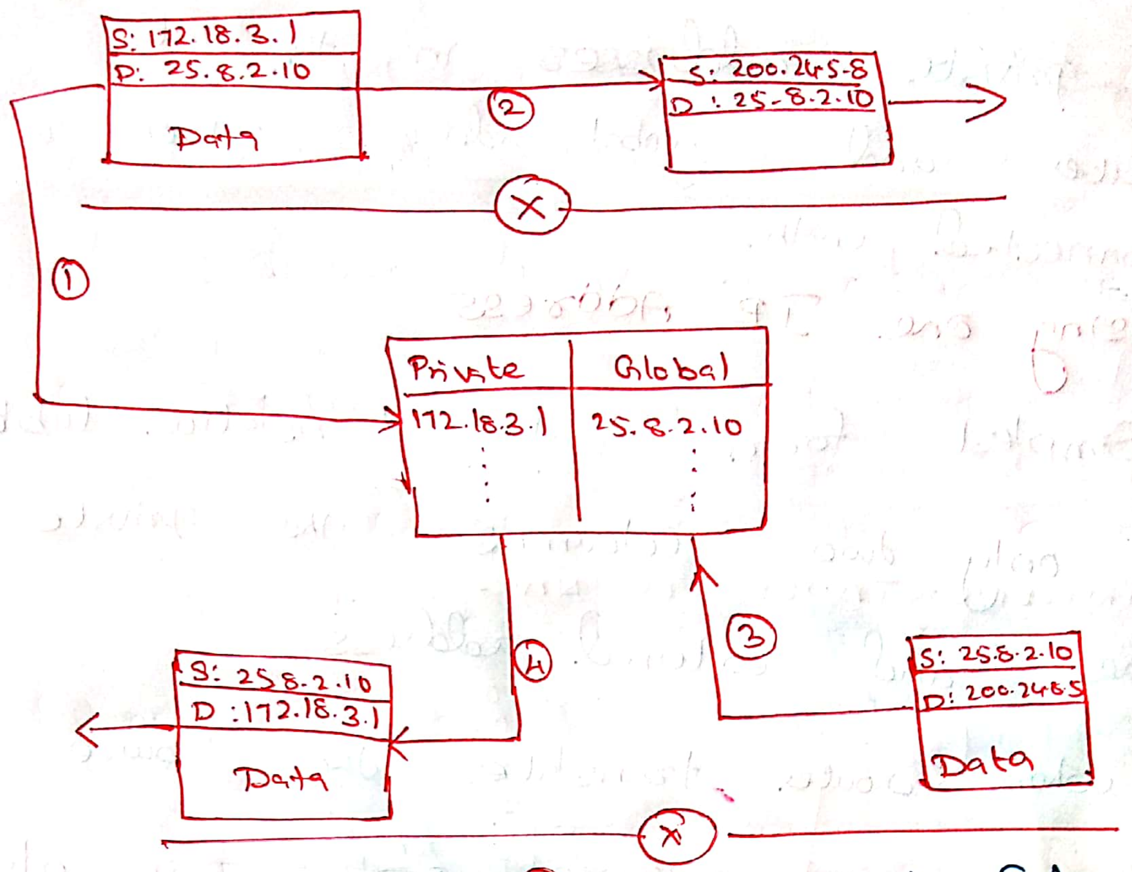
This is the table containing all private addresses in the NAT router and global address which it connected with.

⇒ using one IP Address

Simplest form with translation table has only two coloumns : the private address and external address

- when router translates the source address of the outgoing packet it also make note of the destination address where the packet is going
- when the response comes back from the destination the router uses the source address of the packet to find private address

- In this mode communication must alsways be initiated by the private network



1 -> Make table Entry

2 -> Change Source address

3 -> Access table

4 -> Change destination Address

⇒ Using a pool of IP Addresses:-

The use of one global address by NAT router allow any one private network to connect to global network.

∴ Instead of using only one global address, the NAT router can use four address ∴ four can connect with the same time

⇒ using both IP Address and Port Addresses

To allow many to many relationship between private network host & external server program, we need more information in translation table

(ie) If two ip in private have to communicate with same ip in Global address.

∴ Therefore table will have five coloumns:

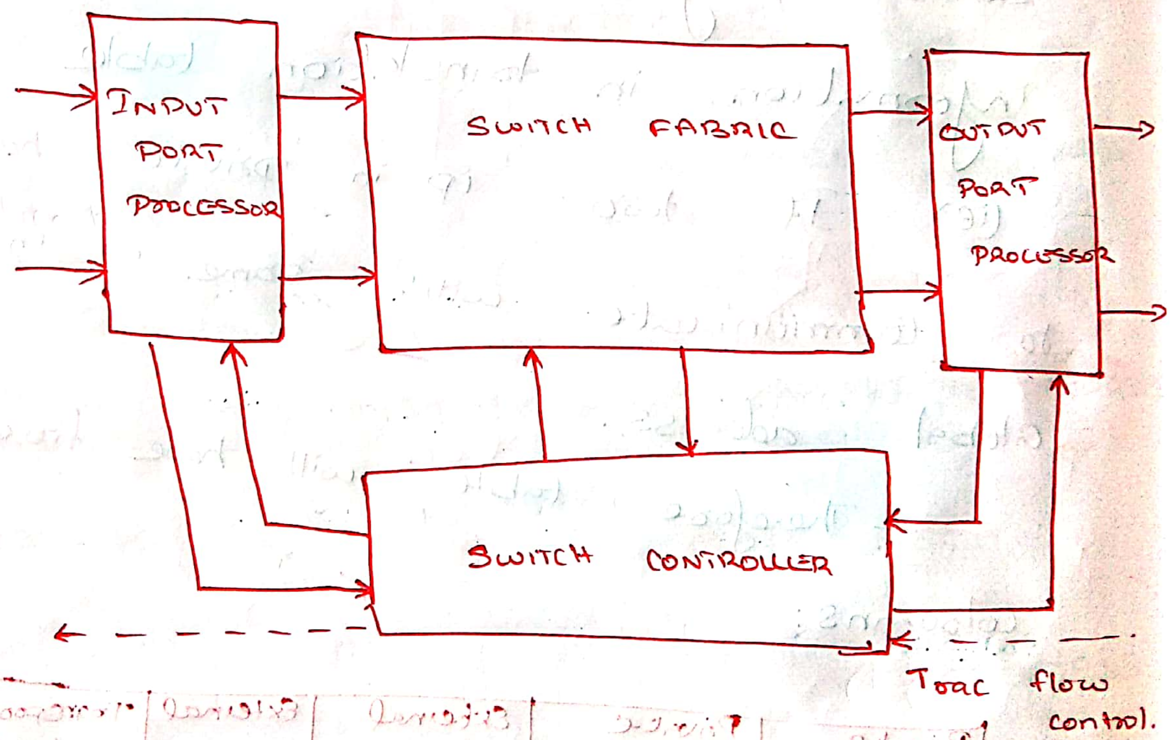
Private Address	Private Port	External address	External Port	Transport protocol
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
⋮	⋮	⋮	⋮	⋮

STRUCTURE OF ROUTER:-

- Routers are the building blocks of wide area Networks

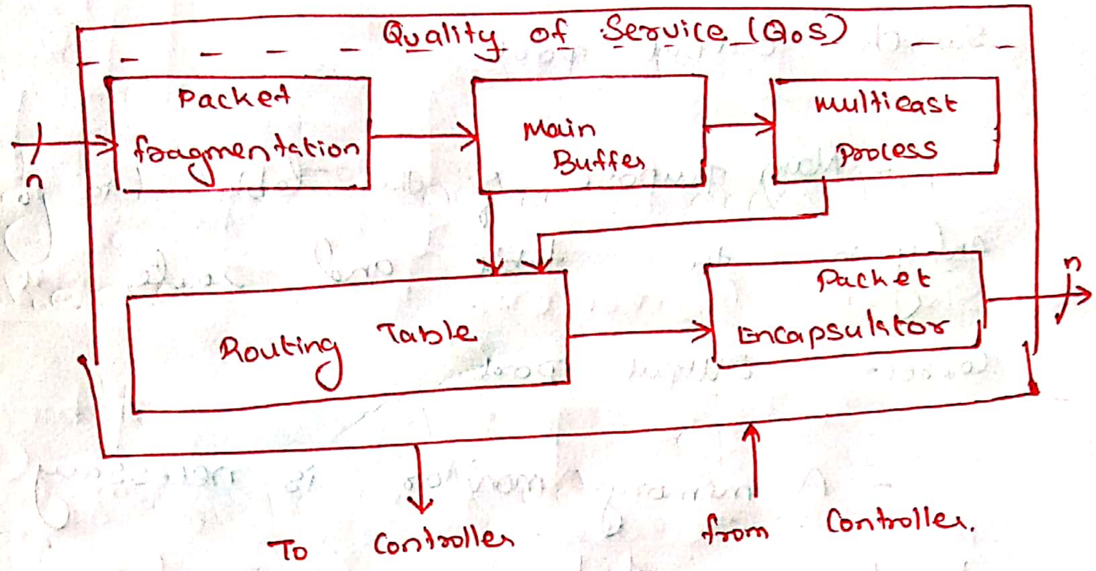
- Packets arrive at n input ports and are routed from n output ports.

- It consist of four main parts: Input port Processor, output port processor, Switch Fabric and switch controller.



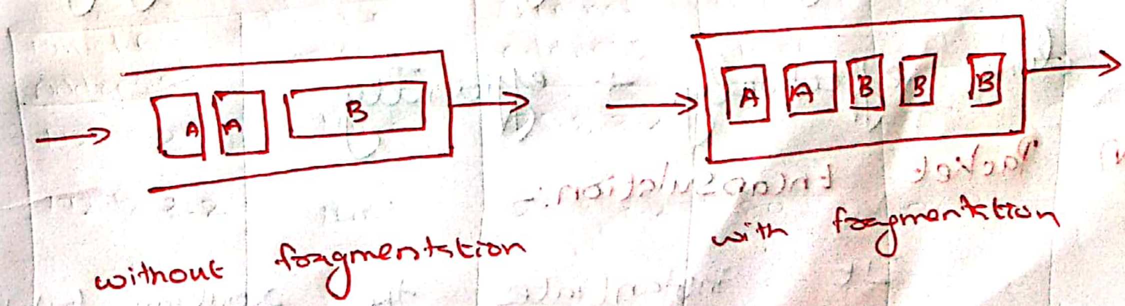
(a) INPUT PORT PROCESSOR (IPP)

- The functionality of data link layer is implemented as a seperate chip in IPP which also provides a buffer to match the speed between the input and the switch fabric.



(i) Packet fragmentation:-

- It converts packets to smaller sizes.
- Large packets cause different issues at network and link layer.
- Packets are splitted into small fragments and then reassembled at the output port processor.



(ii) Routing Table:-

- It is a look up table containing all available destination address and the corresponding switch output port.

- Main purpose of this table is to look up an entry in the table and route it to the correct output port.

- A memory monitor is necessary to keep track on which memory is free as the data packets are received at different time.

(iii) Multicast Process:-

- It is needed for copying packets when multiple copies of packet are expected to be made on a switching node.

- using a memory module copying can be done effectively + efficiently.

(iv) Packet Encapsulation:-

It instantiates the routing table module, performs the routing table look ups and insert the switch output port number into n/w header.

– The serial to parallel multiplexing unit converts an incoming serial byte stream into a fully parallel data stream.

– It helps to determine whether the packet is unicast or multicast.

(V) Congestion Controller

– It shields the switching node from any disorders in the traffic flow.

– It is controlled by sending a reverse warning packets to the upstream node to avoid exceeding traffic.

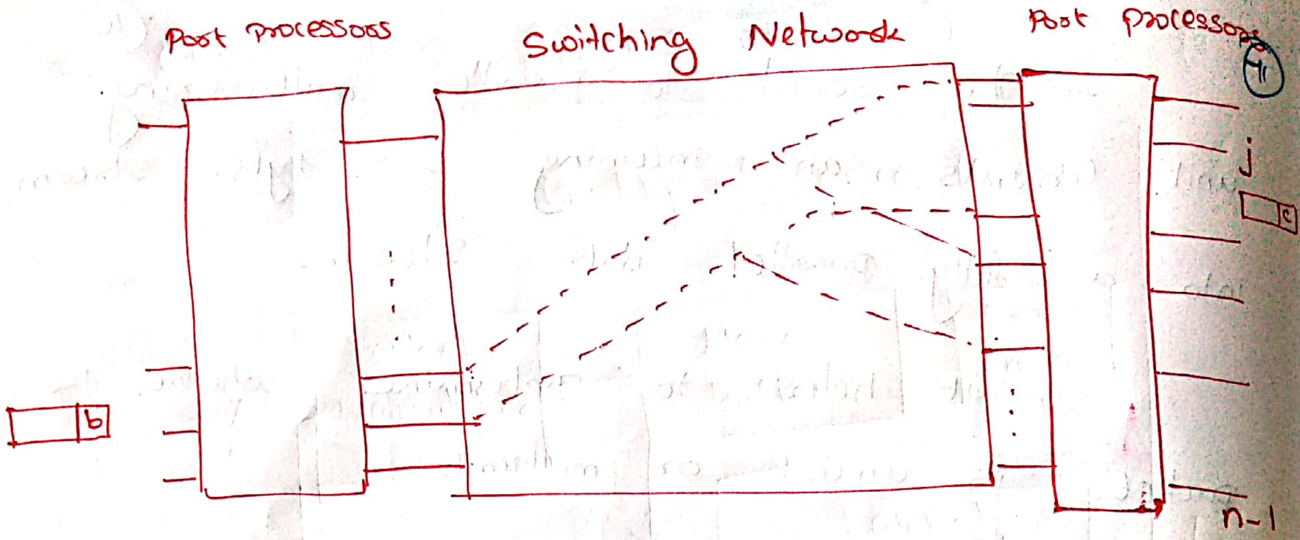
– Spacing between incoming packets is not regular which also causes problems.

⇒ SWITCH FABRIC

– Packets are routed from input ports to desired output ports.

– Packets can also be multicast to more than one output.

– In output port processor, packets are buffered and resequenced in order to avoid packet misordering.

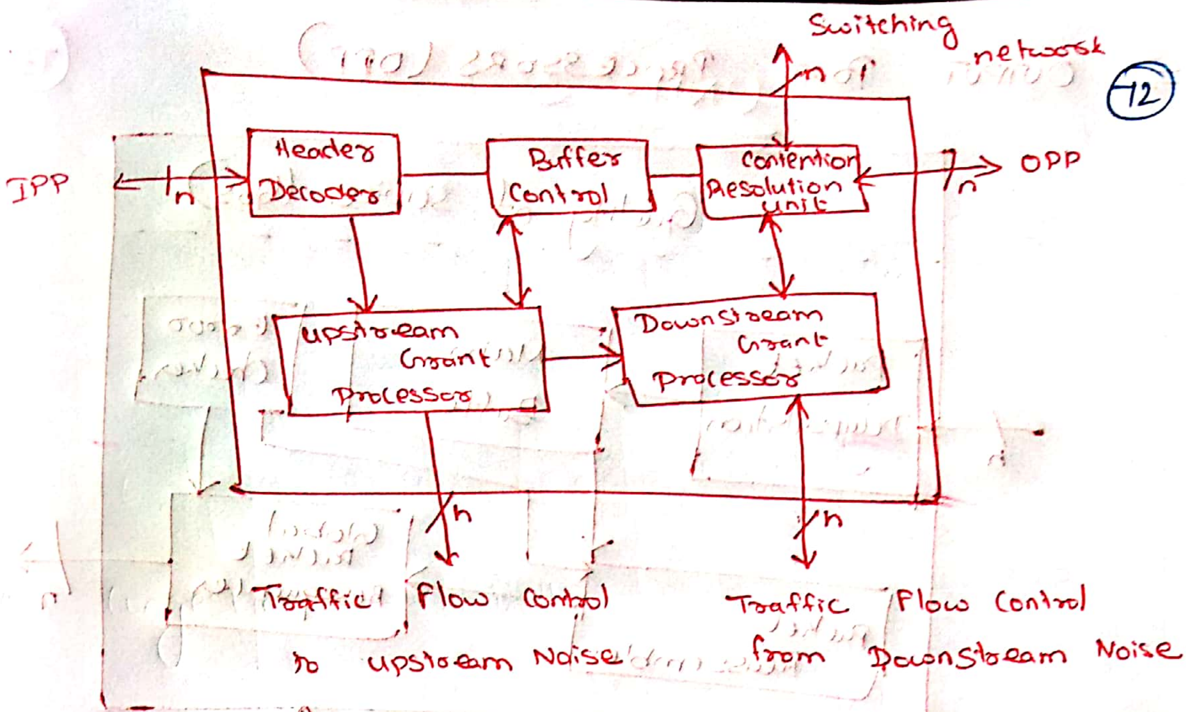


=> SWITCH CONTROLLER:-

- Controller part of a switching system makes decision leading to the transmission of packets to the requested output

- Controller receives packets from an IPP but only the header of packets are processed in the controller.

- The header decoder first converts the control information of an arriving packet into an initial requested output vector.

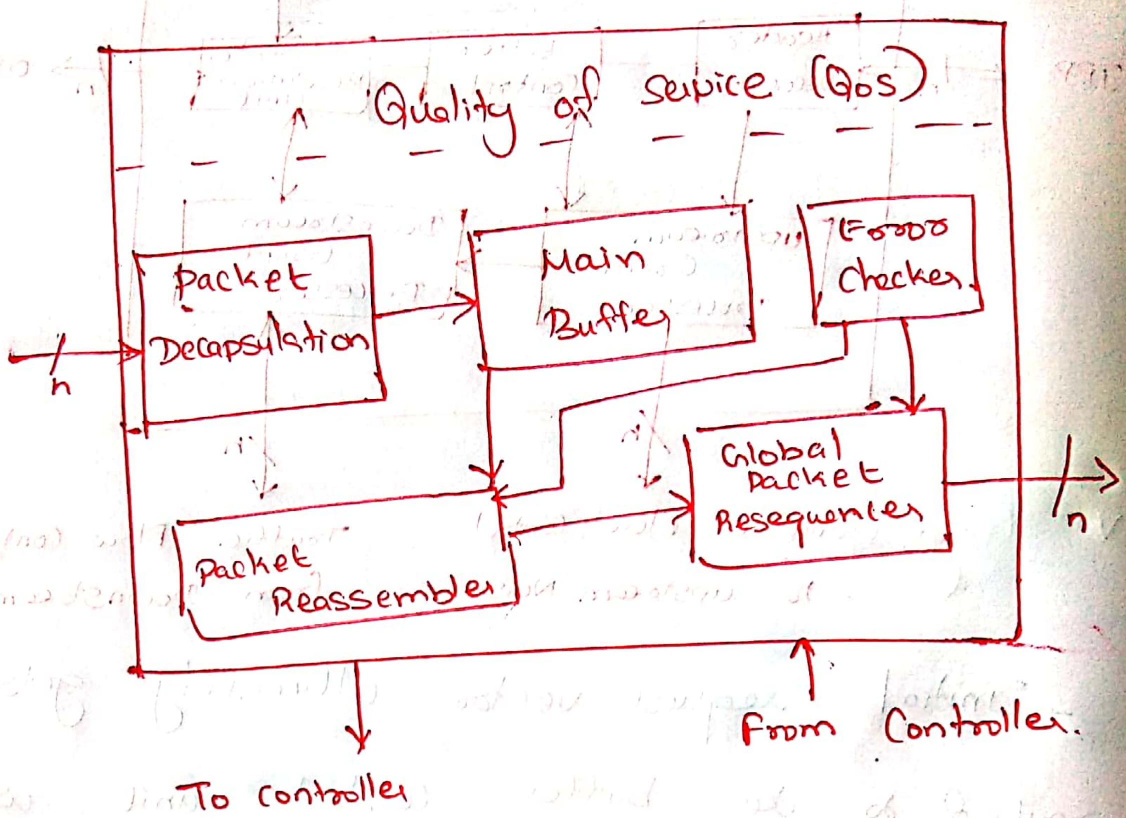


- Initial request vector ultimately gets routed to the buffer control unit, which generates a priority value for each packet to enable it for arbitration.

- The identities of winning packets are transmitted to the switch fabric if traffic flow control signals from downstream neighboring nodes are active

- The upstream grant processor in turn generates a corresponding set of traffic flow control signals, which are sent to the upstream neighboring nodes.

⇒ OUTPUT PORT PROCESSORS (OPP)



- It includes Parallel to Serial multiplexing, main Buffer, local Packet resequencer, global packet resequencer, error checker and packet reassembler

(i) Main Buffer :-

- It serves as OPP central shift Register
- It helps to control the rate of the outgoing packets

(ii) Reassembler and Resequencer: (MAC)

- It reassembles the packet into a single packet based on the information obtained from the fragment field of headers.

- ~~It~~ Packet reassembler buffer is used to combine fragments of IP packets.

- Resequencer's internal buffer stores misordered fragements until a complete sequence is obtained.

(iii) Error checker and CRC

When a user sends a packet or a frame a cyclic redundancy check field is appended to the packet.

- It divides the message by another fixed-binary number in a polynomial form, producing a checksum as the remainder.

- Error checker applies a series of error checking processes on packets to ensure that no errors are on the packets.