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.

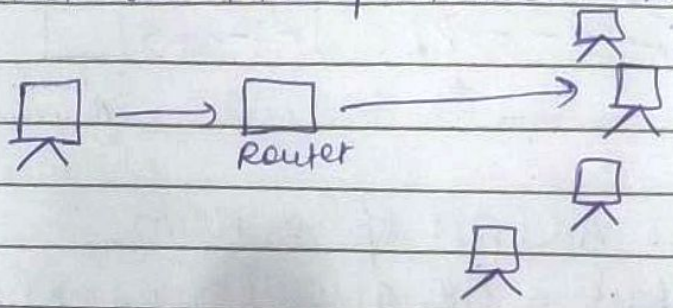
* Types of IPv6 Address :-

(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

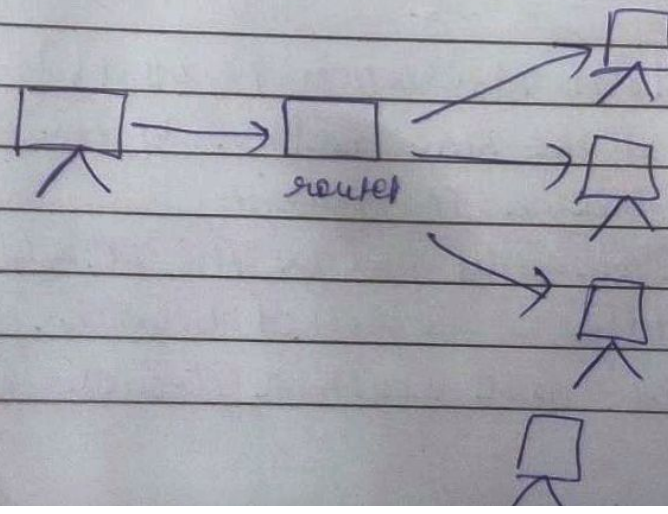


(II) Multicast :

→ 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.

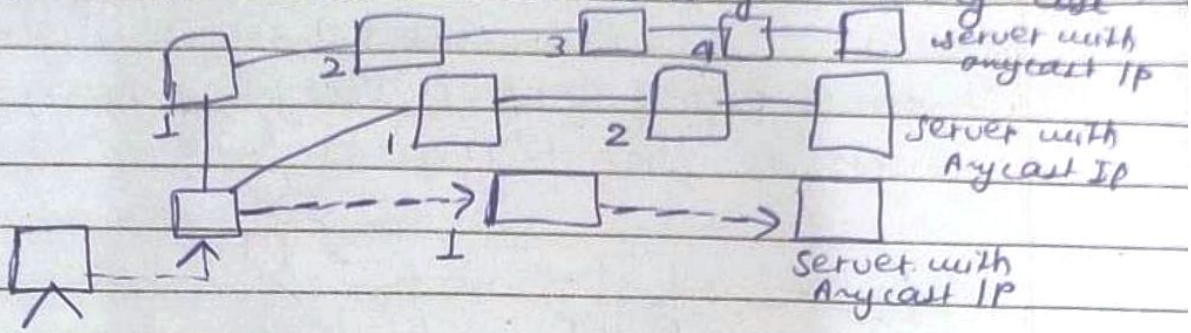


(10) Anycast :-

→ 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.

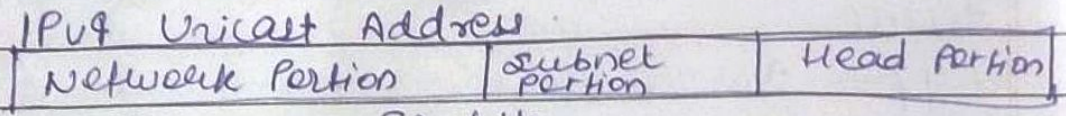
(ii) Dynamic Mapping :-

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

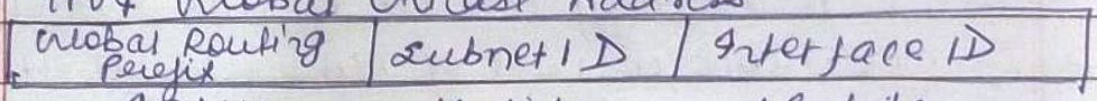
→ Dynamic entries are created automatically.

* 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 :-

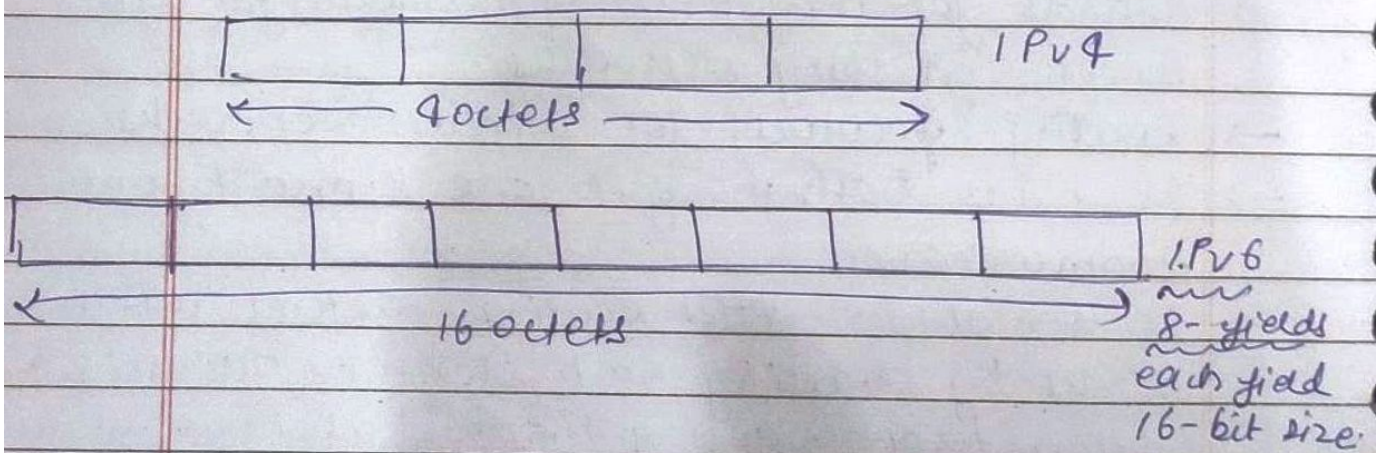
→ Implemented using Contiki Operating System.

→ 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 :-

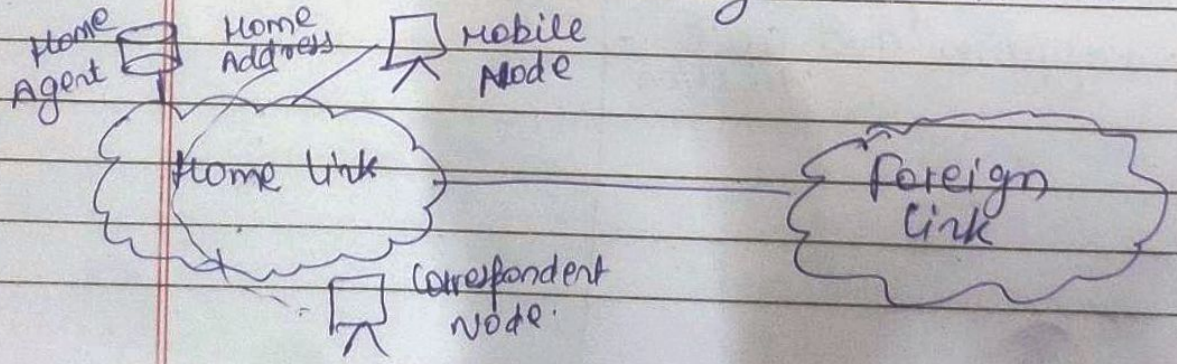
1. Mobile Node → the device that needs IPv6 mobility.
2. Home Link → where Mobile IPv6 device gets its Home Address.
3. Home Address → Permanent Address of Mobile node
4. Home Agent → Home Agent is connected to Home Link and maintains information about all Mobile Nodes, their Home Addresses & their present 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.

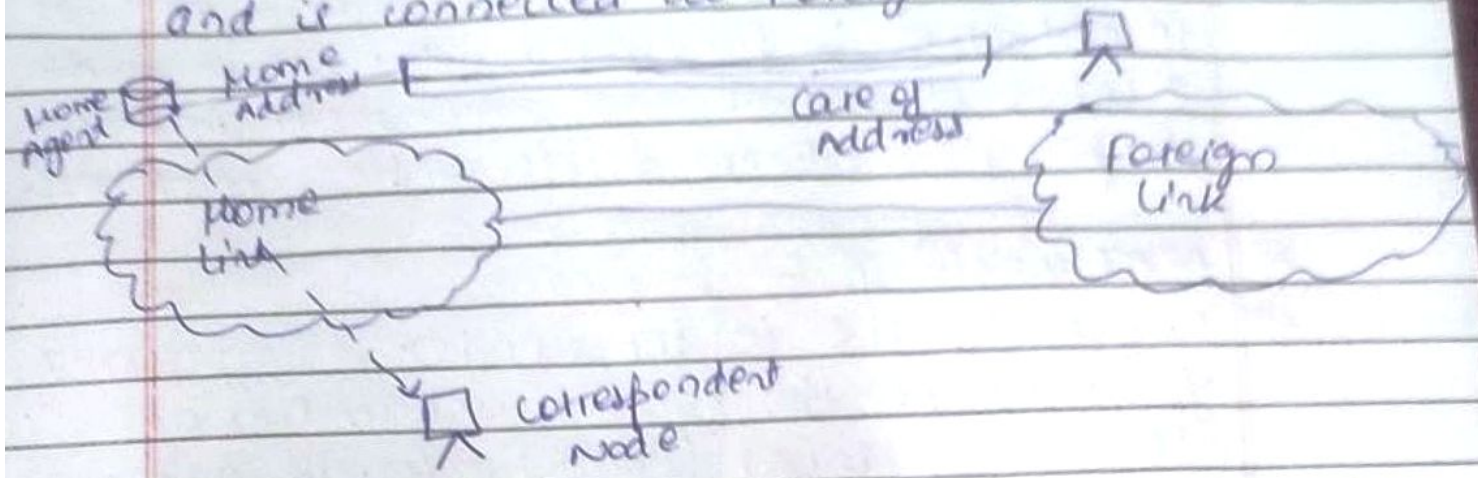
7. Correspondent Node → device that intends to have communication with Mobile Node

* 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

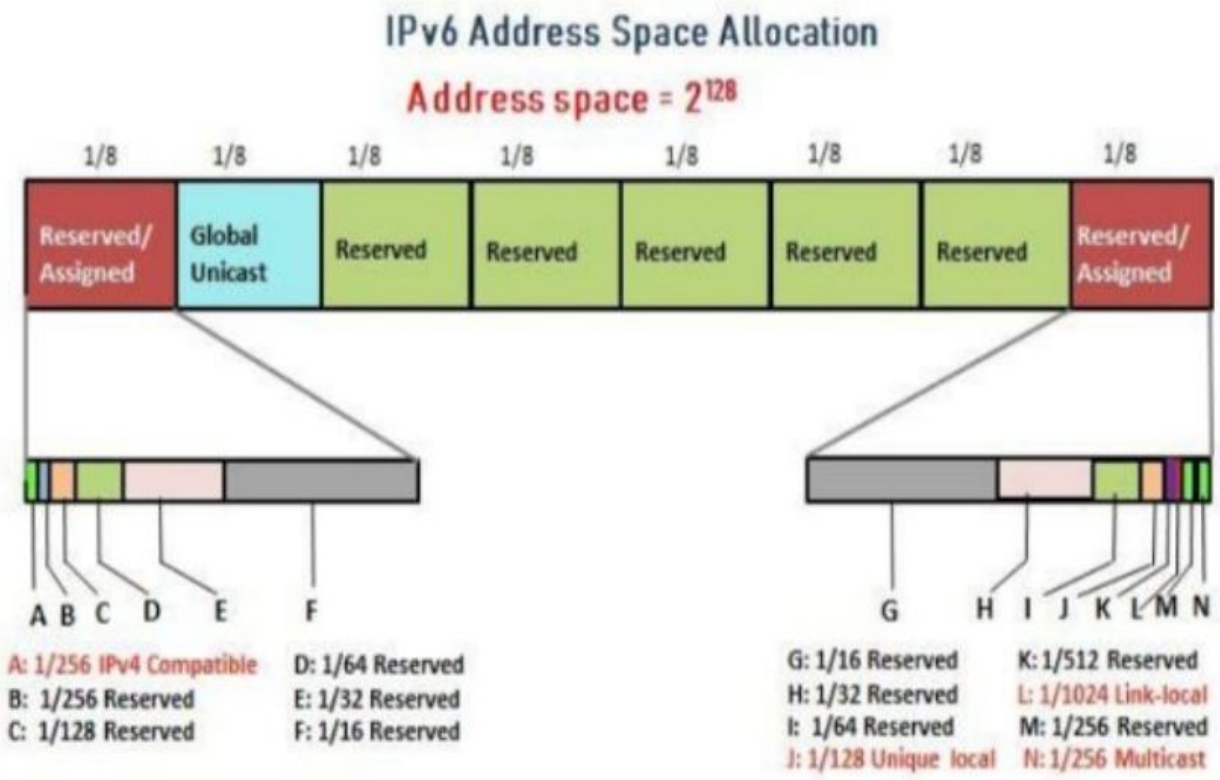
* Disadvantages of NAT :-

(1) Translation results in switching path delays.

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

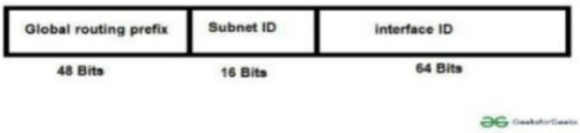
(3) Also, router being a network layer device, should tamper with port numbers but it has to do so because of NAT.

IPv6 Address Space Allocation: The address space of IPv6 is divided into several blocks of varying size and each block is allocated for special purpose. Most of the blocks are still unassigned and have been left aside for future use. To better understand the allocation and the location of each block in address space, we first divide the whole address space into eight equal ranges. This division does not show the block allocation, but we believe it shows where each actual block is located (Figure).



Each section is one-eighth of the whole address space (2125 addresses). The first section contains six variable-size blocks; three of these blocks are reserved and three unassigned. The second section is considered one single block and is used for global unicast addresses. The next five sections are unassigned addresses. The last section is divided into eight blocks. Some of these blocks are still unassigned and some are reserved for special purposes. The figure shows that more than five-eighths of the address space is still unassigned. Only one-eighth of the address space is used for unicast communication between the users.

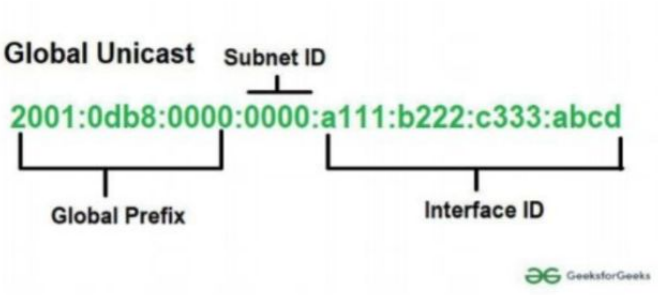
Global Unicast Address: Global Unicast Address is equivalent to IPv4 public address. Global Unicast Addresses in IPv6 are globally identifiable and uniquely addressable.

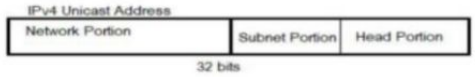


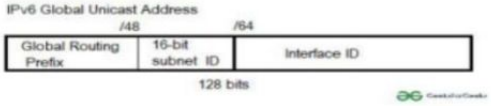
The Most significant 48-bits are designated as global routing prefix which is assigned to a specific automatic system. The three most significant bits of the global routing prefix are always set to 001.

Global Unicast Address (GUA):

- 2000::/3 (First hextet: 2000::/3 to 3FFF::/3).
- Globally unique and routable.
- Similar to public IPv4 addresses.
- 2001:db8::/32 – RFC 2839 and RFC 6890 reserve this range of addresses for documentation.







- 64-bit Interface ID = 18 quintillion (18,446,744,073,709,551,616) devices/subnet .

Autoconfiguration: One of the interesting features of IPv6 addressing is the autoconfiguration of hosts. In IPv6, DHCP protocol can be used to allocate an IPv6 address to a host, but a host can also configure itself.
When a host in IPv6 joins a network, it can configure itself using the following process:
1. The host first creates a link local address for itself. This is by taking the 10-bit link local prefix (1111 1110 10), adding 54 zeros, and adding the 64-bit interface identifier, which any host knows how to generate it from its interface card. The result is a 128-bit link local address.

2. The host then tests to see if this link local address is unique and not used by other hosts. Since the 64-bit interface identifier is supposed to be unique, the link local address generated is unique with a high probability. However, to be sure, the host sends a neighbor solicitation message and waits for neighbor advertisement message. If any host in the subnet is using this link local address, the process fails and the host

cannot autoconfigure itself; it needs to use other means such as DHCP protocol for this purpose.
3. If the uniqueness of the link local address is passed, the host stores this address as its link-local address (for private communication), but it still needs a global unicast address. The host then sends a router solicitation message to a local router. If there is a router running on the network, the host receives a router advertisement message that includes the global unicast prefix and the subnet prefix that the host needs to add to its interface identifier to generate its global unicast address. If the router cannot help the host with the configuration, it informs the host in the router advertisement message (by setting a fl-flag). The host then needs to use other means for configuration.

Renumbering: To allow sites to change the service provider, renumbering of the address prefix (n) was built into IPv6 addressing. Each site is given a prefix by the service provider to which it is connected. If the site changes the provider, the address prefix needs to be changed. A router to which the site is connected can advertise a new prefix and let the site use the old prefix for a short time before disabling it. In other words, during the transition period, a site has two prefixes. The main problem in using the renumbering mechanism is the support of the DNS, which needs to propagate the new addressing associated with a domain name. A new protocol for DNS, called Next Generation DNS, is under study to provide support for this mechanism.

IPv6 Routing Protocols: Like IPv4, IPv6 also supports routing protocols that enable routers to exchange information about connected networks.

Routing protocols can be divided in two categories:

- **Interior Routing Protocol**: Protocols in this category are used within an autonomous system or organization to distribute routes among all routers inside its boundary. Examples: RIP, OSPF.

- **Exterior Routing Protocol**: An Exterior Routing Protocol distributes routing information between two different autonomous systems or organization. Examples: BGP.

There exist two forms of routing protocols:

- **Distance Vector Routing Protocol**: A router running distance vector protocol advertises its connected routes and learns new routes from its neighbors. The routing cost to reach a destination is calculated by means of hops between the source and destination. A router generally relies on its neighbor for best path selection, also known as "routing-by-rumors". RIP and BGP are Distance Vector Protocols.
- **Link-State Routing Protocol**: This protocol acknowledges the state of a Link and advertises to its neighbors. Information about new links is learnt from peer routers. After all the routing information has been converged, the Link-State Routing Protocol uses its own algorithm to calculate the best path to all available links. OSPF and IS-IS are link state routing protocols and both of them use Dijkstra's Shortest Path First algorithm.

IPv6 supports the following routing protocols:

1. RIPng (RIP New Generation)
2. OSPFv3
3. EIGRP for IPv6
4. IS-IS for IPv6
5. MP-BGP4 (Multiprotocol BGP-4)

RIPng: RIPng stands for Routing Information Protocol Next Generation. It is the **Next Generation IP, IPv6** available next level protocol of RIPv2. This is an Interior Routing Protocol and is a Distance Vector Protocol. RIPng has been upgraded to support IPv6.

IPV4 to IPV6 Tunneling : The basic idea behind tunneling methods is that IPv6 will be tunneled over an existing IPv4 network. A number of different tunneling methods are available and can be selected based on the requirements of the situation.

Tunneling provides a way to use an existing **IPv4** routing infrastructure to carry **IPv6** traffic.

The key to a successful **IPv6** transition is compatibility with the existing installed base of **IPv4** hosts and routers. Maintaining compatibility with **IPv4** while deploying **IPv6** streamlines the task of transitioning the Internet to **IPv6**. While the **IPv6** infrastructure is being deployed, the existing **IPv4** routing infrastructure can remain functional, and can be used to carry **IPv6** traffic.

IPv6 or **IPv4** hosts and routers can tunnel **IPv6** datagrams over regions of **IPv4** routing topology by encapsulating them within **IPv4** packets. Tunneling can be used in a variety of ways:

Item	Description
Router-to-Router	**IPv6** or **IPv4** routers interconnected by an **IPv4** infrastructure can tunnel **IPv6** packets between themselves. In this case, the tunnel spans one segment of the end-to-end path that the **IPv6** packet takes.

Item	Description
Host-to-Router	**IPv6** or **IPv4** hosts can tunnel **IPv6** packets to an intermediary **IPv6** or **IPv4** router that is reachable through an **IPv4** infrastructure. This type of tunnel spans the first segment of the packet's end-to-end path.
Host-to-Host	**IPv6** or **IPv4** hosts that are interconnected by an **IPv4** infrastructure can tunnel **IPv6** packets between themselves. In this case, the tunnel spans the entire end-to-end path that the packet takes.
Router-to-Host	**IPv6**/**IPv4** routers can tunnel **IPv6** packets to their final destination **IPv6** or **IPv4** host. This tunnel spans only the last segment of the end-to-end path.

Tunneling techniques are usually classified according to the mechanism by which the encapsulating node determines the address of the node at the end of the tunnel. In router-to-router or host-to-router methods, the **IPv6** packet is being tunneled to a router. In host-to-host or router-to-host methods, the **IPv6** packet is tunneled all the way to its final destination.

The entry node of the tunnel (the encapsulating node) creates an encapsulating **IPv4** header and transmits the encapsulated packet. The exit node of the tunnel (the decapsulating node) receives the encapsulated packet, removes the **IPv4** header, updates the **IPv6** header, and processes the received **IPv6** packet. However, the encapsulating node needs to maintain soft state information for each tunnel, such as the maximum transmission unit (MTU) of the tunnel, to process **IPv6** packets forwarded into the tunnel.

There are two types of tunnels in **IPv6**:

Automatic tunnels

Automatic tunnels are configured by using **IPv4** address information embedded in an **IPv6** address – the **IPv6** address of the destination host includes information about which **IPv4** address the packet should be tunneled to.

Configured tunnels

Configured tunnels must be configured manually. These tunnels are used when using **IPv6** addresses that do not have any embedded **IPv4** information. The **IPv6** and **IPv4** addresses of the endpoints of the tunnel must be specified.

boundary router between an IPv4 and an IPv6 network a translation process maps an IPv4 address to an IPv6 address (or vice versa).

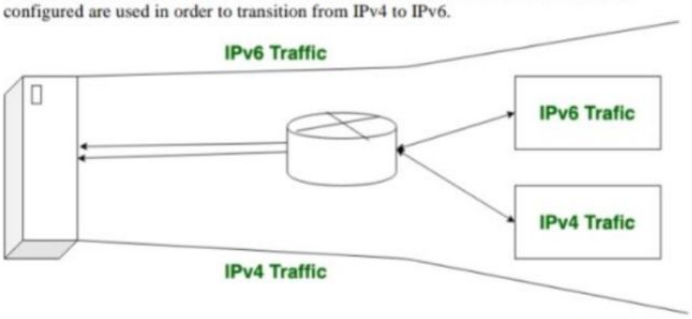
Various organization is currently working with IPv4 technology and in one day we can't switch directly from IPv4 to IPv6. Instead of only using IPv6, we use combination of both and transition means not replacing IPv4 but co-existing of both.

Complete transition from IPv4 to IPv6 might not be possible because IPv6 is not backward compatible. This results in a situation where either a site is on IPv6 or it is not. It is unlike implementation of other new technologies where the newer one is

backward compatible so the older system can still work with the newer version without any additional changes.

To overcome this short-coming, we have a few technologies that can be used to ensure slow and smooth transition from IPv4 to IPv6.

1. Dual-Stack Routers:
In dual-stack router, A router's interface is attached with IPv4 and IPv6 addresses configured are used in order to transition from IPv4 to IPv6.

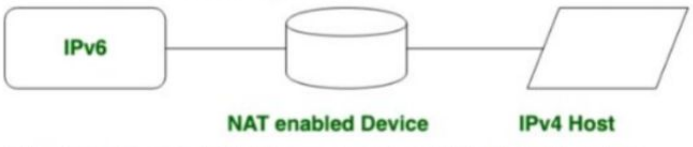


In this above diagram, A given server with both IPv4 and IPv6 addresses configured can communicate with all hosts of IPv4 and IPv6 via dual-stack router (DSR). The dual stack router (DSR) gives the path for all the hosts to communicate with the server without changing their IP addresses.

2. Tunneling:
Tunneling is used as a medium to communicate the transit network with the different IP versions.

In this above diagram, the different IP versions such as IPv4 and IPv6 are present. The IPv4 networks can communicate with the transit or intermediate network on IPv6 with the help of the Tunnel. It's also possible that the IPv6 network can also communicate with IPv4 networks with the help of a Tunnel.

3. NAT Protocol Translation: With the help of the NAT Protocol Translation technique, the IPv4 and IPv6 networks can also communicate with each other which do not understand the address of different IP version.
Generally, an IP version doesn't understand the address of different IP version, for the solution of this problem we use NAT-PT device which removes the header of first (sender) IP version address and add the second (receiver) IP version address so that the Receiver IP version address understand that the request is sent by the same IP version, and its vice-versa is also possible.



In the above diagram, an IPv4 address communicates with the IPv6 address via a NAT-PT device to communicate easily. In this situation, the IPv6 address

Protocols Changed to Support IPv6

- **ICMPv6**: Internet Control Message Protocol version 6 is an upgraded implementation of ICMP to accommodate IPv6 requirements. This protocol is used for diagnostic functions, error and information message, statistical purposes. ICMPv6's Neighbor Discovery Protocol replaces ARP and helps discover neighbor and routers on the link.

- **DHCPv6**: Dynamic Host Configuration Protocol version 6 is an implementation of DHCP. IPv6 enabled hosts do not require any DHCPv6 Server to acquire IP address as they can be auto-configured. Neither do they need DHCPv6 to locate DNS server because DNS can be discovered and configured via ICMPv6 Neighbor Discovery Protocol. Yet DHCPv6 Server can be used to provide these information.

- **DNS**: There has been no new version of DNS but it is now equipped with extensions to provide support for querying IPv6 addresses. A new AAAA (quad-A) record has been added to reply IPv6 query messages. Now the DNS can reply with both IP versions (4 & 6) without any change in the query format.