# Chapter 1 : IPv6 address Fundamental

1) Basics

An IPv6 address is a 128 bit binary number and expressed in hexadecimal form, e.g.

2001:1234:5678:0001:0000:0000:0000:0001/64
(32 hexadecimal numbers)

There is a colon between each 4 hexadecimal numbers. This is for easy reading, just like the "dot-decimal form" of IPv4 address. E.g. 202.175.3.3

/64 means the first 64 bit is the network prefix, it is similar to IPv4 CIDR (Classless Inter-Domain Routing) notation

2) Simplifying IPv6 addresses

Since it is too long to express the IPv6 address, we want to simply it.

e.g. 2001:1234:5678:0001:0000:0000:0000:0001/64 can be simplified as 2001:1234:5678:1:0:0:0:1/64

This is called "Zero compression" – The leading zeros in each segment can be omitted. Continuous zeroes can be further compressed.

2001:1234:5678:0001:0000:0000:0000:0001/64
➔ 2001:1234:5678:1:0:0:0:1/64
➔ 2001:1234:5678:1::1/64
"::" – Double Colon, means a series of 0000 groups. Since the total length of an IPv6 address is 128 bit, the number of zeroes omitted can be calculated.

Another example:

2001:0000:0000:0001:0000:0000:0000:0001/64
➔ 2001:0:0:1:0:0:0:1/64
➔ 2001:0:0:1::1/64
➔ But Note: 2001::1::1/64 is incorrect. It is because there is no way to identify the no. of zeroes omitted in the two double-colon areas.

3) IPv6 Prefix

Let's learn more about IPv6 Prefix.

In IPv4, we use subnet mask to denote the network portion.
e.g. 192.168.1.1 255.255.255.0 → 192.168.1.0 is the network portion
It can be written as : 192.168.1.1/24 (CIDR notation)

In IPv6, we don't use subnet mask. We only use the latter CIDR notation
e.g.
2001:1234:5678:0001:0000:0000:0000:0001/64

The network portion is : 2001:1234:5678:0001:: /64
The host portion is : 0000:0000:0000:0001.

That means there can be a tremendous number of hosts, $2^{64}$.

In IPv6, the network portion of an IP address is basically fixed at /64 and the host portion is always 64 bits.

There is no need for subnetting. Since there are far too many bits in the IPv6 addresses that each organization can be assigned a network prefix of /48.

e.g. A company may be assigned range of IP addresses with a network prefix of 2001:1234:5678:: /48. Then, the company can use 16 bits for the local subnetting.

e.g.
2001:1234:5678:0000:: /64 is the first subnet
to
2001:1234:5678:FFFF:: /64 is the last subnet.

This results in 65536 subnets, which is far more than enough for each company or organization.

In each subnet, there can be 2^64 hosts.

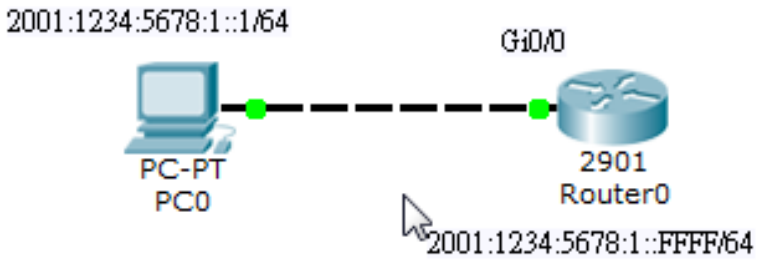
So, the network prefix of a usable IPv6 address is basically fixed at /64 and no further subnetting is needed. This is an advantage over IPv4 because we need to

do quite a lot troublesome IP address subnetting in IPv4.

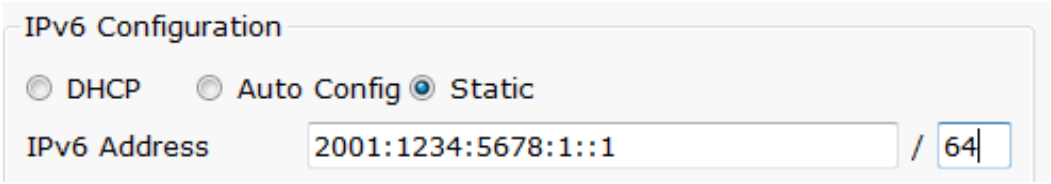
4) Demonstration

Let's use Packet Tracer to show a demonstration of using IPv6 addresses.

Topology:




PC setting:




Router setting:

```
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:1234:5678:1::FFFF/64
```

Ping test:

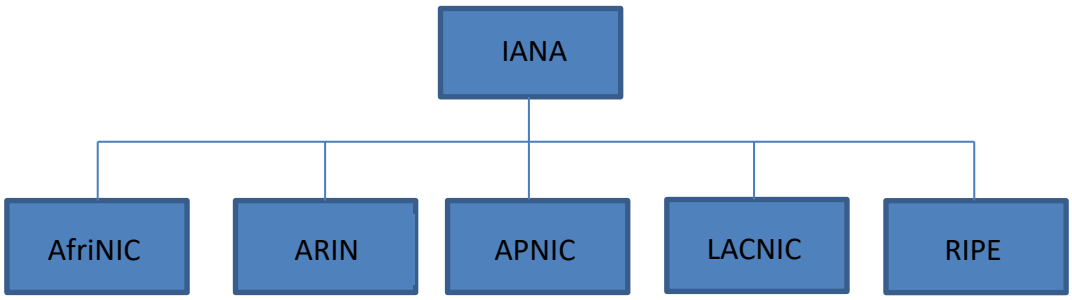
```
PC>ping 2001:1234:5678:1::FFFF

Pinging 2001:1234:5678:1::FFFF with 32 bytes of data:

Reply from 2001:1234:5678:1::FFFF: bytes=32 time=1ms TTL=255
Reply from 2001:1234:5678:1::FFFF: bytes=32 time=0ms TTL=255
Reply from 2001:1234:5678:1::FFFF: bytes=32 time=0ms TTL=255
Reply from 2001:1234:5678:1::FFFF: bytes=32 time=0ms TTL=255
```

# Chapter 2 : Different kinds of IPv6 addresses

It is crucial to understand the different kinds of IPv6 addresses, their principle and usage. In this Chapter, we will introduce the various kinds of commonly used IPv6 addresses.

## 1) 『IPv6 Global Unicast Address 』

IP addresses are allocated by IANA (Internet Assigned Numbers Authority), through 5 RIRs (Regional Internet Registries), which are responsible for 5 different areas on the Earth.




| RIR | Responsible Regions |
|---|---|
| African Network Information Centre (AfriNIC) | Africa region |
| American Registry for Internet Numbers (ARIN) | The United States, Canada, several parts of the Caribbean region, and Antarctica regions. |
| Asia-Pacific Network Information Centre (APNIC) | Asia, Australia, New Zealand, and neighboring countries |
| Latin America and Caribbean Network Information Centre (LACNIC) | Latin America and parts of the Caribbean region |
| Réseaux IP Européens Network Coordination Centre (RIPE NCC) | Europe, Russia, the Middle East, and Central Asia |

The current allocation of public IPv4 addresses is not sequential and continuous, meaning that a geographic region may acquire discontinuous ranges of public IPv4 address. This is due to the historical way of assignment and the insufficient public IPv4 addresses. E.g. For Macau region, it contains a large number of discontinuous, small address ranges, starting with 202.175.x, 27.x.y, 60.x.y, 113.x.y etc. This makes the aggregation of public IPv4 addresses very inefficient.

For IPv6, since it is a new deployment and there are huge numbers of IPv6 addresses. Huge enough to give each piece of sand on the Earth an IPv6 address. So, the assignment of public IPv6 addresses is more systematic.

Currently only 1/8 of the IPv6 addresses are publicly assigned, which is : 2000::/3. What does it means?

It means from 2000:: to 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

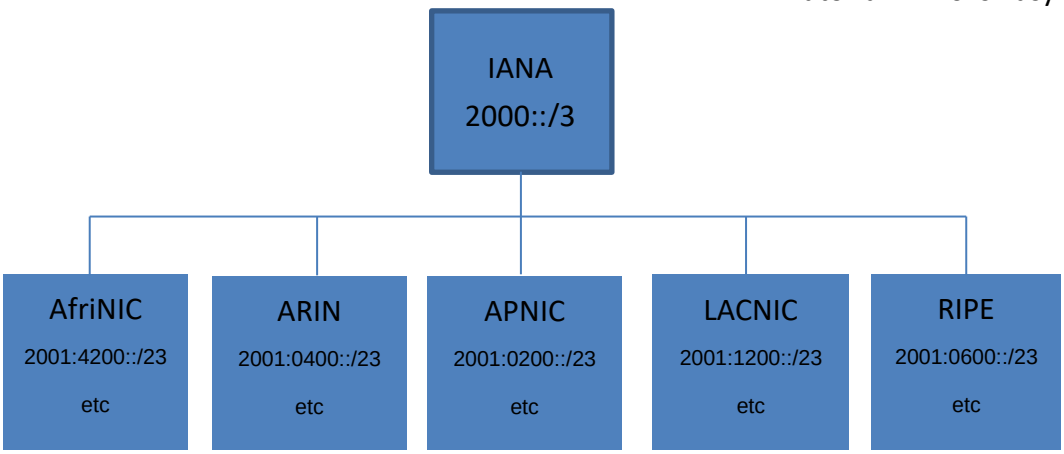
| | |
|---|---|
| 0010 0000 0000 0000 0000 0000 …. 0000 0000<br>2 0 0 0 : 0000:0000:0000:0000:0000:0000:0000:0000 | (Binary)<br>(Hexadecimal) |
| 0011 1111 1111 1111 1111 1111 …. 1111 1111<br>3 F F F : FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF | (Binary)<br>(Hexadecimal) |

And, currently, most of the assigned public IPv6 addresses starts with 2001::/16.

| | |
|---|---|
| 0010 0000 0000 0001 … … … … … … …… … … … … … … … … … … … … … … …<br>2 0 0 1 : … … … … … … … …… … … … … … … … … … … … … … … | (Binary)<br>(Hexadecimal) |

The IANA assigns address blocks to the five RIRs. The following table shows only a small portion of them. Usually, the IANA assigns address block with /23 prefix.

| | | | | |
|---|---|---|---|---|
| 2001:0200::/23 | APNIC | | 2001:0400::/23 | ARIN |
| 2001:0600::/23 | RIPE NCC | | 2001:1200::/23 | LACNIC |
| 2001:4200::/23 | AFRINIC | | | |




For APNIC, it has got 2001:0200::/23. What does 2001:0200::/23 include?

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 0 | 0 | 1 | : 0 | 2 | 0 | 0 | :0000:0000:0000:0000:0000:0000/23 |
| 0010 | 0000 | 0000 | 0001 | 0000 | 0010 | 0000 | 0000 | 0000 0000 … …. … …0000 0000/23 |
| to | | | | | | | | |
| 2 | 0 | 0 | 1 | : 0 | 3 | F | F | :FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/23 |
| 0010 | 0000 | 0000 | 0001 | 0000 | 0011 | 1111 | 1111 | 1111 1111 … …. … … 1111 1111/23 |

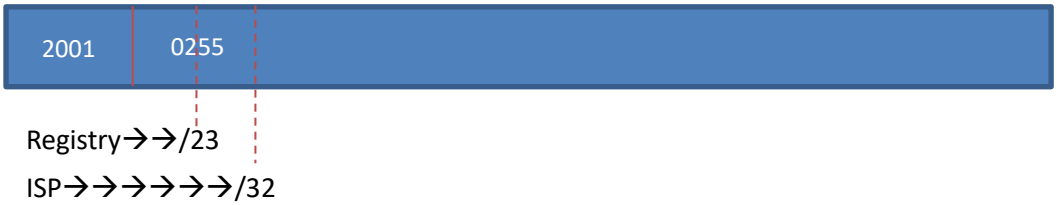
So, APNIC has got this block of IPv6 addresses:


Then, the APNIC assigns address blocks to ISPs.
e.g. APNIC may assign a block of addresses to ISPs like this :

2001:02 55::/32 to ISPa
2001:02 66::/32 to ISPb

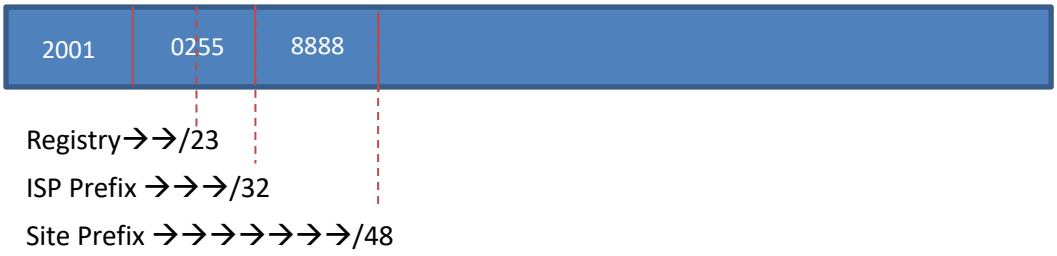
So, ISPa gets a block of IP addresses as follows:

| | |
|---|---|
| 2001:02 55::/32 | 2001:0255:0000:0000:0000:0000:0000:0000<br>to<br>2001:0255:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF |




Then, ISPa assigns blocks of IP addresses to different organization, like this :
e.g.
2001:0255:8888::/48 to Organization A
2001:0255:9999::/48 to Organization B

So, Organization A gets:

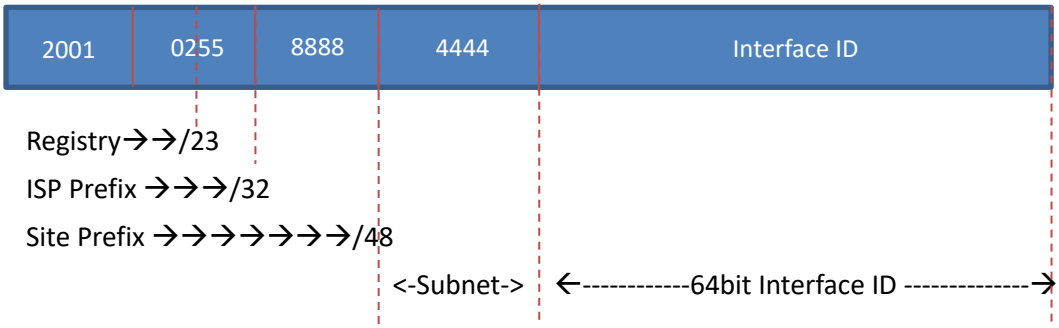



In this point of view, Organization A is referred to as a Site.

Now, the organization can freely use the remaining bits for its own, but, keeping 16 bits for Subnet ID.

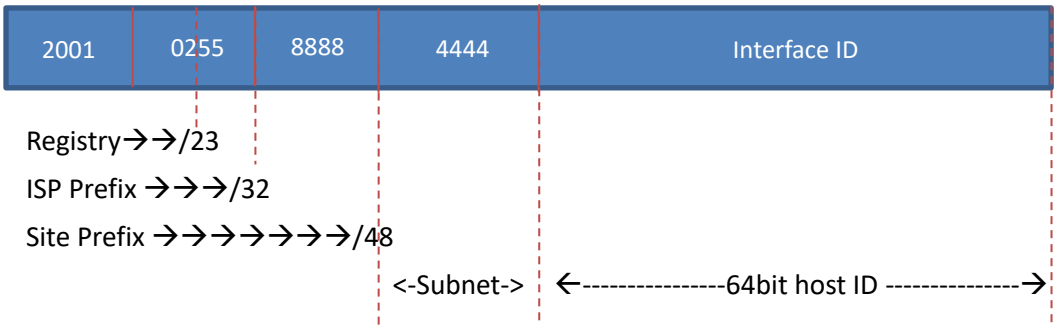
i.e. From 2001:0255:8888:0000::/64 to 2001:0255:8888:FFFF::/64
(The yellow portion is used as Subnet ID.)

Then, for each subnet, there are 64 bits for hosts, all together, 2^64 hosts. This is called Interface ID and is used for identifying IPv6 host interface.



As one organization can have 65536 subnets, with each subnet having $2^{64}$ hosts, this is far more than enough. So, no more subnetting is needed by the organization.

The above resultant IPv6 addresses is publicly reachable in the Internet and is called : 『**IPv6 Global Unicast Address** 』. It is similar to the IPv4 public addresses.

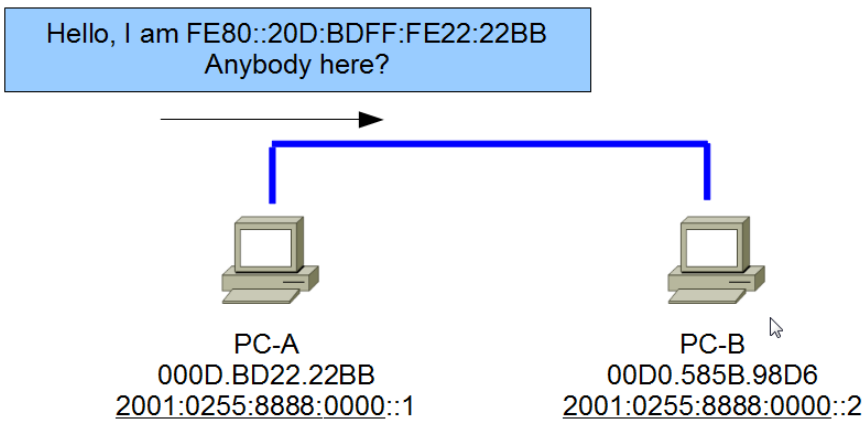



General format:

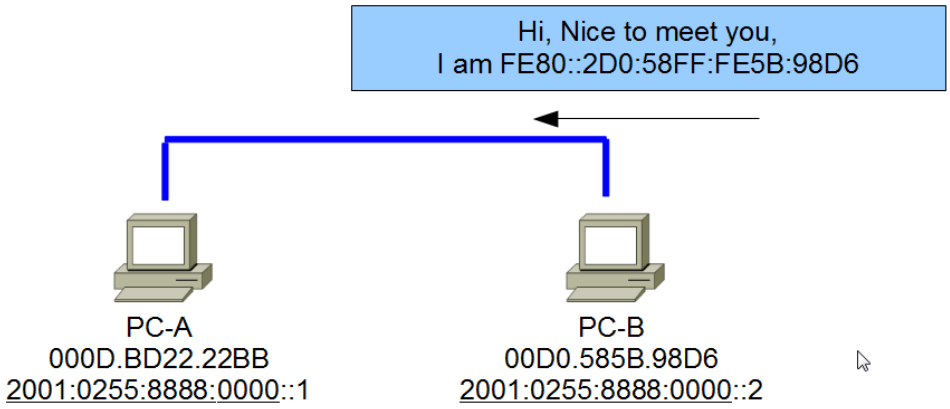

## 2) 『IPv6 Link local (Unicast) Address 』

In IPv6, a network host will try to discover if there is any neighbor nearby.

e.g. PC-A may send out a message like this:



And PC-B may reply:




You will notice that they are not using their Global Unicast address. Instead, they use a kind of IPv6 address called: **"Link Local address"**. In IPv6, **Link Local address** is used to communicate with **neighbors** in the same link or Layer 2 segment.

How is the Link Local address formed?

1) All link local address starts with FE80::/10, in binary : 1111 1110 10.

F E 8 0 ::/10
1111 1110 1000 0000

It ranges from:

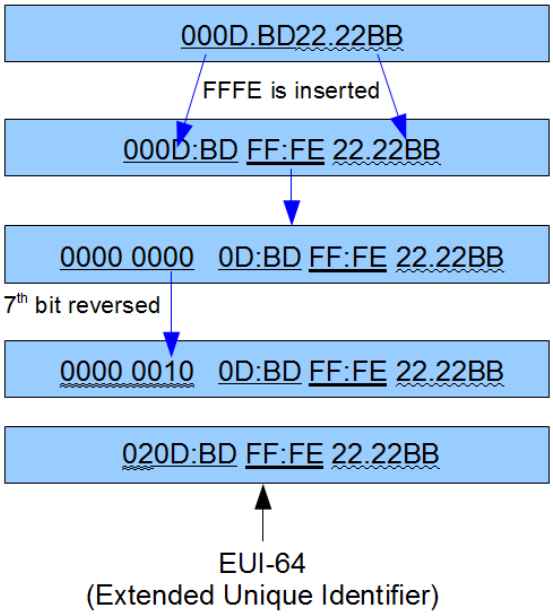
F E 8 0 :0000:0000:0000:0000:0000:0000:0000/10
1111 1110 1000 0000

to

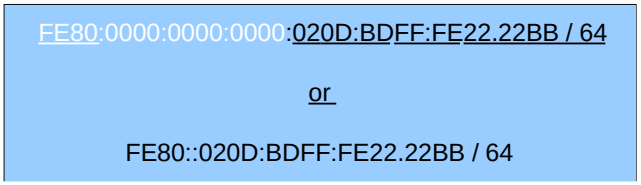
F E B F :FFFF:FFFF:FFFF:FFFF:FFFF::FFFF:FFFF/10
1111 1110 1011 1111

But commonly used Link Local Address starts with "FE80".

2) The MAC-address of the interface is used and converted as **EUI-64 format**.




3) Finally the two parts are combined to form the Link Local address.



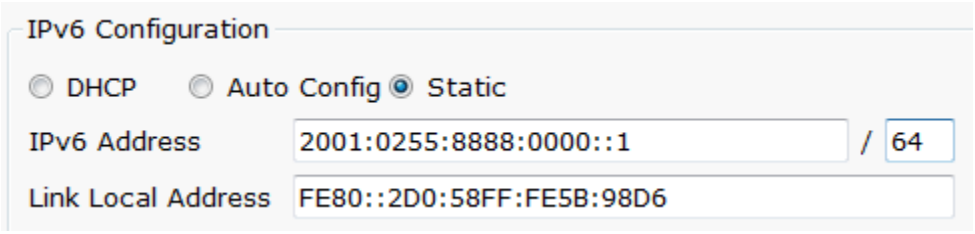

The Link Local address is automatically generated, even though the interface has not been assigned with any IPv6 Global Unicast Address. IPv6 Link Local address is analogous to IPv4 Link Local address, in the range : 169.254.0.0/16. But, their usage is different. An IPv4 host will only get such an address when it is configured to use DHCP server to acquire IP address but no response from any DHCP server is got.

## Different ways of assigning IP address :

Now, let's look more deeply into the actually usage of Link Local Address. To do so, we need to learn about how an IPv6 address can be assigned to an interface.

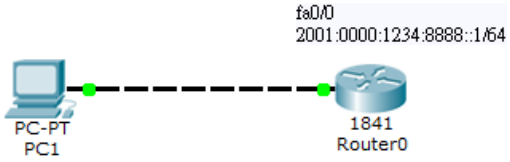
### 1) Static IPv6 address assignment

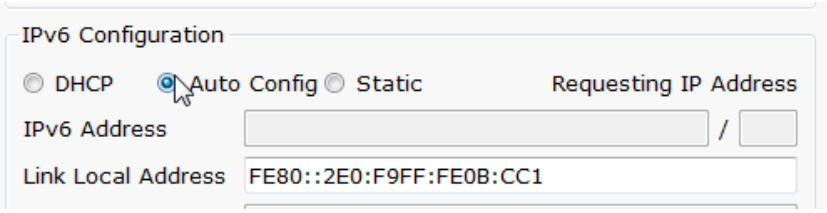
The most straight forward way is static assignment. E.g. On a PC:



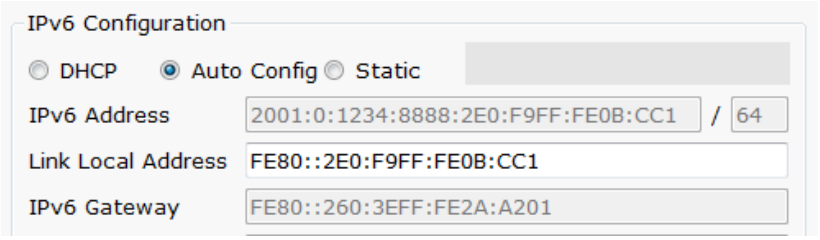

2) Stateless Auto-configuration

Another way, you can configure the PC to get an IPv6 address from its neighboring router. Let's see the following:



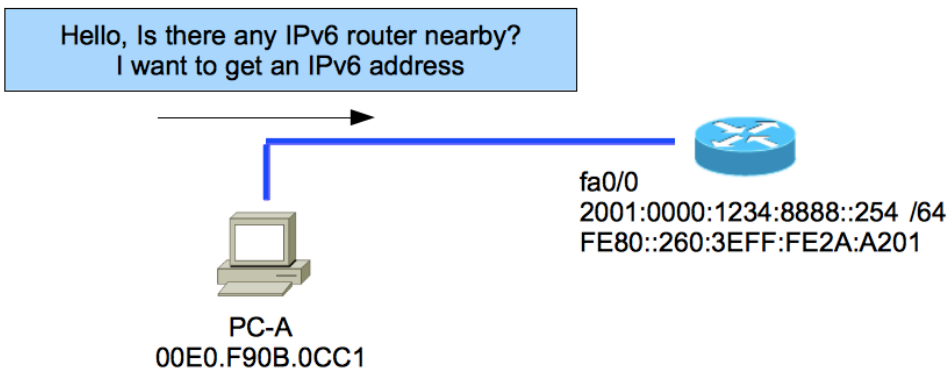




After a few seconds, the PC gets the following IPv6 address:

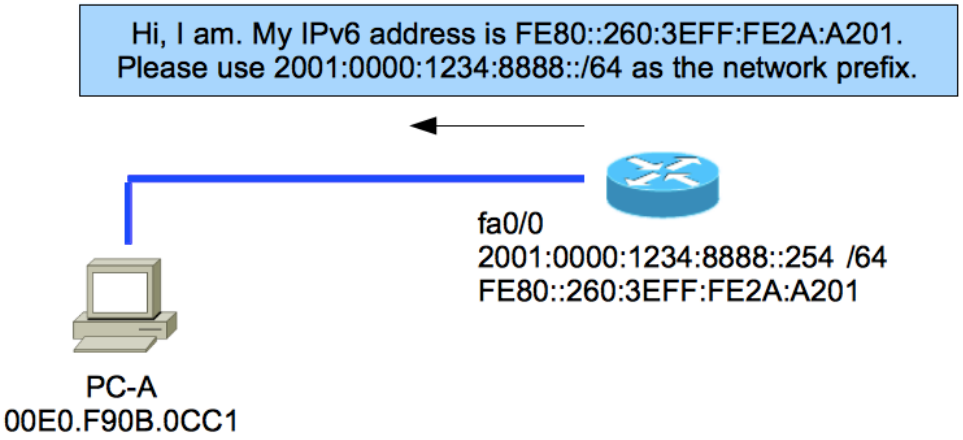



How does the PC get this address?

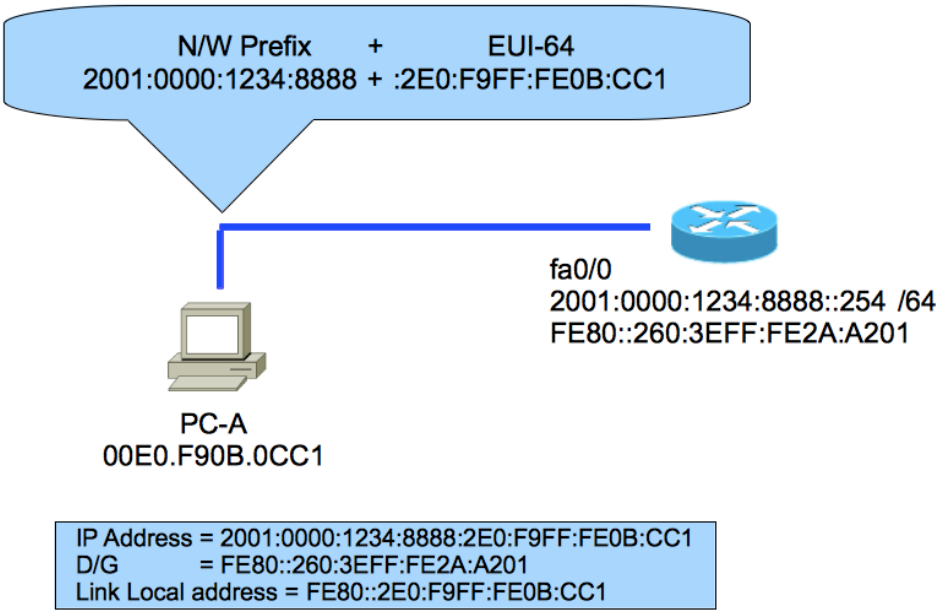
a) The PC sends out a "Router Solicitation" Message, requesting for the network prefix.



b) When a nearby router receives this message, it replies with a “Router Advertisement” Message, including the “Network Prefix” and its “Link Local Address”. In this case, the network prefix is 2001:0000:1234:8888::/64.




c) The PC then takes this network prefix and combines with its EUI-64 host ID to form its IPv6 address. → 2001:0000:1234:8888:2E0:F9FF:FE0B:CC1.




You may notice that the “IPv6 Gateway” is also automatically set. In the Router Advertisement message from the router, there is the link local address of that router interface. So, the PC set this link local address as its IPv6 gateway.

PC:

Router: "show ipv6 interface brief"

```
FastEthernet0/0            [up/up]
    FE80::260:3EFF:FE2A:A201
    2001:0:1234:8888::254
```

Now, you have learnt about one the usage of Link Local address. Remember that packets with destination IPv6 Link Local address will NOT be forwarded by router. So, **The scope of Link Local address is only limited to the Layer 2 segment that it belongs to.**

3) DHCPv6

This will be not be discussed here. But, it works similar to DHCP in IPv4.

## 3) 『Special IPv6 addresses that commonly used』

### 1) Unspecified address

When an IPv6 host has not yet got or assigned any IPv6 address. It will use 0:0:0:0:0:0:0:0 or :: as its source IP address. This is similar to 0.0.0.0 in IPv4.

### 2) Loopback address

In IPv4, the loopback address is in the range 127.0.0.0 / 8 and is typically 127.0.0.1. In IPv6, the loopback address is 0:0:0:0:0:0:0:1 or ::1. This address has a Node-scope, meaning that it is only destined for the Node itself.

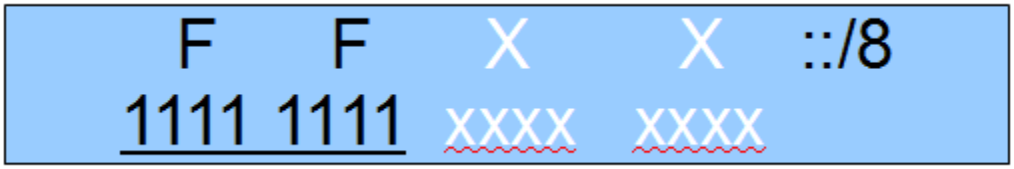
### 3) Default Route address

::/0 is the default route address.

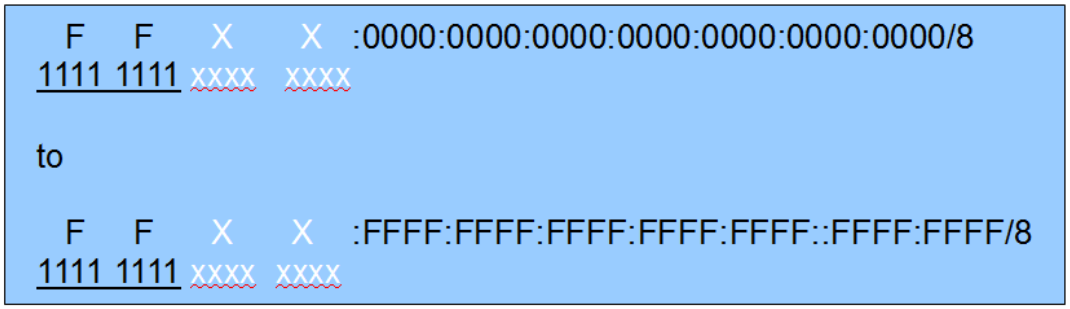
## 4) 『IPv6 Multicast Addresses』

### 1) Formation

In IPv4, multicast addresses are in the range of 224.0.0.0 – 239.255.255.255. What about IPv6? In IPv6, multicast addresses always starts with FF.




It ranges from:




In fact, the 3rd and 4th Octets have special usage/purpose, we will discuss later. That's why we mark them X here.

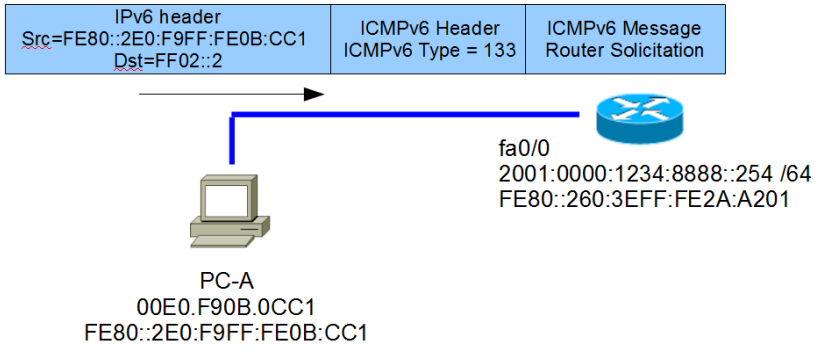
## 2) Typical usage

### a) Router Discovery

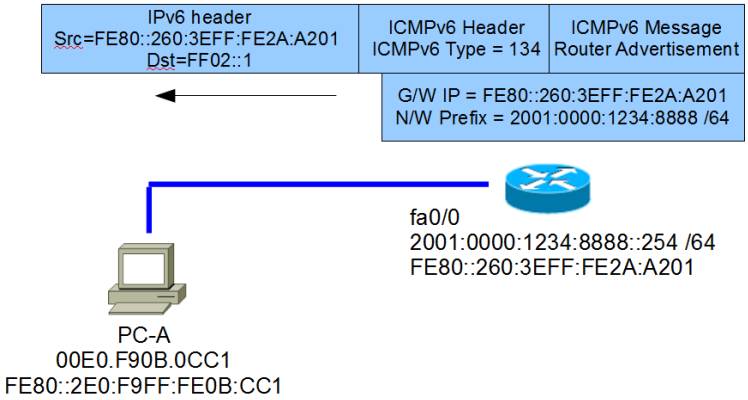
An IPv6 host will try to discovery if there is any router on its local link, esp. when it is configured to get IP address using "Stateless Auto-Configuration".

Let's see the following example.

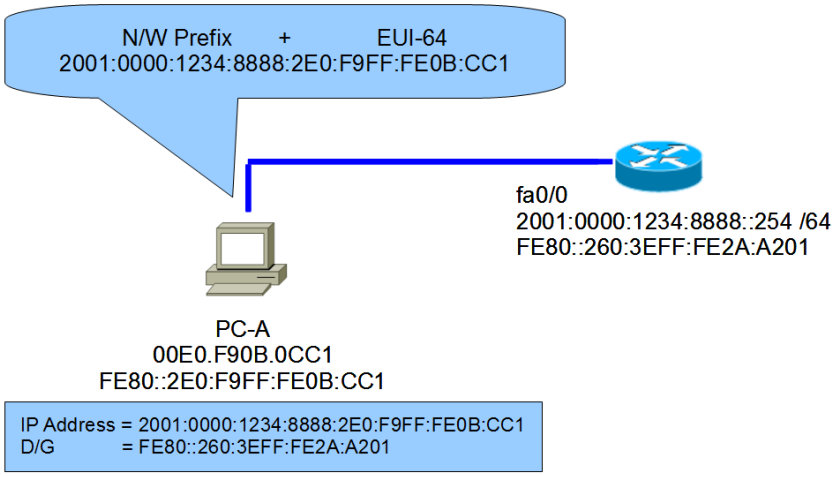
i) The PC-A sends out an ICMPv6 Router Solicitation Message (Type 133) with a source address of FE80::2E0:F9FF:FE0B:CC1, to a destination address of FF02::2, which is a multicast group including “All Routers in the Link Local scope”.




ii) When the router receives this RS Message, it replies with an ICMPv6 Router Advertisement Message (Type 134), with a source address of its Link Local address and a destination address of FF02::1, which includes “All Nodes in the Link Local scope”.



iii) When, PC-A receives this RA, it takes the G/W IP address and the N/W prefix. It uses EUI-64 to generate its Global Unicast IPv6 address.




Now let's examine the 2 IPv6 multicast addresses that we see above:

| F F | Lifetime 0 R P T | Scope | Group ID |
|---|---|---|---|
| F F | 0 | 2 | 2 |

It is a permanently assigned multicast adress
With a link local scope
Group ID = 2 means - All Routers

| F F | Lifetime 0 R P T | Scope | Group ID |
|---|---|---|---|
| F F | 0 | 2 | 1 |

It is a permanently assigned multicast adress
With a link local scope
Group ID = 1 means - All Nodes

All IPv6 enabled routers will join a multicast group of FF02::2 and all IPv6 hosts will join a multicast group of FF02::1.

Below, let's see the general form of IPv6 multicast addresses.

General form of an IPv6 multicast address

| 8 bits | 4 bits | 4 bits | 112 bits |
|---|---|---|---|
| F F | Lifetime<br>0 R P T | Scope | Group ID |

| T = 0 → Permanent multicast address assigned by IANA |
|---|
| T = 1 → Transient multicast address |
| R and P has other usages and is basically 0 |

| Scope = 1 | Node |
|---|---|
| Scope = 2 | Link |
| Scope = 5 | Site |
| Scope = E | Global |

Notes:

- Basically T will be 0, Permanent assigned.
- Scope 1 is Node scope, meaning that this address is valid for this Node.
- Scope 2 is Link-Local scope, meaning that this address is valid for this Layer 2 link and will not be forwarded by routers.
- Scope 5 is Site-Local scope, meaning that this address is valid for this Site / Organization and will not be forwarded outside it.
- Scope E is Global scope. This kind of IPv6 address is Globally reachable.

### 3) Common IPv6 Multicast Addresses

| | | |
|---|---|---|
| FF02::1 | All IPv6 nodes | Link Local Scope |
| FF02::2 | All IPv6 routers | |
| FF02::5 | OSPF routers | |
| FF02::6 | OSPF Designated Routers | |
| FF02::9 | RIP routers | |
| FF02::A | EIGRP Routers | |
| FF02::1:2 | DHCP Srvs/Relay agents | |

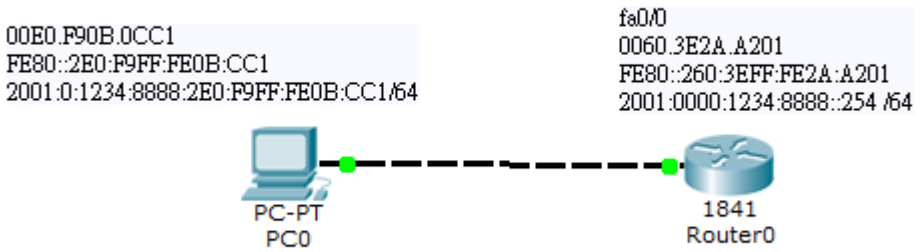
## 5) 『IPv6 Broadcast Address ???』

### 1) No more broadcast in IPv6. Multicast is used instead.

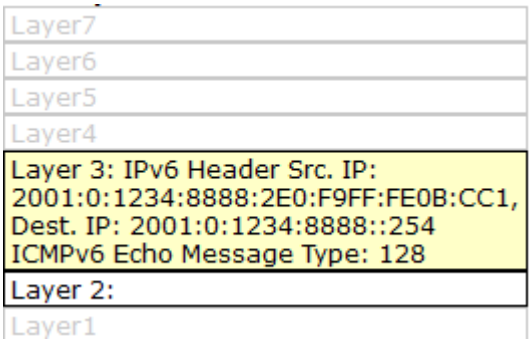
In IPv6, to reduce the impact of broadcast traffic, there is no broadcast mechanism. So, what happen to those protocols that use broadcast in the past? Well, they uses multicast instead. So, let see 1 example.

### Address Resolution Protocol ??

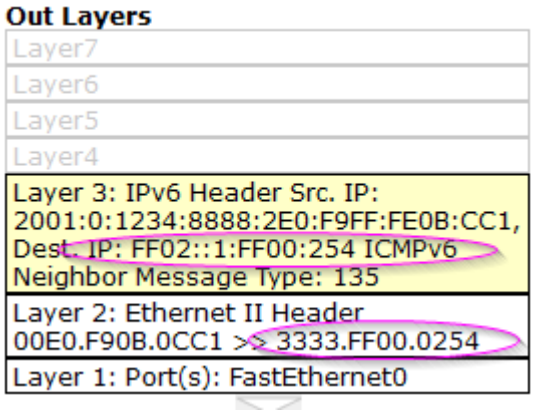
In IPv6, there is no ARP and it is replaced by a mechanism called **Neighbor Solicitation and Neighbor Advertisement.** It works like this. Let's use the Packet Tracer to see the details.



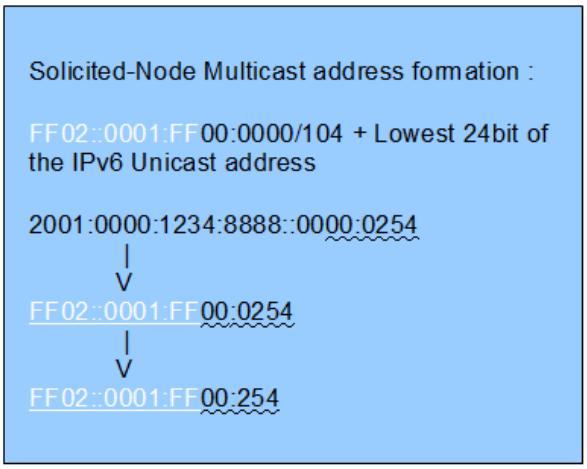
1) From PC0, we issue a ping command : ping 2001:0000:1234:8888::254 to ping Router0. PC0 drafts an ICMPv6 Echo Request packet, but cannot fill up the layer 2 information.




2) PC0 needs to resolve the MAC address of 2001:0000:1234:8888::254 first. So, it drafts an ICMPv6 packet called “Neighbor Solicitation”, with an ICMPv6 type of 135 to resolve the target’s MAC address. You will notice that the destination IP address is not a broadcast address as in ARP. It is a special multicast address: FF02::1:FF00:254. This is called the “Solicited Node Multicast address” of the target.



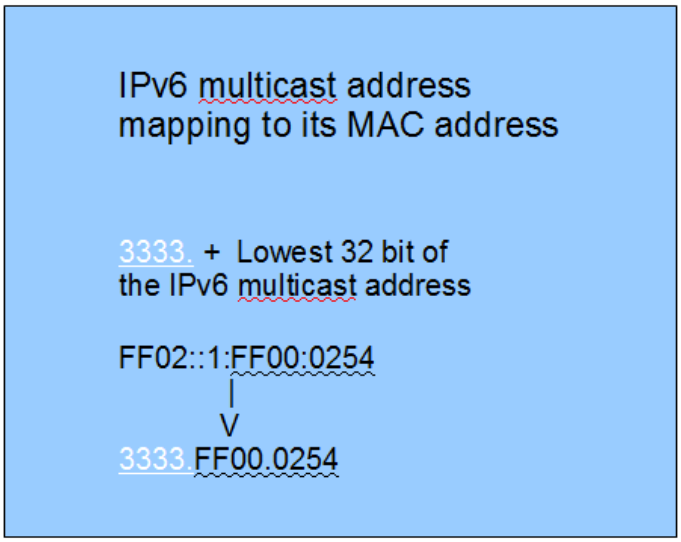

How is this “Solicited Node Multicast address” generated? Let’s see the following.



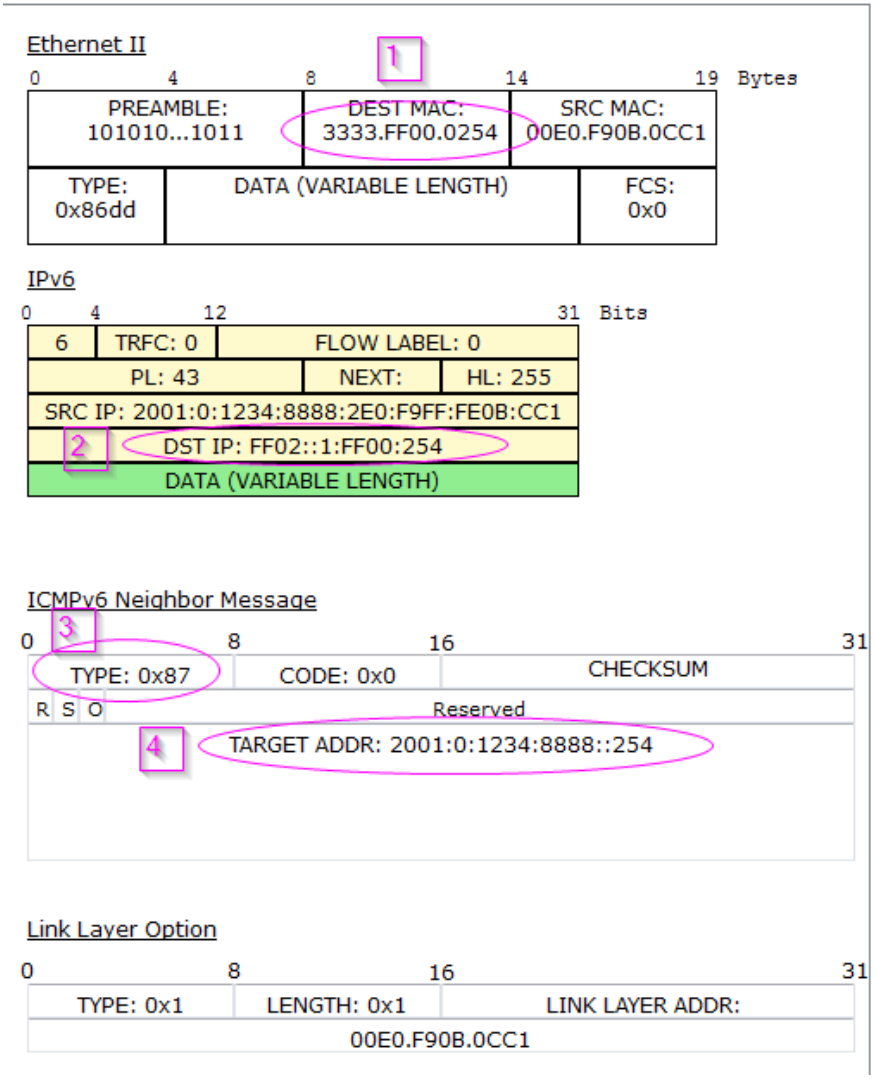

Efficiency of "Solicited Node Multicast address":

Although this is a multicast packet, in fact, basically only Router0 will receive it in this local link. Only Router0 will join the multicast group: FF02::1:FF00:254 since it will be very rare that two hosts in this local link to have their IPv6 addresses with the lowest 24 bits equal. So, this multicast traffic effectively becomes unicast traffic. If the FF02::1 Link Local All Nodes multicast address is used as the destination, this packet will disturb all the IPv6 hosts in the local link. That is why a special "Solicited Node Multicast address" is used.

On the other hand, how does the MAC address: 3333.FF00.0254 obtained? The MAC address of an IPv6 multicast address is obtained as the following:



Now, let's look into the ICMP Neighbor Solicitation Message in more details. It is trying to look up the MAC address of 2001:0:1234:8888::254.



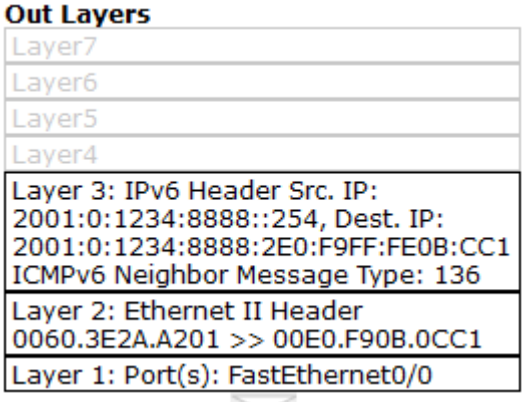

3) When Router0 receives this message, it finds that FF02::1:FF00:254 is destined to itself. Why? Every IPv6 interface will join a multicast group with an ID of "FF02::1:FF"+lowest 24bits of its IPv6 address. This is the "Solicited Node Multicast address". In this case the IPv6 address is 2001:0000:1234:8888::254. So, its "Solicited Node Multicast address" is FF02::1:FF00:254.

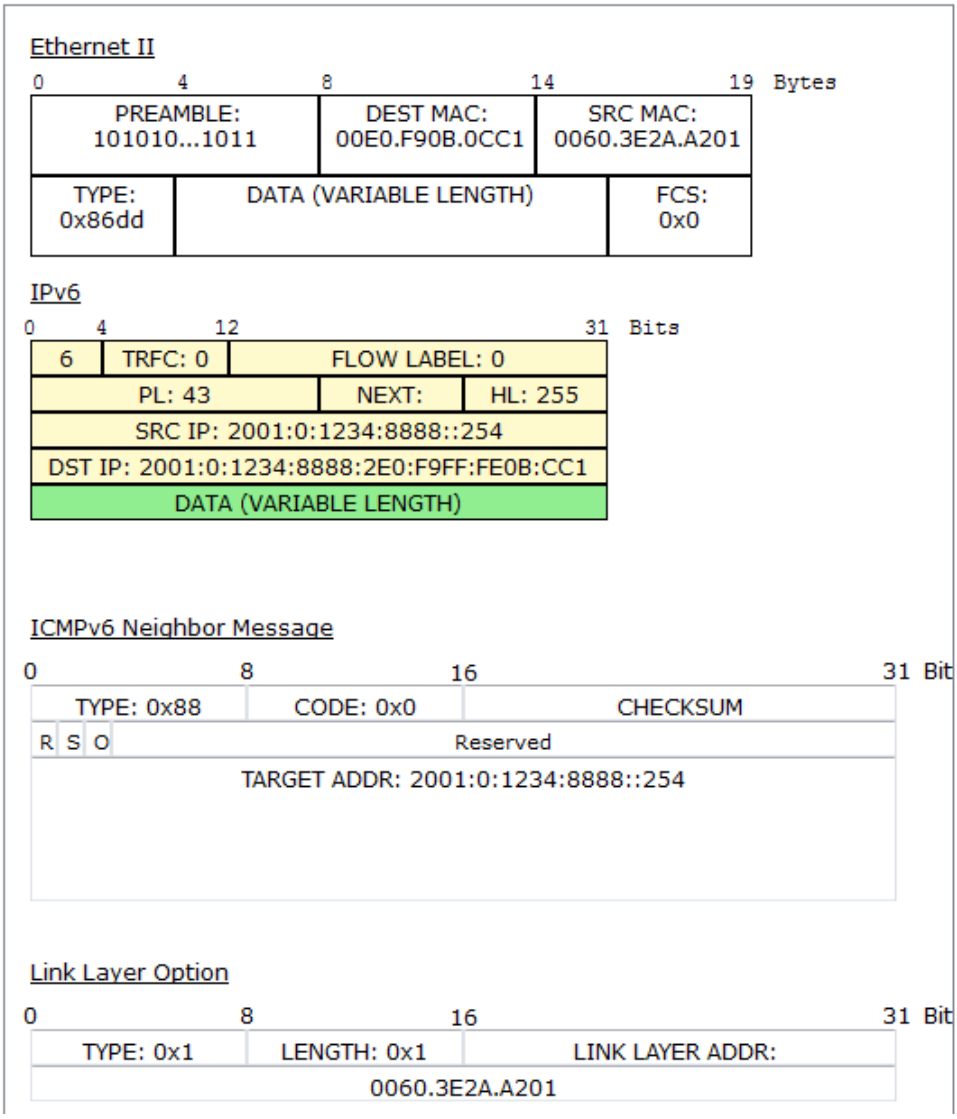
Let's see which multicast groups that fa0/0 of Router0 has joined.

```
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::260:3EFF:FE2A:A201
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:0:1234:8888::254, subnet is 2001:0:1234:8888::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:254
    FF02::1:FF2A:A201
```

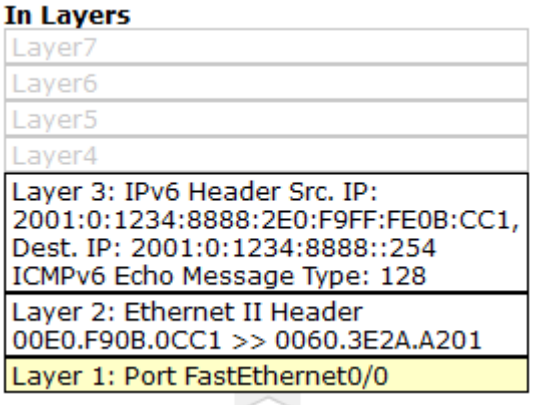
| Joined Multicast Group | Explanation |
|---|---|
| FF02::1 | Multicast group of all IPv6 nodes in link local scope. Router0 is an IPv6 host. |
| FF02::2 | Multicast group of all IPv6 routers in link local scope. Router0 is an IPv6 router. |
| FF02::1:FF00:254 | "Solicited Node Multicast address" of its Global Unicast address: 2001:0:1234:8888::254 |
| FF02::1:FF2A:A201 | "Solicited Node Multicast address" of its Link Local address : FE80::260:3EFF:FE2A:A201 |

4) Router0 replies with an ICMP Neighbor Advertisement, with an ICMPv6 type 136, to PC0, telling PC0 its MAC address. This is a unicast IPv6 packet destined to PC0.

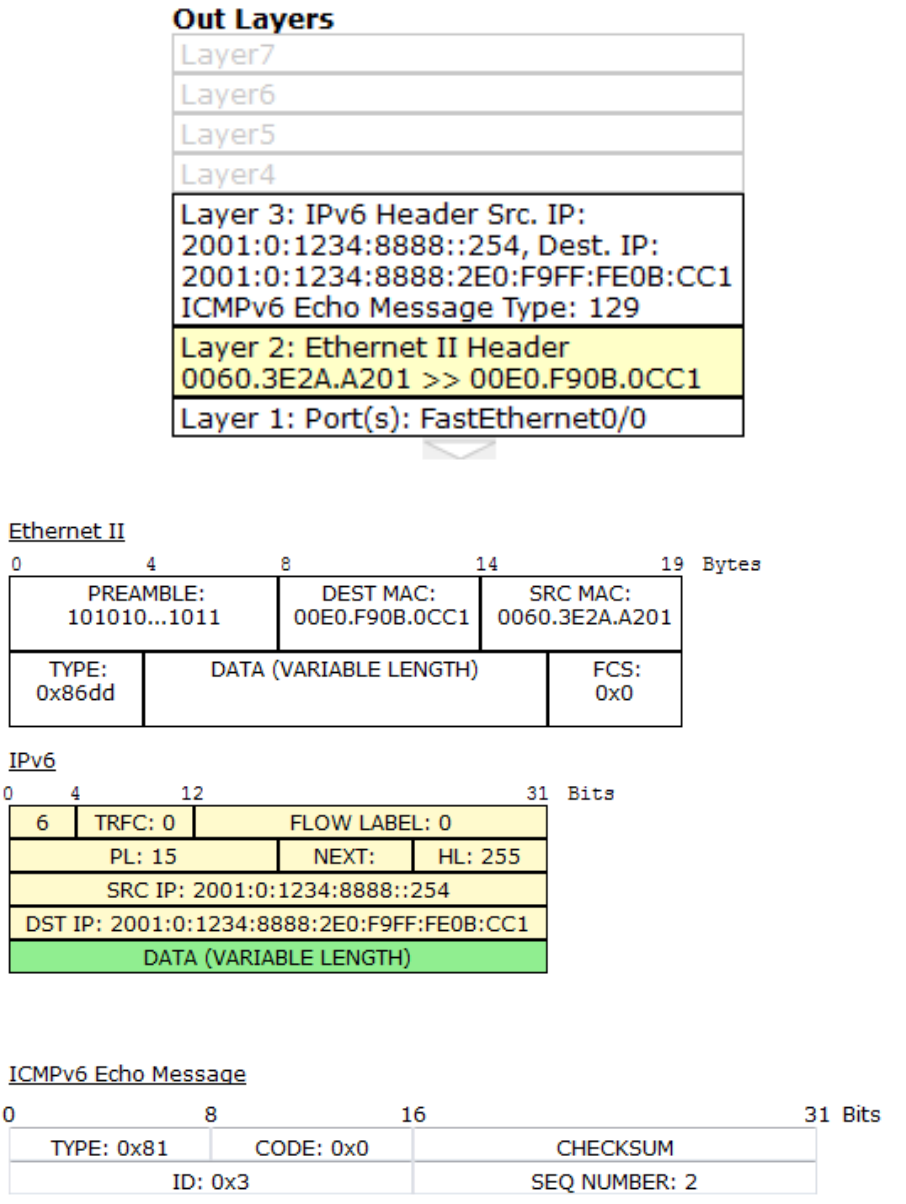





5) Now, PC0 can issue the ICMPv6 Echo request Message, ICMPv6 Type 128, with this resolved MAC address. 0060.3E2A.A201.



6) Finally, Router0 replies with a ICMPv6 Echo Reply Message, ICMPv6 Type 129 back to PC0.

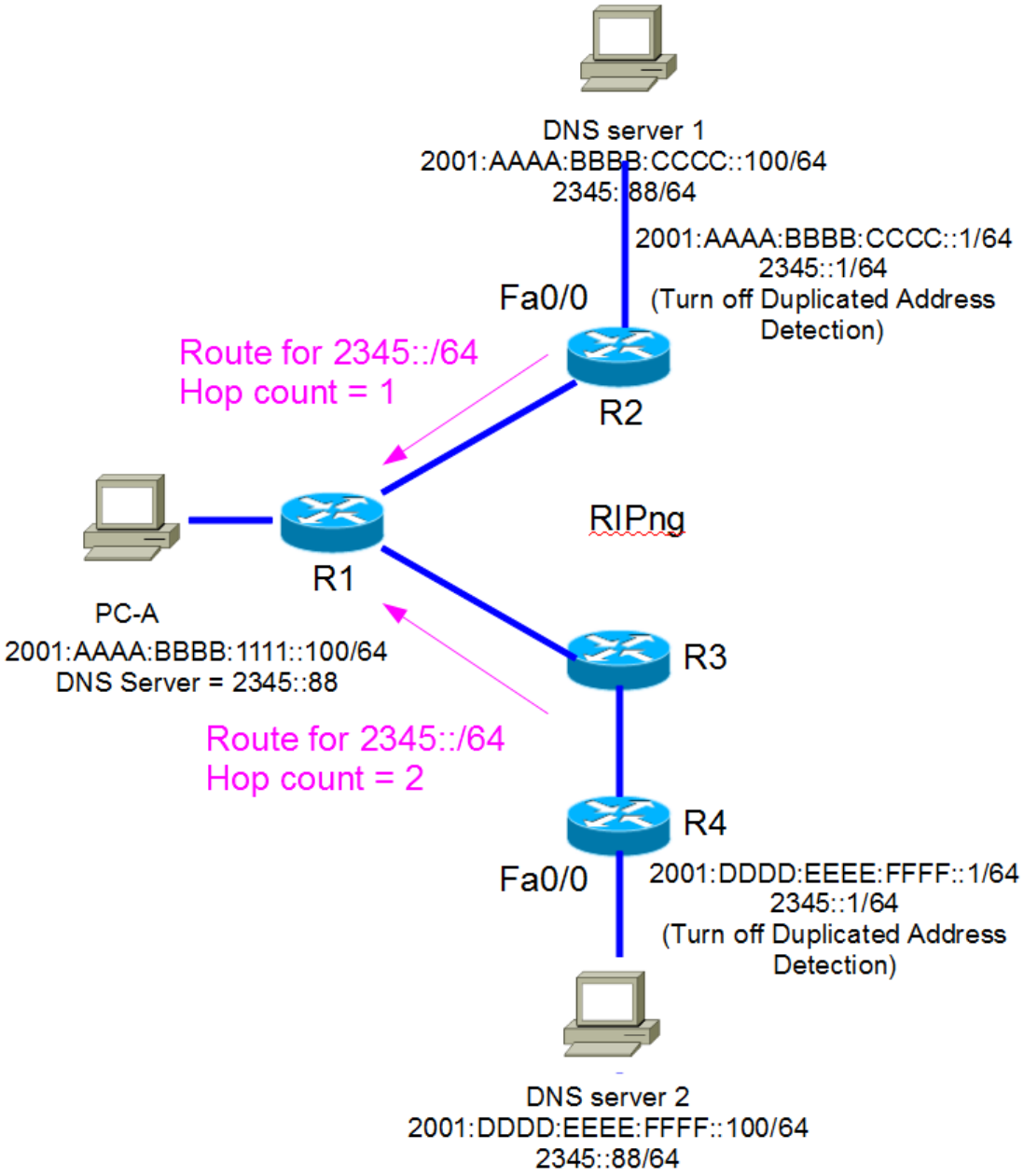



Since the “Solicited Node Multicast address” of the target rarely includes other hosts except the target, it becomes effectively unicast traffic. So, this process of Link Layer address resolution (Neighbor Solicitation and Advertisement) is more efficient that ARP in IPv4.

## 6) 『IPv6 Anycast address』

Anycast address is a new concept. It is usually used for redundancy purpose.

Let's explain the IPv6 Anycast address with the following network topology:



There are two DNS servers, DNS server 1 and DNS server 2, which serves the same sets of DNS zones. They have different IPv6 Global Unicast Addresses - 2001:DDDD:EEEE:FFFF::100/64 and 2001:AAAA:BBBB:CCCC::100/64. But, they each have an extra IPv6 Global Unicast address which is the same: 2345::88/64.

DNS server 1 is connected to Fa0/0 of R2. Fa0/0 of R2 has two IPv6 addresses configured, which corresponds to the 2 different network IDs.
DNS server 2 is connected to Fa0/0 of R4. Fa0/0 of R4 has two IPv6 addresses configured, which corresponds to the 2 different network IDs.
This seems to have duplicated IPv6 addresses in this network. Yes, so, we need to turn off Duplicated Address Detection in R2 and R4 and then it is OK in IPv6.

All the routers run RIPng, so, R1 will receive 2 routes for the network 2345::/64 with different hop count. Of course, in normal situation, the route for 2345::/64 on R1 will direct to R2.

PC-A is configured to use a DNS server of 2345::88. In normal cases, the DNS requests will be forwarded via R1 – R2 and then to DNS server 1. It will process the request and then response.

But, if R2 has some problems and becomes unreachable. R1 will replace the route for 2345::/64 via R3. If now PC-A sends out DNS requests, they will be forwarded via R1 – R3 – R4 and then to DNS server 2.

By this means, redundancy on DNS server is achieved and the IPv6 address : 2345::88 is said to be an IPv6 Anycast address. This mechanism works only with the help of the routers and routing protocols.

IPv6 Anycast addresses share the same range of IPv6 Global Unicast addresses and there is no way to distinguish if an IPv6 address is Anycast or not by just looking at the IPv6 address.

## 7) 『Finally words』

Not all kinds of IPv6 addresses are covered here. Some of them are depreciated and some of them are not very common.
This tutorial helps students to understand IPv6 addressing in a easy-to-understand, step-by-step way.
Hoping this tutorial can help you.

Until next time… …