Marks - 10

Unit - II (Teaching hrs = 08)

Next generation IP.

Unit outcomes

2a. Map the given IPv4 address to IPv6 address.

2b. Describe function of the given step in the stateless auto configuration process.

2c. Outline the given strategy of transition from IPv4 to IPv6

2d. Explain significance of the given field in datagram format of IPv6

TL

2.1 : IP Addressing
- Representation & address space allocation
- Autoconfiguration
- Renumbering

2.2 Transition from IPv4 to IPv6
- Dual stack
- Tunneling
- Header translation

2.3 IPv6 protocol
- packet format
- Extension Header

2.1 IPV6 Addressing

- IPV6 designed to enable high performance and larger address space.
IPV6 was developed due to the address depletion of IPV4.

IPV6 address:-

An IPV6 address is 128 bit long. It consists of 16 bytes

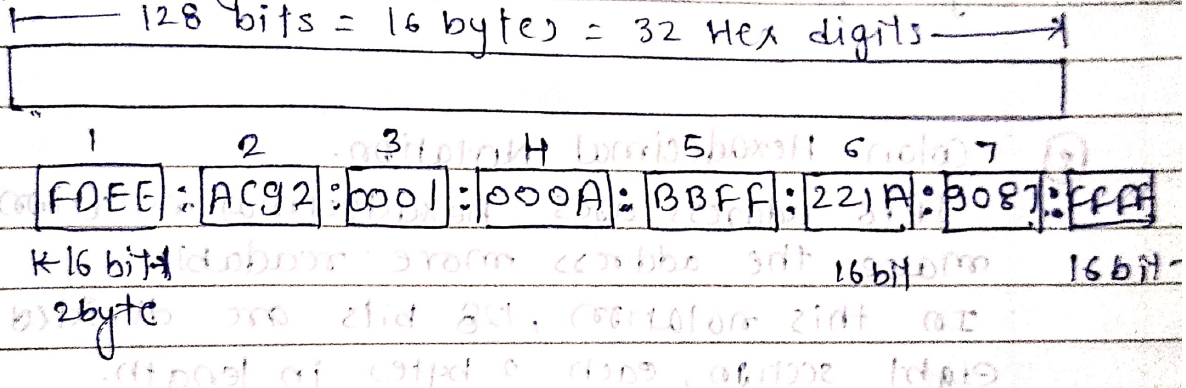


fig: IPV6 address.

Notations:-

- An address is stored in the computer in the binary form, but it impossible for human to handle a 128 bit binary address.
So, following notations included

1) Dotted decimal
2) Colon hexadecimal
3) Mixed representation
4) CIDR notation

① Dotted decimal Notation:-
- This notation is rarely used for IPv6.
- It is used for IPv4 only for the comparison with IPv4 address.
- This notation is superior for 4 byte IPv4 address but it is too long for 16 byte IPv6 address.

eg. 221.14.65.11.105.45.170.34.12.234.18.0.140

② Colon Hexadecimal Notation.
- IPv6 address uses hexadecimal notation to make the address more readable.
- In this notation, 128 bits are divided into eight section, each 2 bytes in length.
- Two bytes in hexadecimal notation require four hexadecimal digit.
- 128 bit hexadecimal address contains 32 hex digits, with every digit is separated by a colon.

ABCD.EF01:2345:6789:ABCD:B201:5482:D08

③ Mixed Representation
- mixed representation of an IPv6 is the combination of dotted decimal and hexadecimal notation.
- This is required during the transition period in which IPv6 addresses that embed IPv4 addresses.

8050:2D9D:DC28:FC57:212.200.31.255

Binary	Decimal	Hexadecimal
0000	00	0
0001	01	1
0010	02	2
0011	03	3
0100	04	4
0101	05	5
0110	06	6
0111	07	7
1000	08	8
1001	09	9
1010	10	A
1011	11	B
1100	12	C
1101	13	D
1110	14	E
1111	15	F

(9) CIDR Notation:

- IPv6 address are fundamentally divided into a number of network ID bits followed by a no of host ID bits.
- IPv6 uses hierachical addressing thus it requires CIDR notation.
- The network identifier is called the prefix and the number of bits used is the prefix length.
- This prefix is represented by a slash
  eg 805B: 2D9D: DC28: FC57: D4C8: FFFF/48.

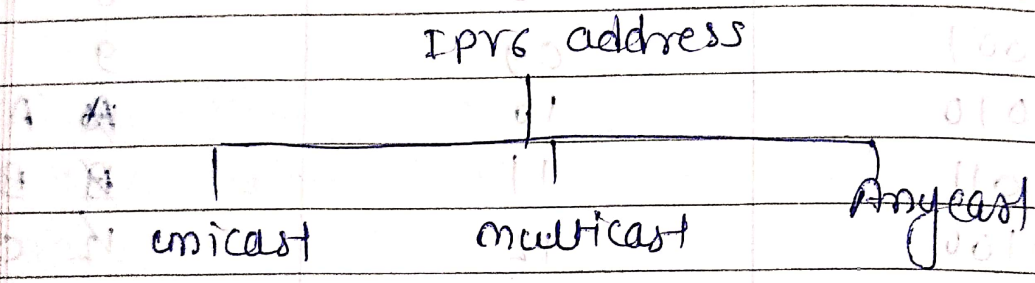
Address space:

2^{128} = 340 trillion trillion trillion

which is a very big number

If we compare this with IPv4 then it can be seen that, the address space of IPv6 is 2^{96} times bigger than that of IPv4

Three Address types:-



① unicast address:-
unicast Address identifies a single network interface. A packet sent to unicast address is delivered to the interface identified by that address

② Anycast address:-
Anycast address is assigned to a group of interfaces. Any packet sent to anycast address will be delivered to only one member interface (mostly nearest host possible)
- No special or separate address block is assigned for anycasting in IPv6.

Multicast addresses :-

multicast address is used by multiple host, called as Group, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address.

Address space allocation:-

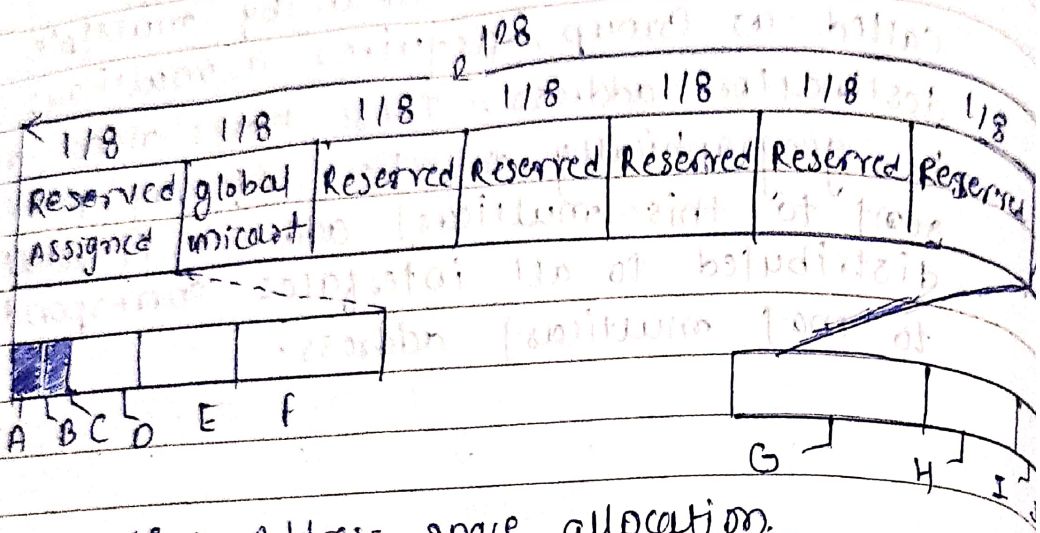


fig: Address space allocation.

A: IPv4 compatible	G: Reserved	M: Reserved
B: Reserved	H: Reserved	N: 1/256 multicast
C: Reserved	I: Reserved	
D: Reserved	J: unique local	
E: Reserved	K: Reserved	
F: Reserved	L: link local	

IPV6 address space is divided into several blocks of varying size and each block is allocated for special purpose.

most of the block are still unassigned and have been left aside for future use.

IPV6 address space is divided into 8 equal ranges.

Each section is one-eight of the whole address space.

In IPV6 address space allocation first and last section contains six and eight variable size block. From which some of the blocks are reserved for

special purpose, some are unassigned and some are used for unicast & multicast communication.

→ The leading bits in the address specify the type of IPv6 address. The variable-length field containing these leading bits is called the formal prefix (FP)

- The allocation support the direct allocation of aggregate global unicast address, local use address & multicast address.
- space is reserved for NSAP, IPX
- address space is unassigned for future use
- The remaining address space can be used for expansion of existing use.
- anycast address are not shown here bez they are allocated out of the unicast address space.

2.3.1 Unicast Addresses:

IPv6 unicast consist of following forms:

1) global unicast addresses - same as public address in IPv4, public IP's helps us to access the internet
2) link local address: these addresses are auto-configure and we get information about this from neighbouring host's. NDP protocol will work here
3) loop back: IPv6 loop back represented in IPv6 as ::1/128
4) unspecified addresses -
when host doesn't know it's own address, then unspecific address used to send

5) unique query to find unknown address of host
ipv4 local : private address similar to

6) embedded address : two parts of embedded address (1) compatible (2) mapped.

Additional address types can be defined in the future.

global unicast addresses are used for global communication. they are similar in function to IPV4 address under CIDR (classless interdomain routing)
48 bit represent the global unicast addres.

(A) local-use address (unique local address):-
It is a unicast address that has only local routability scope. and can have a local or global uniqueness scope.
two types of local-use unicast address
link-local
site-local.
link-local - use for a single link
site-local use on a single site.

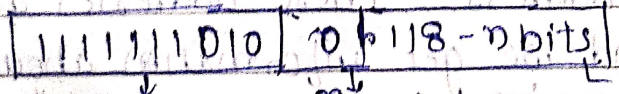


fig: link-local

link local address used for addressing on a single link for purpose such as auto-address configuration.

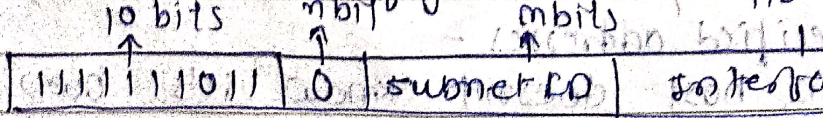


fig: site-local-use address

for both type interface so must be unique

(B) Unspecified Address:

- The unspecified address is a subblock which contains only one address all suffix bits to zero
- During bootstrapping process, when a host does not know it's own address, the unspecified address is used to send on enquiry to find the unknown address of the host.

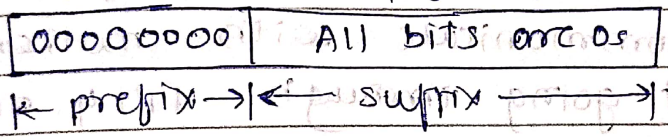


fig - format of the unspecified address.

(C) Loopback address -

address contains only one address which a host uses for testing itself without going into the n/w.

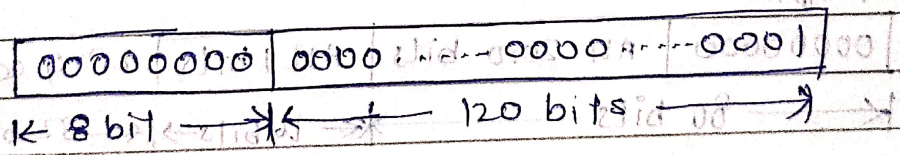


fig - format of the loopback address.

(D) Embedded IPv4 address:-

In migration from IPv4 to IPv6 in this transition period, the host can continue to use their IPv4 address which are embedded in IPv6 address.

two formats are their

1) compatible address
2) mapped address.

(A) compatible address is an IPv6 address with 96 bits of zeros followed by 32 bits of IPv4 address.

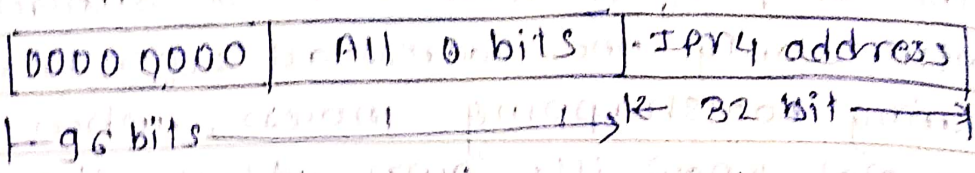


fig- formate of compatible address

used this address used when IPv6 want to communicate with another IPv6 but packet going through IPv4 region or network.

(B) mapped :
used when IPv6 computer wants to communicate with an IPv4 computer.

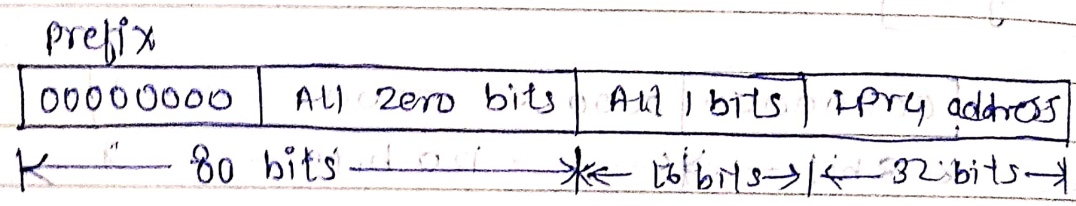
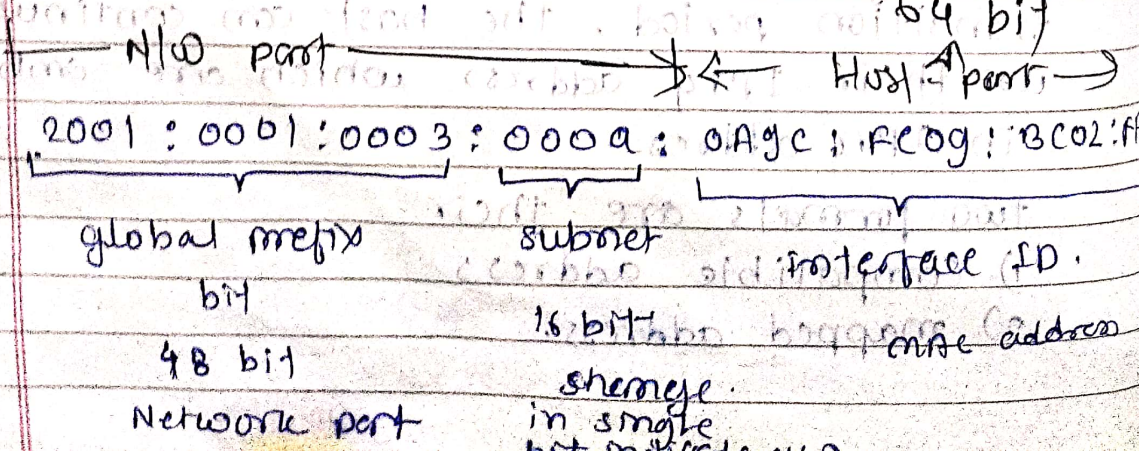


fig ; mapped address.

global unicast address



Features of IPV6 - Winter 2019 2 marks

IPV6 is redesigned entirely. It offers the following features:

a) **Larger Address Space:**
IPV6 uses 2^128 bits address space which is 4 times more than the address space of IPV4.
- This address can accumulate the aggressive requirement of address allotment for almost everything

b) **Simplified Header**
- All unnecessary information & options are moved to the end of IPV6 header, thus IPV6 header is more simplified.
IPV6 header is only twice as bigger than IPV4 provided the fact that IPV6 address is four times longer

c) **end-to end Connectivity**
- Every system now has unique IP address and traverse through the internet without using NAT or other translating components.

d) **Auto-configuration:-**
IPV6 supports both stateful & stateless autoconfiguration of it's host device. absence of a DHCP server does not put a halt on inter segment communication.

e) Fast forwarding / routing
1st part of the header puts all unnecessary information at the end of the header. The information contained in the first part is adequate for a router to take routing decisions.

f) IP sec:-
Initially it was decided that IPv6 must have IPsec security, making it more secure than IPv4.

2.4 Auto configuration

- IPv4 hosts were configure manually later configuration protocol like DHCP enable server to allocate IP automatically
- IPv6 has feature of auto configure or self configure we called it as stateless autoconfiguration (SLAAC).
- If DHCPv6 is there then we called it as stateful.

Stateless autoconfiguration (SLAAC)

IPv6 has new features

1. link-local address
2. multicast
3. Neighbor Discovery (ND) protocol
4. generate interface ID from Data link layer i.e MAC.

- IPv6 uses the Router solicitation & advertisement message to learn IPv6 new prefix, default router IPv6 address from new router.
- After obtaining prefix length and default router IPv6 address from new router, IPv6 new interface can automatically derive a global unicast IPv6 address using EUI-64 method

EUI-64 (extended unique identifier)

↓ command

eg. `2001:0001:0002:0009::64 eui-64`

- 2001:0001:0002 — global 48 bit prefix
- 0009 — subnet id
- 64 eui-64 — will take interface ID from datalink layer

How it take interface ID

eg. suppose, MAC address is

0ABC : D903 : 34E7 - 48 bit mac

so, over here we need to add 16 bit FFFE because interface ID is 64 bit so we get 48 bit mac from datalink + 16 bit FFEE we are going to add. (on 6 digit count add FFFE)

0ABC : D9 | 03 : 34E7

↑ add FFFE here

~~2001 : 0001 : 0002 : 000a : D9FF : FE03 : 34E7~~

2001 : 0001 : 0002 : 000a : 0ABC : D9FF : FE03 : 34E7

global prefix 48 bit | subnet 16 bit | 64 bit interface ID

Note :- This example I take to understand the concept of autoconfiguration practically

By entering eui-64 command interface ID will generate automatically.

The following is a summary of the steps a device takes when using stateless autoconfigution.

Step 1:- Link-local Address generation:

① take 10 bit of link local prefix 1111 1110 10

② add 54 zeros

typically this will be derived from the data link (MAC)

Step 2:- Link-local Address uniqueness test

- It ensures uniqueness.

host then checks for uniqueness of local address. 64 bit interface identifier should be unique.

so host sends neighbor solicitation message using Neighbor Discovery protocol. (NDP)

- It listen for neighbor advertisement in response that indicates another device is already using it's link local address.

if this happen then auto configuration is fail so for that uniqueness is very important

Step 3: Link local address assignment.

- once uniqueness test pass by using (NDP) then device assign link-local address to it's interface

This generated address help to communicate locally we can't access internet using this address for that we need global unique

Step 4: Router contact

node next attempts to contact local router for more information on continuing auto configuration

this can be done by router solicitation & advertisement request

step 5: Router direction
The router provides direction to the node on how to proceed with the auto configuration.
- It may tell the node the stateful config is going (DHCP)
alternately, it will tell the host how to determine its global Internet address.

step 6: global Address configuration
host will configure itself with its globally-unique Internet address.
this address formed from a n/w prefix provided to the host by the router.

Renumbering :-
Renumbering of devices is a method related to auto configuration, like host configuration. It can be implemented using protocol like DHCP, through the use of IP addresses "leases" that expires after a period of time.
under IPv6, network can be renumbered by having routers specify an expiration interval for network prefixes when auto configuration is done.
- they can send a new prefix to tell devices to regenerate their IP address.
devices can actually

Transition from IPv4 to IPv6

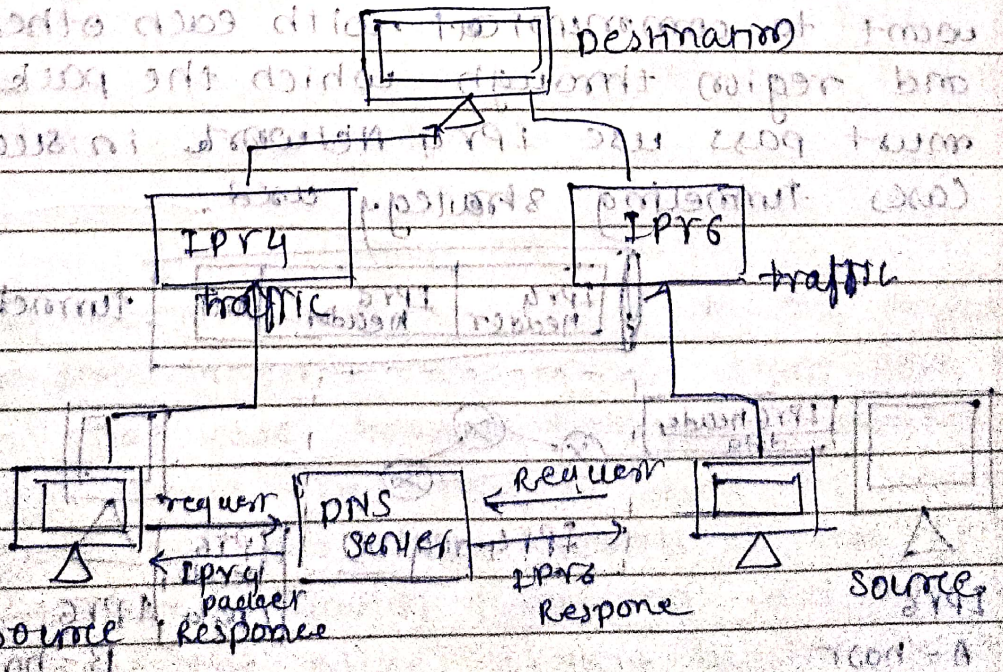
(winter 2019 - 4 marks)

- when we want to send a request from an IPv4 address to an IPv6 address but it is not possible because IPv4 and IPv6 transition is not compatible for soln to this problem, we use some technologies.

a) Dual stack Router,
b) Tunneling
c) Header translation

a) Dual stack Router :-

In dual stack router, a routers interface is attached with IPv4 & IPv6



eg. fig:- Dual stack

Before completly migrating to version 6 it is recommended that all hosts should have a dual stack of protocol at the time of transition.

- simultenously station should run IPv4 & IPv6 IPv4 & IPv6
- A source host send query to the DNS for deciding which version to use while sending a packet to a destination

- A source hosts send IPv4 packet if an IPv4 address is returned by the DNS and send IPv6 packet if DNS return IPv6 address

2) Tunneling :-

when two computers are using IPv6 want to communicat with each other and region through which the packet must pass use IPv4 Network in such cases tunneling strategy used.

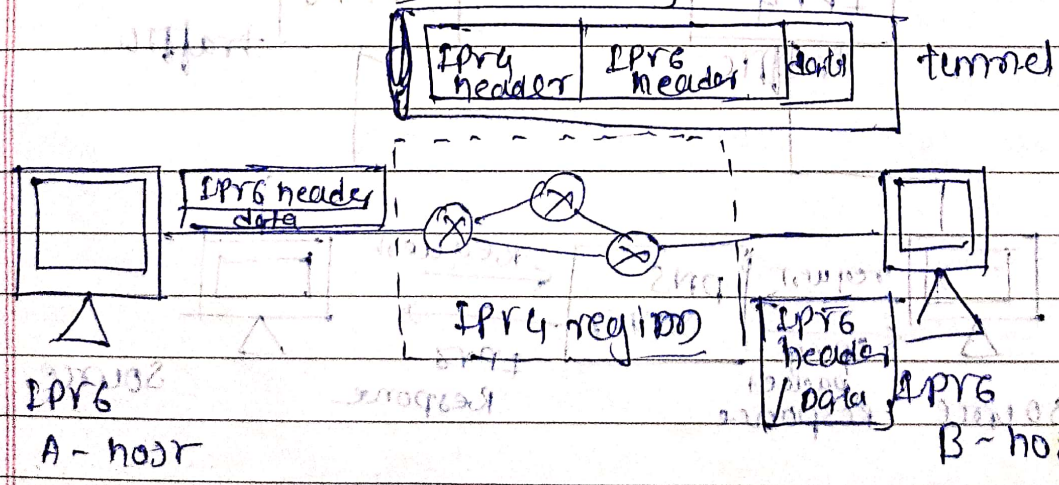


fig: tunneling

- when IPv6 packet enter in IPv4 region it encapsulate in IPv4 packet & when it exit the region it leaves the packet
- It look like IPv6 packet enter is tunnel from one end. encoded with IPv4 & come out from tunnel as IPv6.
- The protocol value set to 41 for holding IPv6 packet by IPv4 packet
tunneling protocol PPoP point to point protocol

8.) Header translation :

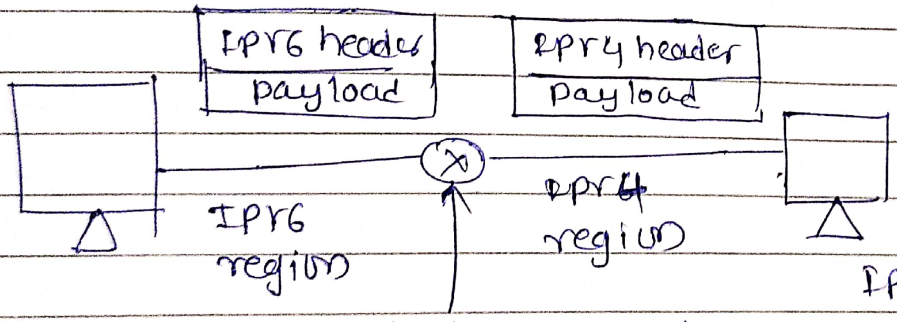


fig - Header translation.

- If some system use IPv4 & the majority of the Internet has moved from IPv4 to IPv6 in that case header translation strategy is used where the receiver does not understand IPv6 but the sender wants to use IPv6 only
- In this situation tunneling will not work because the packet should be in the IPv4 format which has to be understood by the receiver.

- In this strategy through header translation the format of header must be totally changed.
- The IPv6 packet header is converted into an IPv4 header.

Difference between IPV4 and IPV6 (W-19)
2 - marks.

	IPV4	IPV6
1)	IPV4 has 32-bit address length	IPV6 has 128-bit address length.
2)	IPV4 has 2^{32} bits address space.	IPV6 has 2^{128} bits address space
3)	IPV4 address written in dotted decimal notation.	IPV6 address written in hexadecimal & consists of 8 groups containing 4 hex digit.
4)	Length of IPV4 header is minimum 20 byte to 60 byte maximum and it uses 13 fields to identify various control setting	It is static header of 40 bytes in length and has only 8 fields. option information is carried by extension header.
5)	It supports manual and DHCP address configuration.	It support Auto & renumbering address configuration.
6)	In IPV4 end to end connection integrity is unachierable	In IPV6 end to end connection integrity is achierable
7)	source and destination address are of 32 bits	source & destination address are of 128 bit

8) security features is dependent on app thus IPSec support is optional.	IPSEC is inbuilt security feature in the IPV6 protocol.
9) Fragmentation performed by sender & forwarding routers	In IPV6 fragmentation performed only by sender.
10) In IPV4 encryption and authentication facility not provided	In IPV6 encryption & authentication are provided

IPV6 protocol Packet Format

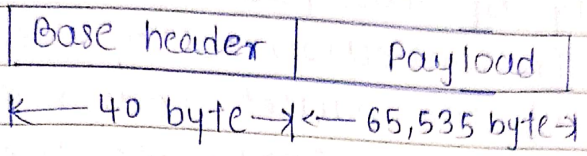


fig : IPV6 packet

- Base header is mandatory part and payload is optional one.

The payload is made up of two parts
1. An optional extension header
2. The upper layer data.

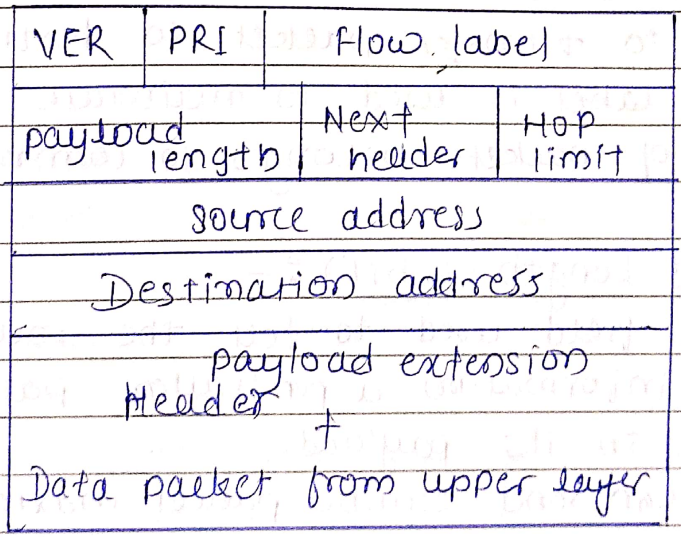


fig: Format of IPV6 Datagram. (Base header)

VER (version) (4 bit) : The contents of 4 bit field defines the version of IP such as IPV4 or IPV6 If VER = 6, then the version is IPV6 i.e 0110.

Priority (4 bit) This 4 bit field contents defines the priority of the packet which is important in connection with the traffic congestion. if the packet comes in flow then according to priority we forword packet & low priority packet discard.

Flow label :(24) It is a 24 bit (3 bytes) It designed for real-time data processing means no delay in data transfer with minimal loss.

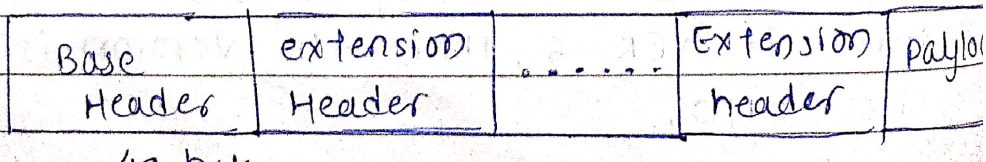
- so datagram service convert in to virtual circuit.
- virtual circuit decide to follow only one path to transfer packet to destination
- flow label is used to maintain the sequence flow of packet belongs to communication

Payload Length (16 bit) :-

This field used to tell the router how much information a particular packet contain in its payload.

you can send jumbo packet maximum 4GB data. for this we need extension header. if the extension header contain Hop by Hop extension header then payload may exceed

Next Header (8 bit)



This field is used to tell the router how much information a particular packet contain in it's payload.

This field is used to indicate either the type of extension header, or if the extension header is not present then it indicate the upper layer.

Hop limit (8 bit) :-

This field is used to ~~indicate either~~ the type of extension header

This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPV4. The value of Hop limit field is decremented by 1 as it passes a link when field reaches 0 the packet discard

Source address (128 bit) : indicate the address of originator of packet

Destination Address (128 bit) :
indicate the destination address.

Extension Header

- IPv6 fixed header keeps only necessary information for router, all other information that is not necessary and rarely used not included in fixed header.
- such information but in extension header
- when extension header are used, IPv6 fixed Next-header field points to the second one and so on.
- If Next header contain the value 59, it indicate that there are no header after this header, not even upper layer Header.

The sequence of extension Header should be

1) IPv6 Header
2) Hop by Hop options header.
3) Destination option header 1
4) Routing header
5) Fragment header
6) Authentication header.
7) encapsulating security payload
8) Destination option header 2

Routing Header :- (43)

Contains methods to support making routing decision. means you can decide the route of packet travel from source to destination. sender decides the path of packet.

Hop by Hop (0) :-

each particular hop we provide information

Fragmentation Header (44)

IPv6 intermediate router can't fragment only source can fragment if value is given in Next header then indicate fragmentation is done.

Authentication Header :- (51)

provide authentication service, password & data integrity maintain.

Destination option (60)

Data only read by destination node

encryption security (50)

Encryption information.

important question of unit 2

Q.1) features of IPv4 describe?
Q.2) difference betn IPv4 and IPv6?
Q.3) what is autoconfiguration in IPv6?
Q.4) explain unicast addresses?
Q.5) explain different transition method of IPv4 & IPv6
Q.6) explain IPv6 extension header
Q.7) Draw and explain IPv6 packet format with neat diagram.