Unit-4

* IPv6 :-

IPv6 is designed to solve many of the problems of the current version of IPv4 :-

① Rapid depletion of the address space :-

→ This led to the use of NATs (Network Address Translator) that map multiple private address to a single public IP address.

→ The main problem by this is processing overhead and lack of end-to-end connectivity.

② Lack of hierarchy support :-

→ Because of its inherent predefined class organization IPv4 lacks fewer hierarchial support.

→ It is impossible to structure the IP addresses in a way that fully maps network topology.

③ Complex Network Configuration :-

→ With IPv4 addresses must be assigned statically or using DHCP.

→ In ideal situation hosts does not rely on the administration of DHCP. Instead they would configure themselves based on network segment in which they are located.

④ Lack of built-in authentication & confidentiality

→ IPv4 does not require support for any mechanism that provides authentication of the exchanged data.

* A new protocol must satisfy
(I) large-scale routing and addressing with low overhead
(II) auto-configuration for various connecting situations.
(III) Built in authentication and confidentiality.

* IPv6 Addressing :-
→ With IPv6 addresses are 128 bits long.
→ One reason for such large address space is to subdivide the available addresses into a hierarchy of routing domains that reflect the network topology.

* Advantages of IPv6 :-
(I) Reliability
(II) Faster speeds → multicast which allows bandwidth-intensive packets to sent to multiple destinations at once.
(III) Stronger security → IP security which provides confidentiality and data integrity.
(IV) Routing efficiency.

* Disadvantages of IPv6 :-
(I) Conversion → Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.

(II) Communication → IPv4 and IPv6 cannot communicate directly, they need intermediate technology.

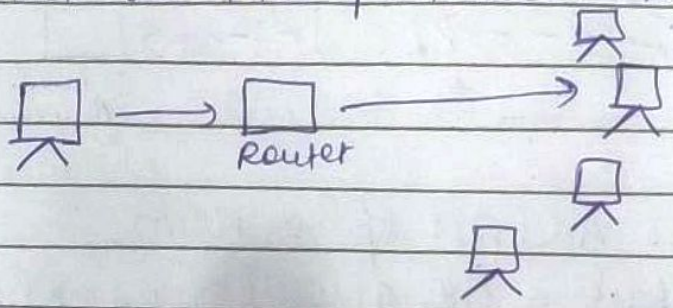
* Types of IPv6 Address :-

(I) Unicast :-

→ IPv6 host/interface is uniquely identified in the network segment.

→ The IPv6 packet contains both source & destination IP addresses.

→ When a network switch or router receives a unicast IP packet, destined to a single host, it sends out one of its outgoing interface which connects to that particular host

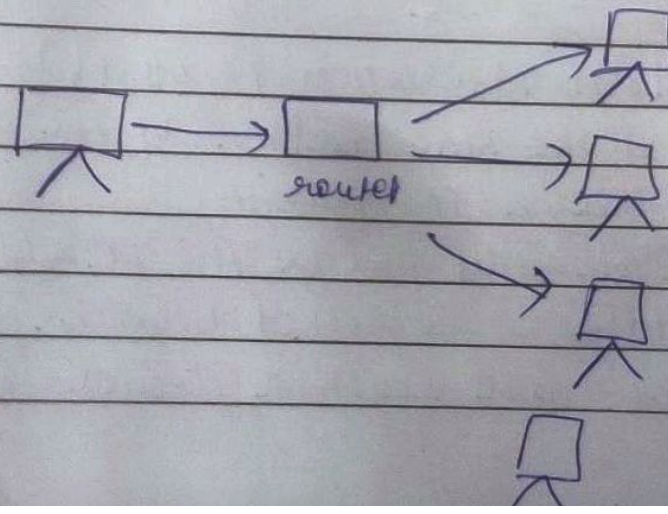


(II) Multicast :

→ The IPv6 packet destined to multiple host is sent on a special multicast address.

→ All the host interested in that multicast information, needs to join that multicast group first.

→ All the interfaces that joined the group receive the multicast packet & process it while others ignore it.

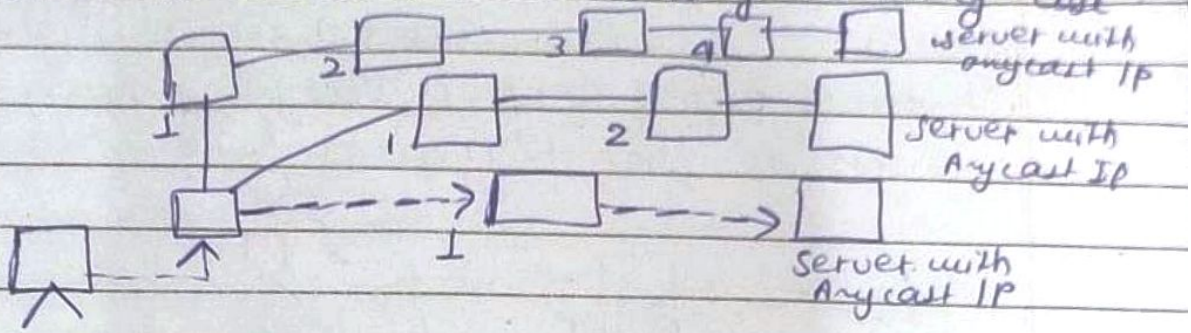


(10) Anycast :-

→ Multiple hosts are assigned Anycast IP address

→ When a host wishes to communicate with a host equipped with Anycast IP address, it sends a Unicast message.

→ That Unicast message is delivered to the host closest to the sender in terms of Routing cost



* What does Address Space Mean :-

→ Address space is the amount of memory allocated for all possible addresses.

→ The system provides each device and process address space that holds a specific ~~position~~ portion of the processor's address space.

→ This can include either physical or virtual addresses.

→ A memory management technique called Virtual Memory can ↑ the size of the address space to be higher than the physical memory.

* ARP (Address Resolution Protocol)

→ Used to find the MAC address of the device from its known IP address.

→ The source device already knows the IP address. The MAC address is required because you cannot communicate with a device in a

local area network without knowing its MAC address.

→ So, the ARP helps to obtain MAC address of the destination device.

IP Address	ARP →	MAC Address

→ The purpose of ARP is to convert 32-bit logical address to the 48-bit physical address (MAC).

→ This protocol works bet^n layer 2 i.e, data link layer where MAC address resides and layer 3 i.e, network layer where IP address resides.

→ IP address is used to locate a device on a LAN and MAC address is used to identify the actual device.

→ Suppose A wants to communicate with B

→ Device A will first look at its internal list known as ARP cache to check if IP address of device B already consists of MAC address.

→ If ARP table consists of MAC address it will simply use that address and start communication.

→ If the table does not consists of the MAC address of device B, then device A sends ARP broadcast message on the network to know which device has specific IP address and ask for its MAC address.

→ Then the device that has matching IP address to the source address sends ARP response message that consists of MAC address of device B.

* Types of Mapping in ARP :-

(i) Static Mapping :-

→ In this IP & MAC address of the device are entered manually in ARP table.

→ The source device has to access the table first if it wants to communicate with destination device.

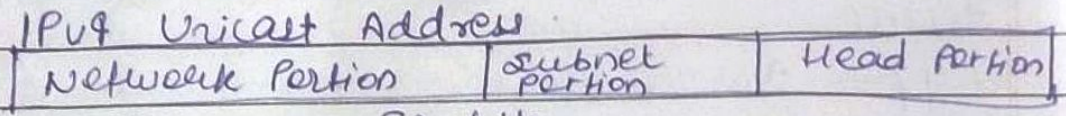
(ii) Dynamic Mapping :-

→ In this if a device knows IP address of other address then by using ARP, this will also find the MAC address.

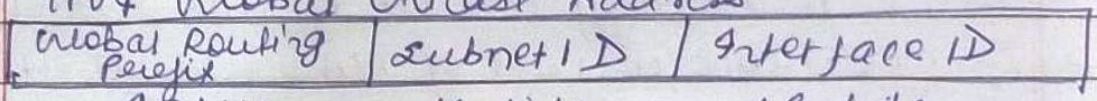
→ Dynamic entries are created automatically.

* Global Unicast Address in CCNA :-

IPv4 Unicast Address



IPv6 Global Unicast Address



(1) Global Routing Prefix :-

→ The most significant 48-bits are assigned as Global Routing Prefix which is assigned to a specific autonomous system.

(2) Subnet ID :- Bet^n Global Routing Prefix & Interface ID

(3) Interface ID :- equal to host part of IPv4 address

* Spring Boot - Auto Configuration :-

→ Spring Boot is heavily attracting developers towards it because of 3 main features :-

(i) Auto configuration
(ii) An opinionated approach to configuration
(iii) The ability to create stand-alone applications.

* Auto-configuration in Spring Boot :-

- @ Conditional annotation acts as a base for the Spring Boot Auto-configuration annotation extension.
- @ Enable Auto Configuration is used to enable the auto-configuration feature.
- This annotation is wrapped inside the @ Spring Boot Application annotation along with @ component scan & @ Spring Boot configuration.

* RPL :-

→ Stands for ~~Low~~ Routing Protocol for low Power and Lossy Networks.
→ Routing protocol for wireless Networks.
→ It holds both many-to-one & one-to-one communication.
→ It is Distance Vector Routing protocol which works by having each router maintain a routing table, giving the best distance from source to destination and which route is used to get there.
→ These tables are updated by exchanging the information with the neighbour having a direct link.

* Modes of RPL :-

1. Storing Mode :-

→ All modes contain entire routing table of RPL domain.

→ Every node knows how to reach every other node directly.

2. Non-Storing Mode :-

→ Only the border routers of the RPL domain contains the full routing table.

* Implementation of RPL Protocol :-

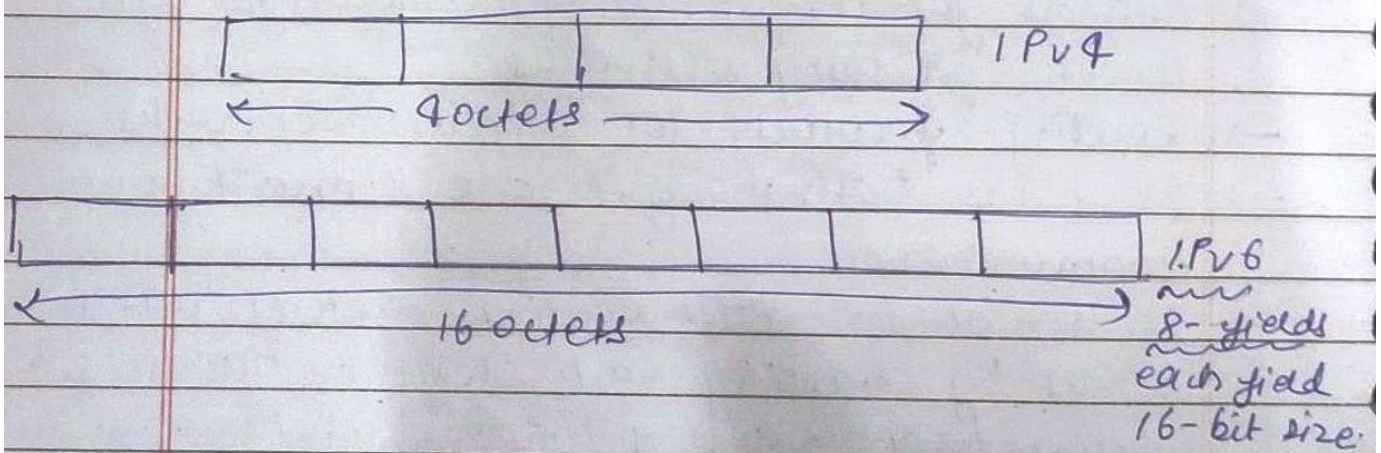
→ Implemented using Contiki Operating System.

→ this OS mainly focuses on low Power Wireless IOT devices.

→ Open source model

→ Other OS → T-Kernel, Eye OS, LiteOS etc.

* Address Format :-



	IPv4	IPv6
(i)	32-bit address	128 bit-address
(ii)	5-classes, A, B, C, D & E	No classes
(iii)	Limited no. of IP address	Has large number of IP addresses.
(iv)	Supports VLSM (Virtual length Subnet Mask). VLSH means that IPv4 converts IP address into a subnet of diff. sizes.	Does not support VLSM.
(v)	Supports manual & DHCP configuration.	Supports manual, DHCP, auto-configuration and renumbering.
(vi)	Generates 4-billion unique addresses	Generates 340 undecillion
(vii)	End-to-end connection integrity is unachievable	Achievable
(viii)	Security depends on the application.	IPSEC is developed for security purpose.
(ix)	IP address is represented in decimal	Hexadecimal
(x)	The checksum field is available	Not available
(xi)	Broadcasting	Multicasting
(xii)	Does not provide encryption and authentication	Provides.

* IPv6 Mobility :

→ IPv6 Mobility provides mechanism for the host to roam around different links without losing any communication / connection and its IP address.

→ Multiple entities are involved :-

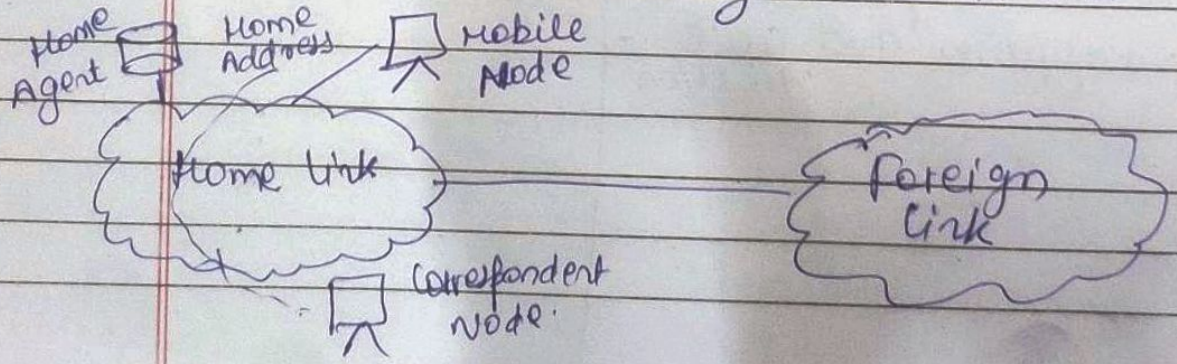
1. Mobile Node → the device that needs IPv6 mobility.
2. Home Link → where Mobile IPv6 device gets its Home Address.
3. Home Address → Permanent Address of Mobile node
4. Home Agent → Home Agent is connected to Home Link and maintains information about all Mobile Nodes, their Home Addresses & their present IP addresses.
5. Foreign Link → Any other link other than Home Link
6. Care-of-Address → When a mobile node gets attached to a Foreign Link, it aquire new IP address of that Foreign Link's subnet.

→ Home Agent maintains information bet? both Home Address and Care-of-Address.

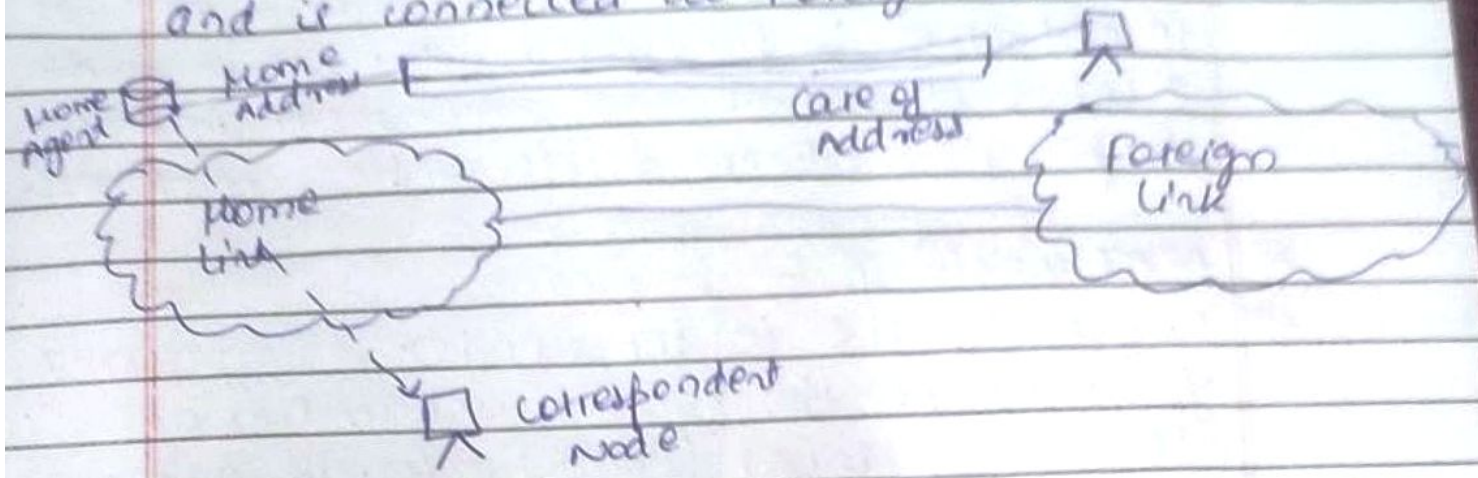
7. Correspondent Node → device that intends to have communication with Mobile Node

* Mobility Operation :

When Mobile Node stays in Home Link



When Mobile Node leaves its home link and is connected to Foreign link.



→ After getting connected to a Foreign link, the Mobile Node aquires an IPv6 address from foreign link. This address is called care-of-address.
→ The Mobile Node sends a binding request to its Home Agent with care-of-Address.
→ The Home Agent binds the Mobile Node's Home Address with the care-of-Address, establishing a Tunnel bet° both.

* Route optimization :-
→ In Route optimization Node, when the Mobile Node receives packets from the correspondent Node.
→ It does not forward replies to Home Agent rather it sends packet directly to the corresponding Node using Home Address as Source Address.

Local → Private
Global → Public

* NAT [Network Address Translation]
→ NAT is a process in which one or more local IP addresses is translated into one or more Global IP address and vice-versa in order to provide internet access to the local hosts

* NAT working :-
→ Generally, the border router is configured for NAT i.e, the router which has one interface in local (inside) network and one interface in the global (outside) network.
→ When a packet traverse outside the local network, then NAT converts the local IP address to Global IP address.
→ When a packet enters local network, the global IP address is converted to local IP address

* Why Mask Port Numbers :-
→ Two hosts A and B are connected
→ Both of them request for same destination on the port no-(say 1000) on the host side at the same time.
→ If NAT only does translation of IP addresses then when their packets will arrive at NAT both of the IP would be masked by public IP address of the network and sent to destination.
→ Destination will send replies to public IP address of the router.

→ On receiving the reply, it will be cleared to NAT as which reply belongs to which host.
→ Hence, NAT masks port numbers as well

* NAT inside and outside Addresses :-
① Inside local address :-
→ IP address assigned to a host inside local network
② Inside global address :-
→ Represents one or more inside local IP addresses to the outside world.
③ Outside local address :-
→ Actual IP address of destination host in local network after translation.
④ Outside global address :-
→ IP address of the outside ~~host~~ destination host before translation.

* NAT Types :-
3-ways to configure NAT

1. Static NAT :-
→ Single unregistered Private IP address is mapped with a legally registered public IP address.
→ one-one mapping bet^n local & global addresses
→ Used for web hosting.
→ Not used in large organization.

2. Dynamic NAT :-

→ An unregistered IP address is translated into a registered (public) IP address from a pool of public IP addresses.

→ If the IP address of the pool is not free then the packet will be dropped as only a fixed no. of private IP addresses can be translated to public addresses.

3. Port Address Translation (PAT) :-

→ Also known as NAT overload.

→ In this many local (private) IP addresses can be translated to a single registered IP address.

→ Port no. are used to distinguish the traffic.

→ Most frequently used as it is cost-effective.

* Advantages of NAT :-

(I) Conserves legally registered IP addresses

(II) Provides privacy as the device's IP addresses, sending and receiving the traffic will be hidden

* Disadvantages of NAT :-

(1) Translation results in switching path delays.

(2) Certain applications will not function while NAT is enabled.

(3) Also, router being a network layer device, should tamper with port numbers but it has to do so because of NAT.