www.howtonetwork.net

# CCNA: IP version 6

## IP version 6 (IPv6)

### Why IPv6?

IPv4 has the following issues:

1. Address depletion
2. Large internet routing tables
3. Lack of true end-to-endness
   - IPv4 is patched to deal with the address depletion issue
   - NAT hides the true source of the network

IPv6 provides the following benefits over IPv4:

- Address space: $2^{128} = 3.4 \times 10^{38}$ addresses
- Global route aggregation
- Elimination of NAT
- Broadcast elimination
- Compatibility for IPv4 network
- Improved security with built-in IPSec
- Stateless Auto-configuration

## IPv6 Address and Representation

An IPv6 address is divided into 8-octets, each consisting of 4 hexadecimal digits separated by a colon. For example:

1. 2345:AF45:00AA:0000:0000:0079:90AB:CDEF
2. FA00:0001:0000:0000:0000:0000:0000:1234

IPv6 address can be shorten:

- Omitting leading zeros. The address in example number one and two can be written as: 2345:AF45:AA:0:0:79:90AB:CDEF, FA00:1:0:00:0:0:0:1234
- Replacing consecutive zeros with a double colon (::). The address in example number two can be written as: FA00:1::1234

Replacing the consecutive zero is actually a two step process. First the leading zeros are omitted, then the consecutive zeros are replaced with double colon

## Network Addressing

Typically 64-bit network and 64-bit host The network portion is further subdivided into:

- 48-bit Global Routing Prefix: allows routing to the site in internet
- 16-bit Subnet ID: allows an administrator to create subnet within a site

An IPv6 address is usually presented as:

| Global Routing Prefix (Usually Assigned by ISP) 48-bits | Subnet ID 16-bits | Host ID (Usually Interface ID) 64-bits |
|---|---|---|

IPv6 addresses don't use the lengthy subnet mask notation; instead CIDR notation is used to indicate the prefix length. For example: FA00:1::/48 mean that 48-bits network

## Address Types

There are three types of IPv6 addresses:

1. Unicast
   - Address for a single interface
   - Packet destined for that address is delivered specifically to that interface
2. Multicast
   - Packet sent to multicast address goes to all SUSCRIBERS. Example: FF02:9
3. Anycast
   - Multiple devices share the same address
   - Router decides what is the closet and send to that system
   - An Anycast address cannot be Source Address (SA) of a packet
   - It is often used to replicate important network resources such as DNS root servers, web servers and multicast rendezvous points (RPs)

## Address Assignment

IPv6 addresses can be assigned in three possible ways:

1. Static configuration with **"ipv6 address"** command
2. Via DHCP for IPv6
3. Stateless Auto-configuration with **"ipv6 address auto-config"** command

## Host Address Assignment

The host address can be assigned in two ways:

1. Static assignment with **"ipv6 address"** command
2. EUI-64 address assignment with **"ipv6 address eui-64"** command. Host address is calculated from the MAC address

The EUI-64 address is calculated in two steps:

1. Invert the seventh most significant bit in MAC address
2. Insert the "FFFE" in the middle

Example: Consider the MAC Address 1234.5679.9012:

1. Invert the 7th most significant bit
   - 1=0001 and 2=0010. Inverting the 7th bit gives us: 0001 0000 = 10. The MAC address becomes: 1034.5679.9012
2. Insert FFFE in the middle
   - The required host address is: 1034:56**FF:FE**78:9012

## Configuration Example: Static IPv6 Address Assignment

***Router R1:***

**ipv6 unicast-routing ← Turn on IPv6 Addressing**

```
!
interface FastEthernet0/0
 ipv6 address 155:1::1/64
 ipv6 enable
```

```
R1#sh ipv6 interface
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::CA00:4FF:FEB4:0 ← Link Local Address
  Global unicast address(es):
    155:1::1, subnet is 155:1::/64 ← Unicast Address
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FFB4:0
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

## Configuration Example: EUI-64 Address Assignment

***Router R1:***

```
Ipv6 unicast-routing
!
interface FastEthernet0/0
 mac-address 1234.5678.9012
 ipv6 address 155:1::/64 eui-64
 ipv6 enable
```

```
R1#sh ipv6 interface
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1034:56FF:FE78:9012
  Global unicast address(es):
    155:1::1034:56FF:FE78:9012, subnet is 155:1::/64 ← Host ID created with EUI-64 address
  Joined group address(es):
    FF02::1
    FF02::1:FF78:9012
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

## IPv6 Transition Techniques

**Dual Stack:** This architecture contains both IPv4 and IPv6 Internet layers with separate protocol stacks containing separate implementations of Transport layer protocols such as TCP and UDP.

**IPv6 over IPv4 tunneling:** Tunneling allow the encapsulation of IPv6 traffic in IPv4 packets for the transmission of IPv6 traffic over IPv4 infrastructure.

Tunneling can be used in a variety of ways:

- **Router-to-Router**: In this configuration IPv6/IPv4 routers connected through IPv4 infrastructure can tunnel IPv6 packets.
- **Host-to-Router or Router-to-Host:** In host-to-router tunneling IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediary IPv6/IPv4 router that is reachable via an IPv4 infrastructure. This type of tunnel spans the first segment of the packet's end-to-end path. In router-to-host tunneling IPv6/IPv4 routers can tunnel IPv6 packets to their final destination IPv6/IPv4 host. This tunnel spans only the last segment of the end-to-end path.
- **Host-to-Host:** IPv6/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.

### Types of Tunnels

- **Static:** These are manually configured tunnel, unlike automatic tunnels the IPv4 address of the tunnel endpoint is not derived are not derived from addresses that are encoded in the next-hop address when forwarding the packet. IPv6 addresses are manually configured on each tunnel interface, and so are the IPv4 tunnel source and IPv4 tunnel destination configured. Static tunnels create a permanent link between two IPv6 domains over an IPv4 infrastructure.
- **Automatic:** These types of tunnel do not require manual configuration. Automatic tunnel includes the following types
- **ISATAP**: Intra-Site Automatic Tunnel Addressing Protocol is used to provide unicast IPv6 connectivity between IPv6/IPv4 hosts across an IPv4 intranet. ISATAP is designed for transporting IPv6 packets within a site where an IPv6 infrastructure is not yet available, ISATAP tunnels allow individual IPv4 or IPv6 dual-stack hosts within a site to communicate with other such hosts on the same virtual link, basically creating an IPv6 network using the IPv4 infrastructure. ISATAP is designed for transporting IPv6 packets within a site, not between sites. ISATAP uses unicast addresses that include a 64-bit IPv6 prefix and a 64-bit interface identifier. The interface identifier is created in modified EUI-64 format in which the first 32 bits contain the value 000:5EFE to indicate that the address is an IPv6 ISATAP address.
- **6to4 Tunnels**: These are point-to-multipoint tunnels used for connecting isolated IPv6 domains over IPv4 infrastructure. 6to4 treats the entire IPv4 Internet as a single NBMA virtual link. An automatic 6to4 tunnel may be configured on an edge router in an isolated IPv6 network, which creates a tunnel on a per-packet basis to an edge router in another IPv6 network over an IPv4 infrastructure. The tunnel destination is determined by the IPv4 address of the border router extracted from the IPv6 address that starts with the prefix 2002::/16, where the format is 2002:edge-router-IPv4-address::/48. Following the embedded IPv4 address are 16 bits that can be used to number networks within the site. The edge router at each end of a 6to4 tunnel must support both the IPv4 and IPv6 protocol stacks. 6to4 tunnels can be configured between edge routers or between a edge router and a host.