ACN - MIDTERM T2.

Name: S. Jyothi
Rollno: B180359CS

1) Features of IPV6 are:

→ expanded addressing capabilities.

→ It also has elimination of "triangle routing" for mobile ip

→ serverless autoconfiguration (plug and play)

- IPV6 supports both stateful and stateless autoconfiguration mode of its host devices. This way, absence of a DHCP server does not put a halt on inter segment communication.

→ End to end connectivity

- every system now has IPaddress uniquely and can traverse through internet without using NAT or other translating components After IPV6 is fully implemented every host can directly reach other hosts on internet with some limitations like firewall, organization policies etc.

→ Larger Address space.

- when compared to IPV4, IPV6 uses 4 times more bits to address a device on internet. This much of extra bits can provide approximately 3.4×10^{38} different combinations of addresses.

→ Simplified and streamlined Header

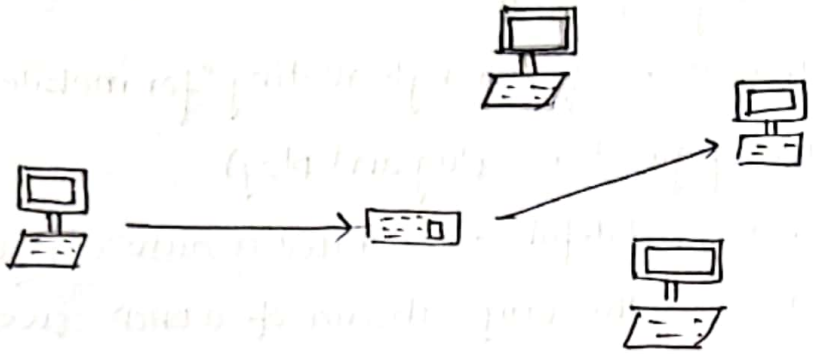
- IPV6's header has been simplified by moving all the unnecessary information and options that are present in IPV4 IPV6 header is only twice as bigger than IPV4 provided the fact that IPV6 address is four times longer.

→ built-in, strong IP-layer encryption and authentication

→ improved support for options/extensions

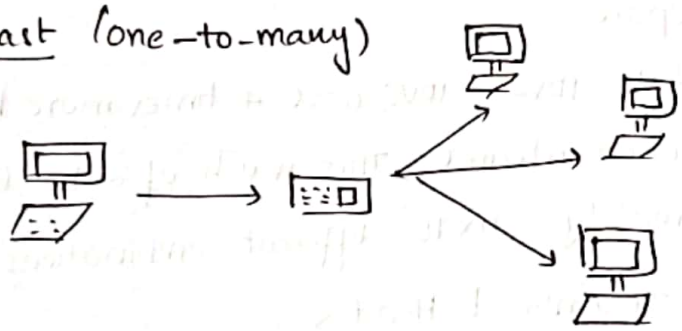
Addressing modes of IPV6 are:

Unicast: (one to one)



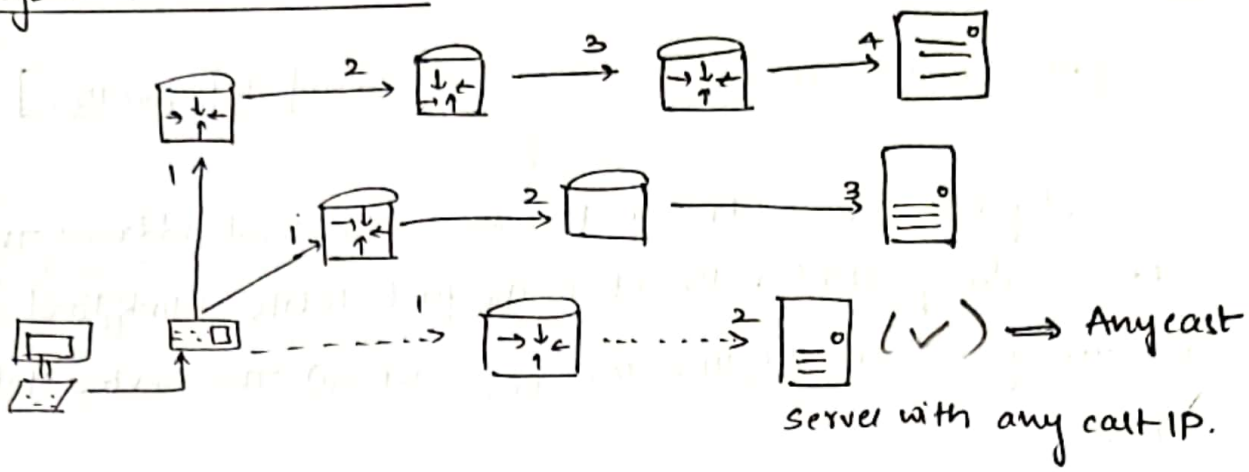
IPV6 interface (host) is uniquely identified in a network segment. The IPV6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment. when a network switch receives a packet, destined to a single host, it sends out one of its outgoing interface which connects to that particular host.

Multicast (one-to-many)



In case of multicast mode it acts same as that of IPV4 The packet destined to multiple hosts is sent on a special multicast address. All host interested in that multicast information, need to join the multicast group first. All the interfaces receive the packet, process them while other hosts which are not interest ignores.

Anycast (one-to nearest):



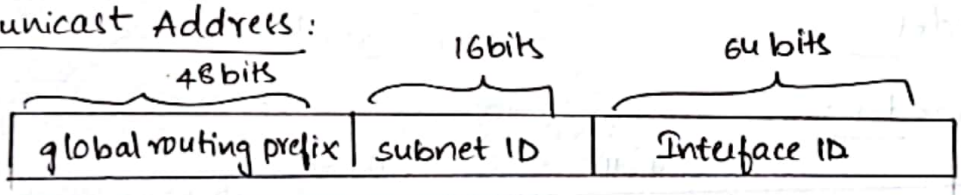
→ In anycast addressing mode, the request is forwarded to the server with the lower routing cost

→ let us take example of abc.com webservers, located in diff continents now a user from europe wants to reach abc.com the DNS point to the server that is physically located in europe itself

→ subnet router anycast address : subnet prefix :: /n

2) IPV6 – Address Formats ~~and Headers~~ :

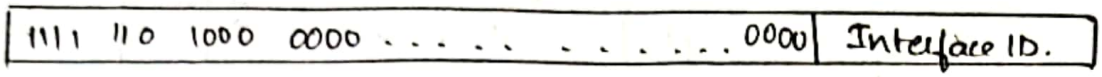
Global unicast Address :



- This address type is equivalent to IPV4's public address. global unicast addresses in IPV6 are globally identifiable and uniquely addressable.
- The most significant 48 bits are designated as global routing prefix which is assigned to specific autonomous system.

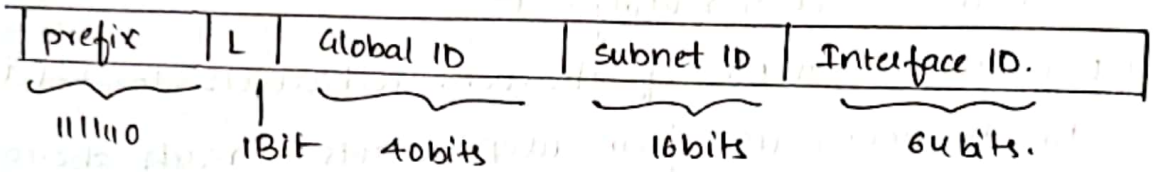
The three most significant bits of global routing prefix set to 001.

Link-Local Address:



Autoconfiqued IDV6 addres is known as link local address. The address always stark with FE80. The first 16 bits of link local addres is always set to 1111 1110 1000 0000 (FE80) The next 48 bits are set to 0.

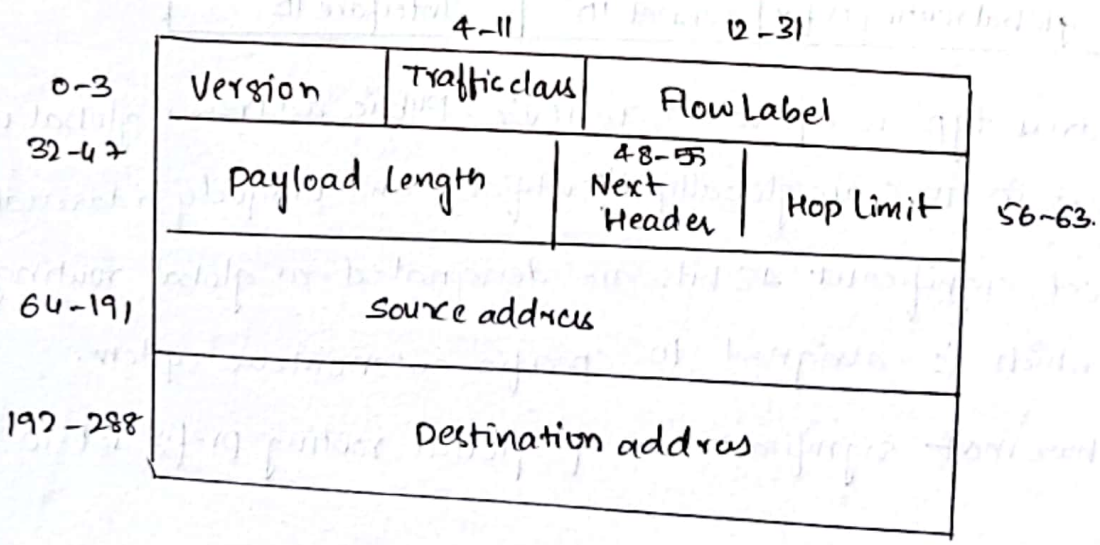
Unique Local Address:



This type of IDV6 is globally unique, but it should be used in local communication. The second half address contain interface ID and the first half is divided among prefix, Localbit, global ID, subnet ID.

3) ## IDV6 Headers:

Fixed header:



Version: It represents the Internet protocol 0110.

Traffic class: 8 bits divided into two parts. The most 6 bits are used for types of service. The least significant 2 bits used for Explicit congenstion notification

Flow label: Used to maintain sequential flow of the packets.

payload length: Tell the routers how much information a particular packet contains in its payload which is composed of extension Header

Next Header: To represent a Extension header is present or not

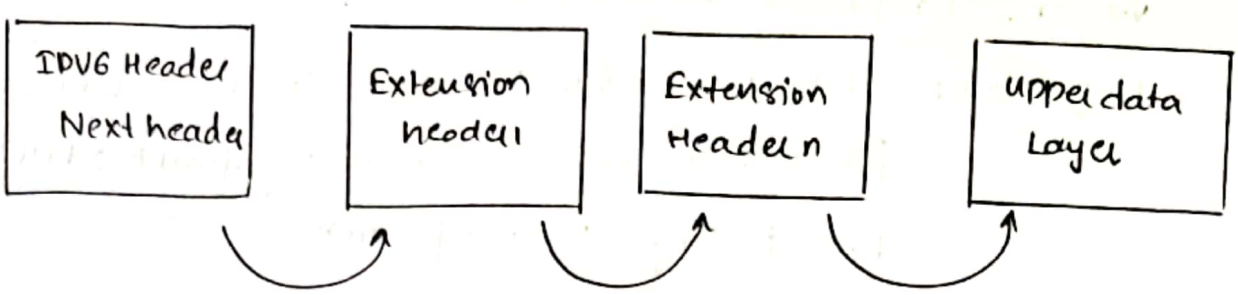
Hop Limit: Used to stop packet loop in a network infinitely

Extension Headers:

Each extension header is identified by distinct value when extension headers are used, IPV6 fixed header's next header field points to first exten header. If there is one more extension header, then 1st extension header's next_header field points to second one and so-on

The sequence should be:

	Next Header value
IPV6 Header	
Hop by Hop options header	0
Destination option header	60
Routing header	43
Fragment header	44
Authonication header	51
Encapsulating payload header	50
upper layer header	



IPV6 – Communication

Neighbour Discovery protocol:

A host in IPV6 network is capable of auto-configuring itself with a unique link-local address. As soon as host gets IPV6 address it joins a no of multicast groups. A host goes through series of states.

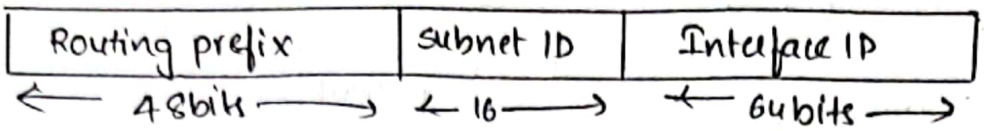
Neighbor solicitation: After configuring all IPV6's manually DHCP server or by auto configuration the host sends a neighbour solicitation message.

DAD (Duplicate Address Detection): when the host does not listen from anything from the segment regarding its neighbour solicalation message.

Neighbour Advertisement:

After assigning the address to its interfaces and making them up and running the host again sends out a neighbour advertisement message.

4) IPV6 - Subnetting:



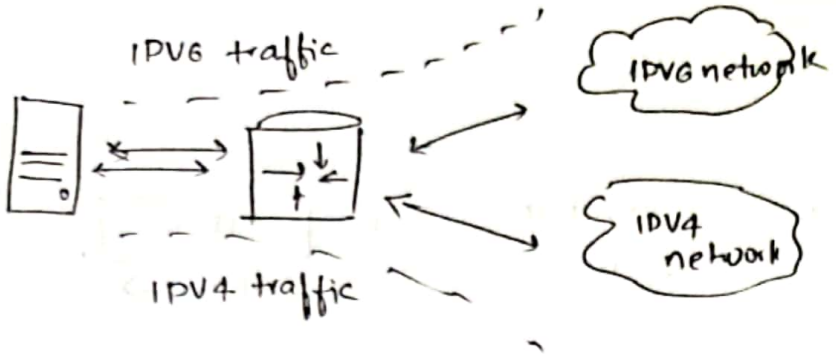
- IPV6 uses 128 bits to represent an address which includes bits to be used for subnetting.
- The second half of the address (atleast significant 64 bits) is always used for hosts only.
  - 16 bits of subnet is equivalent to IPV4's class B network.
  - Using these subnet the organisation can have another 65 thousands of subnets.
  - Thus routing prefix is /64 and host portion is 64 bits
  - we can further subnet the network beyond 16 bits of subnet IP
  - IPV6 subnetting works on the same concept as Variable Length subnet masking in IPV4.
  - /48 prefix can be allocated to an organisation providing it the length up to /64 subnet prefixes each having 65535 subnetworks, having 2^{64} hosts.

Transition from IPV4 to IPV6 :-

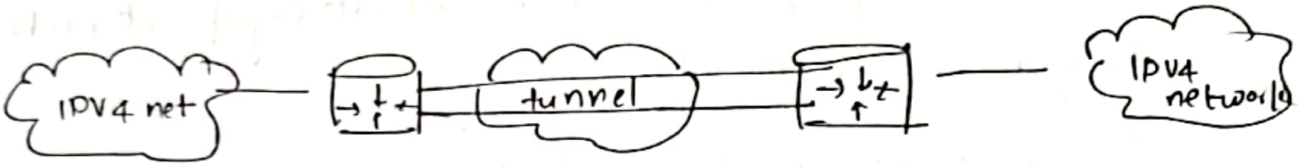
complete transition is not possible because IPV6 is not backward compatible.

Dual Stack Routers

A router can be installed with both IPV4 and IPV6 address configured on its Interfaces pointing to the network of relevant IP scheme.

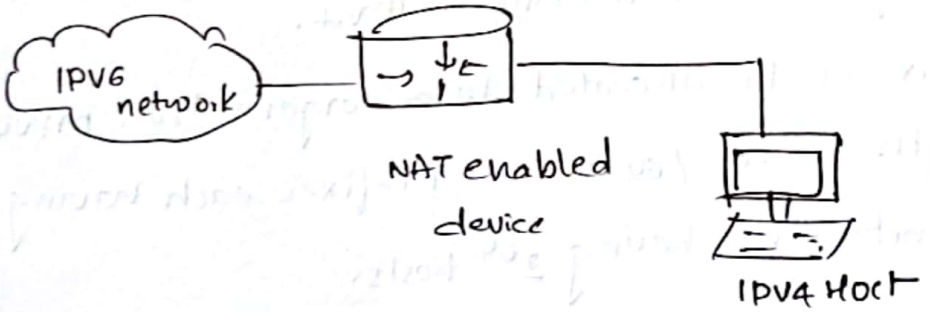


Tunneling:



different IP versions exist on intermediate path or transit networks tunneling provides a better solution where user's data can pass through a non-supported IP version.

NAT protocol Translation :

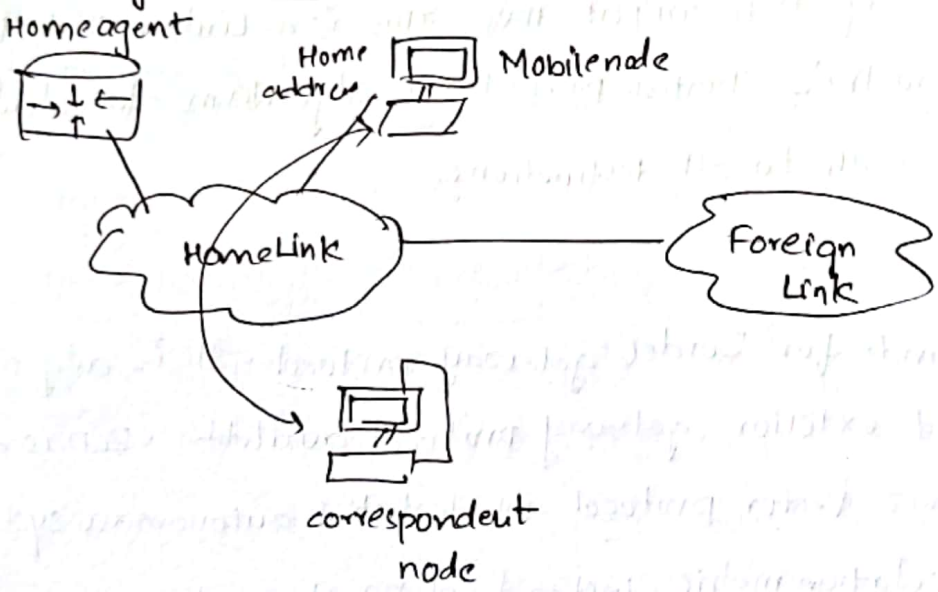


with the help of NAT-PT device actual can take place happens between IPV4 and IPV6 packets. IPV4 sends request to IPV6 enabled server on internet that does not understand IPV4 NAT-PT devices helps to communicate.

5. IPV6 – Mobility

- A mobile host ~~host~~ has one or more home addresses. that are relatively stable associated with host nome in DNS
- when it discovers it is in a foreign subnet i.e not its home subnet it acquires a foreign address then it uses auto configuration to get the address. and also registers the foreign address with a home agent i.e a router on its home subnet.
- packets sent to the mobile's home addresses are intercepted by home agent and forwarded to the foreign address using encapsulation

Mobility operation :-



when a mobile node leaves its home link and is connected to same foreign link the mobility features of IPV6 comes into play. After getting connected to foreign link the mobile node acquires an IPV6 address.

Routing protocols:

1. Interior routing protocol:
   - protocols in this categories are used with an autonomous system or organisation to distribute routes among all routers.

2. Exterior routing protocol:
   information between two different autonomous systems eg: BGP.

3. RIPng
   stands for Routing Information Protocol Next Generation. This is an Interior Routing protocol and is a Distance vector protocol.

4. OSPFV3
   open shortest path first version 3 is an interior routing protocol which is modified to support IPV6. This is a Linked state protocol uses Dijkrastra's Shortest path First algorithm to calculate the best path to all destinations.

5. BGPV4.
   BGP stands for Border gateway protocol. It is only open standard exterior gateway protocol available. BGP is a Distance Vector protocol which takes autonomous system as calculation metric, instead of no of routers as Hop.

6. protocols used in Multicast are:

a) Distance Vector Multicast routing protocol (DVMRP)
   - The first of the multicast routing protocols and hampered by a number of limitations that make this method unattractive for large scale Internet use

- DVRMP is a dense-mode-only protocol
- It uses flood and prune or implicit join method to deliver traffic everywhere and then determine where the uninterested receivers are.

b) Multicast OSPF (MOSPF):

- Extends OSPF for multicast use, but only for dense mode
- MOSPF has an explicit join message so routing devices do not have to flood their entire domain.
- MOSPF uses source based distribution trees in form of (S, G)

c) Bidirectional PIM mode:

- A variation PIM. builds bidirection shared trees that are rooted at rendezvous point (RP) address
- Bidirection traffic does not switch to shortest path trees as in PIM-SM and is therefore optimized for routing state size instead of path length.

---

7) BGP:

- Border Gateway protocol is the postal service of Internet
- when someone drops a letter into a mailbox, the postal service processes that piece of mail and chooses a fast, efficient route to deliver that letter to its recipient.
- similarly when someone submits data across the internet, BGP is responsible for looking at all available paths that data could travel and picking the best route, which usually means hopping between autonomous systems.

IGP:

- Interior gateway protocol, is a type of routing protocol used for distributing routing information within autonomous systems in large internetworks based on TCP/IP. (such as internet)
- They specify how routers within an Autonomous system (AS) exchange routing information with other routers within same as autonomous system.
- This is in contrast to exterior gateway protocols which facilitate the exchange of routing info between different autonomous systems
- examples includes: RIP (Routing Information protocol), OSPF etc...

8) MPLS (Multiprotocol Label Switching)

- MPLS basically converts routed network to something closer to a switched network and offers information transfer speeds that are not available in a traditional IP-routed network.
- It is a mechanism in high performance telecommunications network devices that directs data from one network node to next based on shortest path labels rather than long network addresses.
- It is a mechanism used for transferring data across large data/video/voice networks.
- Each packet entering an MPLS network with a locally significant MPLS label. As the packet passes through the MPLS network, label is replaced with another label or stripped off and the corresponding action is taken based on simply looking up MPLS table.
- Scalable and protocol independent work with IP and ATM.

Few advantages of MPLS are:

1) Improved Network utilization.

- mpls advantage is that it lets you pool the spare bandwidth on every link postponing the date when you need to upgrade the network to cope with increasing demands.

2) Consistent Network performance

- The ability to prioritise traffic on congested links makes it more efficient.

3) Obscures Network complexity.

- It can effectively hide the underlying complexity of the network from devices and users.

4) Easier global changes.

5) Reduced Network congestion.

6) Increased uptime.

→ MPLS reduces downtime by reducing scope for human error.

7) Scalable IP VPN's.