Unit-2 : Next Generation IP

❖ IPv6 Addressing:

Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.
IPv6 is a 128-bits address having an address space of 2^{128}, which is way bigger than IPv4. IPv6 use Hexa-Decimal format separated by colon (:).

Components in Address format :

1. There are 8 groups and each group represents 2 Bytes (16-bits).
2. Each Hex-Digit is of 4 bits (1 nibble)
3. Delimiter used – colon (:)

Need for IPv6:

The Main reason of IPv6 was the address depletion as the need for electronic devices rose quickly when Internet Of Things (IOT) came into picture after the 1980s & other reasons are related to the slowness of the process due to some unnecessary processing, the need for new options, support for multimedia, and the desperate need for security. IPv6 protocol responds to the above issues using the following main changes in the protocol:

1. Large address space

An IPv6 address is 128 bits long .compared with the 32 bit address of IPv4, this is a huge(2 raised 96 times) increases in the address space.

2. Better header format

IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper layer data . This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

3. New options
IPv6 has new options to allow for additional functionalities.

4. Allowance for extension
IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

5. Support for resource allocation
In IPv6,the type of service field has been removed, but two new fields , traffic class and flow label have been added to enables the source to request special handling of the packet . this mechanism can be used to support traffic such as real-time audio and video.

6. Support for more security
The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

In IPv6 representation, we have three addressing methods :

1. Unicast
2. Multicast
3. Anycast

Addressing methods

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

2. **Multicast Address**
   Multicast Address is used by multiple hosts, called as **groups**, 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. And every node is configured in the same way. In simple words, one data packet is sent to multiple destinations simultaneously.

3. **Anycast Address**
   Anycast Address is assigned to a group of interfaces. Any packet sent to an anycast address will be delivered to only one member interface (mostly nearest host possible).

Note: Broadcast is not defined in IPv6.

❖ Address space allocation

Types of IPv6 address:

We have 128 bits in IPv6 address but by looking at the first few bits we can identify what type of address it is.

Prefix	Allocation	Fraction of Address Space
0000 0000	Reserved	1/256
0000 0001	Unassigned (UA)	1/256
0000 001	Reserved for NSAP	1/128
0000 01	UA	1/64
0000 1	UA	1/32
0001	UA	1/16
001	Global Unicast	1/8
010	UA	1/8
011	UA	1/8
100	UA	1/8
101	UA	1/8
110	UA	1/8

Prefix	Allocation	Fraction of Address Space
1110	UA	1/16
1111 0	UA	1/32
1111 10	UA	1/64
1111 110	UA	1/128
1111 1110 0	UA	1/512
1111 1110 10	Link-Local Unicast Addresses	1/1024
1111 1110 11	Site-Local Unicast Addresses	1/1024
1111 1111	Multicast Address	1/256

❖ Auto configuration

The IPv6 addressing scheme is the successor of the IPv4 addressing. The IPv4 addressing scheme used a 32-bit address which translates to over 4 billion unique IPv4 addresses. However, with the expansion of devices that require internet connectivity, this address pool started running out.

The IPv6 addressing scheme is based on a 128-bit address which translates into a database of about 340 Undecillion routable IPv6 addresses (1 Undecillion = 10^{36}).
The IPv6 addressing scheme has two ways in which the hosts acquire an IP address.

- DHCPv6 (Stateful)
- SLAAC (Stateless)

The IPv6 Stateless Address Auto-Configuration (SLAAC):

The Stateless Address Auto-Configuration enables hosts to generate a unique routable IPv6 address on their own. The router is configured to follow the IPv6 SLAAC protocol and sends out a Router Advertisement periodically.

The host can also send a Router Solicitation in order to trigger the Routing Advertisement by the router. The Router Solicitation is sent on the address FF02::2 which is the IPv6 multicast address for all the routers.

The Router Advertisement contains the Prefix Information (prefix (network address), prefix length (subnet mask), and default gateway). The host uses this information to generate an IPv6 address (global unicast address or GUA) for itself. The host then employs Duplicate Address Detection to ensure that its address is unique.

The IPv6 SLAAC Configurations:

In order for the router to be able to send the Router Advertisement and essentially for IPv6 SLAAC to function, these configurations must be set using the CLI of the concerned router.

S.No.	Parameters	Values
1	Enter Router EXEC mode	Router>**enable**
2	Enter global configuration mode	Router#**configure terminal**
3	Enable IPv6 routing	Router(config)#**ipv6 unicast-routing**
4	Enter interface configuration mode	Router(config)#**interface** interface
5	Configure an IPv6 address	Router(config-if)#**ipv6 address** ipv6-address/prefix-length
6	Enable the interface	Router(config-if)#**no shutdown**

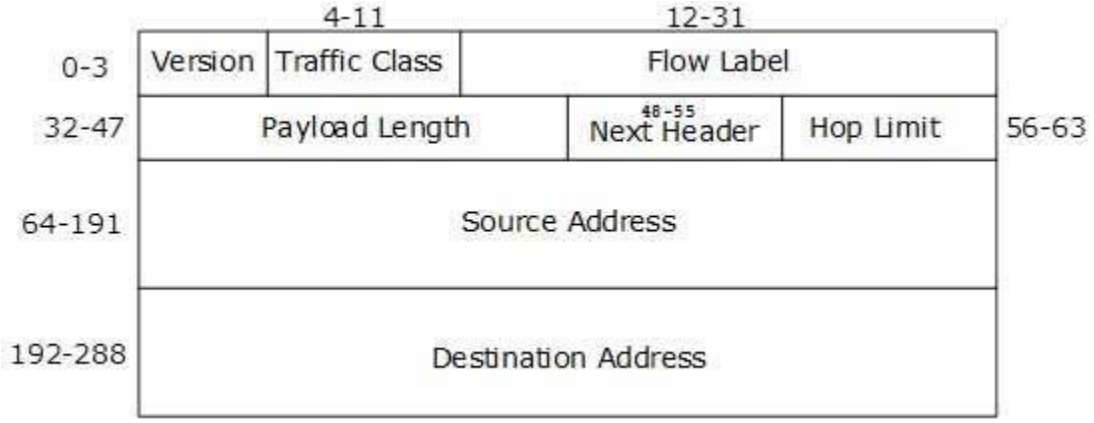
❖ Renumbering

Renumbering of devices is a method related to auto configuration. Like host configuration, it can be implemented using protocols like DHCP, through the use of IP address "leases" that expire after a period of time. Under IPv6, networks can be renumbered by having routers specify an expiration interval for network prefixes when auto configuration is done. Later, they can send a new prefix to tell devices to regenerate their IP addresses. Devices can actually maintain the old "deprecated" address for a while and then move over to the new address.

❖ The IPv6 Protocol Packet Format

The wonder of IPv6 lies in its header. An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

Fixed Header



[Image: IPv6 Fixed Header]

IPv6 fixed header is 40 bytes long and contains the following information.

S.N.	Field & Description
1	Version (4-bits): It represents the version of Internet Protocol, i.e. 0110.
2	Traffic Class (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	Flow Label (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
4	Payload Length (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
5	Next Header (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
6	Hop Limit (8-bits): 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 (router/hop). When the field reaches 0 the packet is discarded.
7	Source Address (128-bits): This field indicates the address of originator of the packet.
8	Destination Address (128-bits): This field provides the address of intended recipient of the packet.

❖ Extension Headers

In IPv6, the Fixed Header contains only that much information which is necessary, avoiding those information which is either not required or is rarely used. All such information is put between the Fixed Header and the Upper layer header in the form of Extension Headers. Each Extension Header is identified by a distinct value.

When Extension Headers are used, IPv6 Fixed Header's Next Header field points to the first Extension Header. If there is one more Extension Header, then the first Extension Header's 'Next-Header' field points to the second one, and so on. The last Extension Header's 'Next-Header' field points to the Upper Layer Header. Thus, all the headers points to the next one in a linked list manner.

If the Next Header field contains the value 59, it indicates that there are no headers after this header, not even Upper Layer Header.

The following Extension Headers must be supported as per RFC 2460:

Extension Header	Next Header Value	Description
Hop-by-Hop Options header	0	read by all devices in transit network
Routing header	43	contains methods to support making routing decision
Fragment header	44	contains parameters of datagram fragmentation
Destination Options header	60	read by destination devices
Authentication header	51	information regarding authenticity
Encapsulating Security Payload header	50	encryption information

The sequence of Extension Headers should be:

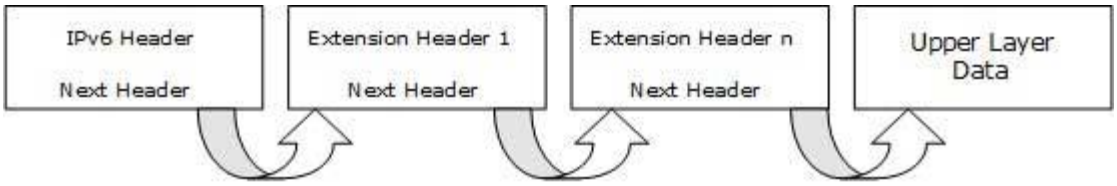
IPv6 header
Hop-by-Hop Options header
Destination Options header[1]
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header[2]
Upper-layer header

These headers:

1. should be processed by First and subsequent destinations.

2. should be processed by Final Destination.

Extension Headers are arranged one after another in a linked list manner, as depicted in the following diagram:



[Image: Extension Headers Connected Format]

❖ ICMPv6 Protocol

ICMP stands for Internet Control Message Protocol.

The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.

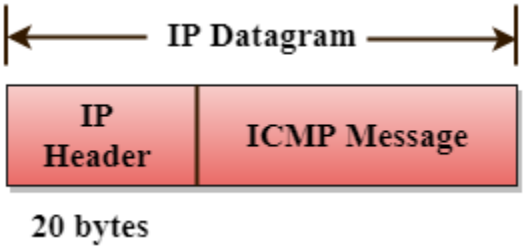
ICMP uses echo test/reply to check whether the destination is reachable and responding.

ICMP handles both control and error messages, but its main function is to report the error but not to correct them.

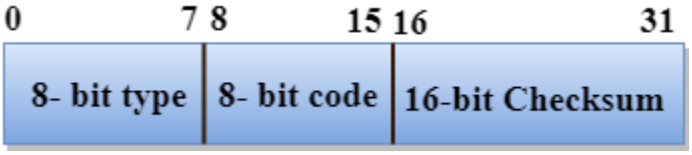
An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.

ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.

ICMP messages are transmitted within IP datagram.



The Format of an ICMP message



The first field specifies the type of the message.

The second field specifies the reason for a particular message type.

The checksum field covers the entire ICMP message.

❖ Error Reporting

ICMP protocol reports the error messages to the sender.

Five types of errors are handled by the ICMP protocol:

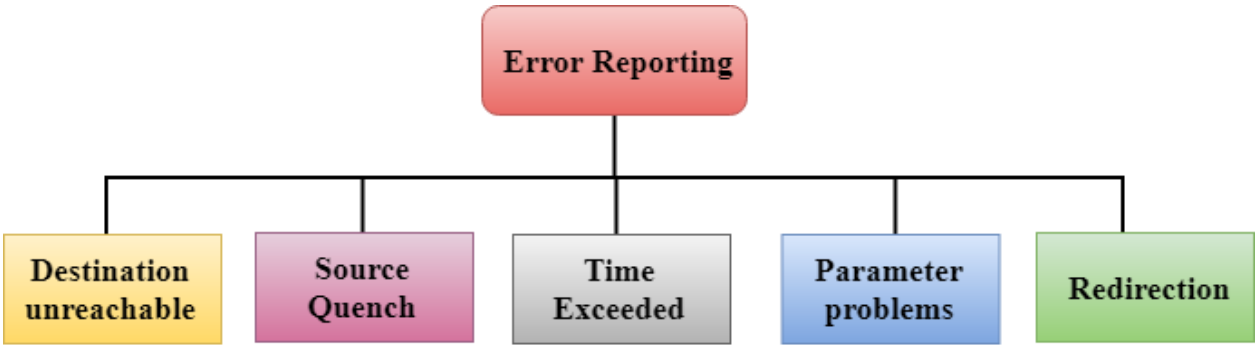
Destination unreachable

Source Quench

Time Exceeded

Parameter problems

Redirection



Destination unreachable: The message of "Destination Unreachable" is sent from receiver to the sender when destination cannot be reached, or packet is discarded when the destination is not reachable.

Source Quench: The purpose of the source quench message is congestion control. The message sent from the congested router to the source host to reduce the transmission rate. ICMP will take the IP of the discarded packet and then add the source quench message to the IP datagram to inform the source host to reduce its transmission rate. The source host will reduce the transmission rate so that the router will be free from congestion.

Time Exceeded: Time Exceeded is also known as "Time-To-Live". It is a parameter that defines how long a packet should live before it would be discarded.

Parameter problems: When a router or host discovers any missing value in the IP datagram, the router discards the datagram, and the "parameter problem" message is sent back to the source host.

Redirection: Redirection message is generated when host consists of a small routing table. When the host consists of a limited number of entries due to which it sends the datagram to a wrong router. The router that receives a datagram will forward a datagram to a correct router and also sends the "Redirection message" to the host to update its routing table.

❖ ICMPv6 informational messages

ICMPv6 informational messages are used for network diagnostic functions and additional critical network functions like Neighbor Discovery, Router Solicitation & Router

Advertisements, Multicast Memberships. Echo Request and Echo Reply (used by many commands and utilities like "ping" for network diagnostics and communication trouble shooting) are also ICMPv6 informational messages. The ICMPv6 informational messages have values for the Type field (8 bit binary number) between 128 and 255.

❖ Neighbor-Discovery Messages:

ICMPv6 ND (Neighbor Discovery) Messages are used for the Neighbor Discovery Protocol (NDP). ND (Neighbor Discovery) Messages includes Router Solicitation & Router Advertisement, Neighbor Solicitation and Neighbor Advertisement.

❖ Group Membership Messages:

ICMPv6 MLD (Multicast Listener Discovery) Messages are used by an IPv6 enabled router to discover hosts who are interested in multicast packets, and the multicast addresses they are interested. MLD (Multicast Listener Discovery) messages are used by MLD (Multicast Listener Discovery) Protocol. MLD (Multicast Listener Discovery) Protocol is the IPv6 equivalent of IGMP (Internet Group Management) Protocol in IPv4.

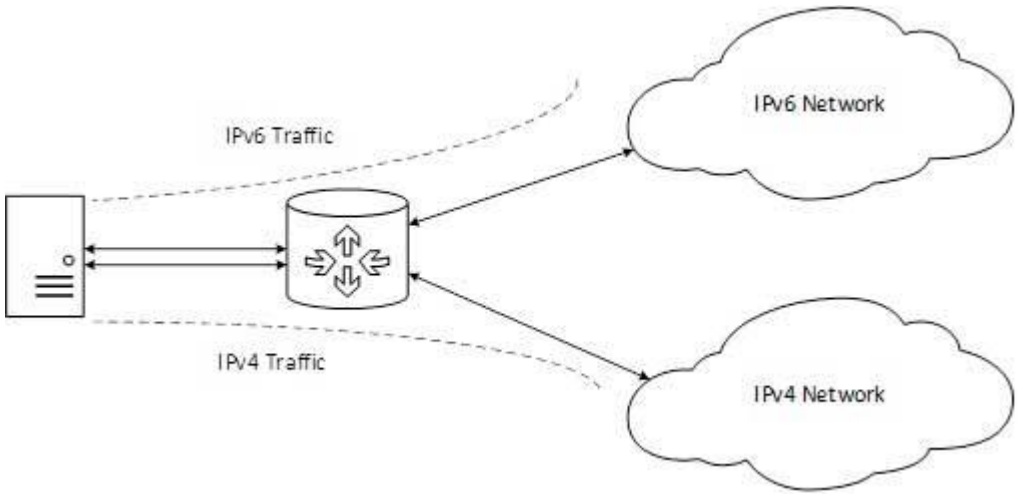
❖ Transition from IPv4 to IPv6-

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.

Dual Stack Routers

A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme.

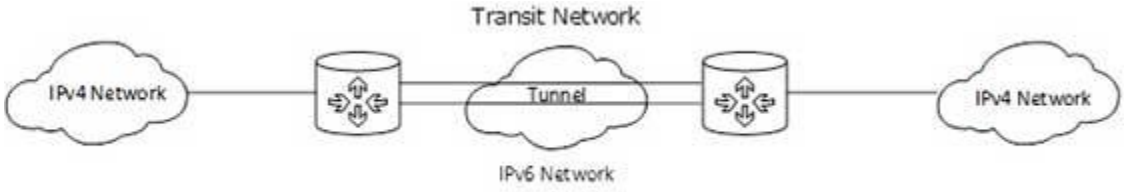


[Image: Dual Stack Router]

In the above diagram, a server having IPv4 as well as IPv6 address configured for it can now speak with all the hosts on both the IPv4 as well as the IPv6 networks with the help of a Dual Stack Router. The Dual Stack Router, can communicate with both the networks. It provides a medium for the hosts to access a server without changing their respective IP versions.

Tunneling

In a scenario where 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.



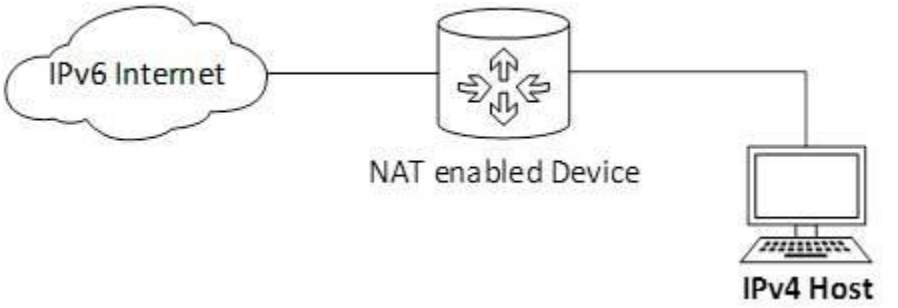
[Image: Tunneling]

The above diagram depicts how two remote IPv4 networks can communicate via a Tunnel, where the transit network was on IPv6. Vice versa is also possible where the transit network is on IPv6 and the remote sites that intend to communicate are on IPv4.

NAT Protocol Translation

This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With the help of a NAT-PT

device, actual can take place happens between IPv4 and IPv6 packets and vice versa. See the diagram below:



[*Image: NAT - Protocol Translation*]

A host with IPv4 address sends a request to an IPv6 enabled server on Internet that does not understand IPv4 address. In this scenario, the NAT-PT device can help them communicate. When the IPv4 host sends a request packet to the IPv6 server, the NAT-PT device/router strips down the IPv4 packet, removes IPv4 header, and adds IPv6 header and passes it through the Internet. When a response from the IPv6 server comes for the IPv4 host, the router does vice versa.