**IPv6 - 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 3.4×1038 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 provided the fact that 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 hosts on the Internet, with some limitations involved like Firewall, organization policies, etc.

* **Auto-configuration**

IPv6 supports both stateful and stateless auto configuration mode of its host devices.

**Stateful** autoconfiguration protocol allows hosts to obtain addresses and other configuration information from a server.

**Stateless** autoconfiguration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers.

This way, absence of a DHCP server does not put a halt on inter segment communication.

* **Faster Forwarding/Routing**

Simplified header puts all unnecessary information at the end of the header. The information contained in the first part of the header is adequate for a Router to take routing decisions, thus making routing decisions as quickly as looking at the mandatory header.

* **IPSec**

Initially it was decided that IPv6 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 any more. It uses multicast to communicate with multiple hosts.

* **Mobility**

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

* **Enhanced Priority Support**

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 the 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 mechanism saves IP addresses and NAT is not required. So devices can send/receive data among 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 take forwarding decisions and forward them as quickly as they arrive.

* **Extensibility**

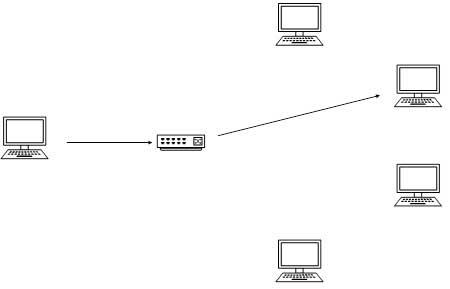
One of the major advantages of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options, whereas options in IPv6 can be as much as the size of IPv6 packet itself.

# IPv6 - Addressing Modes

In computer networking, addressing mode refers to the mechanism of hosting an address 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 the closest distance can be addressed.

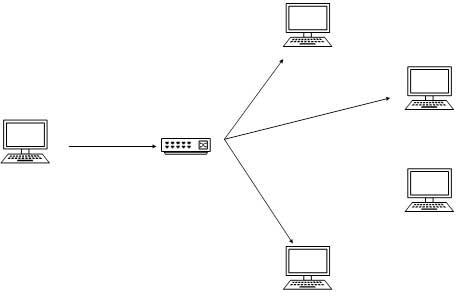
## Unicast

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.When a network switch or a 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.



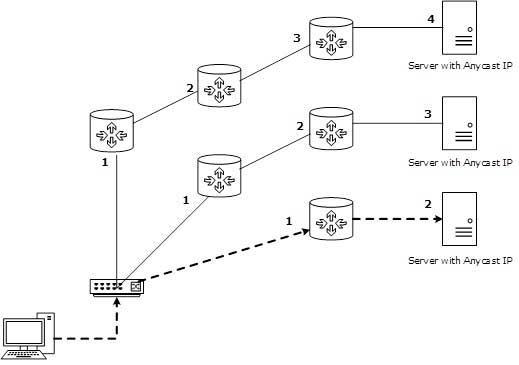
## Multicast

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



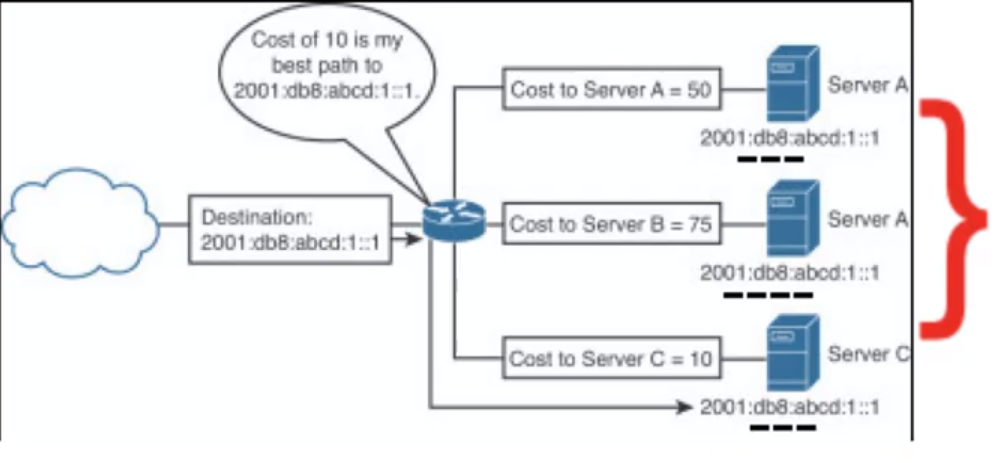
## Anycast

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, it 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.



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

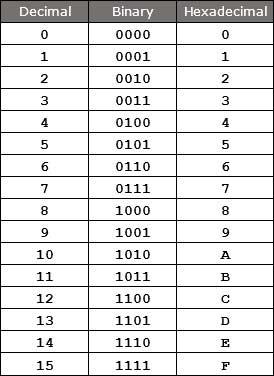
In the above picture, when a client computer tries to reach a server, the request is forwarded to the server with the lowest Routing Cost.



# IPv6 - Address Types & Formats

## Hexadecimal Number System

Before introducing IPv6 Address format, we shall look into Hexadecimal Number System. Hexadecimal is a positional number system that 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 to represent values from ten to fifteen. Every digit in Hexadecimal can represent values from 0 to 15.

[*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 symbols.

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

0010000000000001 0000000000000000 0011001000111000 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. The rules are as follows:

**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 contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):

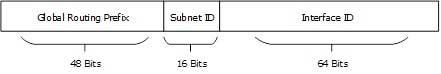
**2001:0000:3238:DFE1:63::FEFB**

**Rule.3:** Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):

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

## Global Unicast Address

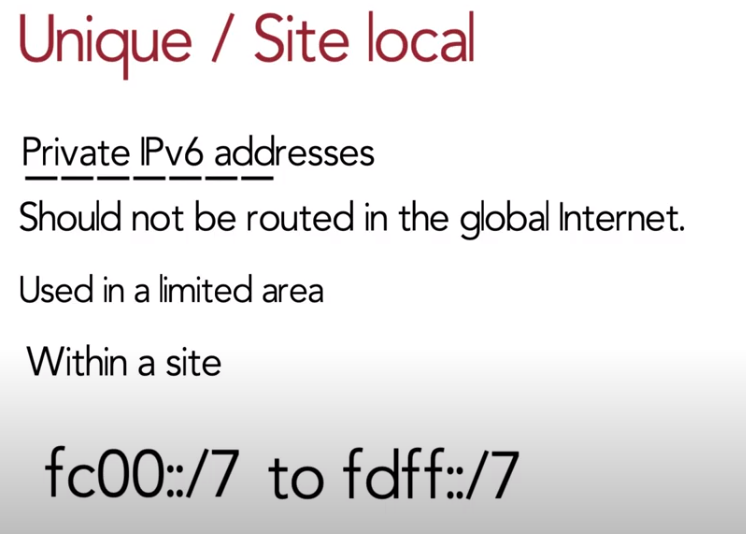
This address type is equivalent to **IPv4’s public address**. Global Unicast addresses in IPv6 are globally identifiable and uniquely addressable.

[*Image: Global Unicast Address*]

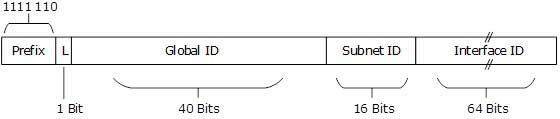
Global Routing Prefix: The most significant 48-bits are designated as Global Routing Prefix which is assigned to specific autonomous system. The three most significant bits of Global Routing Prefix is always set to 001.

## Unique/Site Local Address

This address type is equivalent to **IPv4’s private address**.

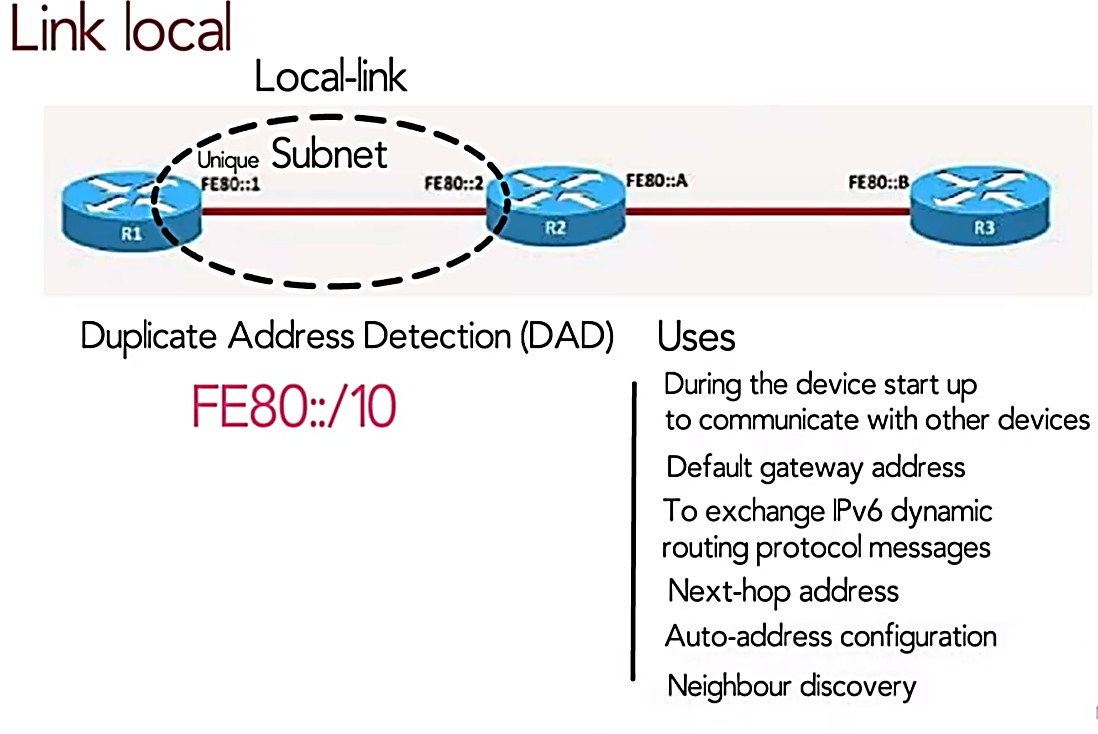


This type of IPv6 address is **globally unique, but it should be used in local communication.** The second half of this address contain Interface ID and the first half is divided among Prefix, Local Bit, Global ID and Subnet ID.

[*Image: Unique-Local Address*]

Prefix is always set to 1111 110. L bit, 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’.

## Link-Local Address

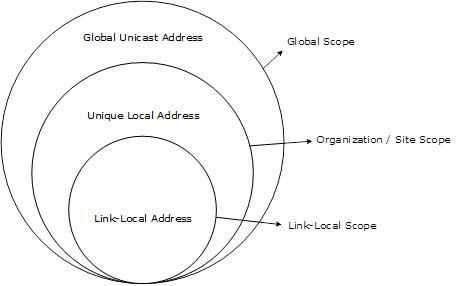


Auto-configured IPv6 address is known as Link-Local address. This address always starts with FE80. The first 16 bits of link-local address is always set to 1111 1110 1000 0000 (FE80). The next 48-bits are set to 0, thus:

https://www.tutorialspoint.com/ipv6/images/link_local_address.jpg[*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.

### 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 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.

# IPv6 - Communication

In IPv4, a host that wants to communicate with another host on the network needs 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 can speak to any host on the subnet. To communicate on layer-3, a host must also 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 a host whose IP address is known, a host sends ARP broadcast and in return, the intended host sends back its MAC address.

In IPv6, there are no broadcast mechanisms. It is not a must for an IPv6 enabled host to obtain an IP address from DHCP or manually configured, but it can auto-configure its own IP.

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 host gets an IPv6 address, it joins a number of multicast groups. All communications related to that segment take place 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 the 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. It 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 response 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.

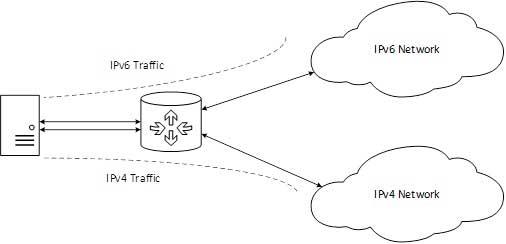
# Transition From IPv4 to IPv6

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

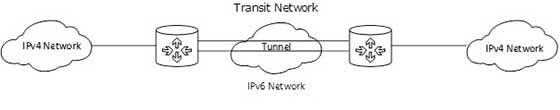
A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme.

[*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

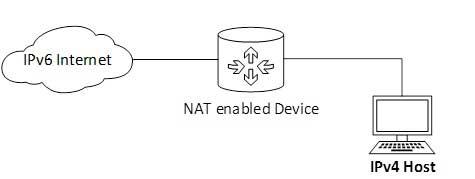
In a scenario where different IP versions exist on intermediate path or transit networks, tunneling provides a better solution where user’s data can pass through a non-supported IP version.

[*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.