IPV6 ADDRESSING

-
-

Address Representation:
Represented by breaking 128 bit into Eight 16-bit segments (Each 4 Hex character each)
Each segment is written in Hexadecimal separated by colons.
Hex digit are not case sensitive.
Rule 1:
Drop leading zeros:
2001:0050:0000:0235:0ab4:3456:456b:e560
2001:050:0:235:ab4:3456:456b:e560
Rule2:
Successive fields of zeros can be represented as "::" , But double colon appear only once in the address.
FF01:0:0:0:0:0:0:1
FF01::1
Note : An address parser identifies the number of missing zeros by separating the two parts and entering 0 until the 128 bits are complete. If two "::" notations are placed in the address, there is no way to identify the size of each block of zeros.
Ipv4 vs ipv6

IPV4	IPV6
1. source and destination addresses are 32 bits.)	1. Source and destination addresses are 128 bits.
2. ipv4 support small address space.	2. Supports a very large address space sufficeint for each and every people on earth.
3. ipv4 header includes checksum.	3. ipv6 header doesn't includes the checksum. (the upper-layer protocol or security extension header handles data integrity)
4. addresses are represented in dotted decimal format. (Eg. 192.168.5.1)	4. Addresses are represented in 16-bit segments Each segment is written in Hexadecimal separated by colons. (Eg. 2001:0050:020c:0235:0ab4:3456:456b:e560
5. Header includes options.	All optional data is moved to IPV6 extension header..
6. Broadcast address are used to send traffic to all	6. There is no IPV6 broadcast address. Instead a link

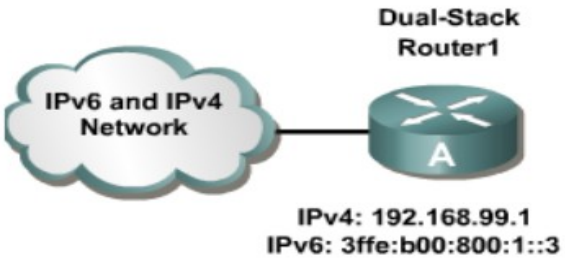
nodes on a subnet.	local scope all-nodes multicast address is used.
7. No identification of packet flow for QOS handling by router is present within the ipv4 header.	7. Packet flow identification for QOS handling by routers is present within the IPV6 header using the flow label field.
8. uses host address (A) resource records in the Domain name system(DNS) to map host names to ipv4 addresses.	8. Uses AAAA records in the DNS to map host names to ipv6 addresses.
9. Both routers and the sending host fragment packets.	9. Only the sending host fragments packets; routers do not.
10. ICMP Router Discovery is used to determine the IPv4 address of the best default gateway, and it is optional.	10. ICMPv6 Router Solicitation and Router Advertisement messages are used to determine the IP address of the best default gateway, and they are required.

IPV6 Transition Mechanism:

1. **Dual Stack**
2. **Tunneling Technique**
3. **Translation technique**

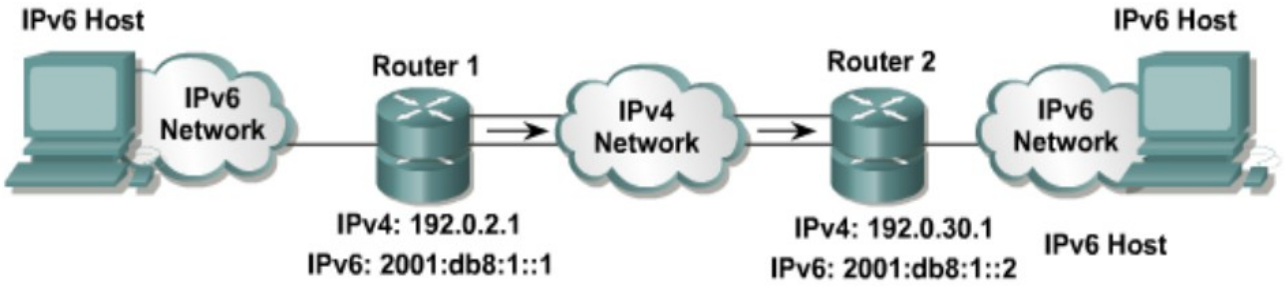
Dual Stack:

Dual stack is an integration method where a node has implementation and connectivity to both Ipv4 and ipv6 network. If both ipv4 and ipv6 are configured on an interface, this interface is dual-stacked.



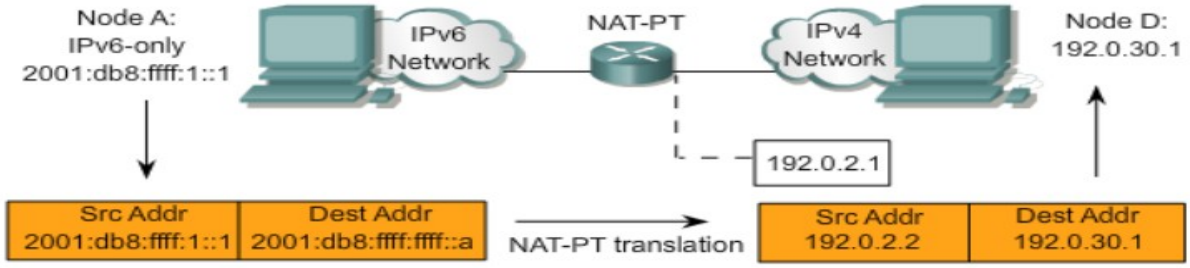
Tunneling Technique

With manually configured IPv6 tunnels, an IPv6 address is configured on a tunnel interface, and manually configured IPv4 addresses are assigned to the tunnel source and the tunnel destination. The host or router at each end of a configured tunnel must support both the IPv4 and IPv6 protocol stacks.



NAT-Protocol Translation (NAT-PT)

is a translation mechanism that sits between an IPv6 network and an Ipv4 network. The translator translates IPv6 packets into IPv4 packets and vice versa.



Source : http://dayaramb.files.wordpress.com/2011/03/computer-network-notes-pu.pdf