NETWORK LAYER : LOGICAL ADDRESSING

- IPv4 ADDRESSES – IPv4 Address is a 32 bit address
  IPv6 is 128-bit address (Provides much flexibility in address allocation)

- The address space of IPv4 is 2^{32} or 4,294,967,296 (4 billion)

- Address space is the total no. of addresses used by the Protocol. If Protocol uses N bits to define an address, the address space is 2^N

DOTTED DECIMAL NOTATION & BINARY NOTATION FOR AN IPv4 ADDRESS

10000000 . 00001011 00000011 00011111

128 . 11 . 3 . 31

EXAMPLE – CHANGE IPv4 address From Dotted decimal notation to binary notation

a) 221 . 34 . 7 . 82 ⟶ 11011101 00100010 00000111 . 01010010

CLASSFUL ADDRESSING

- In Classful addressing, the address space is divided into 5 Classes A B C D & E. Here large Part of available address is wasted

CLASSES IN BINARY & DOTTED-DECIMAL NOTATION

	FIRST BYTE	2nd BYTE	3rd BYTE	4th BYTE
CLASS A	0			
CLASS B	10			
CLASS C	110			
CLASS D	1110			
CLASS E	1111			

a) BINARY NOTATION

	1st	2nd	3rd	4th
CLASS A	0-127			
CLASS B	128-191			
CLASS C	192-223			
CLASS D	224-239			
CLASS E	240-255			

b) DECIMAL NOTATION

110 00001 100000 11 000 11011 11111111

CLASSES & BLOCKS

- Classful addressing has a Problem with each class divi[illegible] into a fixed no, of blocks & fixed block size.

CLASS	No, of Blocks	BLOCK SIZE	APPLICATION
A	128	16,777,216	UNICAST
B	16384	65,536	UNICAST
C	2097152	256	UNICAST
D	1	268,435,456	MULTICAST
E	1	268,435,456	RESERVED

CLASS A BLOCK

- The first bit of class A address is always 0

Lowest no - 00000000 Highest no - 01111111

0 —— 127

No, of blocks - $2^7 = 128$

BLOCK SIZE - $2^{24} - 2 = 16,777,216$ (2 addresses reserved for network & broadcast addr)

CLASS B BLOCK

- 10

Lowest no 100000000 Highest no - 10 111111

128 —— 191

No, of Blocks $= 2^{14} = 16384$

BLOCK SIZE $= 2^{16} - 2 = 65536$

CLASS C BLOCK - 110

Lowest no - 11000000 — 11011111

=) 192 —— 223

No, of Blocks $= 2^{21} = 2^8 - 2$

$\swarrow$ 2097152 256

CLASS D BLOCK - 1110

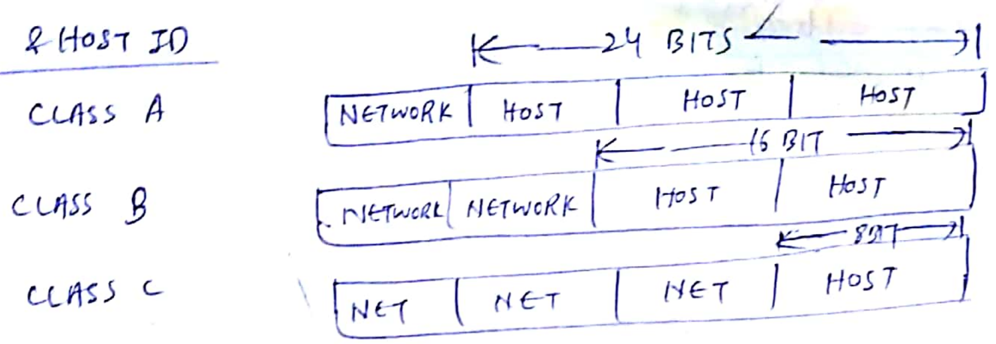
- Lowest no = 1110 0000 - 11011111

224 — 239

No, of Blocks =)

Scanned by CamScanner

NET ID & HOST ID



MASK

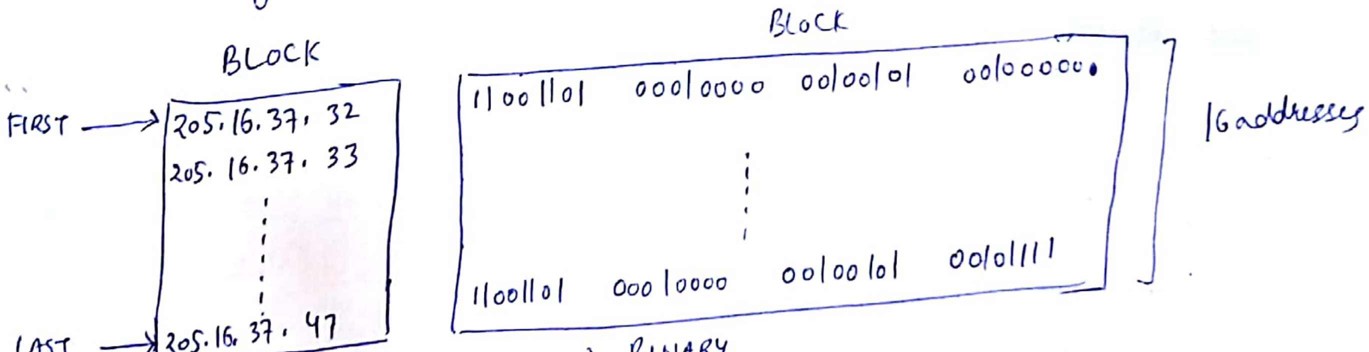
Also called default Mask - a 32 bit no, made of Contiguous Is fallowed by contiguous O's -

					Default SM	CIDR
CLASS A	11111111	00000000	00000000	00000000	255.0.0.0	/⑧ -network bits
CLASS B	11111111	11111111	00000000	00000000	255.255.0.0	/16
CLASS C					255.255.255.0	/24

CLASSLESS ADDRESSING

- To overcome address depletion & give more orgn access to the internet, classless addressing is designed & implemented.

FIG 1 - Shows a block of address, in both binary & dotted decimal notation granted to a small business that needs 16 addresses.



a) DECIMAL b) BINARY

RESTRICTIONS -

① Addresses in a block must be Contiguous, One after another

② No, of addresses in a block must be a Power of 2 (ie $2^4 = 16$)

3. First address must be evenly divisible by no, of addres

NOTE - The first address in a block is normally not assigned to any d it is used as a n/w address that represents the orgn to rest of the world

- In IPv4 addressing, a block of addresses can be defined as

x.y.z.t /n

in which x, y, z, t defines one of the addresses & /n defines the mask.

- The Address & /n notation completely define the whole block (First address ①, last address ② & the no. of addresses ③)

① **First address** – First address in the block can be found by setting the rightmost 32 − n bits to 0's

Example – 205.16.37.39 /28 (one of the address)

what is the first address ?

Sol:- Binary notation of a given address is

128 64 32 16 8 4 2 1

11001101 00010000 00100101 00100111

32 − 28 = 4

11001101 00010000 00100101 00100000

First address | 205 16 37 32 |

② **Last address** – Setting rightmost 32 − n bits to 1's

11001101 00010000 00100101 00100111

32 − 28 = 4

11001101 00010000 00100101 00101111

| 205 16 37 47 |

③ **No. of address** – 2^{32-n}

$\rightarrow 2^{32-28} \Rightarrow 2^4 = \boxed{16}$

128
64
32
16
240

PRIVATE & PUBLIC IP ADDRESSES

Public IP addresses – are assigned by the InterNIC (Internets NIC) & consists of class based n/w ids or blocks of CIDD based addresses that are globally routable to the internet

Private IP address - used for internal n/w. These addresses are not routable to the internet.

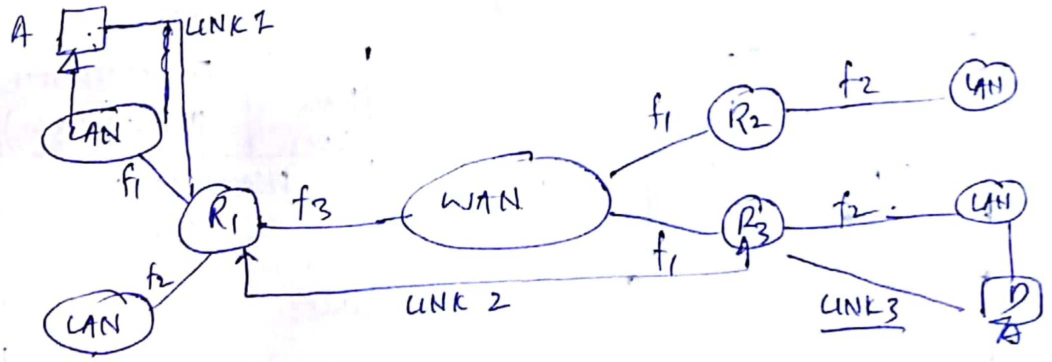
Private address blocks are

10.0.0.0 to 10.255.255.255
172.16.0.0 to 172.31.255.255
192.168.0.0 to 192.168.255.255

NETWORK LAYER : IP

- The main objective of n/w layer is to allow endsystems, connected to different n/w, to exchange information through intermediate systems called router.
- The unit of information in n/w layer is called a Packet

WHY N/W LAYER CAME INTO EXISTENCE



HOP-TO-HOP DELIVERY

Problem – when data arrives at interface f1 of R1, , R1 does not know the interface of the outgoing frame. There is no Provision in Data link (Physical layer) to help R1 make the right decision. The frame does not carry any routing information.

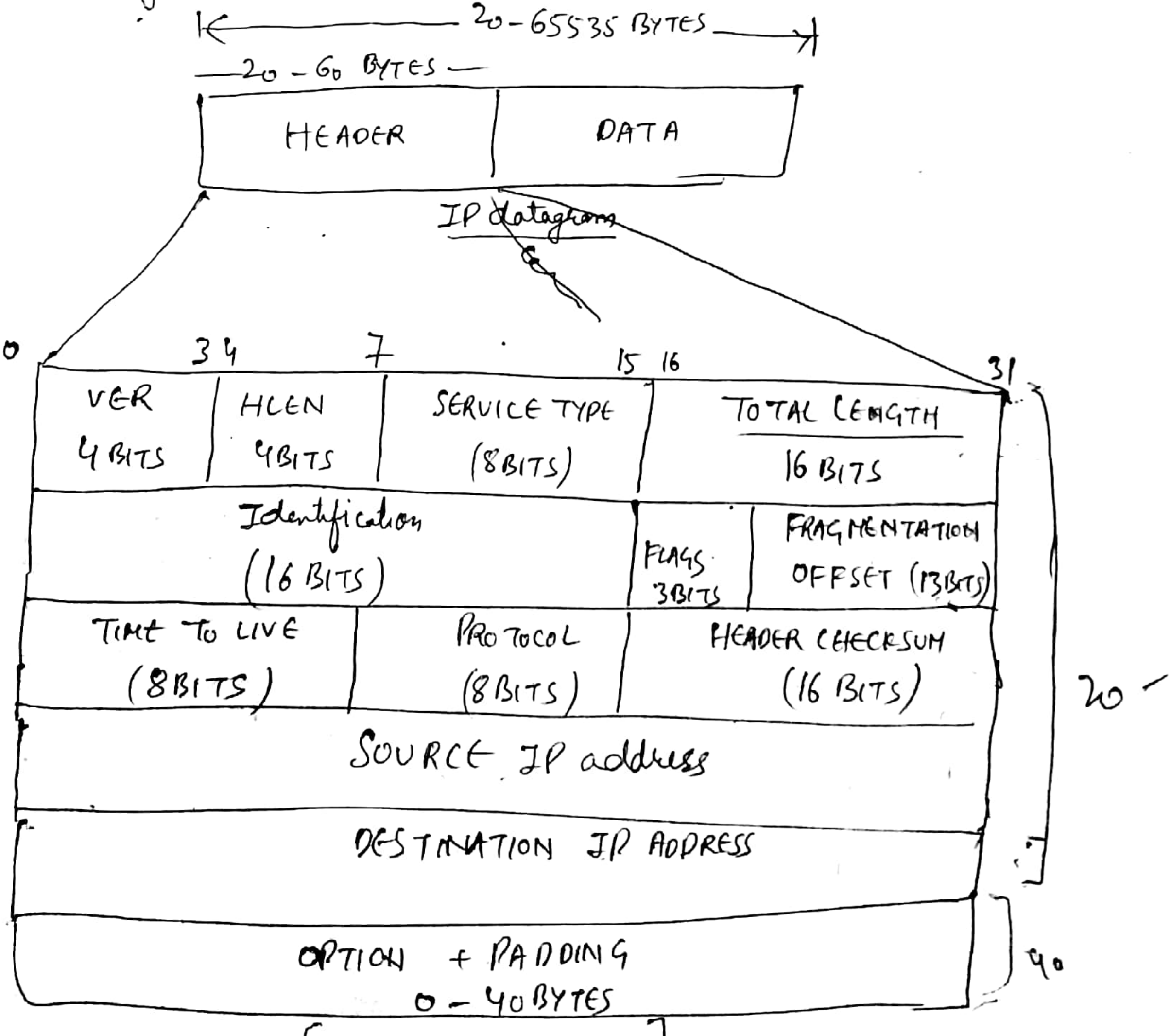
- To solve this, n/w layer was designed which is responsible for host-to-host delivery & for routing the packets through routers & switches

IPV4

- Internet Protocol version 4 (IPV4) is a delivery mechanism used by TCP/IP protocols
- It is an unreliable & connectionless datagram protocol. ie provides no error control or flow control.

DATAGRAM

Packets in the IPV4 layer are called datagrams. IPV4 datagram format is given as.



VER 4 BITS	HLEN 4BITS	SERVICE TYPE (8BITS)	TOTAL LENGTH 16 BITS
Identification (16 BITS)		FLAGS 3BITS	FRAGMENTATION OFFSET (13BITS)
TIME TO LIVE (8BITS)		PROTOCOL (8BITS)	HEADER CHECKSUM (16 BITS)
SOURCE IP address			
DESTINATION IP ADDRESS			
OPTION + PADDING 0 - 40BYTES			

HEADER FORMAT

A datagram is a variable-length Packet consisting of two Parts

① Header ② DATA

Header is 20 to 60 bytes & contains information essential to routing delivery

① VERSION (VER) – 4 bit field defines The version of The IPv4 Protocol. currently version is 4.

If machine is using some other version of IPv4, the datagram is discarded rather Than interpreted incorrectly.

② Header length (HLEN) – This 4 bit field defines total length of the datagram header in 4 bytes.

- when there are no options (no data) the header length is 20 bytes & value of field is 5 (5×4 = 20)   5↓ ×4⟶
- when option field is at its maximum size value of field is 15 (15×4) = 60

③ Services –

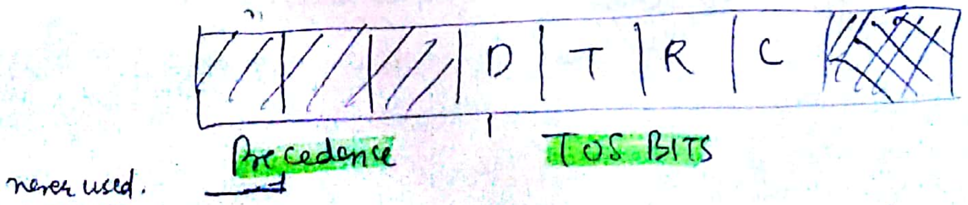
① Service TYPE

Precedence

- First 3 bits are called Precedence bits
- Precedence defines the Priority of datagram in congestion issues
- Datagram with lowest Precedence are discarded first by router in case of congestion
- It is a 3-bit field from 0 to 7

TYPE OF Services

- Next 4 bits are called ToS & Last bit is not used
- It is a 4 bit Subfield with each bit having a special meaning.
- 0000 – Normal
  0001 – Minimum cost
  0010 – Maximum reliability
  0100 – Maximize Through Put
  1000 – Minimize delay



D – Minimum delay
T – Maximum Through Put
R – Max Reliability
C – Minimum Cost

③ Differentiated Services

- In this interpretation, the first 6 bits make up the codepoint subfield & last 2 bits are not used.

  a) when 3 right most bits are 0's, 3 leftmost bits are interpreted same as Precedence bits in the service type interpretation

⑥ Values of Codepoints

Category	Codepoint	Assigning authority
1	XXXXX0	Internet
2	XXXX11	Local
3	XXXX01	Temporary.

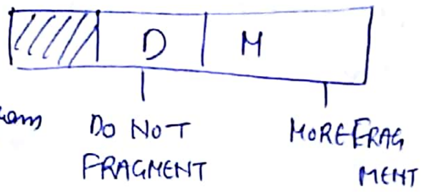
4. **Total length** – 16 bit field defines total length (header plus data) of IPv4 in bytes.

   Length of data = Total length – header length

⑤ **Identification** – 16-bit field identifies a datagram originating from the source host. ~~The~~ All fragments have the same identification number.

The identification no helps the destination in reassembling the datagram.

⑥ **FLAGS** – 3 bit field. The first field is reserved. 2nd field is called do not fragment.



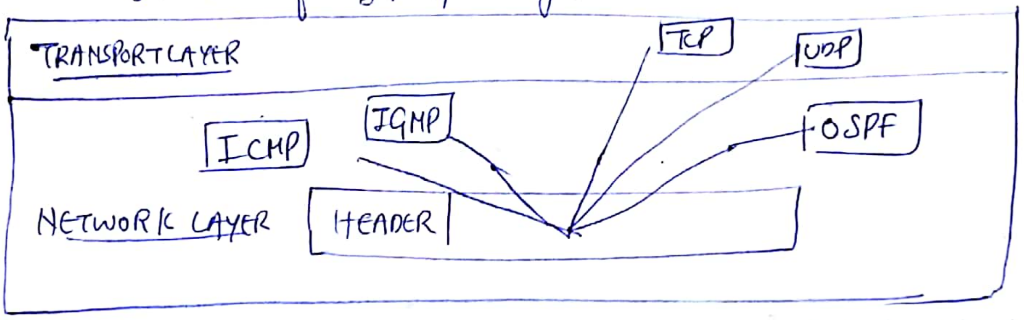
- If its value is 1, machine must not fragment datagram
  010
- If its value is 0, datagram can be fragmented
  0x0

⑦ **Fragmentation offset** – 13 bit field shows relative position of this fragment w.r.t to the whole datagram

⑧ **TIME TO LIVE** – is the no. of hops that a packet is permitted to travel before being discarded by a router.

The datagram is discarded when the value becomes Zero

Protocal - 8 bit field defines higher level Protocal that uses the Services of IPv4 layer.



value	
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

⑩ **CHECKSUM** - IPv4 header checksum is a simple checksum used in version 4 of IP to Protect the header of IPv4 data Packets against data carruption.

⑪ **SOURCE ADDRESS** - 32 bit field defines IPv4 address of The Saurce.

⑫ **DESTINATION ADDRESS** - address of destination.

Example 1 - An IPv4 Packet has arrived with first 8 bits as shown.

01000010

The receiver discards the Packet. why?

Sal:- 4 left most bits (0100) shaw the version. The next 4 bits

Version 4.

(0010) shaw the header length (2×4 = 8 BYTES). The minimum no, of bytes in the header must be 20.

Example 2. In an IPv4 Packet, the value of HLEN is 5 & the value of the Tatal length field is 0x0028. How many bytes of data are being carried by This Packet?

Sal:- HLEN VALUE = 5 &

Tatal no, of bytes in the header is (5×4) = 20 bytes (no option,

Tatal length field is 0x0028 →

8421

1HEX = 4BIT

2×④+8×④

[2×4 +8×4 ⇒ 8 + 32 = 40 BYTES

length of data = Total length − header length

= 40 − 20

= 20 BYTES.

Example 3:- An IPv4 Packet has arrived with first few hexadecimal digits as shown

0x 45000028 0001 | 00000102.

How many hops can this Packet travel before being dropped? The data belong to what upper layer Protocol.

Sol:- To find Time to live (TTL), we skip 8 BYTES (16 hexadecimal digits)

1 HEX = 4 bits

2 HEX = 8 BITS, OR 1 BYTE.

16 HEX = 8 BYTES

So TTL field is the 9th byte ie 01

2HEX

− 8×2

This means Packet can travel only one hop.

- The next is Protocol field which is 02 which means that upper layer Protocol is IGMP.

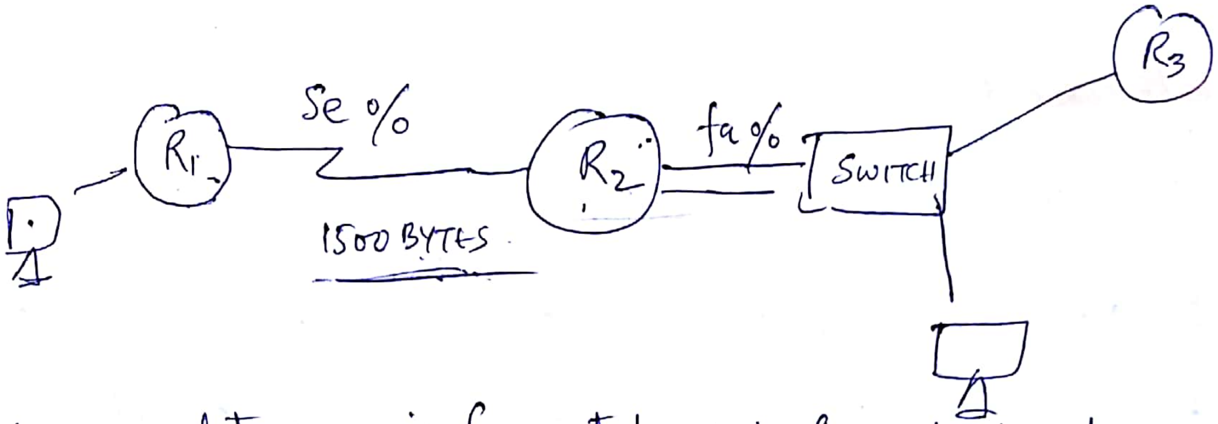
FRAGMENTATION & MTU CONCEPT

- The largest size of data that can be forwarded in network is known as MTU (Maximum Transfer Unit).
  - It depends on Media/n/w type, most likely 1500 bytes use in n/w
- The situation when you have two different type of n/w /media connected with router which have different MTU, in such case router breakes down packet to appropriate size regarding n/w /media Type so that communication takes place.

Breaking Packet into pieces ~~that~~ with header on each Packet is known as Fragmentation.

OR

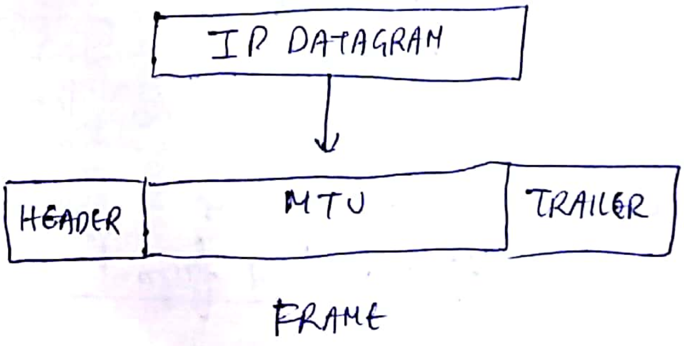
dividing datagram To make it possible to pass through these n/w is called Fragmentation



, when a datagram is fragmented, each fragment has its own header.

MTU FOR SOME N/W's

PROTOCOL	MTU
FDDI	4,352 BYTES
ETHERNET	1500 BYTES
TOKEN RING (4MbPS)	4,464 BYTES
Token RING (16 MbPS)	17,914 BYTES



IPV6 (Logical address)

- 128-bit IP address → IPV4 = 32 bit
- ADDRESS SPACE = $2^n = 2^{128} =$ ____ .
- Address space of IPV_6 is 4 times IPV_4.

IPV6 Advantages

① Larger address space – ↑

② No More need for NAT (Network address Translation)

③ Build in Support for IPsec Security < Encryption / Authentication

④ No More Broadcast ie only
Unicast – one-to one
Multicast – one to many
Anycast – one to closest

Techniques to reduce address shortage in IPv4

- Subnetting
- CIDR
- NAT

IPV_6 address TYPES

- Unicast
- Multicast.
- Anycast.

IPV6 Addressing

- 128 bit address
- Hexadecimal format

2001 : 0db8 : 0000 : 0000 : 1234 : 0000 : 0000 : 3c4d

2001 : 0db8 : 0 : 0 : 1234 : 0 : 0 : 3c4d

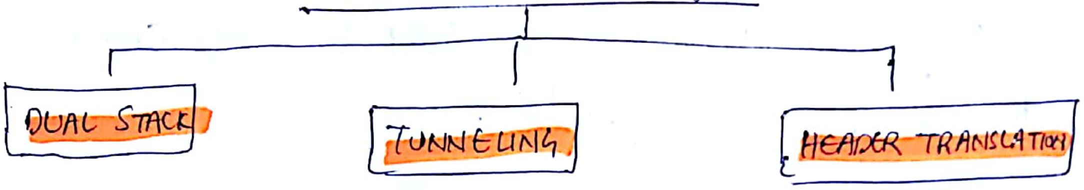
2001 : 0db8 :: 1234 : 0 : 0 : 3c4d

2001 : 0db8 :: 1234 :: 3c4d

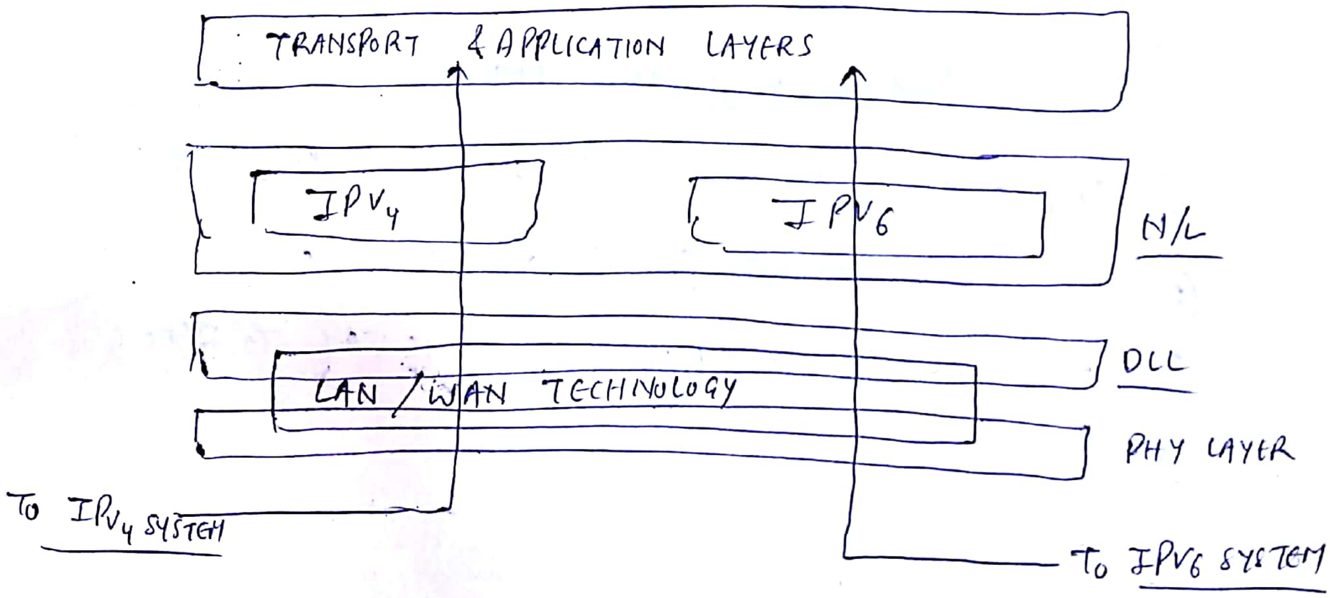
TRANSITION FROM IPv_4 to IPv_6

- Due to huge no. of Systems on the Internet, Transition from IPv_4 to IPv_6 has become a ~~necessa~~ necessity.
- But transition from IPv_4 to IPv_6 cannot happen suddenly.
- The transition must be smooth to prevent any problems b/w IPv_4 & IPv_6 systems.

Three Transition Strategies

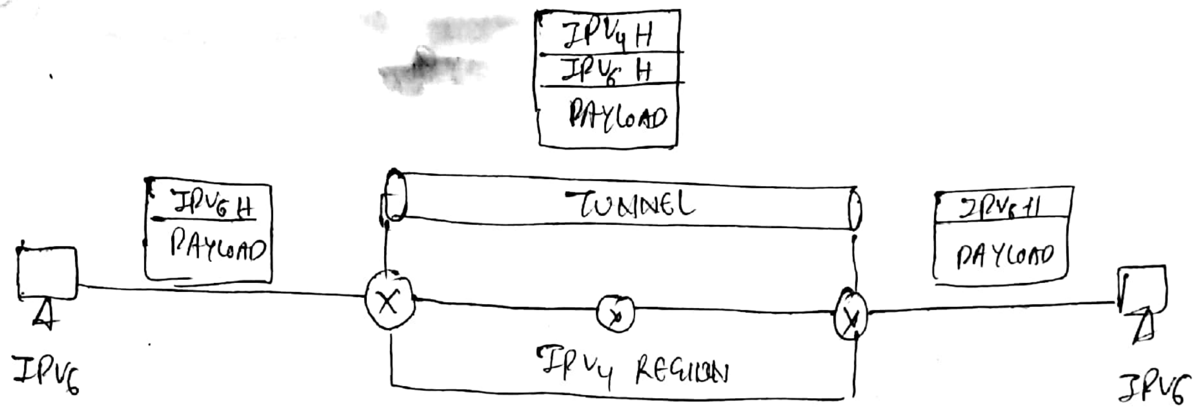


DUAL STACK – All hosts, before migrating completely to version 6, have a dual stack of protocols, until all the internet uses IPv_6.



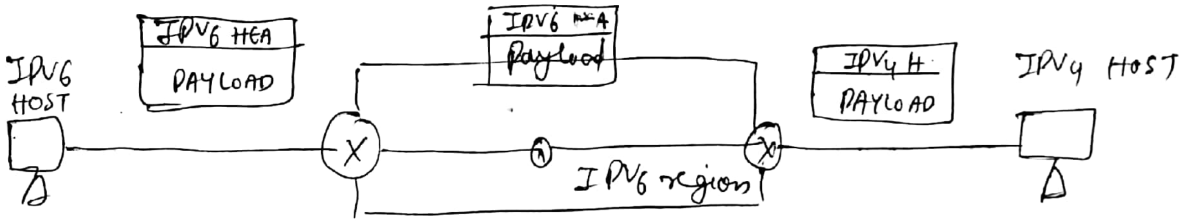
② **TUNNELING** – Strategy used when two computers using IPv_6 want to communicate with each other & packet must pass through a region that uses IPv_4.

- To pass through this region, packet must have IPv_4 address.



③ [redacted] In this Sender wants to USE IPV6 but the recever does not understand IPV6.

- In this case, header format must be totally changed through header translation.



HEADER TRANSLATION PROCEDURE

① IPV6 address is changed to IPV4 address by extracting right most 32 bits

② value of IPV6 Priority field is discarded

③ TYPE OF SERVICE FIELD IN IPV4 IS SET TO ZERO.

④