TELCOMA
AN ISO CERTIFIED COMPANY

Internet Protocol version 6

Full course at
https://telcomaglobal.com

TELCOMA

Brief Introduction To IPv4

Content:

1. IPv4
    - Address type
    - Notations
    - IPv4 Packet Format
2. Network Address Translation (NAT)

IPv4:

Internet Protocol Version 4 (IPv4) is the fourth version of the IP address.

It is a connectionless protocol used in packet-switched networks, such as Internet.

It provides the logical connection between network devices by providing identification to each device.

IPv4 is designed and specified in IETF publication RFC 791.

IPv4:

Address Type:

Address Space is the total number of addresses used by the protocol.

IPv4 is a 32 bit address which means it consist of 2^32 (i.e. 4,294,967,296) address space

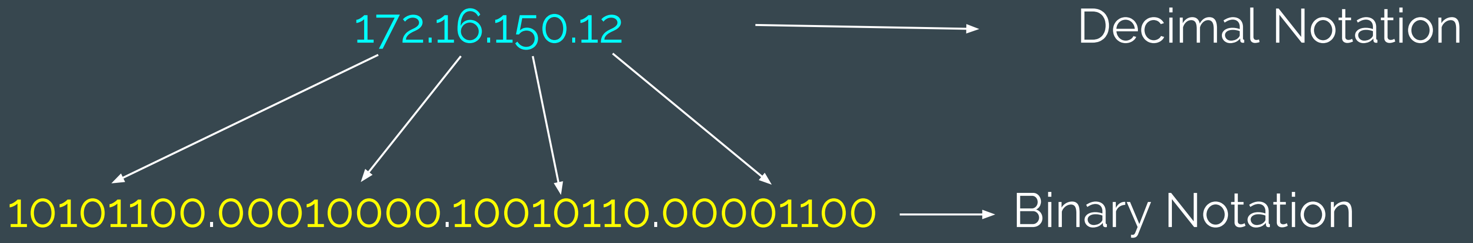
Example: 117.149.29.2 is an IPv4 address

It means 4 billion device can be connected to internet.

IPv4:

Notation: IPv4 address can be represented in two way:

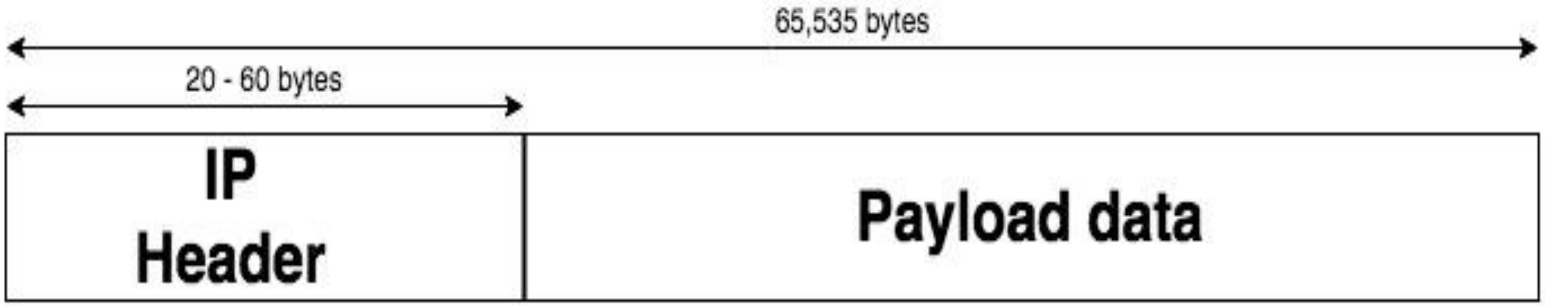
- **Binary Notation**: IPv4 is a 32 bit address in which there are 4 octet each having the bytes.
- **Dotted Decimal Notation**: Each number in dotted decimal notation value ranges from 0 to 255.



172.16.150.12 → Decimal Notation

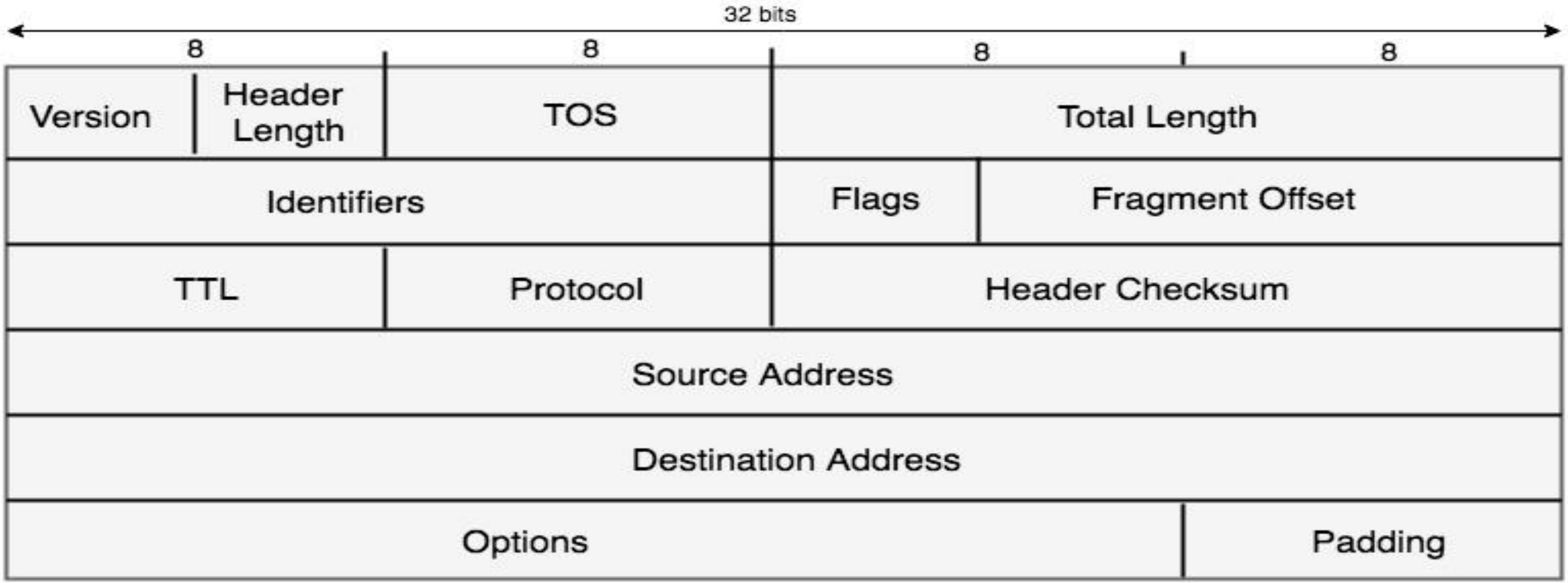
10101100.00010000.10010110.00001100 → Binary Notation

IPv4:



IPv4 Packet Format

IPv4 Header:



Version	Header Length	TOS	Total Length
Identifiers		Flags	Fragment Offset
TTL		Protocol	Header Checksum
Source Address			
Destination Address			
Options			Padding

IPv4 Packet Format

IPv4:

IPv4 Packet Format:

- **Version**:- The four-bit field is set to binary 0100 for IPv4 or binary 0110 for IPv6.
- **Header length:-** It tells the number of 32-bit words in the header.
- **Type of Service(ToS):–** used to carry information about quality of service.
- **Total Length:-** define length of entire IP address.
- **Explicit Congestion Notification (ECN):-** carries information about the congestion seen in the route.

IPv4:

- **Identifiers:–** The identification field is used for uniquely identifying fragments of an original IP datagram.
- **Fragment Offset:-**The fragment offset field is 13 bits long
- **Protocol:-** indicate the protocol used in the data portion of the IP datagram.
- **Header Checksum:-** used for error-checking of the header (16 bit).
- **Source address :-** indicate the IP address of source of packet.
- **Destination address :-** indicates the IP address of receiver of the packet.

IPv4:

- **Flags:–** A 3 bits field is used to control and identify fragments. They are
    - bit 0: Reserved; must be zero.
    - bit 1: Don’t Fragment (DF)
    - bit 2: More Fragments (MF)
- **Time To Live (TTL):-** indicates the maximum time for which a datagram is allowed to remain in the internet system.
- **Options:-** This is an optional field reserved for future use.

IPv4:

Network Address Translation:

NAT stands for Network Address Translation or Network Address Translator.

Network Address Translation is the process where a network device (like firewall) assigns a public address to a computer inside a private network.

In NAT, the private address range is used i.e. 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.

IPv4:

Network Address Translation:

NAT technique works well for computers that only have to access resources inside the network, for example host want to access file servers and printers.

Thus using private address routers inside the private network can route traffic between private addresses with no trouble.

If a host want to access resources outside the network from Internet, then the host must contain public IP address.

In this way (NAT) Network Address Translation works.

IPv4:

Network Address Translation (NAT)

Introduction To IPv6

Content:

1. IPv6
   - Features of IPv6
   - Why we need IPv6 IP address?
   - Advantages

IPv6:

It is a network layer protocol that provides an identification and location of computers on networks and routes the traffic across the Internet.

IPv6 is introduced by the Internet Engineering Task Force (IETF) in 1998.

It was introduced to replace the widely used IPv4 addresses that is considered as the backbone of the modern Internet.

In 2004, Japan and Korea were first in public deployments of IPv6.

IPv6:

Features of IPv6:

- Support 128 bit long source and destination addresses.
- Simplified address header by moving all unnecessary information.
- Provide end to end connectivity
- Faster forwarding/routing due to less detail at header.
- It have IPSec security,which make it more secure than IPv4.
- Use multicast to communicate with multiple hosts (Does not support broadcast)

IPv6:

Features of IPv6:

- Anycast mode for packet routing is introduced.
- It enables hosts to roam in different geographical area and remain connected with the same IP address.
- It use 6 bits DSCP and 2 bits ECN to provide better Quality of Service
- Support smooth transition

IPv6:

Why we need IPv6 IP address?

To make communication possible every device which is connected to internet gets a unique number known as an IP address.

Internet addressing system IPv4, has capacity for about 4.2 billion addresses.

The problem arise with the increase in number of new devices like computers, smartphones, TVs, smart watches, cars etc these addresses are not enough to meet the demand of new devices.

IPv6:

Why we need IPv6 IP address?

Thus, there a shortage of IPv4 addresses occur.

So many methods were adopted to prevent the depletion of IPv4, like Subnetting, VLSM and NAT etc these methods were no longer able to provide IP address to networks for future demands.

IPv6:

<u>Why we need IPv6 IP address?</u>

IPv4 is of 32 bits address, it can provide 2^32 IP addresses.
2^32 = 4294967296
= 4.2 billion

To overcome this limitation IPv6 Addresses are introduced:

IPv6 is of 128 bits which is 4 times of the IPv4 in bits size.
2^128 = 340,282,366,920,938,463,463,374,607,431,768,211,456
Total IP addresses = 340 trillion
Thus, this is the reason with the deployment of IPv6 address.

IPv6:

Advantages:

1. Larger address space
2. Better header format
3. New additional options
4. Allowance for extension
5. More security

IPv6
Protocol Structure

Content:

1. IPv6
    - Address Structure
    - Rules for Address notation
    - Packet format

IPv6:

Structure:

An IPv6 address is of 128 bits long

It is divided into eight 16-bits blocks.

Each block is then converted into 4-digit.

it is represented by Hexadecimal numbers separated by colon symbols.

IPv6 addressing structure is designed in RFC 4291.

IPv6:

Structure:

For example:

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

IPv6:

Structure:

Some rules to shorten the IPv6 address:

Rule.1: Discard leading Zero(es):

Leading zeros of a section can be omitted ,only leading 0s can be dropped not trailing 0s, such as in block 5

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

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

IPv6:

Structure:

Rule 2: Replace consecutive zeros

If two or more blocks contain consecutive zeros, omit them all and replace it with double colon sign “::” such as in 6th and 7th block

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

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

IPv6:

Structure:

Rule 2:

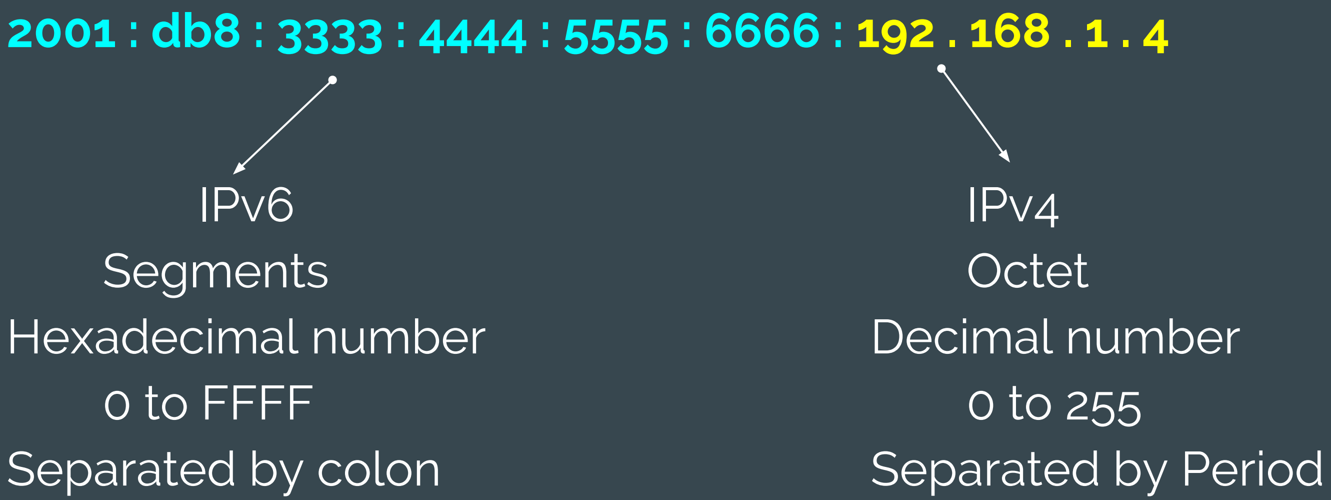
Consecutive blocks of zeroes can be replaced only once,if there are still blocks of zeroes in the address, they can be replaced by single zero, such as in 2nd block

2001 : 0000 : 3238 : DFE1 : 63 : : FEFB
2001 : 0 : 3238 : DFE1 : 63 : : FEFB

IPv6:

Representing IPv6 and IPv4 addresses together:

Format: y:y:y:y:y:y:x.x.x.x



2001 : db8 : 3333 : 4444 : 5555 : 6666 : 192 . 168 . 1 . 4

IPv6
Segments
Hexadecimal number
0 to FFFF
Separated by colon

IPv4
Octet
Decimal number
0 to 255
Separated by Period

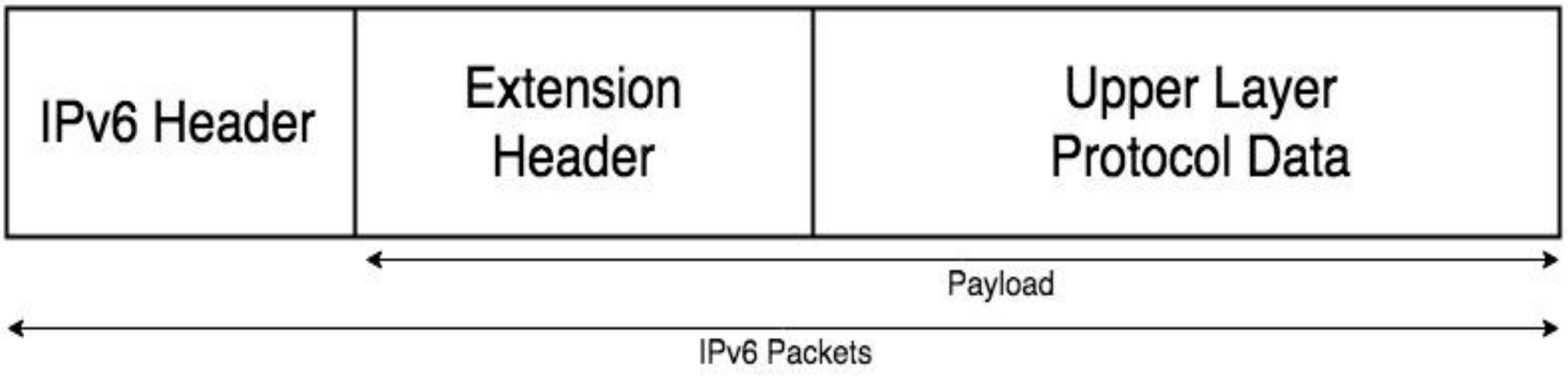
IPv6:

Representing IPv6 and IPv4 addresses together:

IP address: 192 . 168 . 0 . 2 can be represented as x : x : x : x : x : x : 192 . 168 . 0 . 2

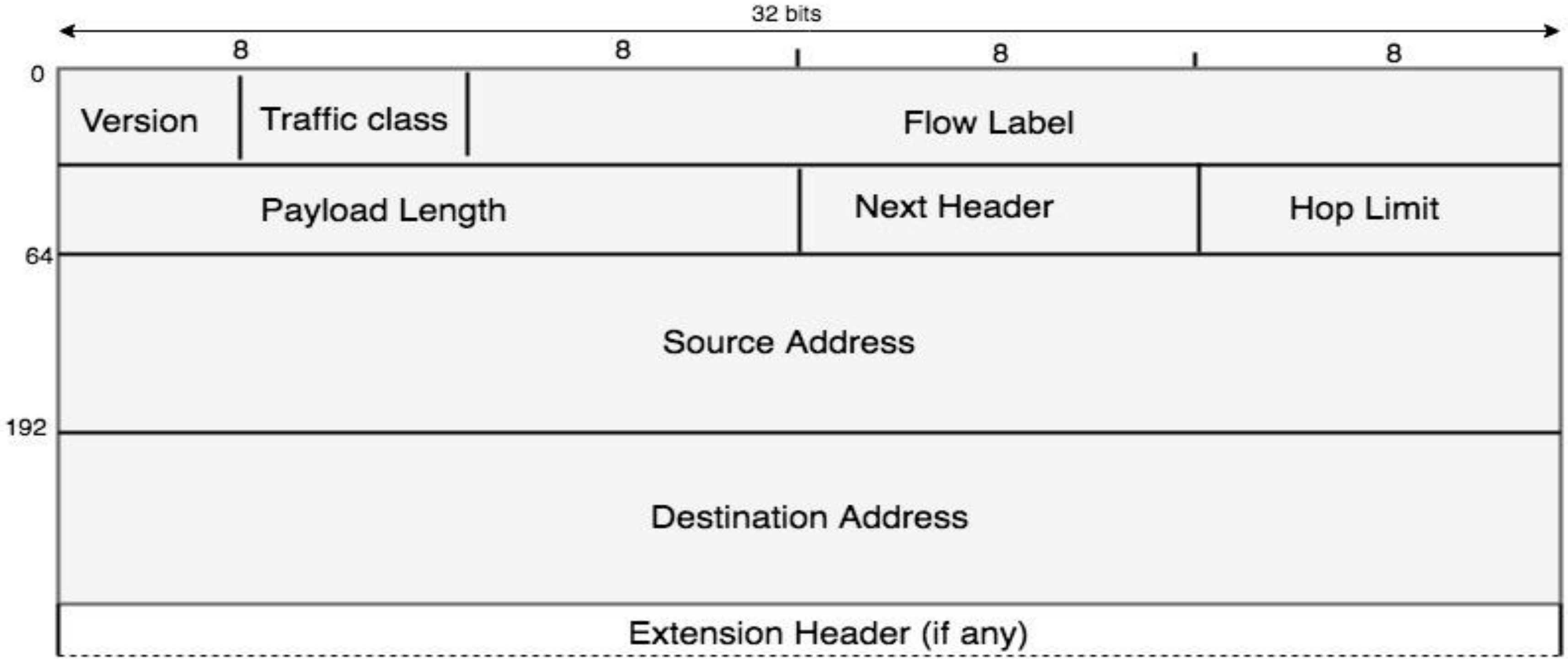
1. Method 1 --- 0 : 0 : 0 : 0 : 0 : 0 : 192 . 168 . 0 . 2
2. Method 2 --- : : 192 . 168 . 0 . 2
3. Method 3 --- : : c0a8 : 2 (Hexadecimal representation)

Structure of IPv6 Packets:



IPv6 Packet Structure

Structure of IPv6 Packets:



32 bits

8 8 8 8

0 Version | Traffic class | Flow Label

Payload Length | Next Header | Hop Limit

64 Source Address

192 Destination Address

Extension Header (if any)

IPv6 Packet Format

IPv6:

IPv6 Packet format:

- **Version:** 4 bit long and remain constant i.e 6 or bit sequence 0110.
- **Traffic Class:** 8 bit long. This field hold two values i.e DS and ECN.
- **Flow Label:** used for giving real-time applications service and also help to detect spoofed packets (20 bit).
- **Payload Length:** When a Hop-by-Hop extension header holds a Jumbo Payload option then the length is set to zero (16 bit).

IPv6:

IPv6 Packet format:

- **Next Header:** specifies the type of the next header (8 bit)
- **Hop Limit:** specifies how many number of devices can be visited by packet. This field replace the time to live field of IPv4. (8 bit)
- **Source Address:** indicate the IP address of source node. (128 bit)
- **Destination Address:** indicate the IP address of destination node. (128 bit)

IPv6
Extension Header
&
Prefix Notation

Content:

1. Extension headers
2. IPv6 Prefix notation

IPv6:

Extension Header:

It is added with a base header.

These are the extension header:

- Hop-by-Hop option
- Source Routing
- Fragmentation
- Authentication
- Encapsulating security payload
- Destination option

IPv6:

Extension Header:

- **Hop-by-Hop option:**

  It is used when the source needs to pass information to all routers visited by the datagram.

- **Destination Option:**

  used to specify packet delivery parameters for either intermediate nodes or the final destination.

IPv6:

Extension Header:

- **Source Routing**:

  specify a source route, which is consist of intermediate nodes travel by packet on its path to the final destination.

- **Fragmentation:**

  Used for fragmentation and reassembling of packet.

IPv6:

Extension Header:

- **Authentication:**

  Authentication extension header contains information used to verify the authenticity of the packet.

- **Encapsulating Security Payload:**

  It contain the information used to verify the confidentiality of the packet.

IPV6:

Prefix Notation:

The prefix-length is a decimal value indicating the number of leftmost contiguous bits of the address.

Example: 2001 : db8 : abcd : 0012 : : 0/64 specifies a subnet with a range of IP addresses from

2001 : db8 : abcd : 0012 : 0000 : 0000 : 0000 : 0000 to

2001 : db8 : abcd : 0012 : ffff : ffff : ffff : ffff

It is represented by using the following format: *IPv6 addresses/Prefix length*

IPV6:

Prefix Notation:

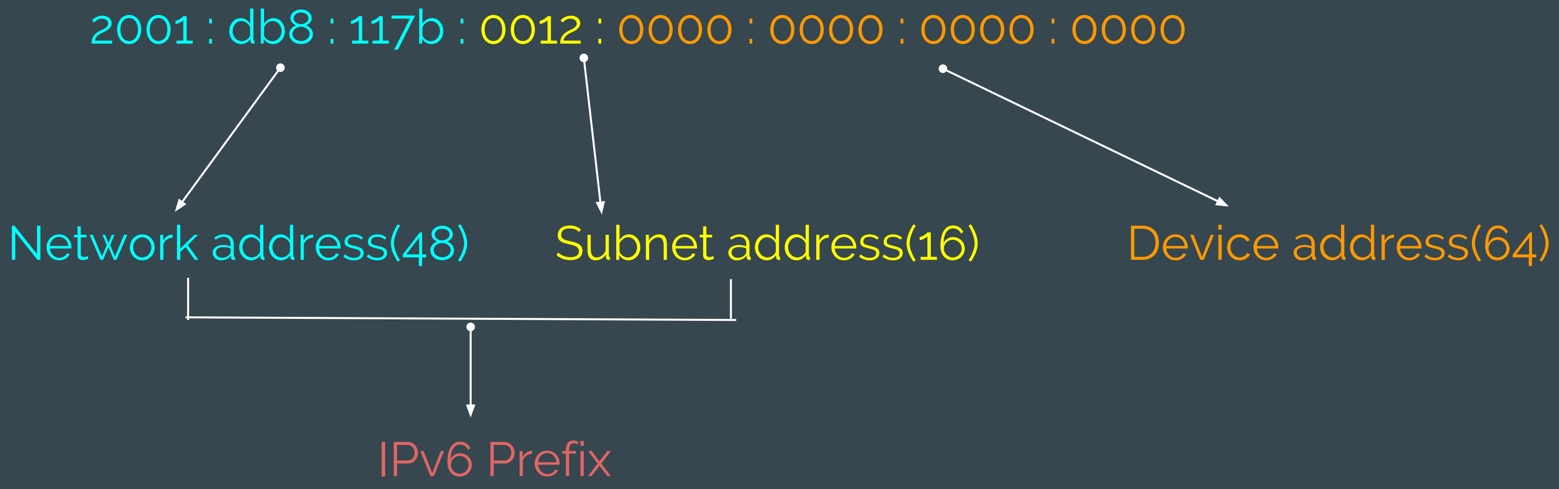
An IPv6 address consist of:

- **Network address** - the first three groupings of numbers in the subnet mask
- **Subnet address** - the fourth grouping of numbers in the subnet mask
- **Device address** - the last four groupings of numbers in the subnet mask

IPV6:

Prefix Notation:

For example,



2001 : db8 : 117b : 0012 : 0000 : 0000 : 0000 : 0000

Network address(48)

Subnet address(16)

Device address(64)

IPv6 Prefix

IPv4 vs IPv6

Content:

1. Comparison of IPv4 and IPv6
2. IPv4 and IPv6 Header

Comparison of IPv4 & IPv6:

IPv4

1. Address length = 32 bits (4 bytes)
2. Header include a checksum and options
3. Fragmentation is performed by routers and sending hosts.
4. IGMP is used to manage local subnet group level.

IPv6

1. Address Length = 128 bits (16 bytes)
2. Checksum is not included in header and optional data is moved to extension header
3. Fragmentation is only done by sending hosts.
4. IGMP is replaced with multicast listener discovery (MLD) messages.

Comparison of IPv4 & IPv6:

IPv4

5. Configured manually or through DHCP
6. Support 576 byte packet size (fragmented)
7. IPsec support is optional
8. ICMP Router Discovery is used

IPv6

5. Doesn,t not require manual configuration or DHCP
6. Support 1280 bytes of packet size (not fragmented)
7. End to end IPsec support is necessary.
8. ICMPv6 Router solicitation and Router advertisement messages are used

IPv4 & IPv6 Header:

IPv4	IPv6
1. Version (0100)	1. Version (0110)
2. Internet Header Length	2. Not present (fixed size 40 bytes)
3. Type of Service	3. Replaced as IPv6 Traffic Class field.
4. Total Length	4. Replaced by the IPv6 Payload Length field
5. Identification	5. Removed in IPv6.
6. Options	6. Removed in IPv6. Add in extension header.

IPv4 & IPv6 Header:

IPv4	IPv6
6. Fragmentation Flags, Fragment Offset	6. Not included (contained in a Fragment extension header)
7. Time to Live	7. Replaced by the IPv6 Hop Limit field.
8. Protocol	8. Replaced by the IPv6 Next Header field.
9. Header Checksum	9. Removed in IPv6.
10. Source Address (32 bits)	10. Source Address (128 bits)
11. Destination Address (32 bits)	11. Destination Address (128 bits)

IPv6
Address Type

Content:

1. IPv6 Address Type

Type of IPv6 address:

The type of network communication in IPv6 are:

1. Unicast Address
2. Multicast Address
3. Anycast Address

Note: IPv6 doesn’t use broadcast address.

Type of IPv6 address:

1. **Unicast Address:**

   Unicast is a type of communication where data is sent from one computer to another computer in a network.

   A unicast address uniquely identifies an interface of an IPv6 node.

   Example for IPv6 Unicast type of network communication: Browsing a website , Downloading a file from a FTP Server etc

Type of IPv6 address:

2. **<u>Multicast Address:</u>**

Multicast is a type of communication where data is send to a group of devices in the network.

A multicast address identifies a group of IPv6 interfaces.

IPv6 multicast data is sent to a group and only members of that group receive the Multicast data.

For example: Online TV

Type of IPv6 address:

3. **Anycast Address:**

   An anycast address is assigned to multiple interfaces.

   In Anycast the packets are routed to the nearest device or interface from a group.

   For example: used in content delivery network (CDN)

IPv6
Unicast Address

Content:

1. Unicast Address Type
2. Address Scope

IPv6 Unicast address:

Type of IPv6 unicast addresses:

1. Global unicast Address
2. Link Local address
3. Unique local address
4. Special address
5. Embedded IPv4

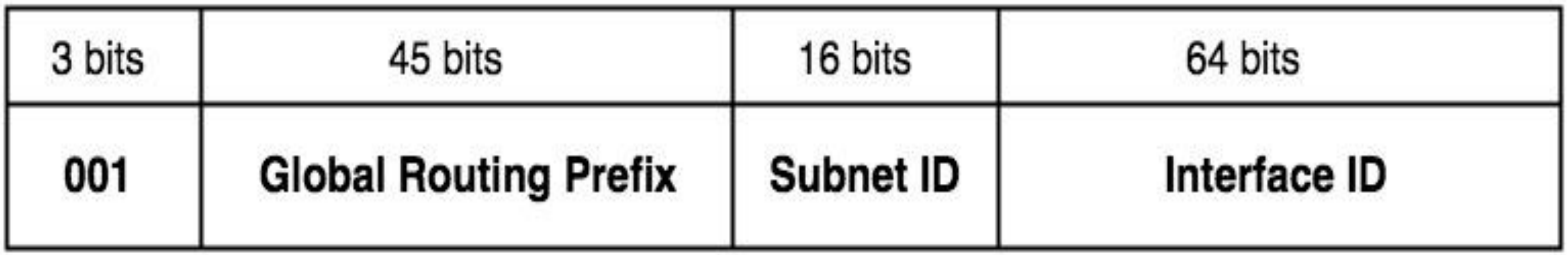
IPv6 Global unicast address:

1. **Global Unicast address:**
   - Similar to IPv4 public IP addresses
   - Assigned by the IANA and used on public networks
   - have a prefix of 2000::/3 (binary 001)

A global IPv6 address consists of two parts:

- Subnet ID – Contains the site prefix and the subnet ID (64 bit)
- Interface ID – Contain the part of MAC address of the interface (64 bit)

IPv6 Global Unicast address:

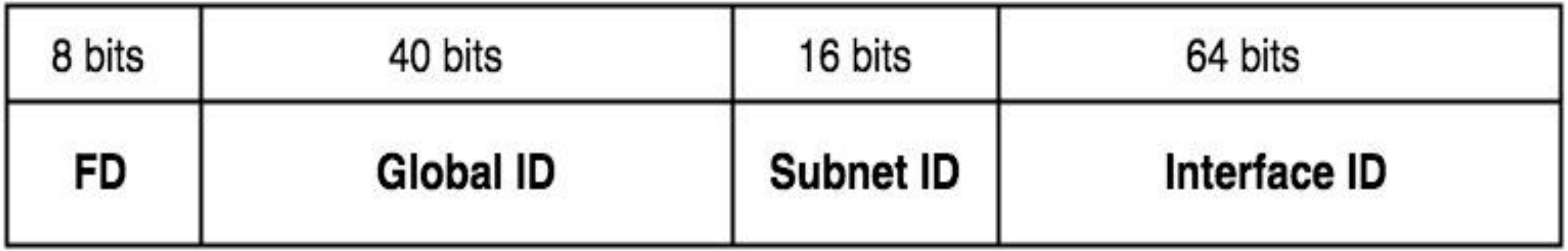


3 bits	45 bits	16 bits	64 bits
001	Global Routing Prefix	Subnet ID	Interface ID

IPV6 Unique local unicast address:

2. **Unique local address**:
   - similar to IPv4 private addresses
   - Globally unique addresses
   - used in private networks such as within corporate site
   - Are not routable on the Internet
   - Configured through DHCPv6
   - have a prefix of FD00 : : / 8

IPv6 Unique local unicast address:

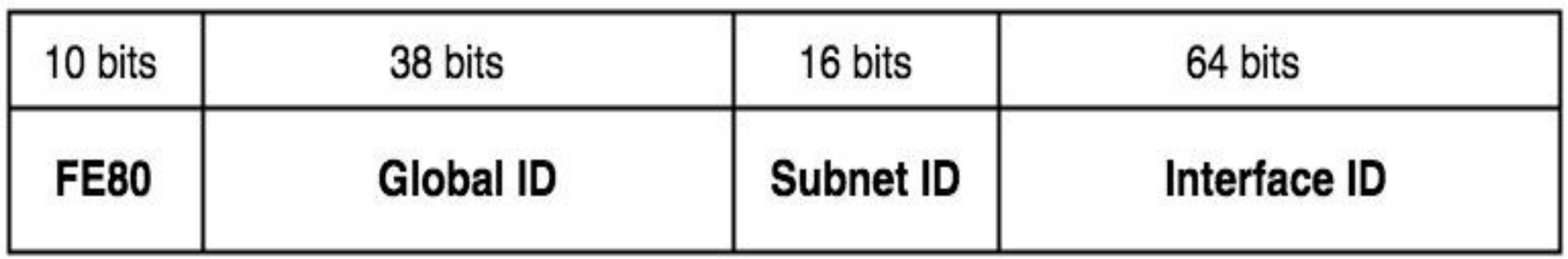


8 bits	40 bits	16 bits	64 bits
FD	Global ID	Subnet ID	Interface ID

IPV6 link local unicast address:

3. **link local address**:
   - Have small scope i.e. only within a network segment
   - Router will not forward packet to another network
   - Configured automatically and manually
   - used for auto-address configuration and neighbour discovery.
   - have a prefix of FE80 : : / 10

IPv6 link local unicast address:



10 bits	38 bits	16 bits	64 bits
FE80	**Global ID**	**Subnet ID**	**Interface ID**

IPv6 Embedded IPv4 Unicast address:

IPv6 transition mechanisms include a technique for device and routers to tunnel IPv6 packets dynamically under IPv4 routing infrastructure.

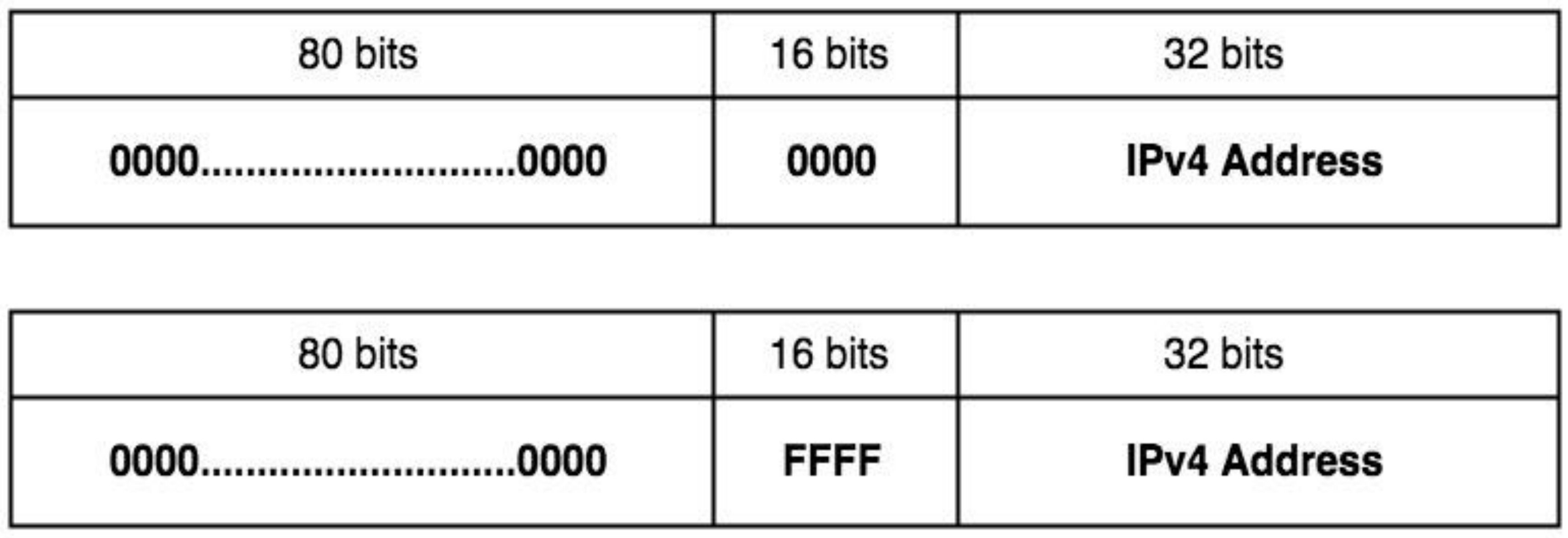
- IPv4-compatible IPv6 address:

  IPv6 nodes are assigned with special IPv6 unicast addresses that carry an IPv4 address in the low-order 32 bits.

- IPv4-mapped IPv6 address:

  used to represent an IPv4 address within the IPv6 address space.
  mainly used internally within the implementation of applications, APIs, and the operating system.

IPv6 Embedded IPv4 Unicast address:



80 bits	16 bits	32 bits
0000............................0000	**0000**	**IPv4 Address**

80 bits	16 bits	32 bits
0000............................0000	**FFFF**	**IPv4 Address**

IPv6 Special Unicast address:

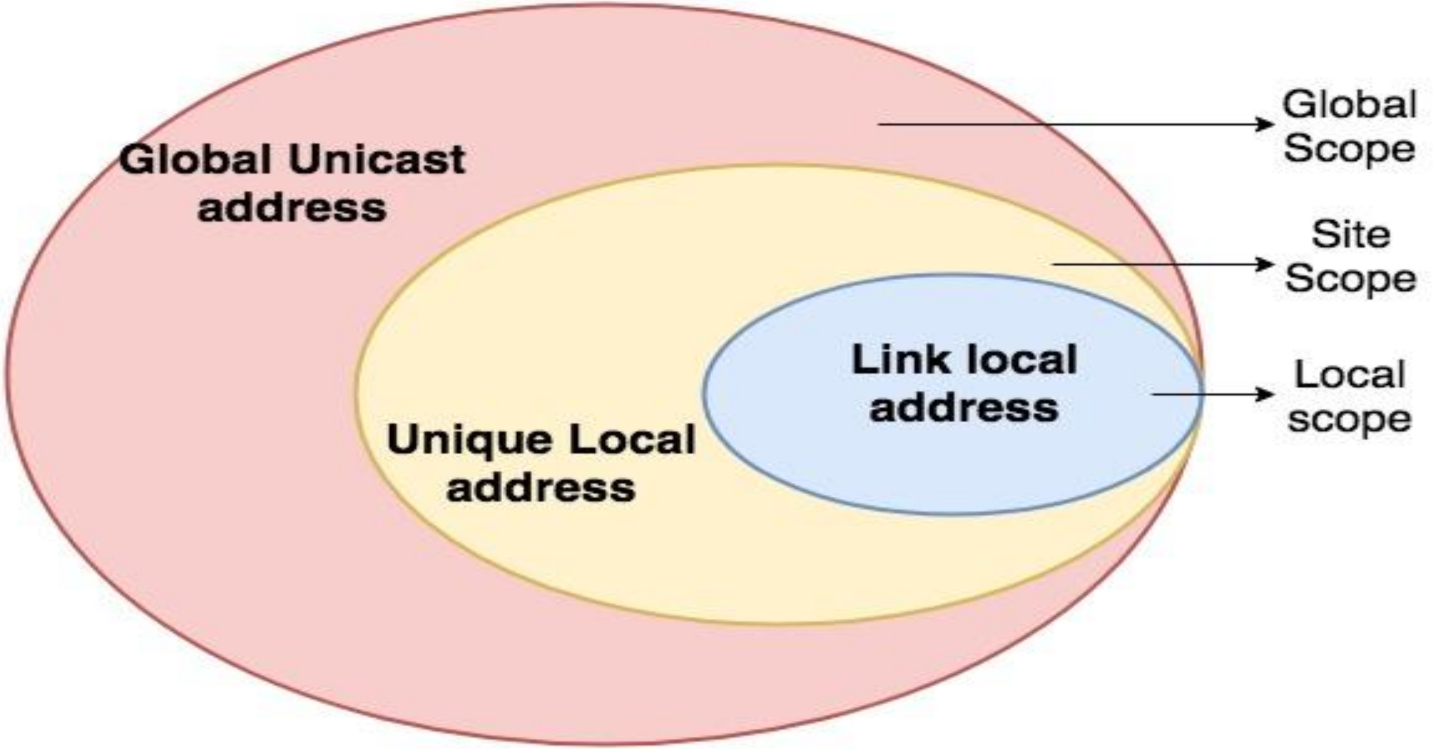
Loopback Unicast address:

- Used by a node to send an IPv6 packet to itself.
- same as an IPv4 loopback address.
- Format 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001 / 128 represented as : : 1

Unspecified Unicast address:

- represented by 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 or : :
- Indicate absence of address

IPv6 Address Scope:



IPv6
Other Address

Content:

1. 6 to 4 Address
2. 6rd Address
3. ISATAP Address
4. Teredo Address

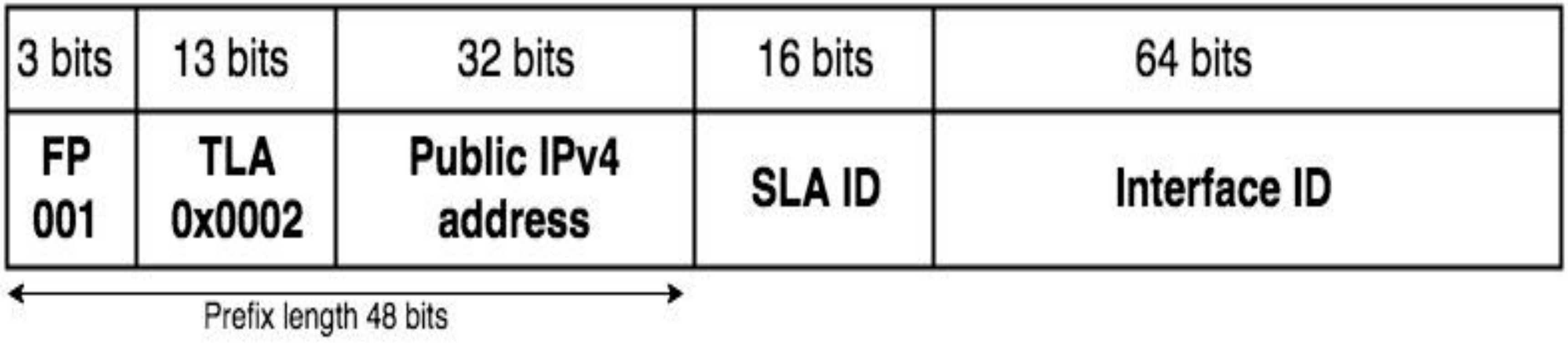
6 to 4 Address:

6to4 is defined to make IPv6 devices or networks communication possible over an IPv4 infrastructure.

IANA has permanently assigned a 13-bit TLA identifier for 6to4 operations within the global unicast address range (001).

- TLA identifier is 0x0002.
- Interface for 6to4 with an IPv4 address of 62 . 2 . 84 . 115, convert it into hexadecimal, the 6to4 prefix will become 2002 : 3e02 : 5473 : : / 48.

6 to 4 Address:



3 bits	13 bits	32 bits	16 bits	64 bits
FP 001	TLA 0x0002	Public IPv4 address	SLA ID	Interface ID

Prefix length 48 bits

6rd Address:

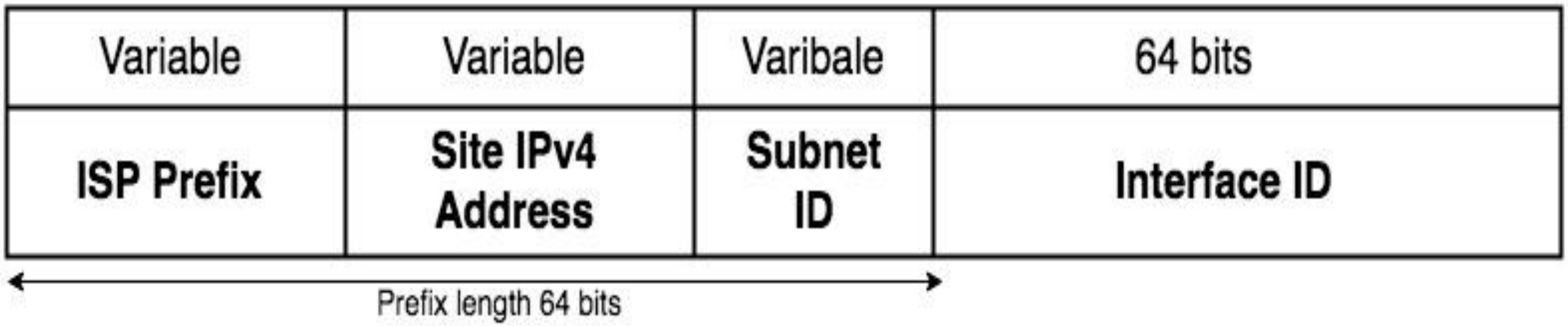
6rd known as IPv6 Rapid Deployment published in 2010

Not have specific prefix

Also not have a fixed boundary

Prefix total length 64 bits (ISP prefix and the site IPv4 address of variable length)

6rd Address:



Variable	Variable	Varibale	64 bits
ISP Prefix	**Site IPv4 Address**	**Subnet ID**	**Interface ID**

Prefix length 64 bits

ISATAP Address:

ISATAP : Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

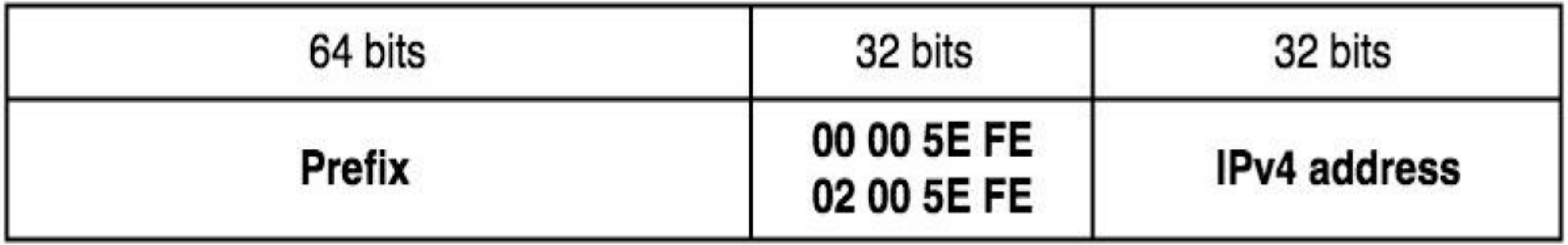
- Automatic tunneling mechanism specified in RFC 5214.
- Designed for dual-stack nodes that are separated by an IPv4 structure
- type identifier : 0xFE
- Type identifier specify an IPv6 address with an embedded IPv4 address

ISATAP Address:

- 64 bits - having same format as global unicast address.
- 32 bits - specifies the EUI-48 format i.e 00-00-5E.
- From 32 first 16 bits of type identifier - Private IPv4 address (0000)
  - Public IPv4 address (0200)
- 8 bit - type identifiers 0xFE - indicate the IPv6 address within embedded IPv4 address
- 32 bit - embedded IPv4 address (decimal or hexadecimal notation)

Example : ISATAP address 2001 : db8 : 510 : 200 : 0 : 5efe : 192 . 168 . 0 . 1

ISATAP Address:



64 bits	32 bits	32 bits
Prefix	**00 00 5E FE** **02 00 5E FE**	**IPv4 address**

Teredo Address:

Teredo is designed to avail IPv6 connectivity to hosts that are present in one or more NATs.

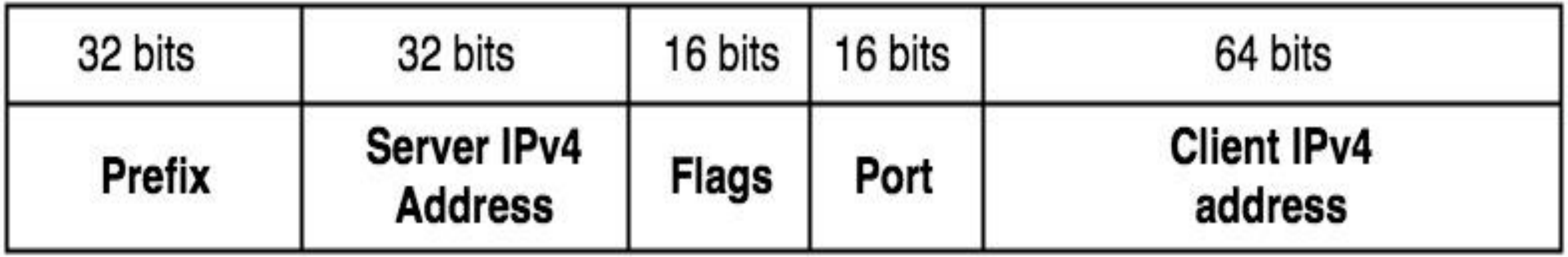
This is done by tunneling the IPv6 packet within UDP.

This method consists of Teredo clients, servers, and relays.

Teredo Address:

- 32 bits - Prefix length (2001 : 0000 : / 32)
- 32 bits - contains the IPv4 address of a Teredo server.
- 16 bits - specifies the type of address and NAT in use.
- 16 bits - Port field contains the mapped UDP port of the Teredo service on the client
- 64 bits - Client IPv4 address field contains the mapped IPv4 address of the client.

Teredo Address:



32 bits	32 bits	16 bits	16 bits	64 bits
Prefix	Server IPv4 Address	Flags	Port	Client IPv4 address

IPv6 Multicast Address

Content:

1. Multicast Address
2. Address format
3. Solicited node multicast address
4. Well known multicast address

IPv6 Multicast address:

An IPv6 multicast address defines a group of devices known as a multicast group.

- Prefix for IPv6 multicast addresses:

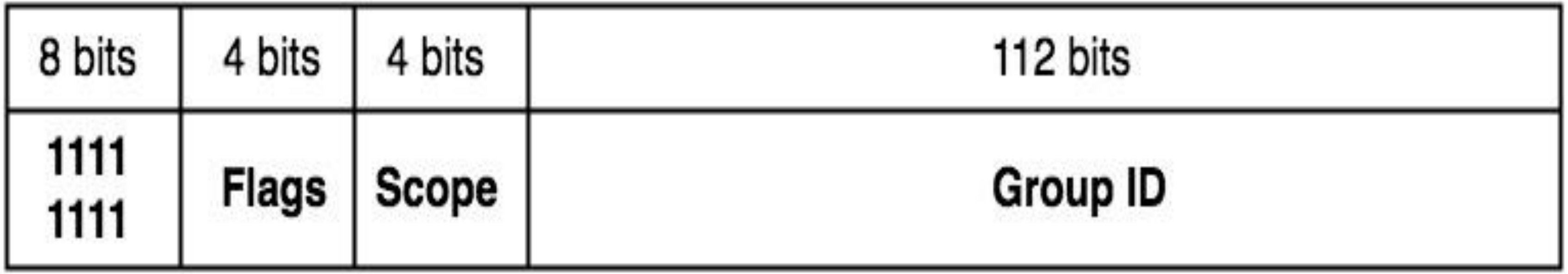
  Hexadecimal ff00 : : / 8

  Binary : 1111 1111 0000 0000

- IPv4 equivalent address

  Decimal 224 . 0 . 0 . 0 / 4

IPv6 Multicast address:



8 bits	4 bits	4 bits	112 bits
1111 1111	Flags	Scope	Group ID

IPv6 Multicast address:

4 bits : Scope

0	Reserved	1	Node local scope
2	Link local scope	3	Unassigned
4	Unassigned	5	Site local scope
6	Unassigned	7	Unassigned
8	Organizational local scope	9	Unassigned
A	Unassigned	B	Unassigned
C	Unassigned	D	Unassigned
E	Global Scope	F	Reserved

IPv6 Multicast address:

8 bits : 1111 1111   represent ff in hex format

4 bits : represent four different flags.

- o (reserved)
- R (rendezvous point)
- P (network prefix)
- T (transient flag).

IPv6 Multicast address:

The T flag denotes the two types of multicast addresses:

Permanent (0):

- Address known as predefined multicast addresses
- assigned by IANA
- include both well-known and solicited multicast.

Non permanent (1):

- dynamically assigned multicast addresses.
- are assigned by multicast applications.

IPv6 Multicast address:

Solicited-Node Multicast Addresses

Prefix ff02 : 0 : 0 : 0 : 0 : 1 : ff00 : : / 104

Used in Layer 3-to-Layer 2 address resolution.

Automatically created using a special mapping of the device's unicast address.

Used efficiently as broadcast address.

IPv6 Multicast address:

Well-Known Multicast Addresses

Prefix ff00 : : / 12

Flag field is always set to 0.

These are predefined or reserved multicast addresses

Examples

- ff02 : : 1 - All IPv6 devices
- ff02 : : 2 - All IPv6 routers
- ff02 : : 5 - All OSPFv3 routers
- ff02 : : a - All EIGRP (IPv6) routers

Required address for Hosts:

- link-local address for each interface
- Assign any of unicast and anycast address
- loopback address
- Multicast address to all nodes
- Solicited-node multicast address for each of its assigned unicast and anycast address
- Multicast address of all other groups to which the host belongs

Required address for Routers:

- The subnet-router anycast address for the interfaces for which it is configured
- Anycast address with which the router has been configured
- Multicast address to all routers
- Multicast address to other groups to which the router belongs

IPv6
Interface ID

Content:

1. Address interface ID

IPv6 Interface ID:

IPv6 has three type of interface ID

1. Manual
2. Modified EUI-64
3. Random

IPv6 Interface ID:

1. **Manual IPv6 Interface ID:**
    - It is assigned manually
    - Used in servers, Internet service and network infrastructure
    - Example fdfd : 90fe : f111 : : 100

      2a03 : 2770 : 11 : 1f04 : faaa : b001 : : 1

IPv6 Interface ID:

2. **Modified EU1- 64 IPv6 Interface ID:**
   - It is assigned by auto addressing
   - Used in mobile devices, LAN hosts and IoT devices
   - Example 2001 : db8 : aa : c10 : 12ca : eeaf : fe11 : 31ef

IPv6 Interface ID:

2. Modified EU1- 64 IPv6 Interface ID:

A 64-bit interface ID is created by inserting the hex number FFFE in the middle of the MAC address of the network card by flipping the 7th binary bit to 1

After this conversion the interface ID is commonly called the modified extended unique identifier 64 (EUI-64).

For example, if the MAC address of a network card is 00 : EE : CC : DD : 55 : 22 then interface ID will be 02EECCFFFEDD5522.

IPv6 Interface ID:

1. Convert MAC addresses in binary format.

   hex MAC address: 00EECCDD5522

   binary: 0000 0000 1110 1110 1100 1100 1101 1101 0101 0101 0010 0010

2. Flip the seventh bit from 0 to 1:

   binary 0000 0010 1110 1110 1100 1100 1101 1101 0101 0101 0010 0010

   Hex MAC address 02EECCDD5522

3. Insert FFFE in the middle of the address:

   Hex: 02EECCFFFEDD5522 and the interface ID 02EE:CCFF:FEDD:5522.

IPv6 Interface ID:

3. **Random IPv6 Interface ID:**

   - It is generated by auto configured address.
   - Used in enabling and disabling security of LAN hosts according to usage
   - Example 2001 : db8 : aa : c10 : 33c1 : cc3f : f711 : 312f

ICMPv6

Content:

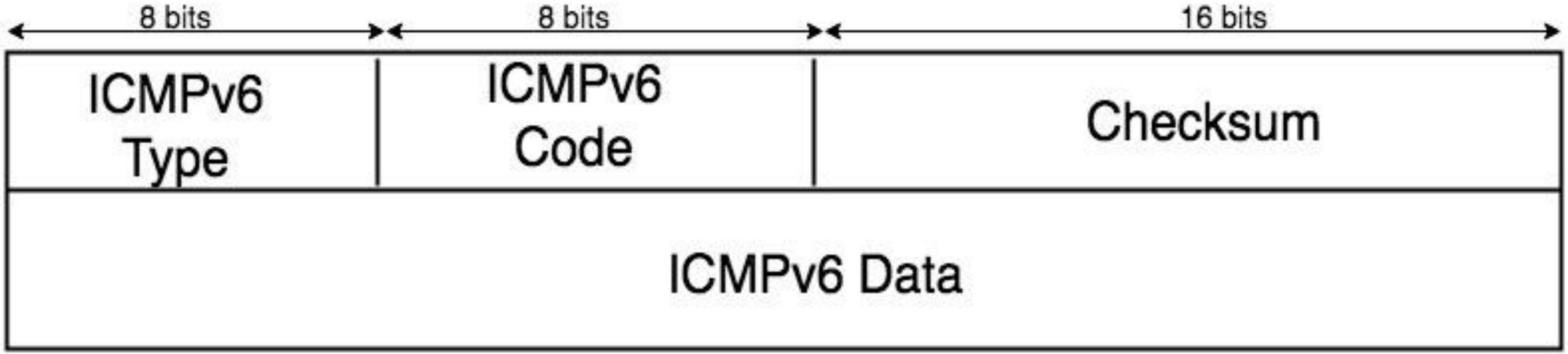
1. ICMPv6
2. Packet format

ICMPv6:

ICMPv6 : Internet Control Message Protocol Version 6

- New version of ICMP
- Offers collective solution to different function which is earlier performed by ICMP, ARP and IGMP
- Multipurpose protocol
- Value in next header field is 51

ICMPv6:



8 bits

8 bits

16 bits

ICMPv6 Type

ICMPv6 Code

Checksum

ICMPv6 Data

ICMPv6 Packet format

ICMPv6:

Packet format:

- Type : indicate the type of message (8 bits)

  High-order bit = 0 (value range from 0 to 127) - indicates an error message
  High-order bit = 1 (value range from 128 to 255) - indicates an information message

- Code : give more detail about the message type (8 bits)
- Checksum : used for detection of error (16 bits)
- Data : contain information according to the type of message (variable)

ICMPv6:

Type of ICMPv6 message:

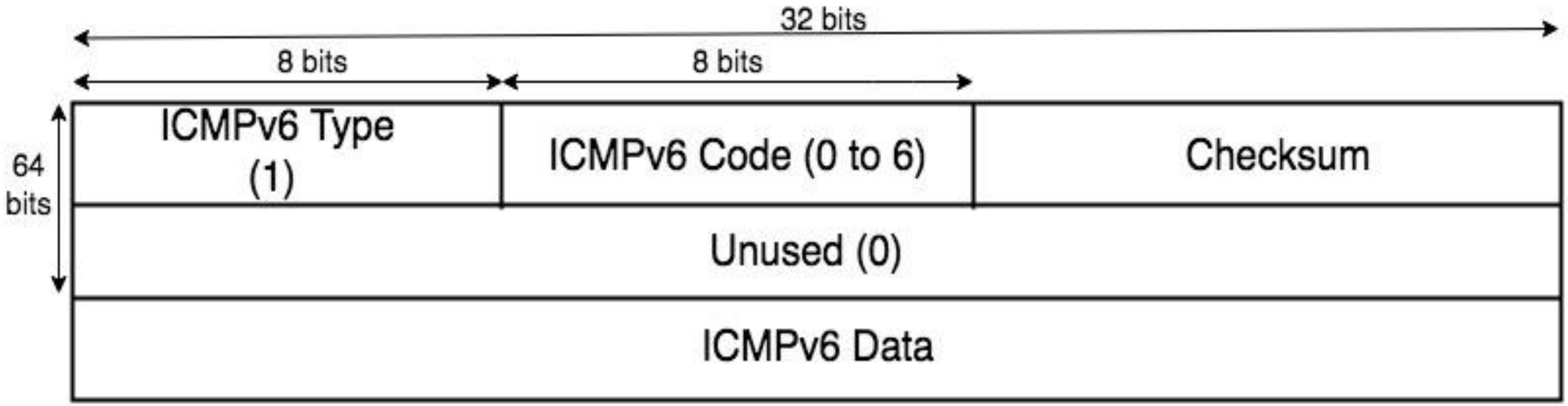
1. Error Message:
   - Destination Unreachable (message type 1)
   - Packet Too Big (message type 2)
   - Time Exceeded (message type 3)
   - Parameter Problem (message type 4)
2. Informational Message
   - Echo Request (message type 128)
   - Echo Reply (message type 129)

ICMPv6 Messages

Content:

1. ICMPv6 Error Message
2. ICMPv6 Informational Message

ICMPv6 Error Message:



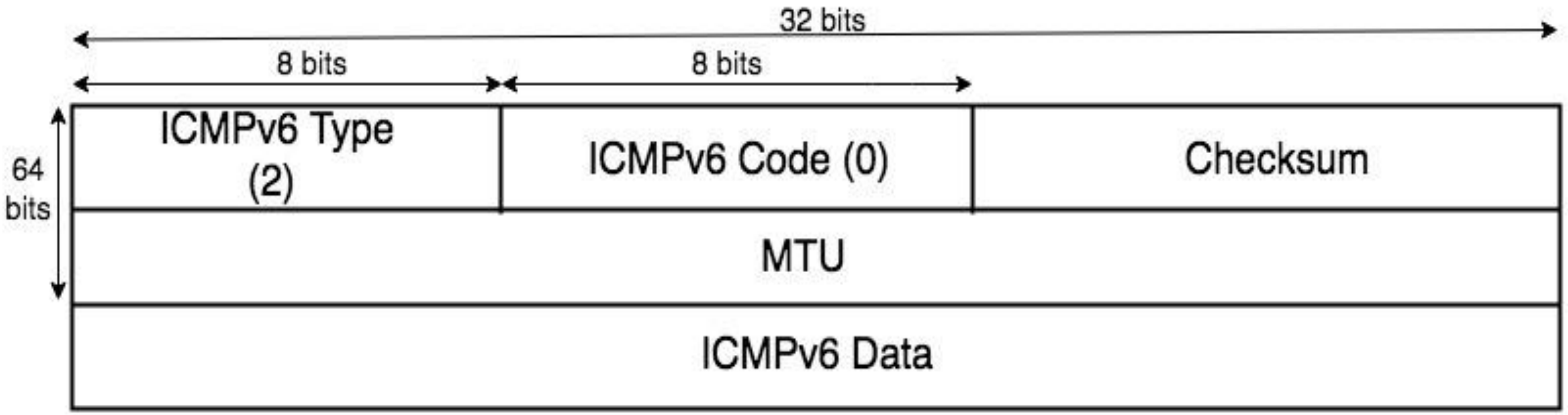
ICMPv6 Destination Unreachable

ICMPv6 Error Message:

Destination Unreachable:

- Generated when IP packet is not delivered.
- Error Message is send back to the source host of the packet.
- Value of type field = 1
- Value of code field = 0 to 6
- Data field will contain original data as ICMPv6 packet.

ICMPv6 Error Message:



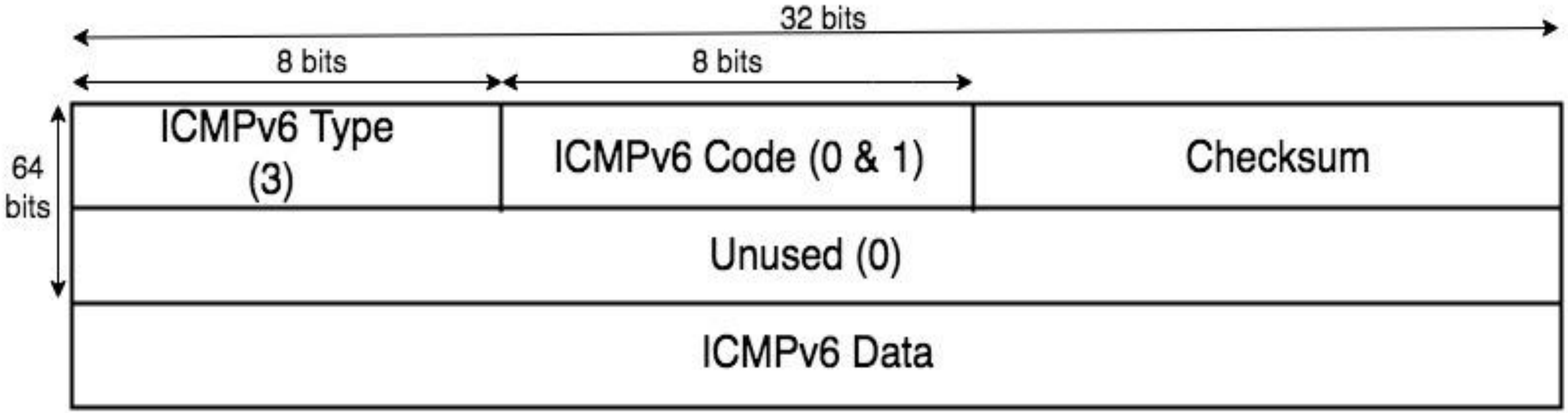
ICMPv6 Packet too big

ICMPv6 Error Message:

Packet Too Big :

- Generate this error when packet size become greater than MTU value.
- Packet will be discarded by the network.
- Error Message is send to the source host of the packet.
- Value of Type field = 2
- Value of code field = 0 (unused)
- Value of MTU field = MTU size of next hop limit.

ICMPv6 Error Message:



ICMPv6 Type (3)

ICMPv6 Code (0 & 1)

Checksum

Unused (0)

ICMPv6 Data

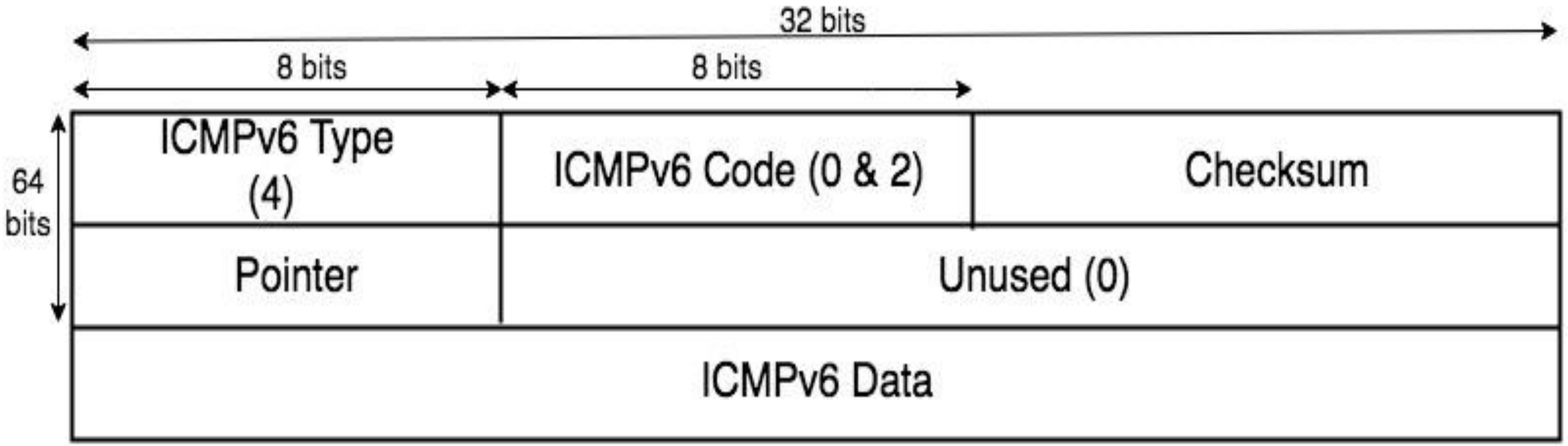
ICMPv6 Time Exceeded

ICMPv6 Error Message:

Time Exceeded :

- Error indicate the initial hop limit set by sender is too low.
- Hop limit is set in network to eliminate routing loops
- Value of Type field = 3
- Value of Code field = 0 and 1
- Value of Unused field = 0

ICMPv6 Error Message:



32 bits

8 bits

8 bits

64 bits

ICMPv6 Type (4)

ICMPv6 Code (0 & 2)

Checksum

Pointer

Unused (0)

ICMPv6 Data

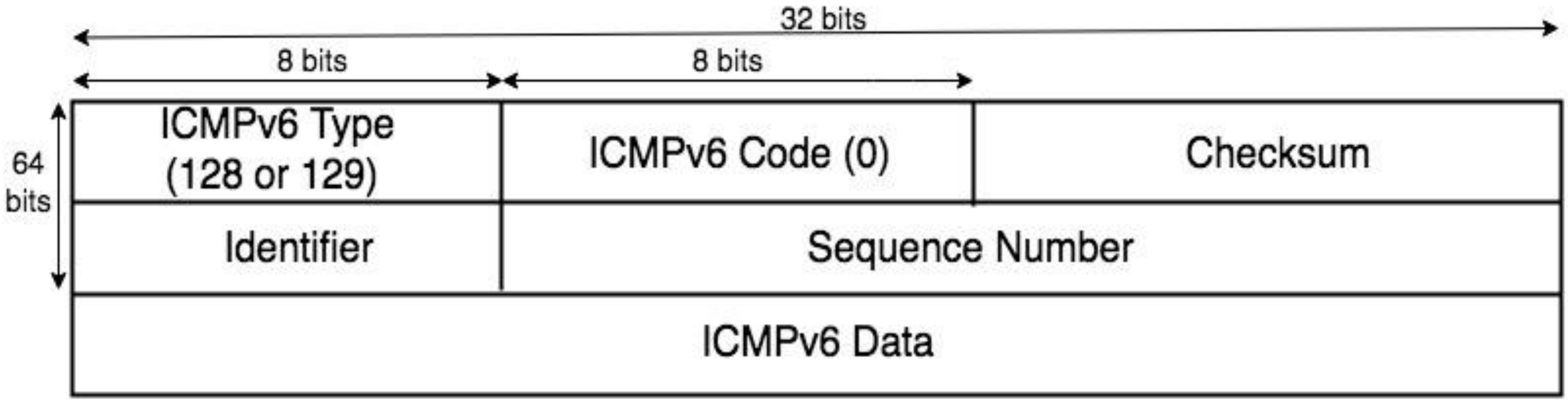
ICMPv6 Parameter Problem

ICMPv6 Error Message:

Parameter Problem :

- Error generated when IPv6 node is not able to complete the processing or identifying the type of IPv6 packet.
- Value of Type field = 4
- Value of Code field = 0 to 2
- Value of Pointer = identifies the offset where the error was detected.

ICMPv6 Informational Message:



ICMPv6 Type (128 or 129)	ICMPv6 Code (0)	Checksum
Identifier	Sequence Number	
ICMPv6 Data		

ICMPv6 Echo Request or Echo Reply Message

ICMPv6 Informational Message:

Echo Request and Echo Reply message :

- Used in TCP/IP utilities : Ping (Packet InterNet Groper)
- The source device sends an **echo request** message to particular destination device
- The destination device, if available send back **echo reply** message.
- Type value = 128/ 129 and Code value = 0 (unused)
- Identifiers and sequence number : used to check sync between request and replies

Neighbour Discovery

Content:

1. Neighbour Discovery
2. Utilization
3. Improvement in IPv4 Protocol

Neighbor Discovery:

Specified in RFC 4861

It’s a combination of:

- Address Resolution Protocol
- ICMP Router Discovery and Redirect
- Neighbor Unreachability Detection
- Duplicate IP address Detection

Neighbor Discovery:

Functions of NDP :

1. Neighbor Discovery
2. Router Discovery
3. Stateless Address Auto Configuration (SLAAC)
4. Address Resolution
5. Neighbor Unreachability Detection (NUD)
6. Duplicate Address Detection(DAD)
7. Redirection

Neighbor Discovery:

Utilization:

- For Stateless Autoconfiguration
- Information regarding network prefix or routes configuration
- To detect duplicate IP address
- To regulate the addresses of nodes at layer 2 on same link
- Finding neighbouring routers to forward the packet
- Tracing reachable and non reachable neighbouring nodes
- Finding changes in link layer address.

Neighbor Discovery:

Improvement in IPv4 Protocol:

- Router Discovery add to base protocol
- Router advertisement contain link layer addresses for the router and prefix of a link
- The reassembling of a network is done by neighbor discovery. It also provide IP authentication and security
- Multiple prefix are assigned to one link.

Neighbor Discovery:

Improvement in IPv4 Protocol:

- Neighbor Unreachability Detection detect the failed connectivity and not send messages to unreachable neighbor.
- The request above the hop limit value of 255 is not processed
- Routers advertise MTU on the link
- Router advertisement also enable the stateless Address auto configuration.

Neighbor Discovery:

Neighbour Discovery Protocol is of five types:

1. Pair of Neighbor Solicitation / Neighbor Advertisement message
2. Pair of Router Solicitation / Router Advertisement message
3. ICMP Redirect message

ND Router Messages

Content:

1. Router Solicitation Message
2. Router Advertisement Message

Router Messages:

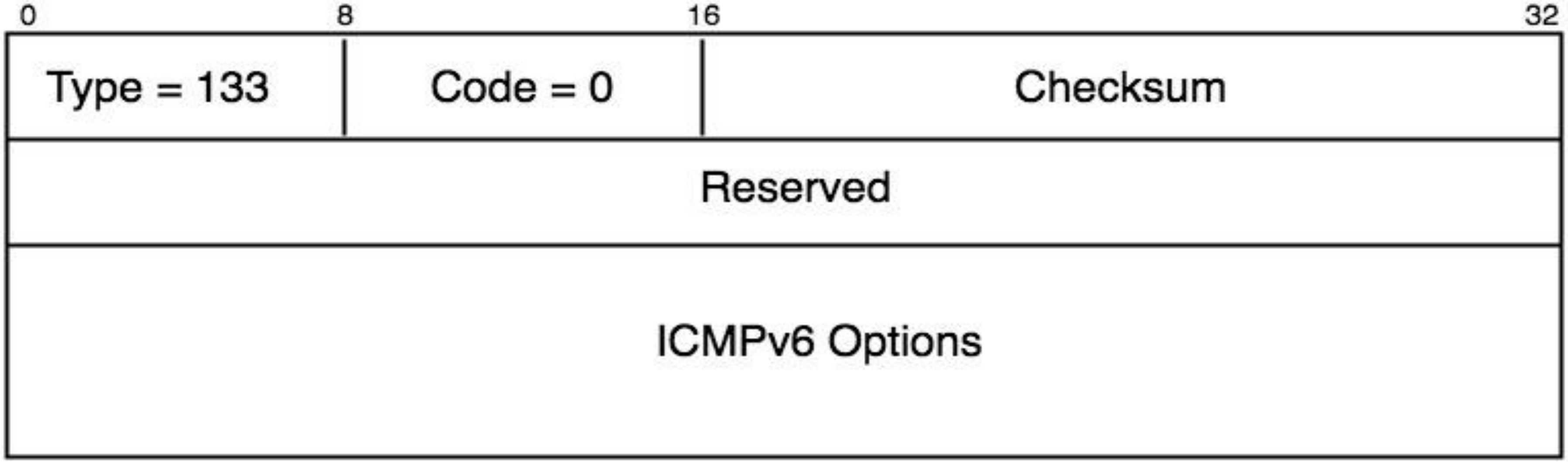
1. Router Solicitation / Router Advertisement message

Router Advertisement messages is send by router at regular intervals.

Devices request Router Advertisements by issuing a Router Solicitation message.

This operation will trigger routers to immediately issue Router Advertisements , irrespective of the regular interval.

Router Solicitation Message:



0 8 16 32

Type = 133	Code = 0	Checksum
Reserved		
ICMPv6 Options		

Router Messages:

Router Solicitation message format

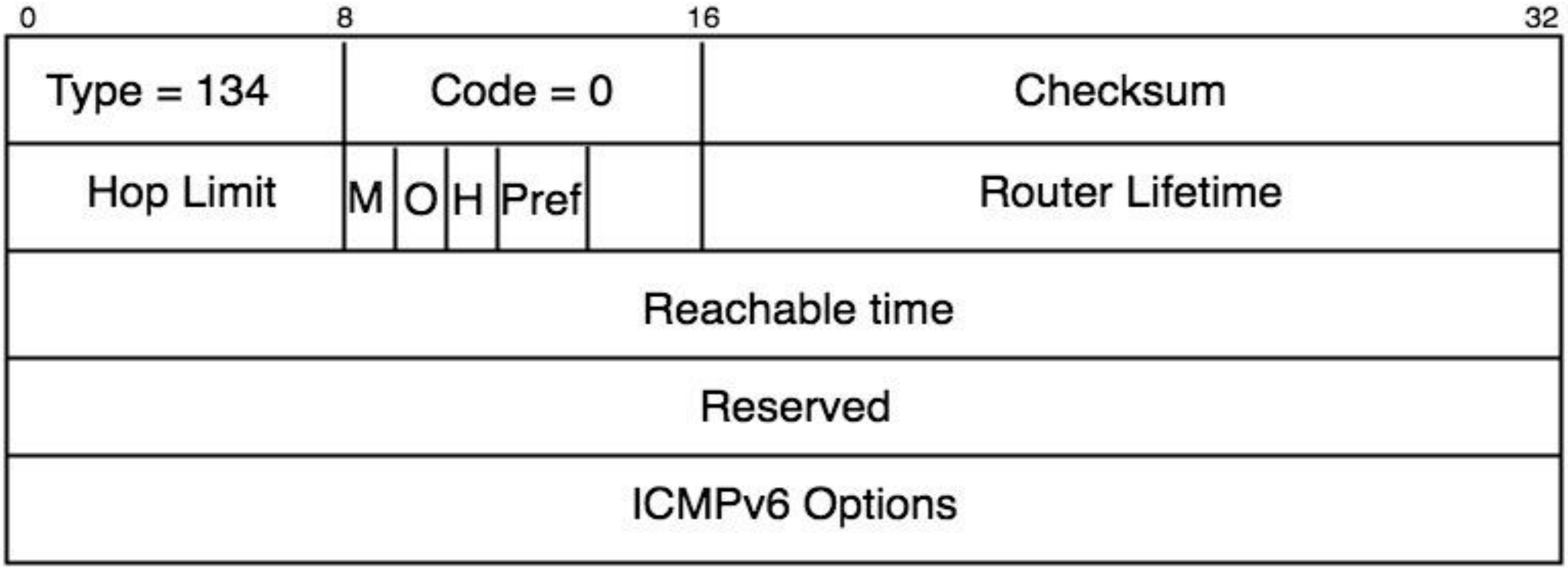
- Destination address : Multicast address for all routers ff02 : : 2 as a
- Hop limit is set to 255
- ICMP Type field value 133 (value for the Router Solicitation message)
- Code field is unused and set to 0.
- Checksum (2 bytes)
- Unused (4 bytes) reserved for future use. The sender sets them to 0, and the receiver ignores those fields.

Router Messages:

Router Solicitation message format

- Option Field :
  - if the address of the sending host is known a option contain the link-layer address of the sending host.
  - If the Source address on the IP layer is the unspecified (all-zeros) address, this field is not used.

Router Advertisement Message:



Router Messages:

Router Advertisement message format:

- Destination address Multicast address for all-nodes ff02 : : 1 (for periodic advertisement)
- Destination address : interface address that originate the solicitation message (for solicited advertisement)
- Hop limit : set to 255.
- ICMP Type field : 134 (Router Advertisement message)
- Code field : 0 (Unused)

Router Messages:

Router Advertisement message format:

- Hop Limit field used to configure all nodes on a link
- M-Flag (1 bit) specifies which configuration to be used:
  - Bit value - 0- Nodes use Stateless Address Autoconfiguration.
  - Bit value - 1 - Nodes use Stateful Autoconfiguration (DHCPv6).
- O-Flag show whether nodes on this link use DHCPv6 for some additional information.
  - Bit value - 0- Nodes will use DHCPv6 for address related information.
  - Bit value - 1 - Nodes use DHCPv6 for non address-related information

Router Messages:

Router Advertisement message format:

- H Flag i.e Home Address Flag
    - Bit value - 1 : It act as a home agent for the link.
- Pref Flag i.e Preference flag is optional extension defines the Route information (2 bits)
- Next 3 bits are set to 0 and reserved for future use.

Router Messages:

Router Advertisement message format:

- Route Lifetime - 16 bits long and have maximum value of time is 18.2 hours
  - Bit value -1 indicate that router is used as default router.
  - Bit value -0 indicate that router is not used as default router.
- Reachable Time - 32 bits indicate time in milliseconds when nodes are considered reachable. NUD algorithm is used here
  - Bit value - 0 indicate that value is not declared

Router Messages:

Router Advertisement message format:

- Retrans Time - 32 bits used by ARP and NUD mechanisms. It indicate the time in milliseconds between retransmitted Neighbor Solicitation messages.
    - Bit value - 0 indicates router is not configured with a retransmission timer.
- Options - it contain three different information: source link layer address, MTU size and Prefix information.

ND Neighbor Message

Content:

1. Neighbor Solicitation Message
2. Neighbor Advertisement Message

Neighbor Messages:

1. Neighbor Solicitation / Advertisement message:

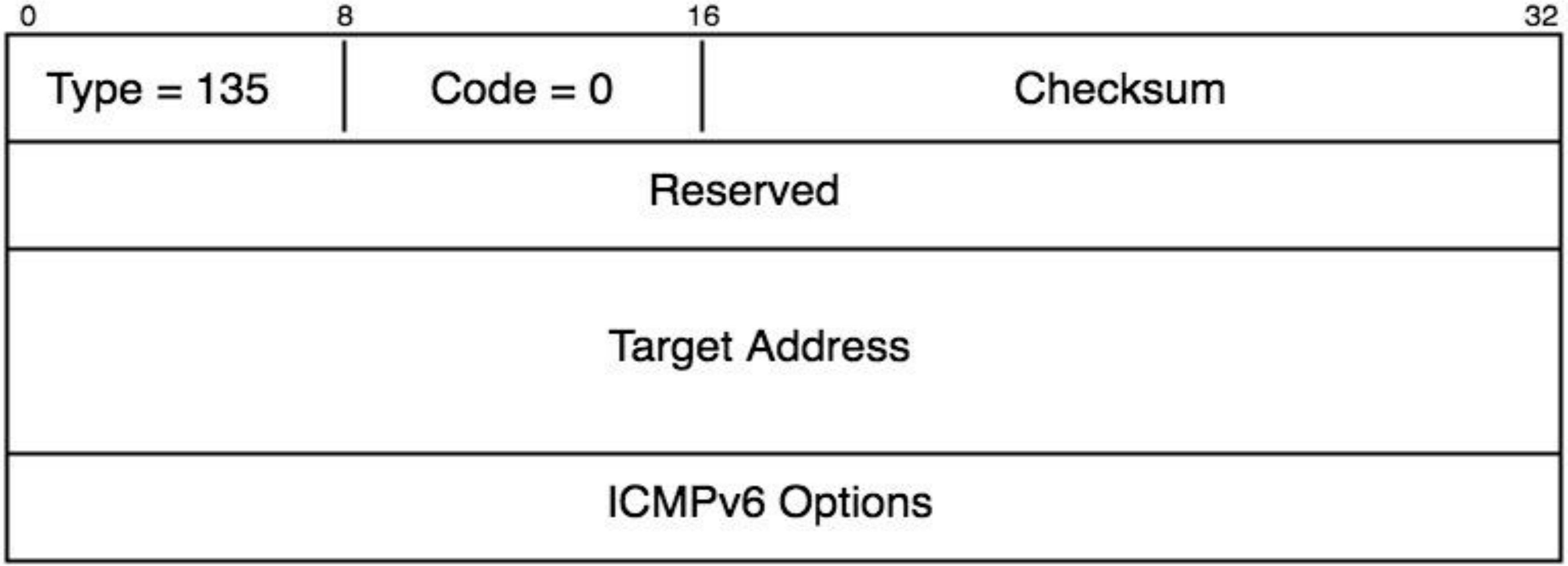
   Neighbor solicitations : used by nodes to get the link layer address of a neighbor and to check weather a neighbor is still reachable via a cached link layer address or not.

   Destination address : Multicast address

   Neighbor advertisements : used by nodes to respond to a Neighbor Solicitation message

   Destination address : Unicast

Neighbor Solicitation Message:



0 8 16 32

Type = 135

Code = 0

Checksum

Reserved

Target Address

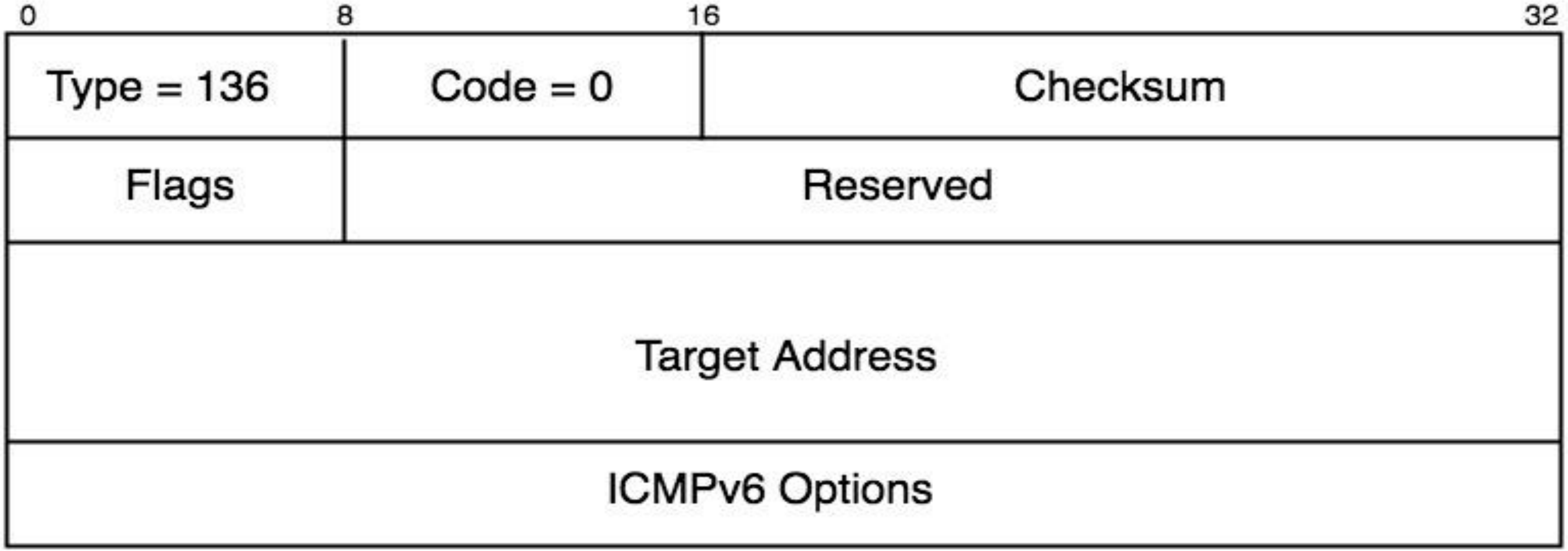
ICMPv6 Options

Neighbor Messages:

Neighbor Solicitation Message:

- Type : 135 indicate neighbor solicitation message (8 bits)
- Code : 0 (unused) (8 bit)
- Checksum : (16 bits) detect error bit
- Reserved : 32 bits reserved for future use and set to 0
- Target address : used in neighbor advertisement and redirect message. (multicast message is not used here) (128 bits)
- Option field : (variable) contain link layer source address

Neighbor Advertisement Message:



<table>
<tr><td>Type = 136</td><td>Code = 0</td><td colspan="2">Checksum</td></tr>
<tr><td>Flags</td><td colspan="3">Reserved</td></tr>
<tr><td colspan="4">Target Address</td></tr>
<tr><td colspan="4">ICMPv6 Options</td></tr>
</table>

Neighbor Messages:

Neighbor Advertisement Message:

- Type : 136 indicate neighbor advertisement message (8 bits)
- Code : 0 (unused) (8 bit)
- Checksum : (16 bits) detect error bit
- R flag i.e. Router Flag is set to 1 indicate that sender is router (1 bit)
- S flag i.e. Solicited flag is set while sending the response to neighbor solicitation message (1 bit)

Neighbor Messages:

Neighbor Advertisement Message:

- O flag : Override flag indicate the information of advertisement message that it override existing neighbor cache entries and update any cached link layer address. (1 bit)
- Remaining 29 bits are reserved for future use and set to 0.
- Target address : address of the sender of solicited message (128 bits)
- Option field : (variable) contain target link layer address

Neighbor Messages:

Neighbor Advertisement Message:

Source address	Destination Address	Message Type
All Zeros	All router Multicast Solicited Node Multicast	SLAAC DAD
Unicast	Solicited Node Multicast Unicast	Resolve Link Layer Addr Unreachability Detection

ND
Redirect Message
&
Security

Content:

1. Redirect Message
2. Neighbor Discovery Security

Redirect Message:

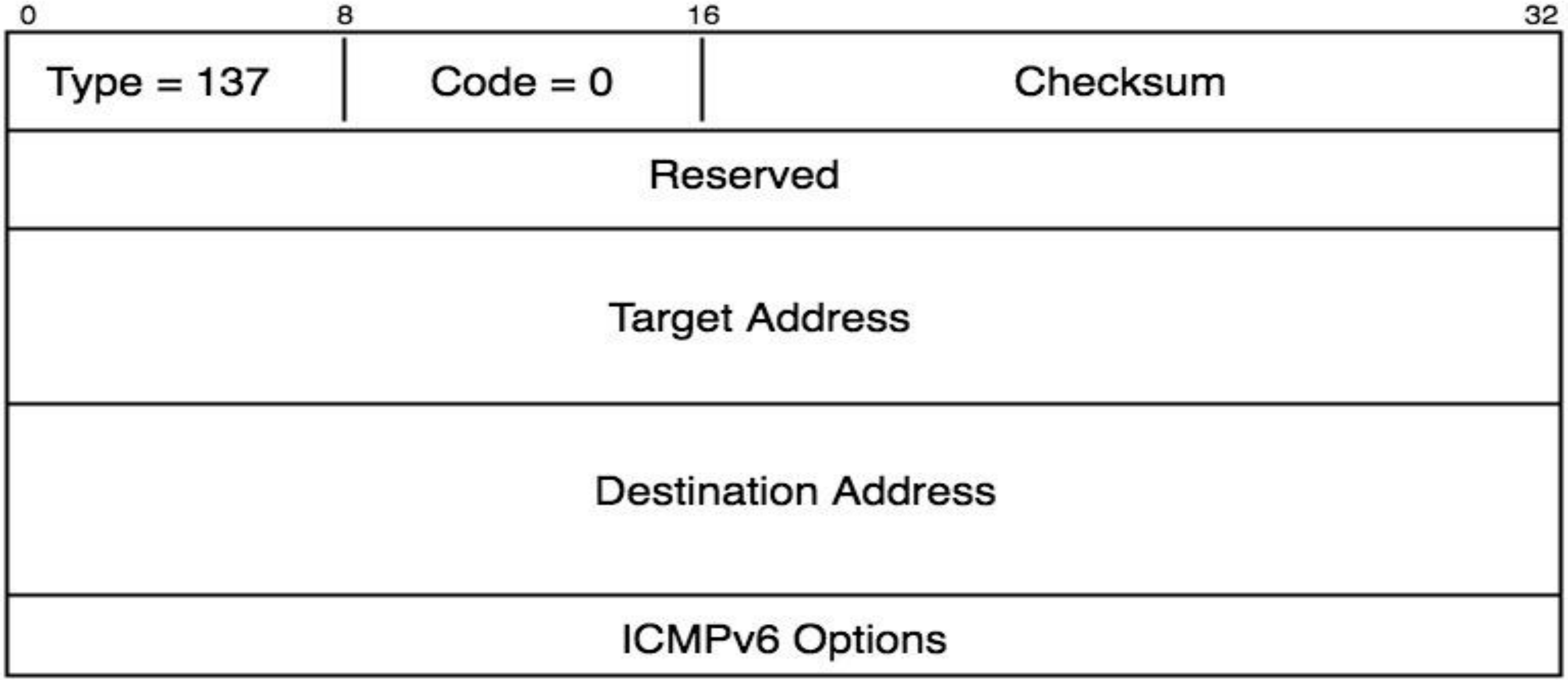
1. ICMP Redirect Message:

   Used by router

   It send information to the host over the link about the availability of a better path to particular destination.

   It also indicate that the distance of the destination device that it is a neighbor on a same link or a node on a remote subnet.

Redirect Message:



0	8	16	32
Type = 137	Code = 0	Checksum	
Reserved			
Target Address			
Destination Address			
ICMPv6 Options			

Redirect Message:

ICMP Redirect Message:

- Type : 137 indicate Redirect message (8 bits)
- Code : 0 (unused) (8 bit)
- Checksum : (16 bits) detect error bit
- Reserved : 32 bits reserved for future use and set to 0
- Target address : address of next best hop (128 bits)
- Destination address : Address of destination node
- Option field : contain target link layer source address and redirect header

Neighbor Discovery Security:

SEND (Secure Neighbor Discovery) is a working group who define the protocol that is used to secure the Neighbor discovery message.

It is used in a system where physical security of system is vulnerable to attack and Neighbour discovery security have a more concern.

Three trust models are defined to secure:

- Corporate Intranet
- Public wireless access network
- Pure Ad-hoc network

Neighbor Discovery Security:

Component defined under SEND are:

1. Authorising the Router : before using it as default router. Here *Certification Path Solicitation Advertisement messages* are used to discover a certification path to the trusted router in network
2. *Cryptographically Generated Process* (CGA) it detect the integrity of a sender of a ND message by verifying it claimed address. Pair of public private keys are shared between nodes before communication.
3. *RSA signature* : Protect all messages transfer, related to ND and RD
4. *Timestamp* and *Nonce* option to prevent packet relay attack.

Autoconfiguration
&
Path Discovery

Content:

1. SLAAC
2. Network Renumbering
3. Path MTU Discovery

Autoconfiguration:

IPv6 address have a ability to autoconfigure automatically in the network.

Benefits of Autoconfiguration:

- Less workload on network administrator
- Easy configuration of large addresses

Autoconfiguration::

Autoconfiguration Methods:

1. **Stateful Autoconfiguration** : IPv6 addresses are assign with help of DHCP.

2. **Stateless Autoconfiguration** : Devices and routers have 64 bit prefix and 64 bits of interface ID.

   Interface ID address are derived with help of EUI-64 process.

   SLAAC use ND Protocol to configure address.

SLAAC:

SLAAC provides plug-and-play IP connectivity in two phases:

- Phase 1 – Link-Local address assignment
- Phase 2 – Global address assignment

SLAAC:

Phase 1 – Link-Local Address : used for providing local connectivity

1. Generation of link local address
2. Execution of DAD algorithm
3. Assigning Link Local address

SLAAC:

Phase 2 – Global Address : used for providing global connectivity

1. Sending Router Advertisement message
2. Generating Global address
3. Execution of DAD algorithm
4. Assignment of Global address

SLAAC:

States of IPv6 Addresses :-

1. Tentative Address
2. Preferred Address
3. Deprecated Address
4. Duplicate Address
5. Valid Address
6. Invalid Address

SLAAC:

How to generate interface ID:

1. Permanent IPv6 address:
2. Temporary IPv6 address:

Network Renumbering:

Renumbering a network means replacing an old prefix with a new prefix.

Reasons for replacing the Prefix:

- Change of provider, which usually implies a change of prefix.
- Movement from IPv4 world to the IPv6 world,
- Concept of having multiple addresses to a node.

Path MTU Discovery:

PMTUD is a technique

- Determine the MTU size on the network path between two nodes.
- Goal is to avoid IP fragmentation.
- Standardized for IPv4 in RFC 1191 and for IPv6 in RFC 1981.
- This also support multicast destination.

Path MTU Discovery:

1. Device believe that the Path MTU is the same as the MTU of the first hop link and it uses that size.
2. ICMPv6 Packet Too Big message is send,If the packet is too big for a intermediate router along the path to deliver the packet to the next link, the router discards the packet .
3. ICMP message includes the MTU size of the next hop link.
4. The device use same MTU for sending further packets to the same destination.
5. When the packets received at the final destination, the Path MTU discovery process ends

IPv6
MLD & MRD

Content:

1. Multicast Listener Discovery
2. MLDv1
3. MLDv1 Packet Format
4. MLDv2
5. MLDv2 Packet Format
6. Multicast Router Discovery

MLD:

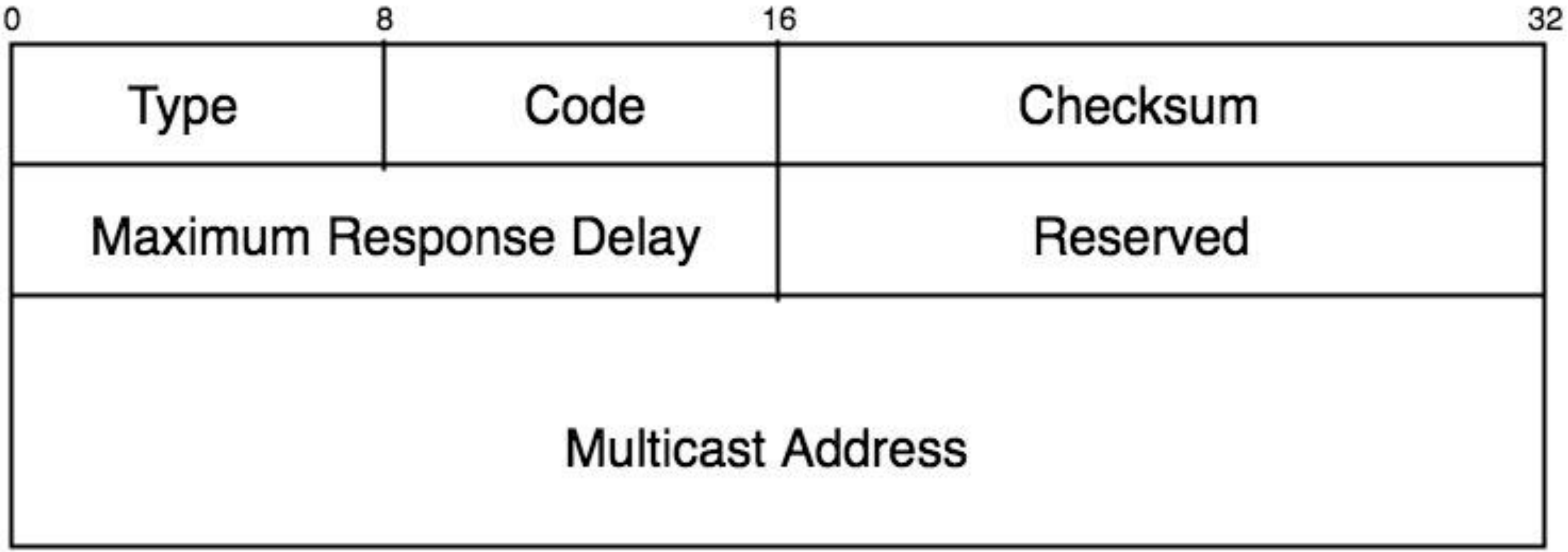
Multicast Listener Discovery is used by IPv6 devices to discover multicast listeners in a directly linked network.

Protocol Independent Multicast (PIM) routing technique is used for forwarding multicast messages.

There are two versions of MLD:

- MLD version 1 : Based on IGMPv2 for IPv4 (RFC 2710)
- MLD version 2 : Based on IGMPv3 for IPv4 (RFC 3810 and RFC 4606)

MLDv1:



0	8	16	32
Type	Code	Checksum	
Maximum Response Delay		Reserved	
Multicast Address			

MLDv1:

- Type : Value is set to 130 for Multicast Listener Query
  Value is set to 131 for Multicast Listener Report
  Value is set to 132 for Multicast Listener Done
- Code : Set to 0
- Maximum Response Delay : used in query message only.
- Multicast Address : Set to 0 (General Query)

  Set to multicast group address (Address Specific query)

MLDv1:

Message Type	Destination Address
General Query	Link-local scope all-nodes (ff02::1)
Multicast Address-Specific Query	The multicast address being queried
Report	The multicast address being reported
Done	Link-local scope all-routers (ff02::2)

MLDv2:

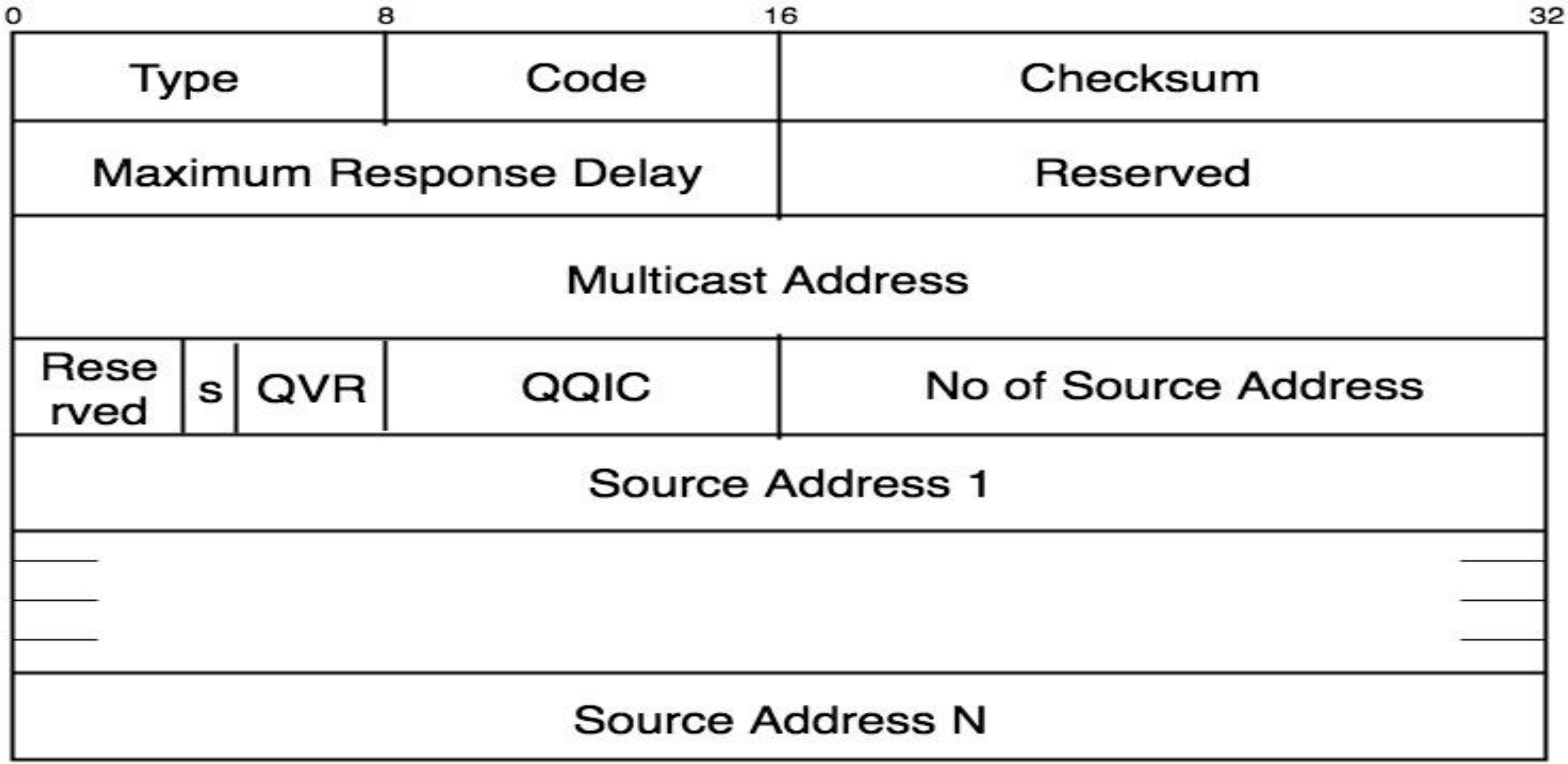
MLDv2 is similar to MLDv1 but it has a ability where node can do “Source Filtering“.

Have a combination of SSM and ASM.

Two filter mode to support SSM are:

- INCLUDE
- EXCLUDE

MLDv2:



0 8 16 32

Type | Code | Checksum

Maximum Response Delay | Reserved

Multicast Address

Rese rved | s | QVR | QQIC | No of Source Address

Source Address 1

Source Address N

MLDv2:

- Type : Value 130 for Multicast Listener Query
  Value 143 for Multicast Listener Report version 2 (RFC 3810)
- Reserved : 4 bit set to zero
- S Flag : Suppress Router Side Processing (1 bit) used to suppress the normal timer update of router
- QVR : Querier’s Robustness Variable (3 bits) used for synchronization of all MLDv2 routers

MLDv2:

- QQIC : Querier’s Query Internal Code (8 bit) also used for synchronization purposes
- N : Number of Sources (16 bit) no of source address present
- Source address: Variable length , contain source address

MLDv2:

Type of Query:

1. General Query : give information about which multicast address have listener on an attached link.
2. Multicast Address Specified Query : give information about if particular multicast address has an listener on an attached link or not.
3. Multicast Address & Source Specifier Query : give information about if any of the source from the specified list of multicast address has any listener on an attached link or not

MRD:

Multicast Router Discovery is used to search multicast routers. (RFC 4286)

It does not have any specified routing protocol.

Types of messages in MRD are:

1. Multicast Router Advertisement (151)
2. Multicast Router Solicitation (152)
3. Multicast Router Termination (153)

IPv6 Routing Part 1

Content:

1. MDT
2. Types of MDT
3. PMI

Routing:

Multicast Distribution Tree (MDT) :

Multicast capable routers create distribution trees.

This tree is used to find best path for multicast traffic from source to various receiver.

The root at the source of traffic is called Shortest Path Tree (SPT).

The process of finding the upstream neighbor is called Reverse Path Forwarding (RPF).

Routing:

The two basic types of multicast distribution trees:

- Source trees
- Shared trees

Routing:

1. **Source Trees** :

   The simplest form of a MDT is a source tree having its root and branches.

   Its roots act as a source.

   Branches form a spanning tree providing network to the the receiver.

   This tree uses the shortest path through the network, it is also referred to as a shortest path tree (SPT).

Routing:

2. **Shared Tree** :

   As source trees have their root at the source.

   Shared trees use a single common root i.e. placed at some chosen point in the network.

   This shared root is called a Rendezvous Point (RP).

Routing:

Source Trees

Advantage : Create optimal path between the source and the receivers.

Disadvantage : Large memory consumption

Shared Trees

Advantage : low memory requirement

Disadvantage : Path between source and receivers is not optimal.

Routing:

Protocol Independent Multicast :

It is a process of building Multicast Distribution Tree (MDT)

The topology information is maintained in the Tree Information base (TIB).

Type of multicast routing Protocol are:

1. PIM - SM (Spare Mode)
2. PIM - SSM (Source Specific Multicast)
3. PIM - Bidir (Bidirectional)

IPv6 Routing Part 2

Content:

1. Routing table
2. Routing table entities
3. How router make routing table.
4. Type of Routes
   - Static Routes
5. Static Routing Protocol
6. Dynamic Routing Protocol
7. Autonomous System
8. IGP and EGP

Routing Table:

Routing Table is a set of rules which determine where to route the packet in the Internet protocol (IP) network.

Every packets which are traveling in network , contain IP address of source and destination device.

When router receive these packet it match the address with the information that routing table contain and find the best route to transfer packet.

Routing tables can be maintain dynamically or manually.

Routing Table:

IPv6 Routing Table entities:

1. IPv6 Prefix and Prefix Length
2. Next Hop Address
3. Next Hop interface
4. Metric
5. Timer
6. Routing Protocol used

Routing Table:

How Router create Routing tables?

In a network, when a sender device sends the packet to the destination device then sender add IP address of both the devices.

Then the packet goes to router.

Router examine the packet and find its IP addresses in its Routing table.

When router gets the perfect match, then it determine the perfect route (cost effective route) to forward the packet in the network.

Type of Routes:

Static Route:

Static route are configured manually by network administrator.

When any change in the network occur then administrator manually update the static route according to the changes.

It is used for simple and small network.

More secure route.

Type of Routes:

Static Route:

Type of Static Route:

1. Directly attached IPv6 static route
2. Fully specified IPv6 static route
3. Floating IPv6 static route
4. Default IPv6 static route

Static Routing Protocol:

A static route is a special route which is configured by network administrator manually.

Static routing is a type of network routing technique used for manual configuration and selection of a network route.

Static routing is not a routing protocol; instead, it is the routing technique.

Dynamic Routing Protocol:

Dynamic routing protocol is used to find best route to forward the packet to the destination.

The common protocol used by dynamic routing protocols are RIPng, OSPFv3, ISIS and BGP etc.

Dynamic Routing protocol can be divided into :

- IGP (Interior Gateway Protocol)
- EGP (Exterior Gateway Protocol)

Dynamic Routing Protocol:

1. **Interior Gateway Protocol:**

Interior Gateway Protocol is a set of routing protocol which are used within one autonomous system.

For example: RIPng, OSPFv3 , IS-IS etc

It mainly search and calculate routes within an autonomous system.

Dynamic Routing Protocol:

2. **Exterior Gateway Protocol:**

Exterior Gateway Protocol is used to connect different autonomous system such as BGP .

It control communication between different autonomous system with routing policies and route filtering mechanism.

IPv6
Routing Protocol
Part 1

Content:

1. RIPng
2. OSPFv3

Routing Protocol:

RIPng:

Known as Routing Information Protocol next generation.

In IPv4 Protocol it is known as RIP only

Based on Distance vector Algorithm .

Concept for RIPng is taken from RIPv1 and RIPv2

Specified in RFC 2080 (jan 1997)

Routing Protocol:

RIPng: Distance vector Algorithm

This mechanism calculate the cost (metric) of a route. (Hop count)

RIPng support maximum of 16 hop count.

The distance greater than 16 hop count considered to be unreachable

Convergence time is the time taken by device to know about all routes in the network.

Routing Protocol:

Limitation of RIPng:

1. RIPng network area is limited i.e. only upto 16 hop count
2. Presence of Routing loop cause increase in convergence time
3. It does not measure other real time parameters such as link load reliability and delay
4. Any change in the network structure cause the instability in network.

Routing Protocol:

OSPFv3:

Stands for open shortest path first version 3

Specified in RFC 5340

Introduce to eliminate the limitation of RIPng such as small network area, high convergence time and low metric etc.

OSPF consist of large routing table to accomodate large number of routes

It choose best path in a network on the basis of “Link state”.

Routing Protocol:

OSPFv3:

OSPF routers keep information about the state of all network connections or links between the network.

In case of link failure, it also converges on a new loop-free routing structure within seconds.

It computes the shortest-path tree for each route using link state routing algorithm (LSA) or shortest path first algorithm (SPF).

It calculate shortest path using a method based on Dijkstra's algorithm.

Routing Protocol:

OSPFv3: Similarities between OSPFv2 and OSPFv3

- Both are link-state IGP routing protocols
- Both use ABR and ASBR.
- Both use the SPF calculation with Dijkstra's SPF algorithm
- Both use metrics that are based on interface bandwidth
- Both have 5 common protocol packet types: Hello, Database description (DBD), Link-state request (LSR), Link-state update (LSU), Link-state acknowledgment (LSA)
- They have the same LSA flooding and aging timers

Routing Protocol:

OSPFv3: Similarities between OSPFv2 and OSPFv3

- They use different address families
- Introduces new LSA format and has different packet format
- It runs per-link rather than per-subnet
- It supports multiple instances on a single link, Interfaces can have multiple IPv6 addresses
- It uses link local address
- Neighbor Authentication done with IPsec (AH)

IPv6
Routing Protocol
Part 2

Content:

1. ISIS
2. EIGRP
3. BGP

Routing Protocol:

ISIS:

Stands for Intermediate system - intermediate system.

Defined in RFC 5308.

IS-IS defines the exchange of routing information between Intermediate Systems (routers) in network

Integrated IS-IS is an interior routing protocol based on link state updates.

Routing Protocol:

ISIS:

Integrated IS-IS provides information about variable-length fields (Type, Length, Value fields, or TLVs) in all IS-IS packets (Hello, LSP, and SNP).

NLPID tells about the network layer protocol which is assigned by ISO with a value of 142 (0x8E).

Type of TLV for IPv6 IS-IS

- IPv6 Reachability TLV (Type 236)
- IPv6 Interface Address TLV (Type 232)

Routing Protocol:

EIGRP:

Stands for Enhanced Interior Gateway Protocol (EIGRP)

It runs in an autonomous system called EIGRP domain.

Aim : Eliminating limitations of a distance vector routing protocol without developing another link state based protocol.

EIGRP is a hybrid protocol combining the best of both protocol.

Diffuse Update Algorithm (DUAL) is used to calculate the routes.

Routing Protocol:

EIGRP:

Advantage: Fast convergence time , loop-free operations

Only routers affected by a change are involved.

EIGRP supported different network layer protocols.

The semantics of the different protocols are implemented using protocol-dependent TLVs (Type, Length, Value) fields.

Routing Protocol:

BGP:

Stands for Border Gateway Protocol

Defined in RFC 4760.

BGP is an exterior routing protocol used to exchange information about the reachability of networks between Autonomous Systems.

Each AS receives a unique AS number assigned by the numbering authority, such as IANA and RIRs like ARIN, RIPE NCC etc.

IPv6
QoS

Content:

1. QoS
2. Architecture of QoS
3. Flexibility in IPv6 Header

QoS:

To meet the demand of accessing real time services efficiently , IPv6 provide a QoS feature.

QoS protocols have the task of providing different packet streams with priorities and metrics such as

- Bandwidth
- Delay
- Interpacket delay variation (jitter)
- Packet loss

QoS:

QoS protocol consist of two main architecture:

1. Integrated services (IntServ)
2. Differentiated services (DiffServ)

Note : Both services use traffic policies and provide QoS feature in both LAN and WAN network.

QoS:

1. **Integrated Services Architecture (Intserv):**

   This architecture offers a capability to allocate Bandwidth to different flows.

   Based on a model that provide assistance from end to end connectivity during transmission of IP packets.

   RSVP is a part of intserv architecture.

   It is a signalling protocol used to reserve bandwidth and other QoS resources across on IP network.

QoS:

2. **Differentiated Services (DiffServ):**

   This architecture is design to provide scalability and usability in large network and internet.

   DS Domain : is a neighbouring group of routers having similar service policy that is implemented on all routers.

   DS Region : is a set of neighbouring DS domain.

   Packet Classifiers : check the packet header information.

QoS:

Types of Packet classifiers:

1. Behavior Aggregate Classifier (BA) :

   Classify packets based on the DS field

2. Multifield Classifier (MF) :

   Classify packets based on the different header fields

QoS:

It include two different fields in IPv6 header:

1. **Traffic Class Field :**

   Consist of two fields such as DSCP (6 bit) and ECN (2 bits)

2. **Flow Label Field :**

   Used by Source to label the packets .

   Value ranges from 00001 to FFFFF

   Practically not used

DHCPv6

Content:

1. DHCPv6
2. Terms related to DHCPv6
3. Multicast addresses
4. Ports
5. DHCPv6 Header Format
6. DHCP Authentication

DHCPv6:

DHCPv6 stands for Dynamic Host Configuration Protocol version 6

Specified in RFC 3315

IPv6 use combination of SLAAC and DHCPv6 for address configuration in network.

SLAAC is used for IPv6 address configuration using ND protocol.

DHCPv6 server is used to provide additional information including DNS server IP address, DNS domain and other DHCPv6 options.

For Dual stack network, two separate DHCP server are required (DHCPv4 & DHCPv6).

DHCPv6:

Terms related to DHCPv6 :

1. DHCP Client : sends request to a DHCP server to get configuration info
2. DHCP Server : configured to reply the client request
3. DHCP Relay Agent : it is configured when no DHCP server is present on Client link.
4. DHCP Unique Identifier (DUID) : Each DHCP server and clients have DUID
5. Identity Association (IA) : set of addresses assigned to client.
6. Identity Association Identifier (IAID) : is a identity chosen by Client.
7. Transaction ID : values used to match request and replies.

DHCPv6:

DHCPv6 Multicast addresses:

1. **All_DHCP_Relay_Agents_and_Server :**

   Address : #02 : : 1 : 2
   DHCP clients use this address to reach DHCP agents on their link.
   DHCP does not require link local address of agents

2. **All_DHCP_Server_Address :**

   Address : ff05 : : 1 : 3
   DHCP relay agent use this site scoped address to reach all DHCP server within a site.

DHCPv6:

DHCPv6 UDP Ports:

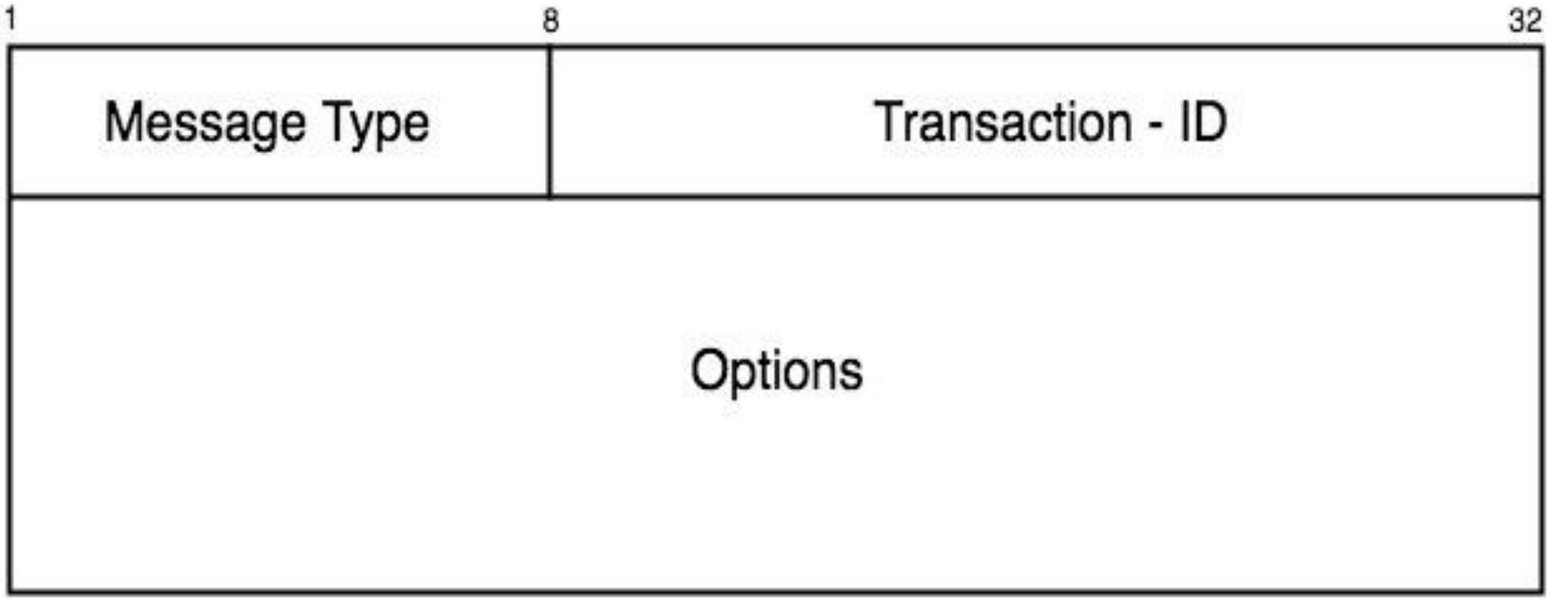
1. **UDP Port 546 - Client Port :**

   Client listen DHCP messages on this port.
   DHCP server and relay use this port as a destination port to reach to the client.

2. **UDP Port 547 - Server / Agent Port :**

   DHCP servers and relays listen DHCP request messages on this port.
   DHCP client use this port as destination port to reach the DHCP server and relays.

DHCPv6:



1

8

32

Message Type

Transaction - ID

Options

DHCPv6:

Client-Server Message Header Format:

- Message type : (1 byte) indicate type of message
- Transaction ID : (3 byte) used to troubleshoot servers. For each request, client generate a new transaction ID.
- Option : (variable length) provide configuration information and parameters
  - Option code : 2 byte tells the type of option
  - Option length : 2 byte indicate length of option
  - Option Data : variable and contain information configured for the options

DHCPv6:

Authentication Header format :

- Option code : 2 byte set to value 11
- Option length : 2 byte
- Protocol : 1 byte two kind of protocols are defined
- Algorithm : 1 byte indicate type of algorithm used
- RDM (Replay Detection Method) : 1 byte type of method used
- Replay Detection : 8 byte give replay detection information
- Authentication Information : Variable length and give detail about authentication process

IPv6
DNS

Content:

1. DNS
2. DNS Server
3. DNS Terms
4. How DNS Server work?
5. Happy Eyeball
6. DNS Security Extension

DNS:

Domain Name System (DNS) is a powerful, extensible and flexible system use for resolving name over an entire internet.

DNS use TCP port 53 and UDP port 53.

This technology make easier for the people to remember the words rather than numbers.

For example, As we want to open a web page, we type www.goggle.com instead of typing its ip address as http://2001:4860:4860::8844

DNS Server:

DNS server is a collection of computers that want to join domain name system.

They work as a team and collectively known as DNS root servers.

The internet name of this computer team is “.” (“dot”).

DNS servers are organized in a hierarchical form.

DNS root servers are the top level domain servers

DNS Terms:

1. **Domain Namespace:**

   The naming system on which DNS is based is a hierarchical and imaginary tree structure called the domain namespace.

   It includes all the possible names that could be used within a single system.

   Each node in the DNS tree represent a DNS name.

Domain Namespace:

DNS Terms:

2. **Name Server:**

It include:

DNS name server: is a computer that has DNS software installed on it. It is specifically designed for managing the different domain names.

Zone: is a container which holds the records of a single domain.

Record: is a line in a data contained by zone which maps an FQDN (fully qualified domain name) to an IP address.

DNS Terms:

IPv6 defined the two type of record type:

1. Quad A - AAAA type record : RFC 3596
2. A6 type record - RFC 2874

DNS Terms:

3. **Name Resolution:**

Name Resolution means successfully mapping a DNS domain or hostname to an IP address.

DNS can resolve name in three ways:

- By Broadcasting (Small Network)
- By locally consulting the locally stored hosts text file.
- By contacting a DNS server.

How DNS Server works?:

DNS Dual Stack Queries:

In the case of Dual stack network, when a host query a DNS server for service name by entering an URL in the browser.

The client send the two DNS request. A record and AAAA record.

The DNS can use either of them or both to answer the query according to the DNS configuration.

When client receives two address, then a address is chosen according to default address selection rules.

DNS Happy Eyeball:

It is used to improve the client experience in a dual stack network.

Defined in RFC 6555

Operation:

> When a client gets two addresses for a given service such as IPv4 and native IPv6 address.
>
> By default it connect to IPv6 address by initiating a TCP handshake.
>
> If no reply is occured of the request the the client wait for long for timeout and use IPv4 address.

DNS Happy Eyeball:

The reply not come due to the slow and broken IPv6 path.

With the implementation of Happy eyeball technology, the client can try both the protocol and then use the faster one for the communication.

DNS Security Extension:

DNS security extension (DNSSEC) is an authentication and authorization protocol to provide security to DNS server.

The DNSSEC is a suite of Internet Engineering Task Force (IETF) specifications.

DNSSEC is implemented through (Extension mechanism for DNS) EDNS

IPsec

Content:

1. Security Triads
2. Non Repudiation
3. IPsec
4. Security Association
5. Key Management

Security:

Two triads define the security standards:

1. CIA (Confidentiality, Integrity , Availability)
2. AAA (Authentication , Authorization , Accounting)

Non Repudiation is not included in the CIA and AAA triads.

Security:

Basic Security Elements:

1. **Encryption** - provide confidentiality

   Further two type of encryption: Secret Key Cryptography
   Public Key Cryptography

2. **Secure Checksum and Hash** - provide integrity

Security:

IPsec :

Specified in RFC 4301

Define the Security Architecture for both IPv6 and IPv4 version.

It create a boundary between the protected and unprotected area.

The security requirement in IPsec is defined by a security Policy Database (SPD)

Security:

IPsec : define

- Security requirements and mechanisms at the network layer
- How to use cryptographic algorithms for encryption and authentication
- Security policies and security associations between communication devices.
- Protocol for encryption (Encapsulating Security Payload)
- Protocol for authentication (Authentication Header)
- Key management

Security:

Security Association (SA) :

SA are the set of agreements between communication devices.

3 elements of agreements are : keys, Encryption or authentication and additional parameters for algorithm.

SA are unidirectional.

SA have two mode of transports:

1. Transport Mode
2. Tunnel Mode

Security:

Key Management :

IPsec use the cryptographic keys.

IKE Internet Key Exchange specifies a protocol that allow for the exchange and negotiation of parameters for SA.

- IKEv1 - Internet Key Exchange version 1
- IKEv2 - Internet Key Exchange version 2

Security:

IKEv1 - Internet Key Exchange version 1 :

Specified in RFC 2409 and updated in RFC 4109

This include 3 protocols:

1. ISAKMP (Internet Security Association and Key Management Protocol)
2. Oakley Key Determination Protocol
3. SKEME (Versatile Secure Key Exchange Mechanism for the Internet)

IKEv1 use UDP on port 500 and 4500

Security:

IKEv2 - Internet Key Exchange version 2 :

Specified in RFC 5996

Bring enhancement in the IPsec while using with NAT , for Authentication and for remote address acquisition.

Simplified use of IKE by replacing eight different initial exchange with single four message exchange.

Reduced error due to reliable protocol as all messages are sequenced and acknowledge.

IPv6 Transition

Content:

1. Transition from IP address
    - Dual Stack
    - Tunneling
    - Header translation

Transition:

To make communication possible between every device in network we need transition from IPv4 to IPv6.

Types of transition are:

1. Dual stack
2. Tunneling
3. Header Translation

Transition:

1. **Dual Stack:**

In Dual Stack, a router or a host is equipped with both IPv4 and IPv6 protocol version.

Modes of operation:

- IPv4 only node
- IPv6 only node
- IPv4 & IPv6 node

Transition:

1. **<u>Dual Stack:</u>**

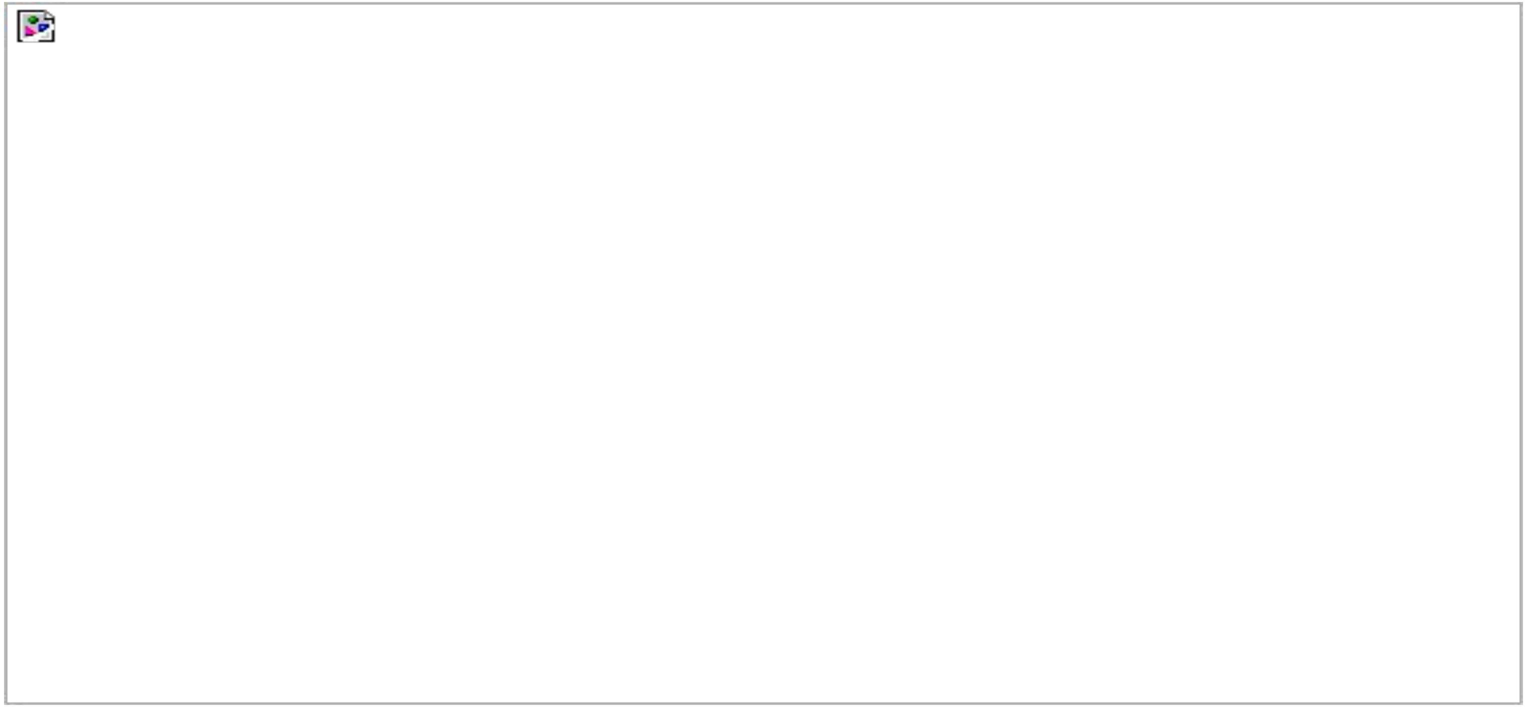
Advantage :

- Smooth shift of traffic from IPv4 to IPv6.
- No tunneling or translation is required.
- Best performance, stability and efficiency of network.

Disadvantage :

- Take more memory and CPU Power.
- Complicated Troubleshooting Process.

Transition:



Dual Stack Transition

Transition:

2. **Tunneling:**

   Tunneling is a technique in which one protocol is encapsulated in the header of another protocol.

   This is done to make the smooth transition of packets from infrastructure of another protocol.

   Components of Tunneling Process:

   - Tunnel Management
   - Encapsulation at the tunnel entry point
   - Encapsulation at the tunnel exit point

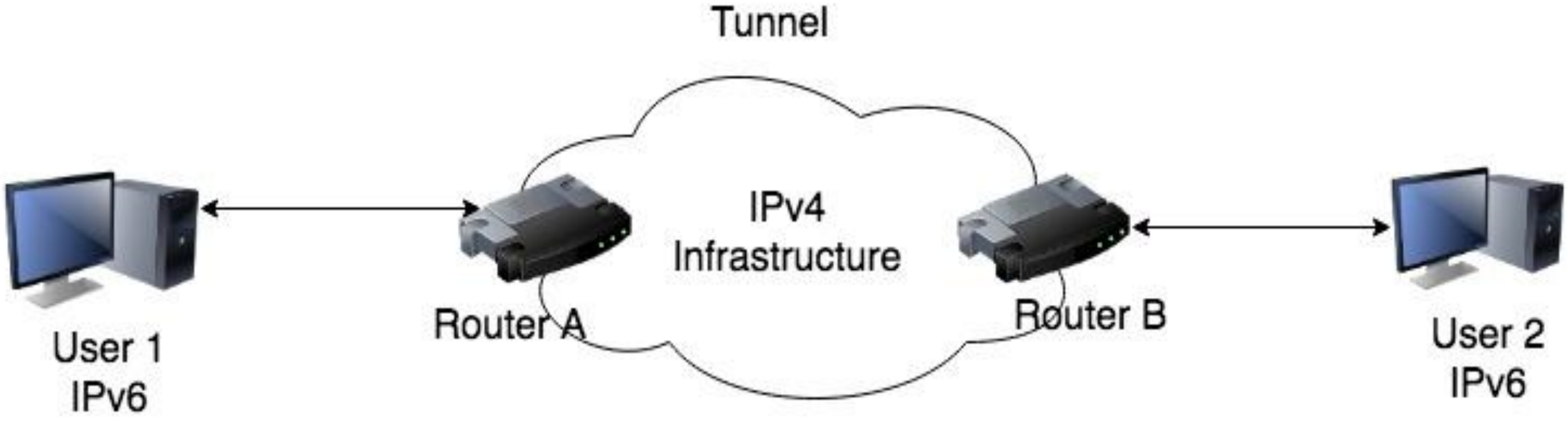
Transition:

2. **Tunneling:**

Type of Tunneling:

1. Manually Configured Tunneling
2. Automatic Tunneling

Transition:



Tunneling

Transition:

2. **Tunneling:**

   IPv6 Packet Encapsulation Steps:

   1. **Entry point of the tunnel :**
      - Decrement the Hop limit value by one
      - Encapsulate incoming packet into IPv4 header
      - Encapsulated packet transmitted the tunnel
      - Fragment IPv4 packet if necessary

Transition:

2. **Tunneling:**

IPv6 Packet Encapsulation Steps:

2. **Exit point of the tunnel :**

   - Receive the encapsulated packet
   - Check the source of the packet
   - If packet is fragmented, it reassemble it at exit point.
   - Removes the IPv4 header
   - Send IPv6 original header to destination

Transition:

3. **Header Translation:**

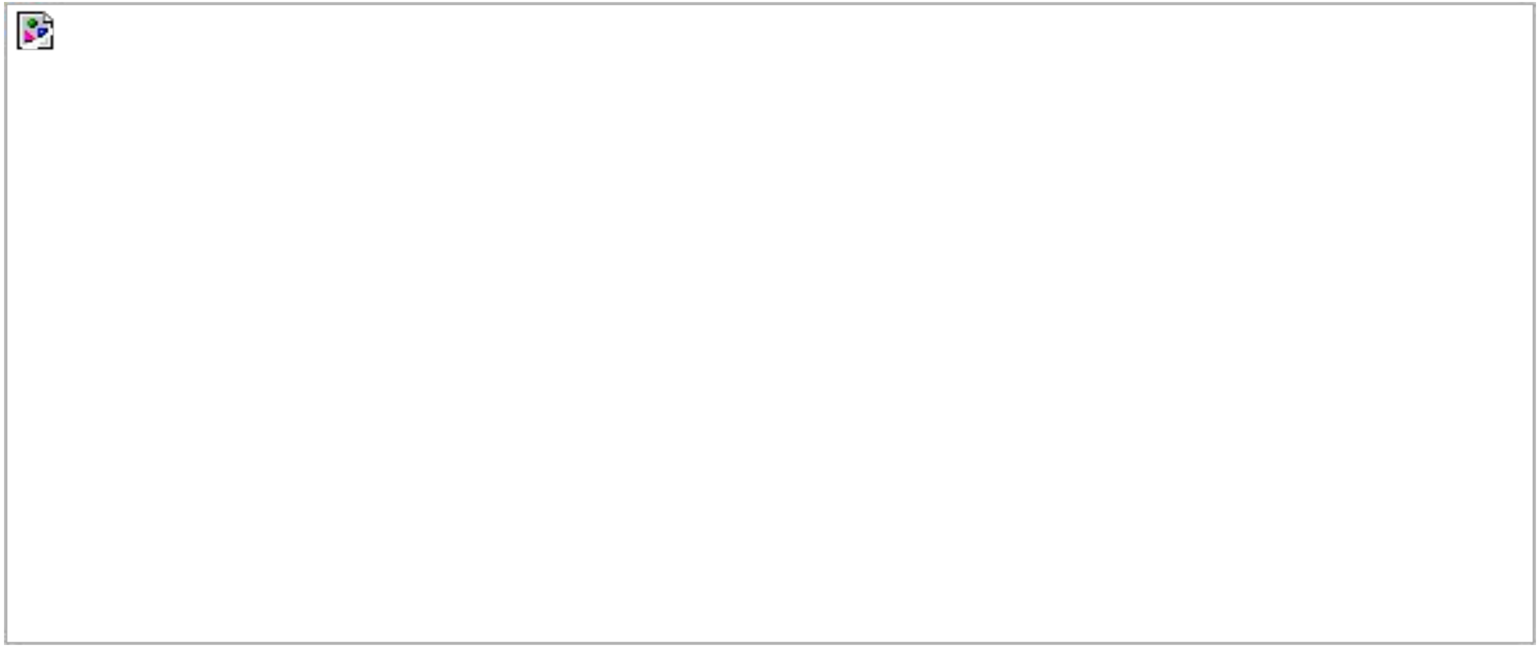
   In a network, when a transmitter device transmit a packet in IPv6 format and the receiver still work at IPv4 format.

   Then the tunneling technique will not work.

   So, header translation technique is used in which header of IPv6 packet is converted to an IPv4 packet.

   Header Translation use the mapped address to translate IPv6 to IPv4 address.

Transition from IPv4 to IPv6:



Header Translation

NAT-PT:

- Stands for Network Address Translation-Protocol Translation
- It is a protocol translation mechanism done in two directions.
- The static NAT defines a one-to-one mapping from one IP subnet to another IP subnet in each direction.
- Advantage : End devices and networks can choose any address either IPv4 addresses or IPv6 addresses and traffic run from any side.

IPv6
Based Mobile

Content:

1. Mobile IPv6
2. Features
3. Operations

Mobile IPv6:

Mobile IPv6 is an IETF standard

It is used to add roaming capabilities to mobile devices in IPv6 network.

Specified in RFC 3775

Advantage : Mobile devices attached with IPv6 can change their point-of-attachment to the IPv6 network without changing their IP address.

Mobile IPv6 is mainly targeted for mobile devices.

Mobile IPv6:

Need of Mobile IPv6:

To attain mobility for mobile devices, connections to mobile IPv6 nodes are made (without user interaction) with a specific address

It is always assigned to the mobile node, and through which the mobile node is always reachable.

Two type of address are assigned to Mobile device:

1. Home Address
2. Care of Address

Mobile IPv6:

Terms related to Mobile IPv6:

- Home subnet prefix: corresponding to a mobile node's home address.
- Home link : On which a mobile node's home subnet prefix is defined.
- Mobile node : node that can change its point of attachment from one link to another while still being reachable via its home address.
- Correspondent node : A peer node with which a mobile node is communicating.
- Home agent : A router on a mobile node's home link node

Mobile IPv6:

- Foreign subnet prefix : Any IP subnet prefix other than the mobile node's home subnet prefix.
- Foreign link : Any link other than the mobile node's home link.
- Registration : Mobile node sends a Binding Update to its home agent or a correspondent node for registration
- Binding : Association of the home address of a mobile node with a Care-of address.
- Return Routability Procedure : authorize registrations by the use of a cryptographic key exchange.

Mobile IPv6:

Mobile IPv6 uses the IPv6 features:

1. Address auto-configuration
2. Neighbor discovery
3. Extension header.

Both types of auto-configuration are used such as stateless (Network prefix + interface ID) and stateful autoconfiguration (DHCPv6).

Working of Mobile IPv6:

- When Mobile node is within the home link

  Home address is the IPv6 address As long as the mobile node is at home, it receives packets through regular IP routing mechanisms

- When the mobile node is away from home on a foreign link:

  it has an Care-of address. It receives the Care-of address through regular IPv6 mechanisms such as SLAAC (Stateless Address Autoconfiguration) or DHCPv6 when connecting to the new link.

Mobile IPv6:

Proxy Mobile IPv6:

Network-based mobility management protocol

Standardized by IETF and specified in RFC 5213.

It is a protocol for building a common and access technology independent of mobile core networks,

It accommodate various access technologies such as WiMAX, 3GPP, 3GPP2 and WLAN based access architectures.