IPv6 - Quick Guide

Overview

Internet Protocol version 6, is a new addressing protocol designed to incorporate whole sort of requirement of future internet known to us as Internet version 2. This protocol as its predecessor IPv4, works on Network Layer (Layer-3). Along with its offering of enormous amount of logical address space, this protocol has ample of features which addresses today's shortcoming of IPv4.

Why new IP version?

So far, IPv4 has proven itself as a robust routable addressing protocol and has served human being for decades on its best-effort-delivery mechanism. It was designed in early 80's and did not get any major change afterward. At the time of its birth, Internet was limited only to a few Universities for their research and to Department of Defense. IPv4 is 32 bits long which offers around 4,294,967,296 (2^{32}) addresses. This address space was considered more than enough that time. Given below are major points which played key role in birth of IPv6:

- Internet has grown exponentially and the address space allowed by IPv4 is saturating. There is a requirement of protocol which can satisfy the need of future Internet addresses which are expected to grow in an unexpected manner.
- Using features such as NAT, has made the Internet discontiguous i.e. one part which belongs to intranet, primarily uses private IP addresses; which has to go through number of mechanism to reach the other part, the Internet, which is on public IP addresses.
- IPv4 on its own does not provide any security feature which is vulnerable as data on Internet, which is a public domain, is never safe. Data has to be encrypted with some other security application before being sent on Internet.
- Data prioritization in IPv4 is not up to date. Though IPv4 has few bits reserved for Type of Service or Quality of Service, but they do not provide much functionality.
- IPv4 enabled clients can be configured manually or they need some address configuration mechanism. There exists no technique which can configure a device to have globally unique IP address.

Why not IPv5?

Till date, Internet Protocol has been recognized has IPv4 only. Version 0 to 3 were used while the protocol was itself under development and experimental process. So, we can assume lots of background activities remain active before putting a protocol into production. Similarly, protocol version 5 was used while experimenting with stream protocol for internet. It is known to us as Internet Stream Protocol which used Internet Protocol number 5 to encapsulate its datagram. Though it was never brought into public use, but it was already used.

Here is a table of IP version and their use:

Decimal	Keyword	Version
0-1		Reserved
2-3		Unassigned
4	IP	Internet Protocol
5	ST	ST Datagram mode
6	IPv6	Internet Protocol version 6
7	TP/IX	TP/IX: The Next Internet
8	PIP	The P Internet Protocol
9	TUBA	TUBA
10-14		Unassigned
15		Reserved

Brief History

After IPv4's development in early 80s, the available IPv4 address pool begun to shrink rapidly as the demand of addresses exponentially increased with Internet. Taking pre-cognizance of situation that might arise IETF, in 1994, initiated the development of an addressing protocol to replace IPv4. The progress of IPv6 can be tracked by means of RFC published:

- 1998 – RFC 2460 – Basic Protocol
- 2003 – RFC 2553 – Basic Socket API
- 2003 – RFC 3315 – DHCPv6
- 2004 – RFC 3775 – Mobile IPv6
- 2004 – RFC 3697 – Flow Label Specification
- 2006 – RFC 4291 – Address architecture (revision)
- 2006 – RFC 4294 – Node requirement

June 06, 2012 some of Internet giants chose to put their Servers on IPv6. Presently they are using Dual Stack mechanism to implement IPv6 parallel with IPv4.

Features

The successor of IPv4 is not designed to be backward compatible. Trying to keep the basic functionalities of IP addressing, IPv6 is redesigned entirely. It offers the following features:

- **Larger Address Space:**

  In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4×10^{38} different combinations of addresses. This address can accumulate the aggressive requirement of address allotment for almost everything in this world. According to an estimate, 1564 addresses can be allocated to every square meter of this earth.

- **Simplified Header:**

  IPv6's header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4 providing the fact the IPv6 address is four times longer.

- **End-to-end Connectivity:**

  Every system now has unique IP address and can traverse through the internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other host on the Internet, with some limitations involved like Firewall, Organization's policies, etc.

- **Auto-configuration:**

  IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way absence of a DHCP server does not put halt on inter segment communication.

- **Faster Forwarding/Routing:**

  Simplified header puts all unnecessary information at the end of the header. All information in first part of the header are adequate for a Router to take routing decision thus making routing decision as quickly as looking at the mandatory header.

- **IPSec:**

  Initially it was decided for IPv6 to must have IPSec security, making it more secure than IPv4. This feature has now been made optional.

- **No Broadcast:**

  Though Ethernet/Token Ring are considered as broadcast network because they support Broadcasting, IPv6 does not have any Broadcast support anymore left with it. It uses multicast to communicate with multiple hosts.

- **Anycast Support:**

  This is another characteristic of IPv6. IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, sends the packet to the nearest destination.

- **Mobility:**

  IPv6 was designed keeping mobility feature in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with same IP address. IPv6 mobility feature takes advantage of auto IP configuration and Extension headers.

- **Enhanced Priority support:**

  Where IPv4 used 6 bits DSCP (Differential Service Code Point) and 2 bits ECN (Explicit Congestion Notification) to provide Quality of Service but it could only be used if the end-to-end devices support it, that is, the source and destination device and underlying network must support it.

  In IPv6, Traffic class and Flow label are used to tell underlying routers how to efficiently process the packet and route it.

- **Smooth Transition:**

  Large IP address scheme in IPv6 enables to allocate devices with globally unique IP addresses. This assures that mechanism to save IP addresses such as NAT is not required. So devices can send/receive data between each other, for example VoIP and/or any streaming media can be used much efficiently.

  Other fact is, the header is less loaded so routers can make forwarding decision and forward them as quickly as they arrive.

- **Extensibility:**

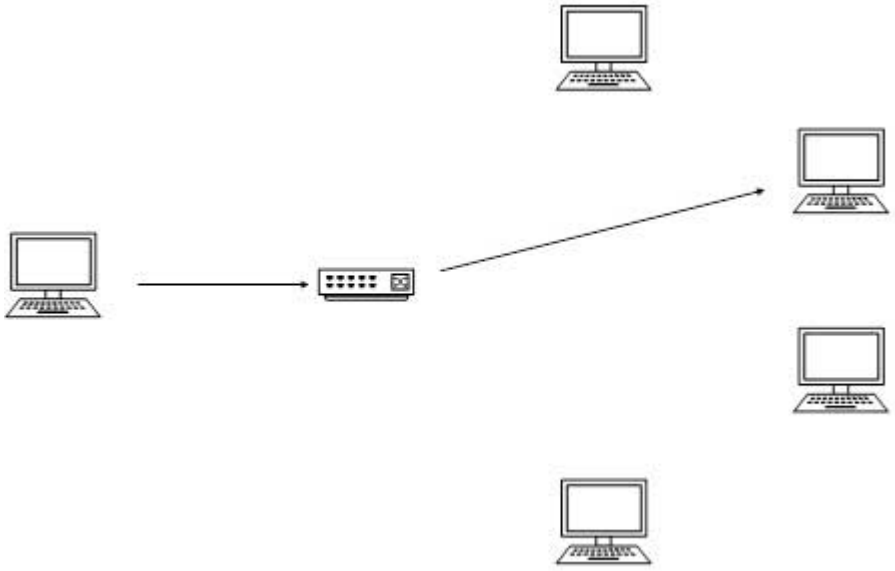
  One of the major advantage of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options whereas options in IPv6 can be as much as the size of IPv6 packet itself.

Addressing Modes

In computer networking, addressing mode refers to the mechanism how we address a host on the network. IPv6 offers several types of modes by which a single host can be addressed, more than one host can be addressed at once or the host at closest distance can be addressed.

Unicast

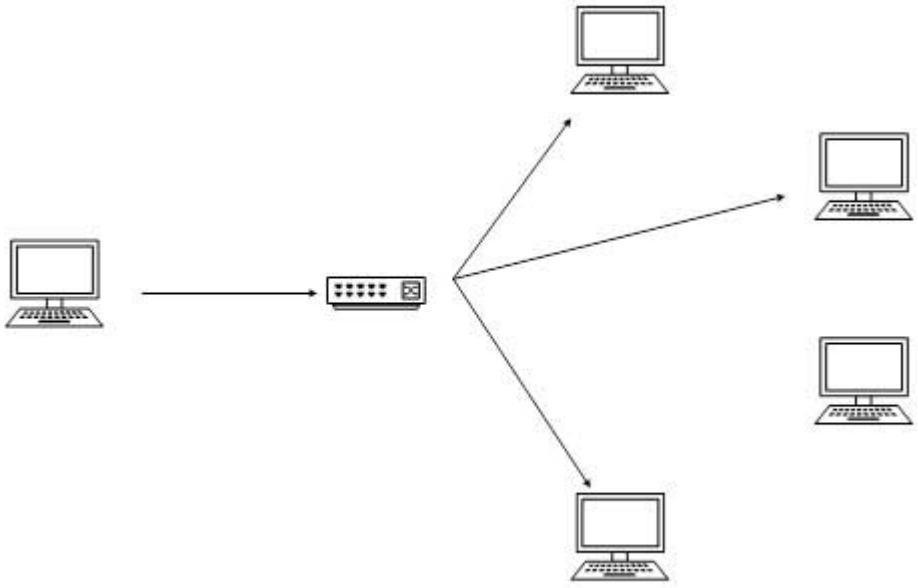
In unicast mode of addressing, an IPv6 interface (host) is uniquely identified in a network segment. The IPv6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment. A network switch or router when receives a unicast IP packet, destined to single host, sends out to one of its outgoing interface which connects to that particular host.



[*Image: Unicast Messaging*]

Multicast

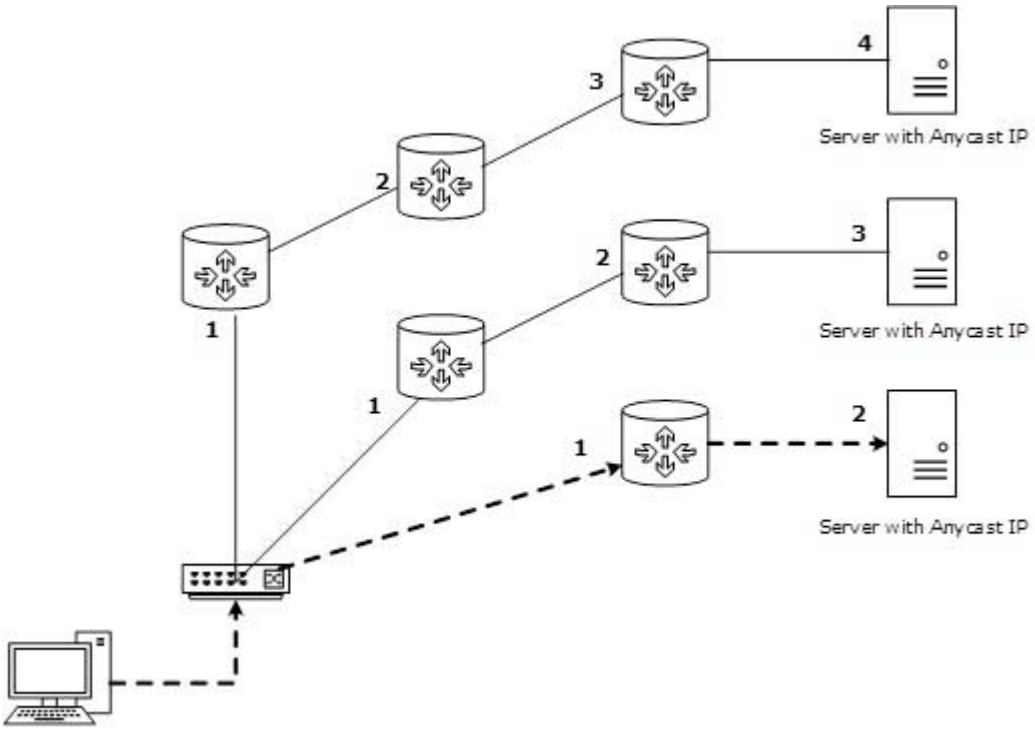
The IPv6 multicast mode is same as that of IPv4. The packet destined to multiple hosts is sent on a special multicast address. All hosts interested in that multicast information, need to join that multicast group first. All interfaces which have joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information.



[*Image: Multicast Messaging*]

Anycast

IPv6 has introduced a new type of addressing, which is called Anycast addressing. In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, sends a Unicast message. With the help of complex routing mechanism, that Unicast message is delivered to the host closest to the Sender, in terms of Routing cost.



[*Image: Anycast Messaging*]

Let’s take an example of TutorialPoints.com Web Servers, located in all continents. Assume that all Web Servers are assigned single IPv6 Anycast IP Address. Now when a user from Europe wants to reach TutorialsPoint.com the DNS points to the server which is physically located in Europe itself. If a user from India tries to reach Tutorialspoint.com, the DNS will then point to Web Server physically located in Asia only. Nearest or Closest terms are used in terms of Routing Cost.

In the above picture, When a client computer tries to reach a Server, the request is forwarded to the Server with lowest Routing Cost.

Address Types

Hexadecimal Number System

Before introducing IPv6 Address format, we shall look into Hexadecimal Number System. Hexadecimal is positional number system which uses radix (base) of 16. To represent the values in readable format, this system uses 0-9 symbols to represent values from zero to nine and A-F symbol to represent values from ten to fifteen. Every digit in Hexadecimal can represent values from 0 to 15.

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

[*Image: Conversion Table*]

Address Structure

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbol.

For example, the below is 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

> 0010000000000001 0000000000000000 0011001000110100 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011

Each block is then converted into Hexadecimal and separated by ':' symbol:

> 2001:0000:3238:DFE1:0063:0000:0000:FEFB

Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. These rules are:

Rule:1 Discard leading Zero(es):

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):

> 2001:0000:3238:DFE1:63:0000:0000:FEFB

Rule:2 If two of more blocks contains consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):

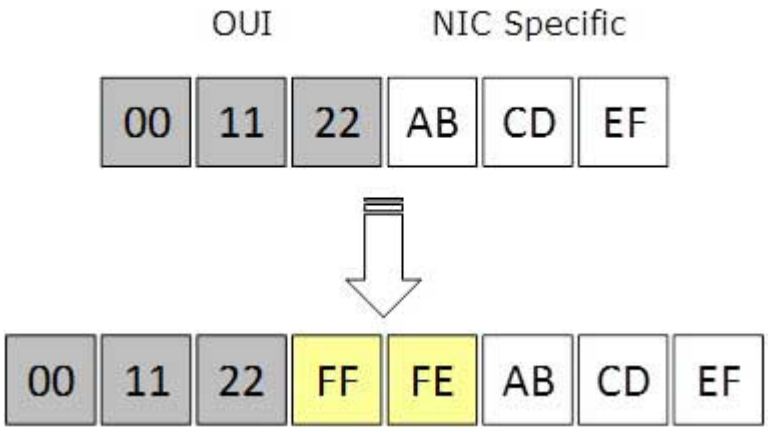
> 2001:0000:3238:DFE1:63::FEFB

Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address they can be shrink down to single zero, such as (2nd block):

> 2001:0:3238:DFE1:63::FEFB

Interface ID

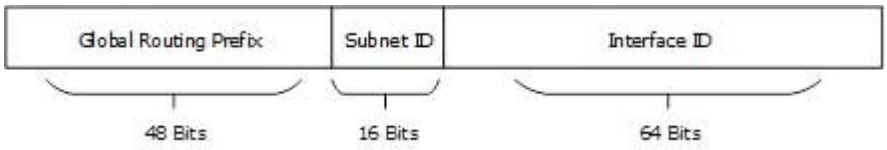
IPv6 has three different type of Unicast Address scheme. The second half of the address (last 64 bits) is always used for Interface ID. MAC address of a system is composed of 48-bits and represented in Hexadecimal. MAC address is considered to be uniquely assigned worldwide. Interface ID takes advantage of this uniqueness of MAC addresses. A host can auto-configure its Interface ID by using IEEE's Extended Unique Identifier (EUI-64) format. First, a Host divides its own MAC address into two 24-bits halves. Then 16-bit Hex value 0xFFFE is sandwiched into those two halves of MAC address, resulting in 64-bit Interface ID.



[*Image: EUI-64 Interface ID*]

Global Unicast Address

This address type is equivalent to IPv4's public address. Global Unicast addresses in IPv6 are globally identifiable and uniquely addressable.



[*Image: Global Unicast Address*]

Global Routing Prefix: The most significant 48-bits are designated as Global Routing Prefix which is assigned to specific Autonomous System. Three most significant bits of Global Routing Prefix is always set to 001.

Link-Local Address

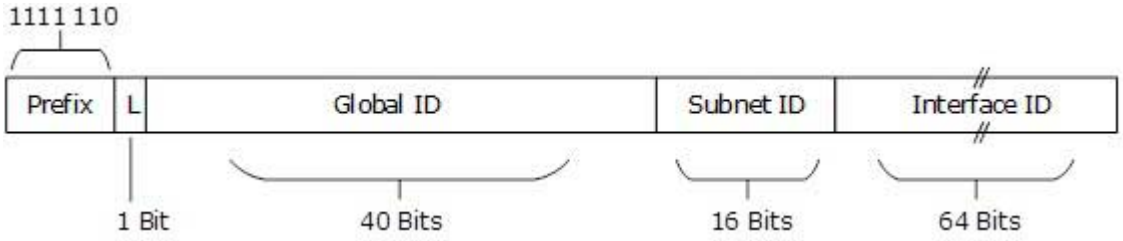
Auto-configured IPv6 address is known as Link-Local address. This address always starts with FE80. First 16 bits of Link-Local address is always set to 1111 1110 1000 0000 (FE80). Next 48-bits are set to 0, thus:

[*Image: Link-Local Address*]

Link-Local addresses are used for communication among IPv6 hosts on a link (broadcast segment) only. These addresses are not routable so a Router never forwards these addresses outside the link.

Unique-Local Address

This type of IPv6 address which is though globally unique, but it should be used in local communication. This address has second half of Interface ID and first half is divided among Prefix, Local Bit, Global ID and Subnet ID.



[*Image: Unique-Local Address*]

Prefix is always set to 1111 110. L bit, which is set to 1 if the address is locally assigned. So far the meaning of L bit to 0 is not defined. Therefore, Unique Local IPv6 address always starts with 'FD'.

Scope of IPv6 Unicast Addresses:

[*Image: IPv6 Unicast Address Scope*]

The scope of Link-local address is limited to the segment. Unique Local Address are though locally global but are not routed over the Internet, limiting their scope to an organization's boundary. Global Unicast addresses are globally unique and recognizable. They shall make the essence of Internet v2 addressing.

Special Addresses

Version 6 has slightly complex structure of IP address than that of IPv4. IPv6 has reserved few addresses and address notations for special purposes. See the table below:

Special Addresses:

IPv6 Address	Meaning
::/128	Unspecified Address
::/0	Default Route
::1/128	Loopback Address

- As shown in the table above 0:0:0:0:0:0:0:0/128 address does not specify to anything and is said to be an unspecified address. After simplifying, all 0s are compacted to ::/128.
- In IPv4, address 0.0.0.0 with netmask 0.0.0.0 represents default route. The same concept is also applie to IPv6, address 0:0:0:0:0:0:0:0 with netmask all 0s represents default route. After applying IPv6 simplying rule this address is compressed to ::/0.
- Loopback addresses in IPv4 are represented by 127.0.0.1 to 127.255.255.255 series. But in IPv6, only 0:0:0:0:0:0:0:1/128 address represents Loopback address. After simplying loopback address, it can be represented as ::1/128.

Reserved Multicast Address for Routing Protocols:

IPv6 Address	Routing Protocol
FF02::5	OSPFv3
FF02::6	OSPFv3 Designated Routers
FF02::9	RIPng
FF02::A	EIGRP

- The above table shows reserved multicast addresses used by interior routing protocol.
- All addresses are reserved in similar IPv4 fashion

Reserved Multicast Address for Routers/Node:

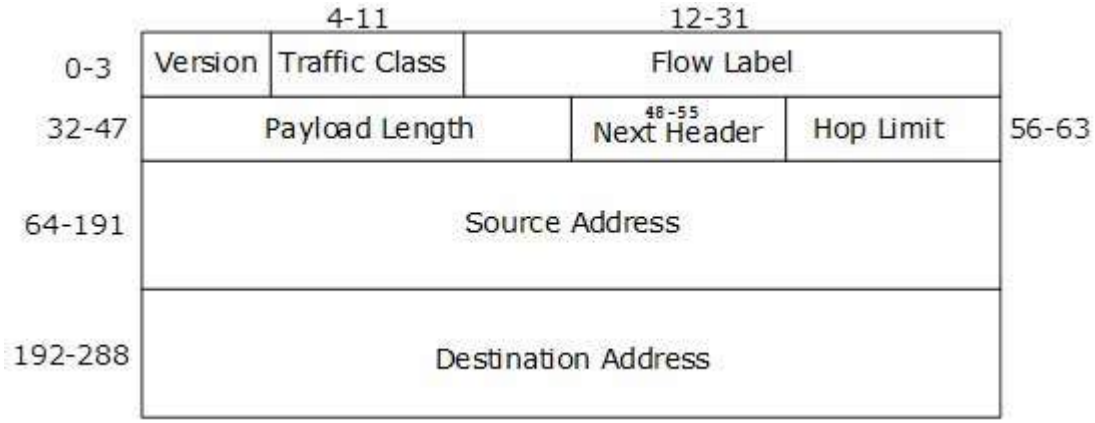
IPv6 Address	Scope
FF01::1	All Nodes in interface-local
FF01::2	All Routers in interface local
FF02::1	All Nodes in link-local
FF02::2	All Routers in link-local
FF05::2	All Routers in site-local

- These addresses helps routers and hosts to speak to available routers and hosts on a segment without being configured with an IPv6 address. Hosts use EUI-64 based auto-configuration to self-configure an IPv6 address and then speaks to available hosts/routers on the segment by means of these addresses.

Headers

The wonder of IPv6 lies in its header. IPv6 address is 4 times larger than IPv4 but the IPv6 header is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All necessary information which is essential for a router is kept in Fixed Header. Extension Header contains optional information which 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): This represents the version of Internet Protocol, i.e. 0110.
2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. Most significant 6 bits are used for Type of Service, which tells the Router what services should be provided to this packet. 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 which helps the router to identify that this packet belongs to a specific flow of information. This field helps to 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 this 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 Extension Headers contain Hop-by-Hop Extension Header than 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 Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU is 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 information which is necessary and avoiding information which is either not required or is rarely used. All such information, is put between the Fixed Header and 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 first Extension Header's 'Next-Header' field point to the second one, and so on. The last Extension Header's 'Next-Header' field point to Upper Layer Header. Thus all headers from point to the next one in a linked list manner.

If the Next Header field contains value 59, it indicates that there's no header 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

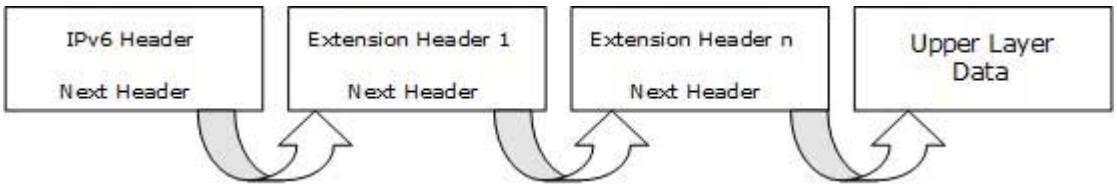
The sequence of Extension Headers should be:

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 diagram below:



[*Image: Extension Headers Connected Format*]

Communication

In IPv4, a host which wants to communicate with some other host on the network, needs first to have an IP address acquired either by means of DHCP or by manual configuration. As soon as a host is equipped with some valid IP address, it is now able to speak to any host on the subnet. To communicate on layer-3, a host also must know the IP address of the other host. Communication on a link, is established by means of hardware embedded MAC Addresses. To know the MAC address of host whose IP address is known, a host sends ARP broadcast and in revert the intended host sends back its MAC address.

In IPv6, there's no broadcast mechanism. It is not a must for an IPv6 enabled host to obtain IP address from DHCP or manually configured, but it can auto-configure its own IP. Then, how would a host communicates with others on IPv6 enabled network?

ARP has been replaced by ICMPv6 Neighbor Discovery Protocol.

Neighbor Discovery Protocol

A host in IPv6 network is capable of auto-configuring itself with a unique link-local address. As soon as it is equipped with an IPv6 address, it joins a number of multicast groups. All communications related to that segment happens on those multicast addresses only. A host goes through a series of states in IPv6:

- **Neighbor Solicitation**: After configuring all IPv6's either manually, or by DHCP Server or by auto-configuration, the host sends a Neighbor Solicitation message out to FF02::1/16 multicast address for all its IPv6 addresses in order to know that no one else occupies same addresses.
- **DAD (Duplicate Address Detection)**: When the host does not listen from anything from the segment regarding its Neighbor Solicitation message, it assumes that no duplicate address exists on the segment.
- **Neighbor Advertisement**: After assigning the addresses to its interfaces and making them up and running, the host once again sends out a Neighbor Advertisement message telling all other hosts on the segment, that it has assigned those IPv6 addresses to its interfaces.

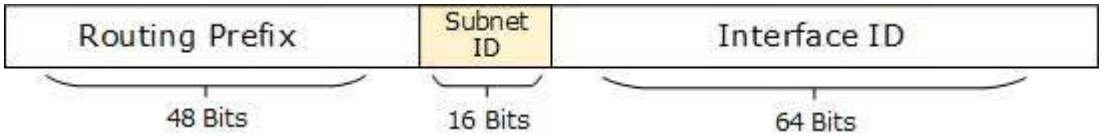
Once a host is done with the configuration of its IPv6 addresses, it does the following things:

- **Router Solicitation**: A host sends a Router Solicitation multicast packet (FF02::2/16) out on its segment to know the presence of any router on this segment. This helps the host to configure the router as its default gateway. If its default gateway router goes down, the host can shift to a new router and makes it the default gateway.
- **Router Advertisement**: When a router receives a Router Solicitation message, it responses back to the host advertising its presence on that link.
- **Redirect**: This may be the situation where a Router receives a Router Solicitation request but it knows that it is not the best gateway for the host. In this situation, the router sends back a Redirect message telling the host that there is a better 'next-hop' router available. Next-hop is where the host will send its data destined to a host which does not belong to the same segment.

Subnetting

In IPv4, addresses were created in classes. Classful IPv4 addresses clearly defines the bits used for network prefixes and the bits used for hosts on that network. To subnet in IPv4 we play with the default classful netmask which allows us to borrow hosts bit to be used as subnet bits. This results in multiple subnets but less hosts per subnet. That is, when we borrow host bit to create a subnet that costs us in lesser bit to be used for host addresses.

IPv6 addresses uses 128 bits to represent an address which includes bits to be used for subnetting. Second half of the address (least significant 64 bits) is always used for Hosts only. Therefore, there is no compromise if we subnet the network.



[*Image: IPv6 Subnetting*]

16 Bits of subnet is equivalent to IPv4's Class B Network. Using these subnet bits an organization can have more 65 thousands of subnets which is by far, more than enough.

Thus routing prefix is /64 and host portion is 64 bits. We though, can further subnet the network beyond 16 bits of Subnet ID, borrowing hosts bit but it is recommended that 64 bits should always be used for hosts addresses because auto-configuration requires 64 bits.

IPv6 subnetting works on the same concept as Variable Length Subnet Masking in IPv4.

/48 prefix can be allocated to an organization providing it the benefit of having up to /64 subnet prefixes, which is 65535 sub-networks, each having 2^{64} hosts. A /64 prefix can be assigned to a point-to-point connection where there are only two hosts (or IPv6 enabled devices) on a link.

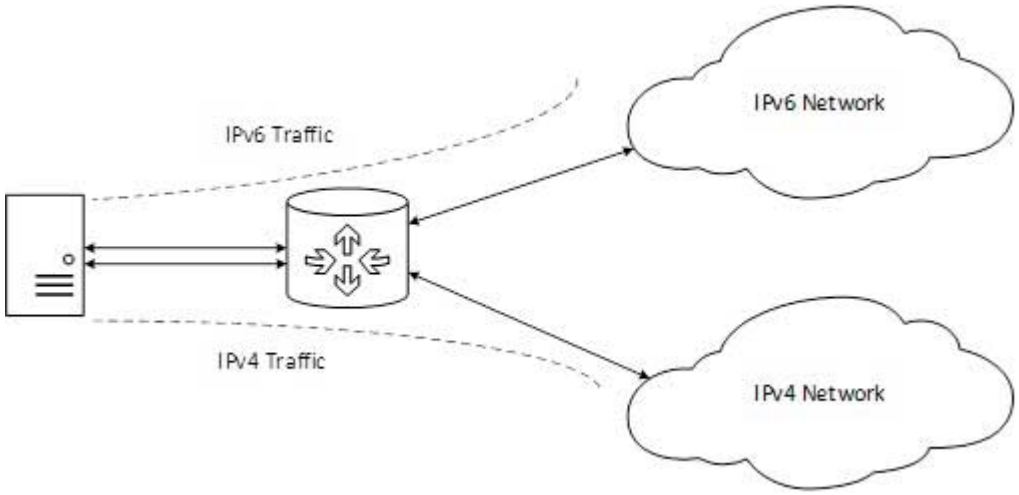
IPv4 to IPv6

One problem in transition from IPv4 to IPv6 completely is that IPv6 is not backward compatible. This results in a situation where either a site is on IPv6 or it is not. Unlike an implementation of new technology where the newer one is backward compatible so the older system can still work with the newer without any additional changes.

To overcome this short-coming, there exist few technologies which can be used in 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.

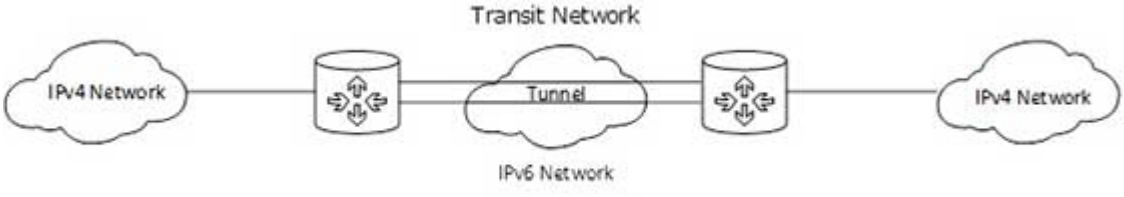


[*Image: Dual Stack Router*]

In above diagram, a Server which is having IPv4 as well as IPv6 address configured for it now can speak with all hosts on IPv4 network and IPv6 network with help of Dual Stack Router. Dual Stack Router, can communicate with both networks and provides a medium for hosts to access Server without changing their respective IP version.

Tunneling

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

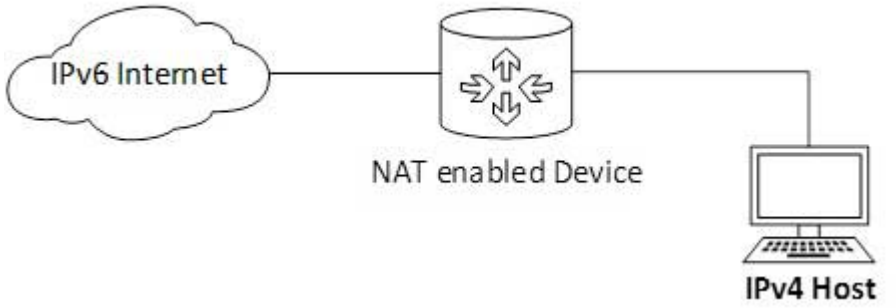


[*Image: Tunneling*]

The above diagram depicts how two remote IPv4 networks can communicate via Tunnel, where the transit network was on IPv6. Vice versa is also possible where transit network is on IPv6 and remote sites which intends 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 help of NAT-PT device, actual conversion 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 IPv6 enabled Server on Internet which does not understand IPv4 address. In this scenario, NAT-PT device can help them communicate. When IPv4 host sends a request packet to IPv6 Server, 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 IPv6 Server comes for IPv4 host, the router does vice versa.

Mobility

When a host is connected to one link or network, it acquires an IP address and all communication happens using that IP address on that link. As soon as, the same host changes its physical location, that is, moves into some different area / subnet / network / link, its IP address changes accordingly and all communication happening on the host using old IP address, goes down.

IPv6 mobility provides a mechanism which equips a host with an ability to roam around among different links without losing any communication/connection and its IP address.

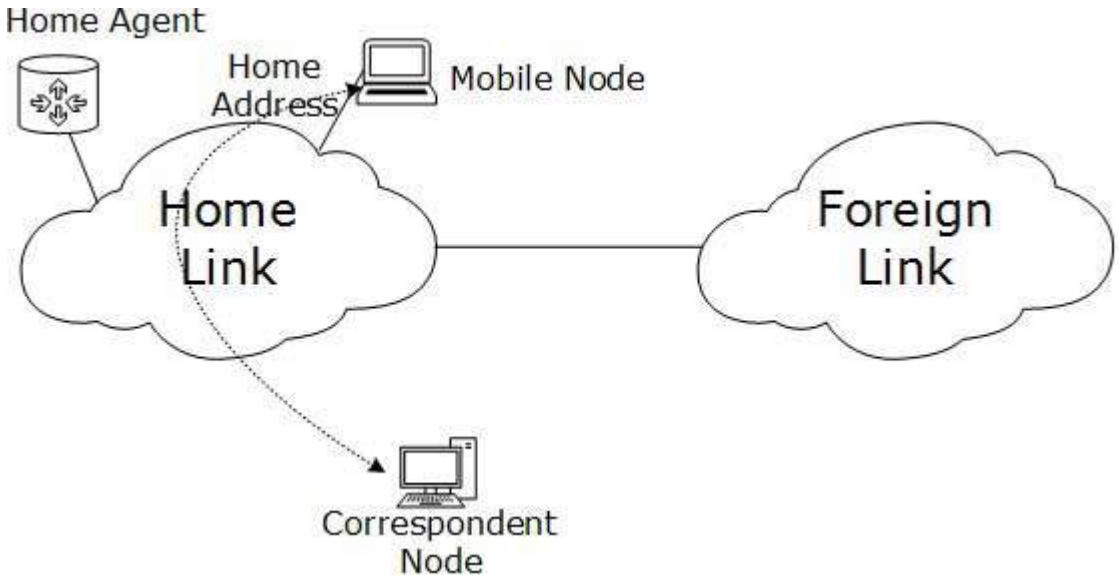
Multiple entities are involved in this technology:

- **Mobile Node**: The device which needs IPv6 mobility.
- **Home Link**: This link is configured with the home subnet prefix and this is where the Mobile IPv6 device gets its Home Address.

- **Home Address**: This is the address which Mobile Node acquires from Home Link. This is permanent address of Mobile Node. If the Mobile Node remains in the same Home Link, the communication among various entities happens as usual.
- **Home Agent**: This is a router which acts as registrar for Mobile Nodes. Home Agent is connected to Home Link and maintains information about all Mobile Nodes, their Home Addresses and their present IP addresses.
- **Foreign Link**: Any other Link which is not Mobile Node's Home Link.
- **Care-of Address**: When a Mobile Node attaches to a Foreign Link, it acquires a new IP address of that Foreign Link's subnet. Home Agent maintains the information of both Home Address and Care-of Address. Multiple Care-of addresses can be assigned to Mobile Node, but at any instance only one Care-of Address has binding with Home Address.
- **Correspondent Node**: Any IPv6 enable device which intends to have communication with Mobile Node.

Mobility Operation

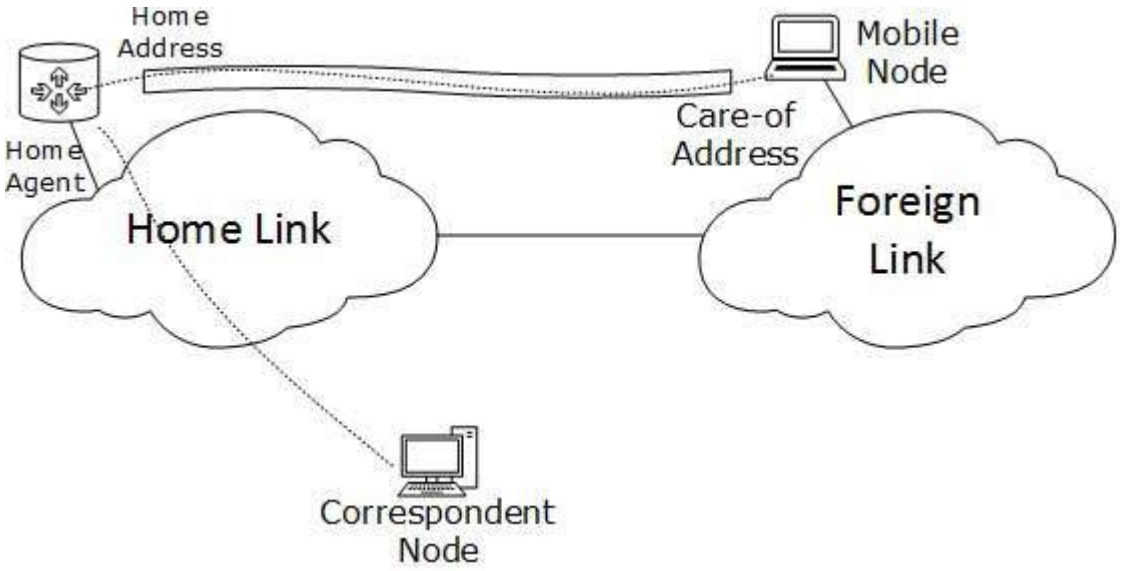
When Mobile Node stays in its Home Link, all communications happen on its Home Address. As shown below:



[*Image: Mobile Node connected to Home Link*]

When Mobile Node leaves its Home Link and is connected to some Foreign Link, the Mobility feature of IPv6 comes into play. After connecting to Foreign Link, Mobile Node acquires an IPv6 address from Foreign Link. This address is called Care-of Address. Mobile Node sends binding request to its Home Agent with the new Care-of Address. Home Agent binds Mobile Node's Home Address with Care-of Address, establishing a Tunnel between both.

Whenever a Correspondent Node tries to establish connection with Mobile Node (on its Home Address), the Home Agent intercepts the packet and forwards to Mobile Node's Care-of Address over the Tunnel which was already established.



[*Image: Mobile Node connected to Foreign Link*]

Route Optimization

When a Correspondent Node initiate communication by sending packets to Mobile Node on Home Address, these packets are tunneled to Mobile Node by Home Agent. In Route Optimization mode, when the Mobile Node receives packet from Correspondent Node, it does not forward replies to Home Agent. Rather it sends its packet directly to Correspondent Node using Home Address as Source Address. This mode is optional and not used by default.

Routing

Routing concepts remain same in case of IPv6 but almost all routing protocol have been redefined accordingly. We have seen in Communication in IPv6 segment, how a host speaks to its gateway. Routing is a process to forward routable data choosing best route among several available routes or path to the destination. A router is a device which forwards data which is not explicitly destined to it.

There exists 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, Link-State Routing Protocol uses its own algorithm to calculate best path to all available links. OSPF and IS-IS are link state routing protocols and both uses Dijkstra's Shortest Path First algorithm.

Routing protocols can be divided in two categories:

- **Interior Routing Protocol**: Protocols in this categories are used within an Autonomous System or organization to distribute routes among all routers inside its boundary. Examples: RIP, OSPF.
- **Exterior Routing Protocol**: Whereas an Exterior Routing Protocol distributes routing information between two different Autonomous Systems or organization. Examples: BGP.

Routing protocols

- **RIPng**

  RIPng stands for Routing Information Protocol Next Generation. This is an Interior Routing Protocol and is a Distance Vector Protocol. RIPng has been upgraded to support IPv6.

- **OSPFv3**

  Open Shortest Path First version 3 is an Interior Routing Protocol which is modified to support IPv6. This is a Link-State Protocol and uses Djikrasta's Shortest Path First algorithm to calculate best path to all destinations.

- **BGPv4**

  BGP stands for Border Gateway Protocol. It is the only open standard Exterior Gateway Protocol available. BGP is a Distance Vector protocol which takes Autonomous System as calculation metric, instead of number of routers as Hop. BGPv4 is an upgrade of BGP to support IPv6 routing.

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. Though 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

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 DNS can reply with both IP versions (4 & 6) without any change in query format.

Summary

IPv4 since 1982, has been an undisputed leader of Internet. With IPv4's address space exhaustion IPv6 is now taking over the control of Internet, which is called Internet2.

IPv4 is widely deployed and migration to IPv6 would not be easy. So far IPv6 could penetrate IPv4's address space by less than 1%.

The world has celebrated 'World IPv6 Day' on June 08, 2011 with a purpose to test IPv6 address over Internet in full. On June 06, 2012 the Internet community officially launched IPv6. This day all ISPs who were offering IPv6 were to enable it on public domain and were to keep it enable. All the device manufacturer also participated to offer IPv6 by-default enabled on devices.

This was a step towards encouraging Internet community to migrate to IPv6.

Organizations are provided plenty of ways to migrate from IPv4 to IPv6. Also organization, willing to test IPv6 before migrating completely can run both IPv4 and IPv6 simultaneously. Networks of different IP versions can communicate and user data can be tunneled to walk to the other side.

Future of IPv6

IPv6 enabled Internet version 2 will replace todays IPv4 enabled Internet. When Internet was launched with IPv4, developed countries like US and Europe took the larger space of IPv4 for deployment of Internet in their respective countries keeping future need in mind. But Internet exploded everywhere reaching and connecting every country of the world increasing the requirement of IPv4 address space. As a result, till this day US and Europe have many IPv4 address space left with them and countries like India and China are bound to address their IP space requirement by means of deployment of IPv6.

Most of the IPv6 deployment is being done outside US, Europe. India and China are moving forward to change their entire space to IPv6. China has announced a five year deployment plan named China Next Generation Internet.

After June 06, 2012 all major ISPs were shifted to IPv6 and rest of them are still moving.

IPv6 provides ample of address space and is designed to expand today’s Internet services. Feature-rich IPv6 enabled Internet version 2 may deliver more than expected.