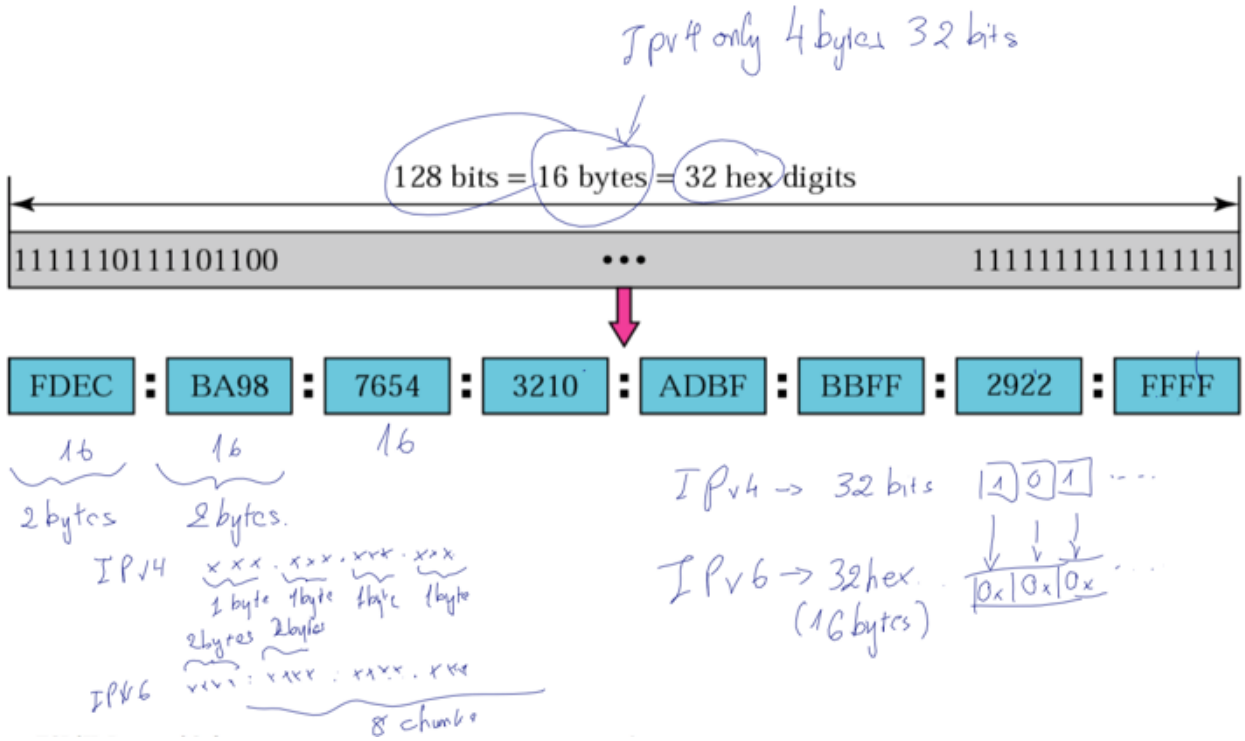
Chapter 04 - IPv6

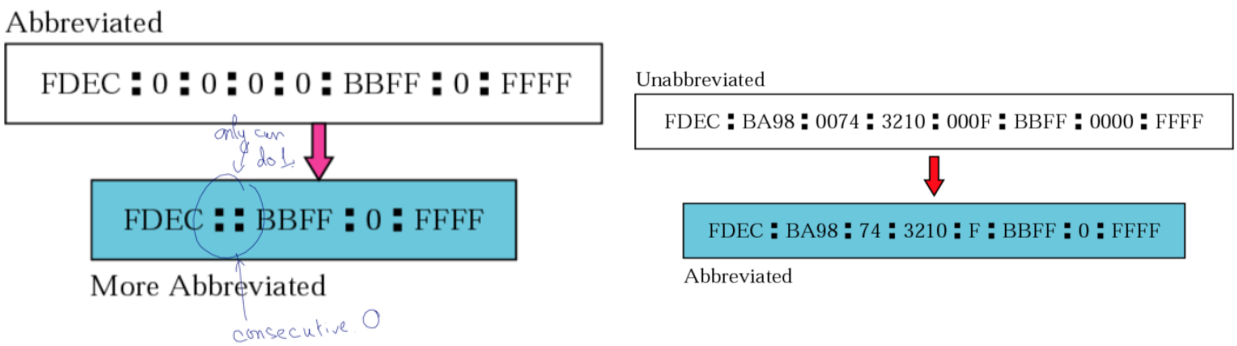
IPv6 Protocol

IPv6 Addresses

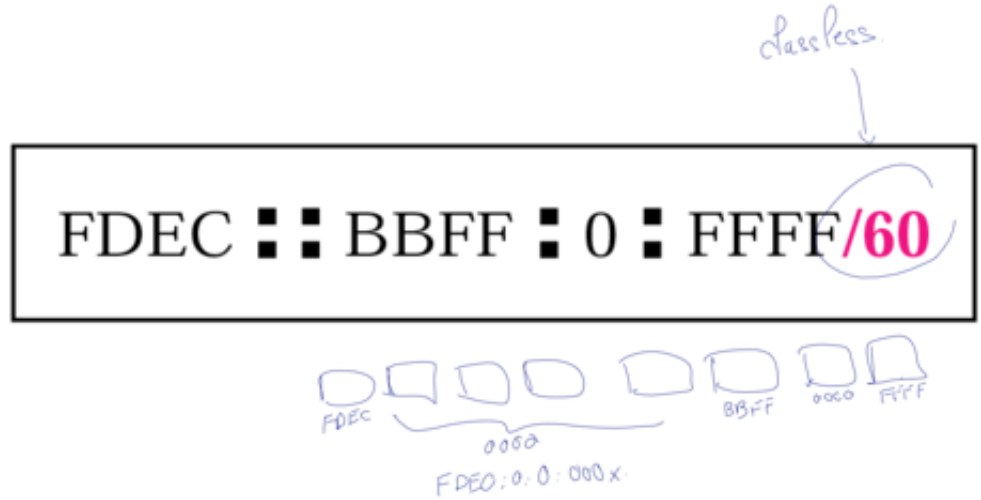
- The IP address in IPv6 is 128-bit long, which is or 32 hex digits, or 16 bytes.
  - The address is broken down to 8 chunks, each has **4 hex digits**. (Note: each hex digit represents 4 bits, so 2 hex digits represent 1 byte, 4 hex digits = 2 bytes)



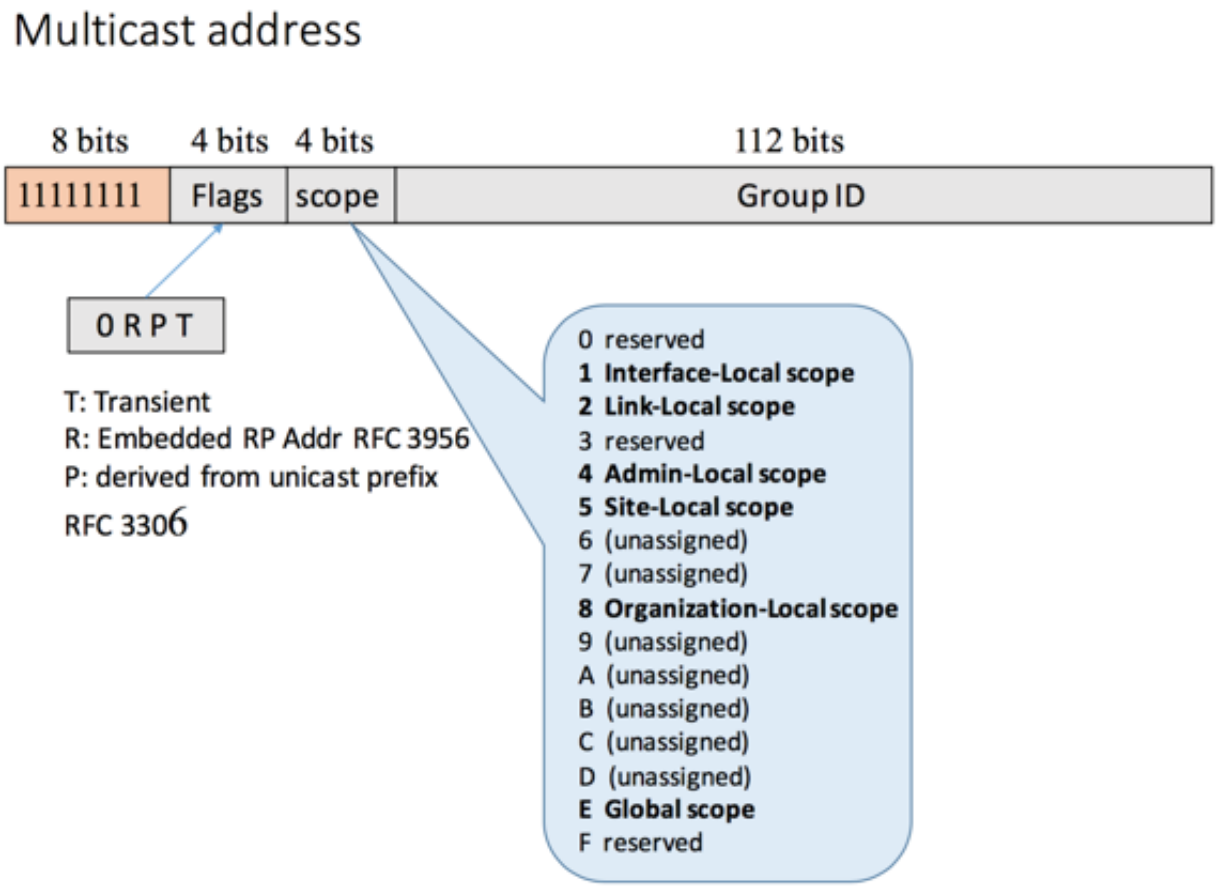
- The address can be abbreviated (shorten) for '0' values.



- IPv6 is classless, i.e. class defined by /x.



- **Address Type**
  - **Unspecified** is an IPv6 address in the block of ::/128, all 0s, equivalent to **0.0.0.0 in IPv4**, only used for source address.
  - **Loopback** is an IPv6 address in the block of ::1/128, used for the loopback address of the local host which is the **equivalent of the 127.0.0.1 in IPv4**.
  - **Multicast** is an IPv6 address in the block of FFxx::/8, prefixed with 1111 1111, then followed by 4 flag bits, and 4 scope bits, and then the 112 bits group ID of devices that subscribe to receive the packets. It is equivalent to **224.0.0.0/4 in IPv4**. IP Multicast is a method of **sending data to a group of hosts in a single transmission**. The same IP Multicast Address is used for both the sending host & the receiving hosts. Sending host would use it as the destination to send the message to while the receiving hosts use it to subscribe to or in other words, inform the network that they want to receive the message sent to that multicast address.



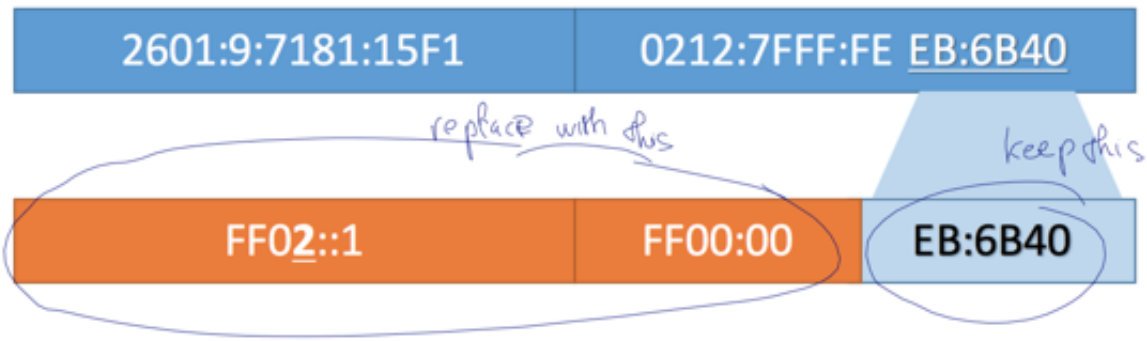
- Group ID of the **well known IPv6 Multicast**

Well-known IPv6 multicast addresses

Address	Description
FF02::1	All nodes on the local network segment
FF02::2	All routers on the local network segment
FF02::5	OSPFv3 All SPF routers
FF02::6	OSPFv3 All DR routers
FF02::8	IS-IS for IPv6 routers
FF02::9	RIP routers
FF02::A	EIGRP routers
FF02::D	PIM routers
FF02::16	MLDv2 reports (defined in RFC 3810)
FF02::1:2	All DHCP servers and relay agents on the local network segment (defined in RFC 3315)
FF05::1:3	All DHCP servers on the local network site (defined in RFC 3315)

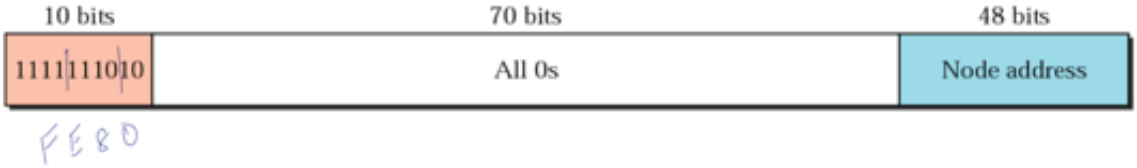
- **Solicited-Node Multicast Address**: to have a solicited node multicast address (for each of its configured unicast or anycast address), takes the last 24 bits of its IPv6 Unicast or Anycast address and append to FF02::1:FF00:00/104.

Taking the last 24 bits of IPv6 Unicast or Anycast address and append to FF02::1:FF00:0/104

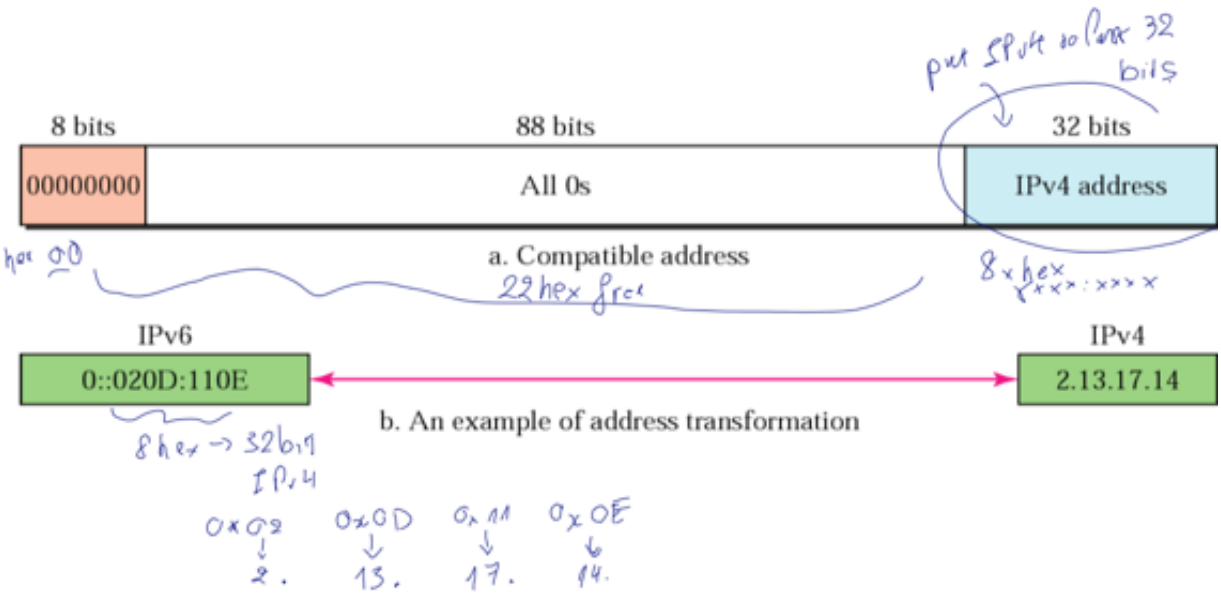


A host is required to join a Solicited-Node multicast group for each of its configured unicast or anycast addresses

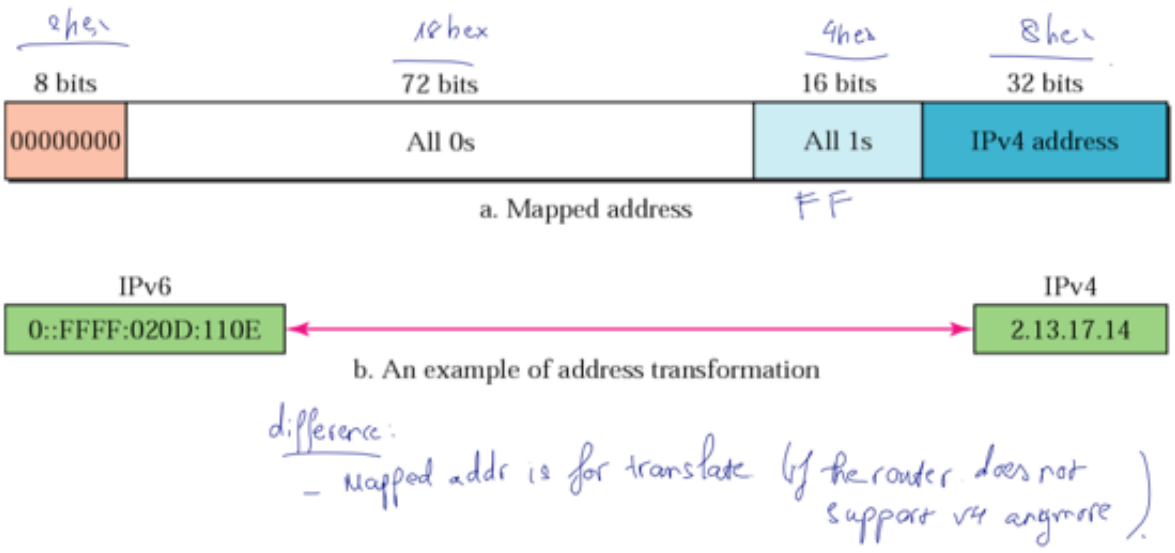
- **Link Local Unicast** is an IPv6 address in the block of FE80::/10, prefixed with 1111 1110 10. If a host doesn't have any IP address assigned and also failed to receive a DHCP address, the host gets assigned an address within the **169.254.0.0/16 block in IPv4**, which is **equivalent to IPv6 link local address, FE80::/10 prefix**.



- **Compatible address**: stores the 32bit IPv4 address in the last 32 bits (8 hex, 2 chunks), probably deprecated over Mapped address.



- **Mapped address**: is a mechanism to represent IPv4 address in a v6. With this mechanism, the application need only do a listen using the IPv6 API, and it can accept both IPv4 and IPv6 connections through the same API. If the destination address in the sockaddr structure is a mapped address, it'll go through the IPv4 stack, otherwise it'll use the IPv6 stack.



- **Unique Local Address** (ULA) is an IPv6 address in the block of FC00::/7, is the approx **IPv6 counterpart of IPv4 private address** (192.168, 172.0, 10.0)
- **Global Unicast Address** is a public routable address, obtained by registering through

ICANN. It **contains 48 bits global routing prefix** (similar to subnet mask, a numerical value written in CIDR notation that we use to determine how many bits counting from the left are used for the network/subnet portion of the IP address), followed by 16 bit subnet and 64 bit interface ID.

48 bits	16 bits	64 bits
Global Routing Prefix	Subnet	Interface ID
2000:0000:0000	0000	0000:0000:8190:3426

- The **48 bit global routing prefix** is broken up into 4 chunks, to identify major site:
  - **Prefix** (3 bits): all set to 1s.
  - **TLA ID** (top level aggregator ID - 13 bits): Allocate to ISP level.
  - **Reserved block** (8 bits): reserved for future.
  - and **NLA ID** (Next Level Aggregator ID - 24 bits).

3 bits	13 bits	8 bits	24 bits
Prefix	TLA ID	Reserved	NLA ID

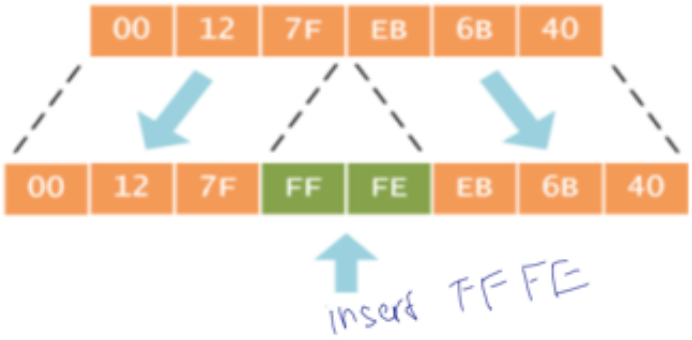
- **16 bits Subnet ID** & **64 bits Interface ID** is for used within the organization

Summary

Name	Prefix	IPv6	IPv4 Equivalent
Unspecified		`::/128`	0.0.0.0
Loopback		`::1/128`	127.0.0.1
Multicast	`FF00`	`FF00::/8`	224.0.0.0/4
Link Local Unicast	`FF80`	`FF80::/10`	169.254.0.0/16
Mapped address	`0::FFFF`	`0::FFFF:{4hex}:{4hex}` (last 8 hex is 32 bit IPv4 IP address)	Any IPv4 address
Unique Local Address	`FC00`	`FC00::/7`	10.0., 172.0., 192.168.

EUI-64

- A 64-bit interface identifier is most commonly derived from its 48-bit MAC address. A MAC address 00:0C:29:0C:47:D5 is turned into a 64-bit EUI-64 by inserting FF:FE in the middle: 00:0C:29:FF:FE:0C:47:D5.



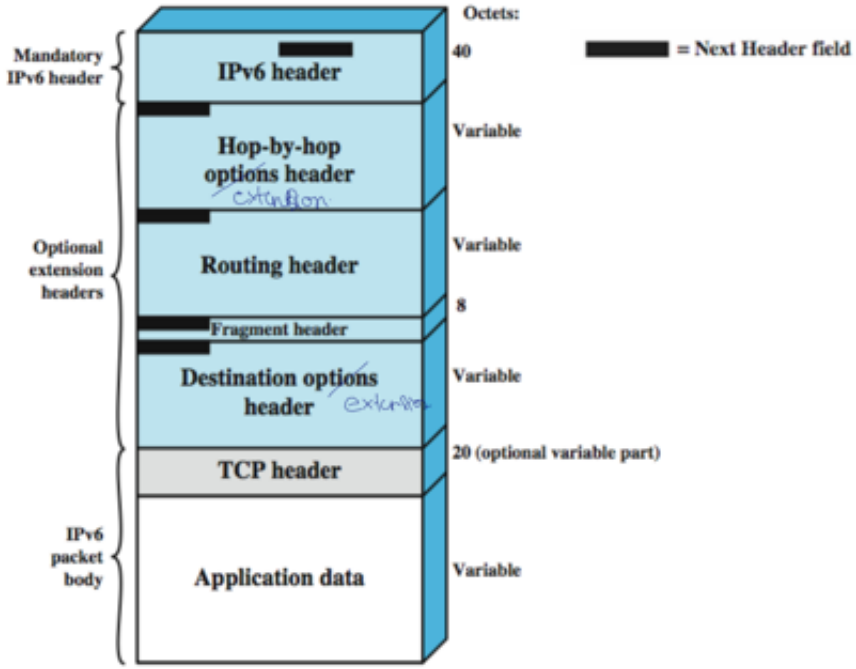
- And invert the 7th bit (Universal/Local flag)

3 types of IPv6 Addresses

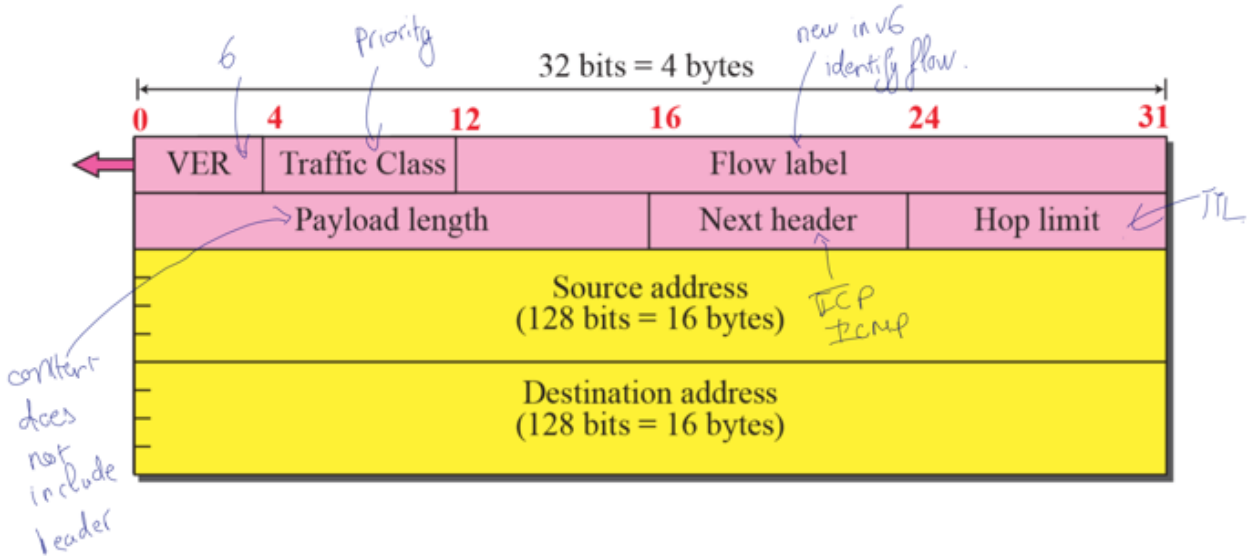
- Unicast: to a single interface
- Anycast: to an interface of the group/set
- Multicast: to all interfaces of the group/set

IPv6 Datagram Structure

IPv6 Packet (PDU) Structure

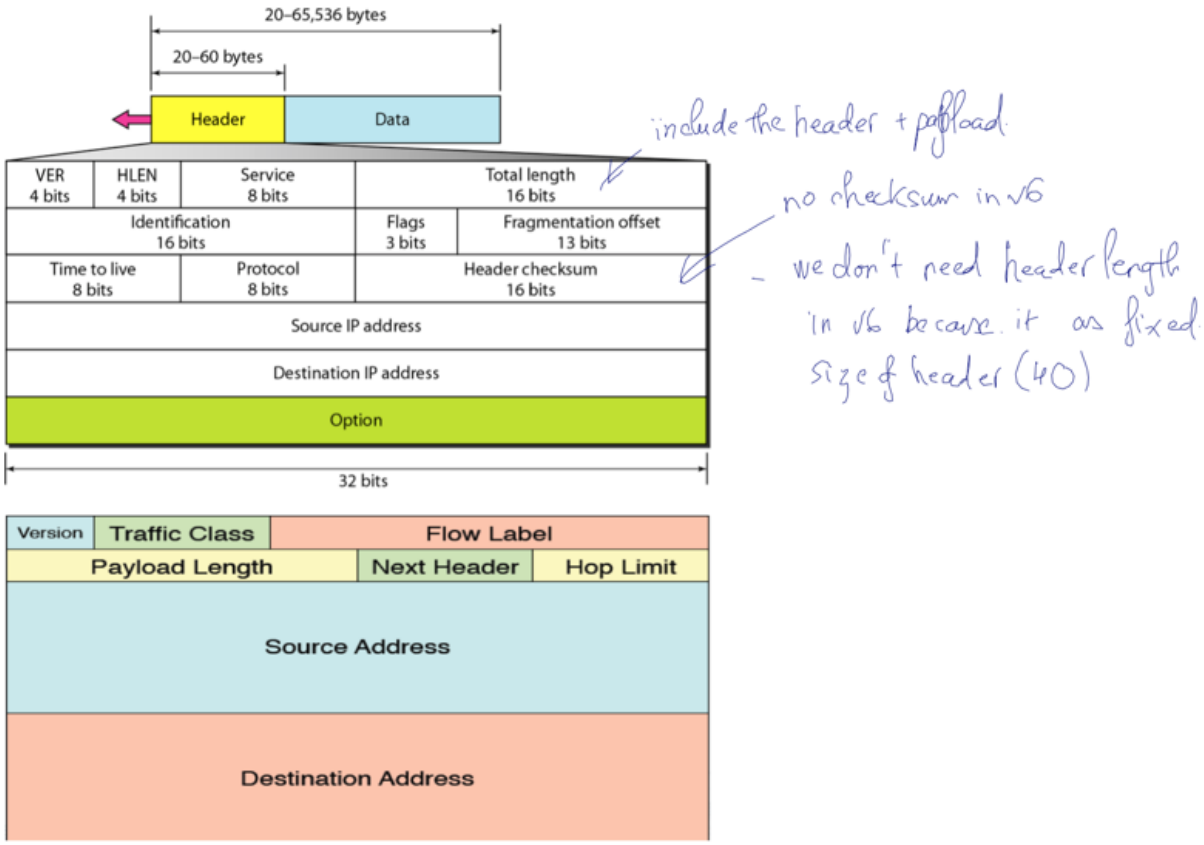


- **IPv6 Header**

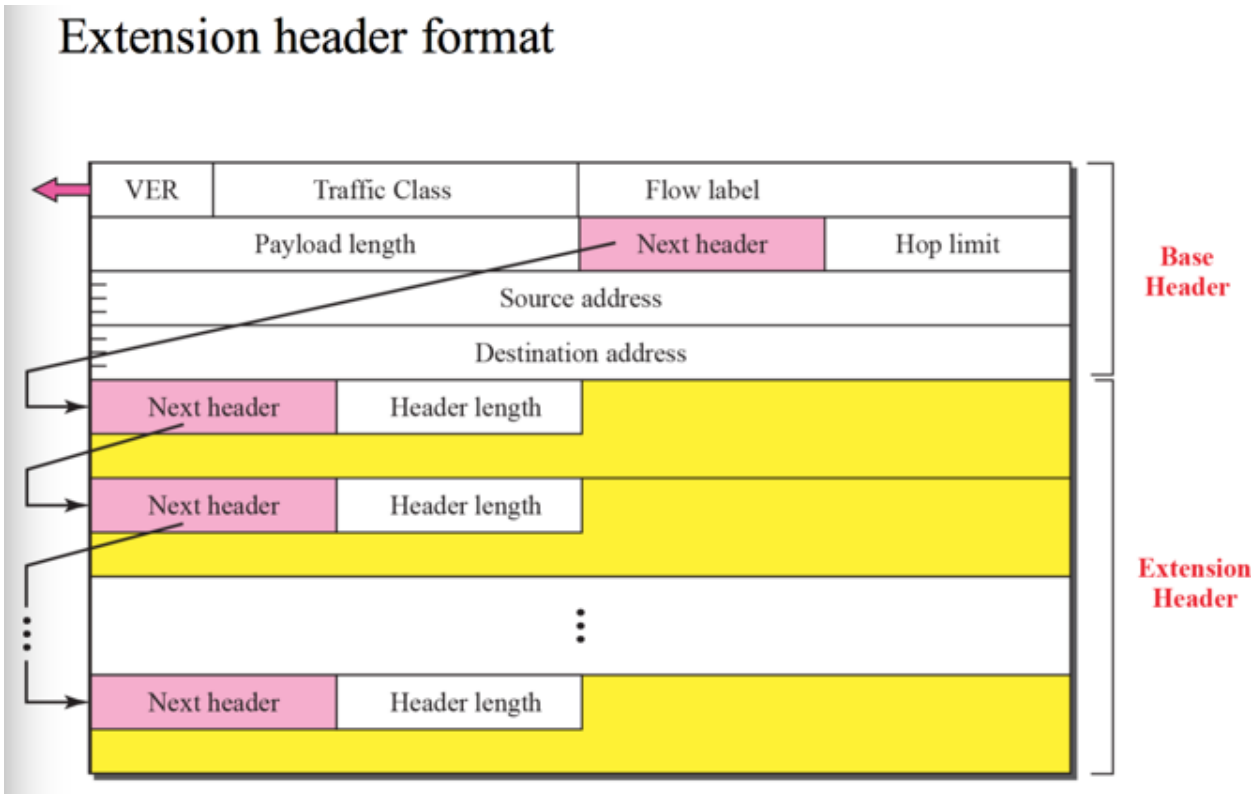


- **Compare IPv4 and IPv6 Headers**

IPv4 and IPv6 Header



- IPv6 Extension Header



- **Protocol Number for Extension Header**

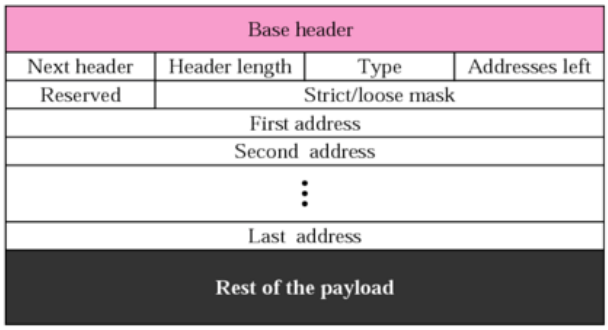
Extension Header

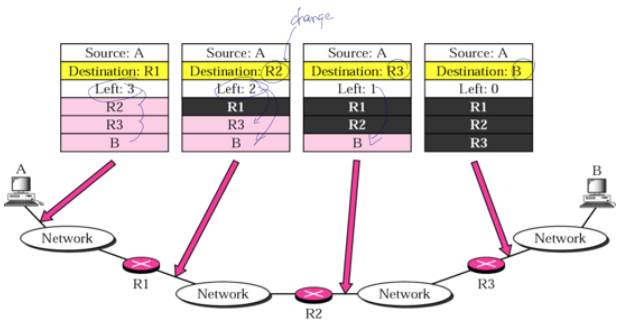
Extension Header	Type	Description
Hop-by-Hop Options	0	Options that need to be examined by all devices on the path.
Destination Options (before routing header)	60	Options that need to be examined only by the destination of the packet.
Routing	43	Methods to specify the route for a datagram (used with Mobile IPv6).
Fragment	44	Contains parameters for fragmentation of datagrams.
Authentication Header (AH)	51	Contains information used to verify the authenticity of most parts of the packet.
Encapsulating Security Payload (ESP)	50	Carries encrypted data for secure communication.
Destination Options (before upper-layer header)	60	Options that need to be examined only by the destination of the packet.
Mobility (currently without upper-layer header)	135	Parameters used with Mobile IPv6.

Next header codes

Code	*Next Header*
0	Hop-by-hop option
58	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (No next header)
60	Destination option

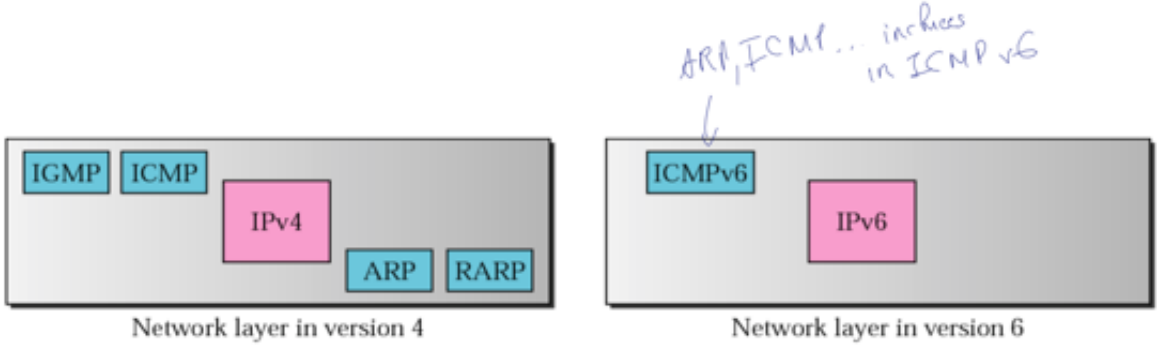
- Source Routing (Extension Header)





ICMPv6

- in IPv6 network layer, all ARp, IGMP... is merged into ICMPv6.



- ICMP protocol is 1 in v4, and 58 in v6.
- ICMPv6 protocol used for reporting errors, performing diagnostics (ICMP), perform Neighbor Discovery, report multicast memberships (IGMP), and ARP.
- There are **2 categories of ICMP messages**: Error Reporting, and Query.
  - **Error Reporting** (type value from 0 to 127): to provide feedback to a source Destination Unreacheable, Packet too big (NEW - needed in IPv6 and not IPv4 because IPv4 does fragmentation while IPv6 does not), Time exceeded, Parameter Problems, Redirection.

Error messages

Type	Description	References
1	Destination unreachable	RFC 2463
2	Packet too big	RFC 2463
3	Time exceeded	RFC 2463
4	Parameter problem	RFC 2463

Comparison of error-reporting messages in ICMPv4 and ICMPv6

Type of Message	*Version 4*	*Version 6*
Destination unreachable	Yes	Yes
Source quench	Yes	No
Packet too big	No	Yes
Time exceeded	Yes	Yes
Parameter problem	Yes	Yes
Redirection	Yes	Yes

  - **Query** (type value from 128 to 255): Echo (request/reply), router solicitation and advertisement, neighbor solicitation and advertisement, group membership. Comparison of Query Msg in ICMPv4 v/s ICMPv6:

Informational messages

Type	Description	References
128	Echo request.	RFC 2463
129	Echo reply.	RFC 2463

Type of Message	*Version 4*	*Version 6*
Echo request and reply	Yes	Yes
Timestamp request and reply	Yes	No
Address mask request and reply	Yes	No
Router solicitation and advertisement	Yes	Yes
Neighbor solicitation and advertisement	ARP	Yes
Group membership	IGMP	Yes

Path MTU Discovery for IPv6

Differences between MTU in IPv4 v/s IPv6

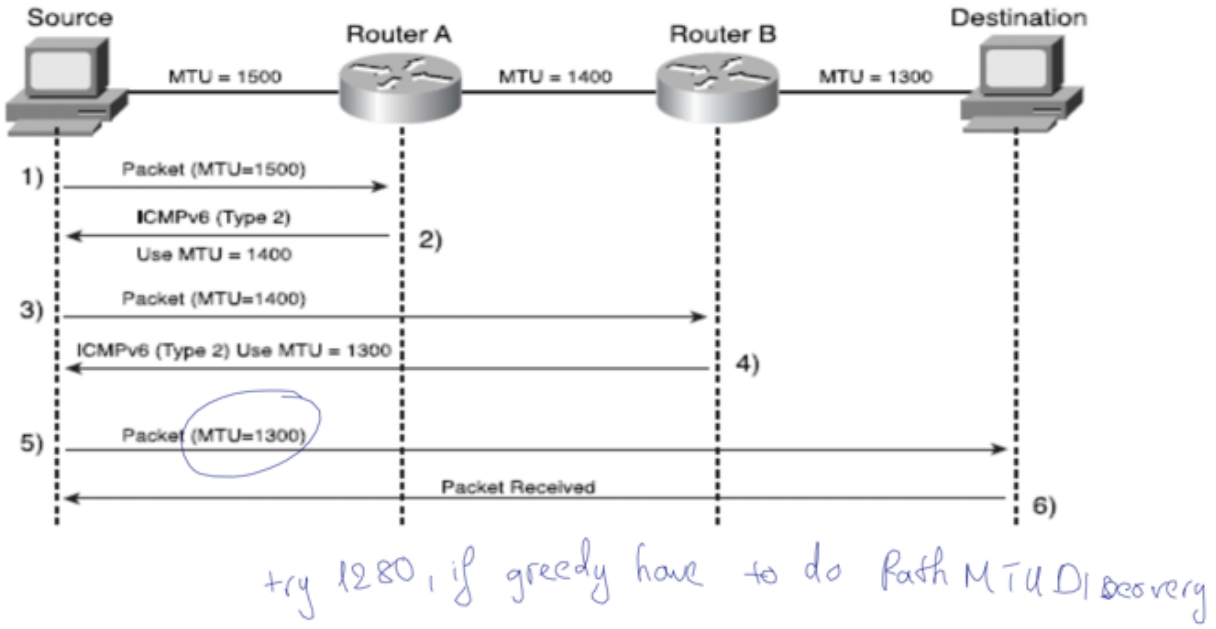
- Increase default MTU in IPv6 to 1280 bytes, was 576 bytes in IPv4.
- No En Route Fragmentation in IPv6 in routers (source node can).
- MTU Size Error Feedback is created (since there is no fragmentation in IPv6).
- the fragmentation section in IPv4 (2nd row in the header) becomes optional Fragment extension header in IPv6.

Path MTU Discovery Process

- Since there is no more En Route Fragmentation, the source needs to have a mechanism to decide what size to use. It can use Default MTU = 1280, or using Path MTU Discovery feature to **discover the minimal MTU on a path** to a particular destination.

1. The sending node assumes that the path MTU is the link MTU of the interface on which the traffic is being forwarded.
2. The sending node sends IPv6 packets at the **path MTU size**.
3. If a router on the path is unable to forward the packet over a link with a link MTU that is smaller than the size of the packet, it discards the IPv6 packet and sends an **ICMPV6 Packet Too Big message back to the sending node**. The ICMPV6 Packet Too Big message contains the link MTU of the link on which the forwarding failed.
4. The sending node sets the path MTU for packets being sent to the destination to the value of the MTU field in the ICMPv6 Packet Too Big message.
5. The sending node starts again at step 2 and repeats steps 2 through 4 for as many times as are necessary to discover the path MTU.

Flow Diagram:



IPv6 NDP (Neighbor Discovery Protocol)

Definition

IPv6 ND is a **set of messages and process that determine relationship between neighboring nodes**, in replacement of ARP, ICMP Router Discovery, and ICMP Redirect in IPv4.

- Host Router Discovery Functions
  - Router Discovery: find out which routers on the local network.
  - Prefix Discovery: to determine what network they are on.
  - Parameter Discovery: to find out parameters such as MTU of local links
  - Address Auto-configuration: to be able to configure automatically base on info provided by the router.
- Host-Host Communication
  - Address Resolution (ARP): determines the MAC address from IP address.
  - Next-Hop Determination: looking for the next destination address of an IP datagram.
  - Duplicate Address Detection (**DAD**): determine if an address already exists on the network.

Mechanism

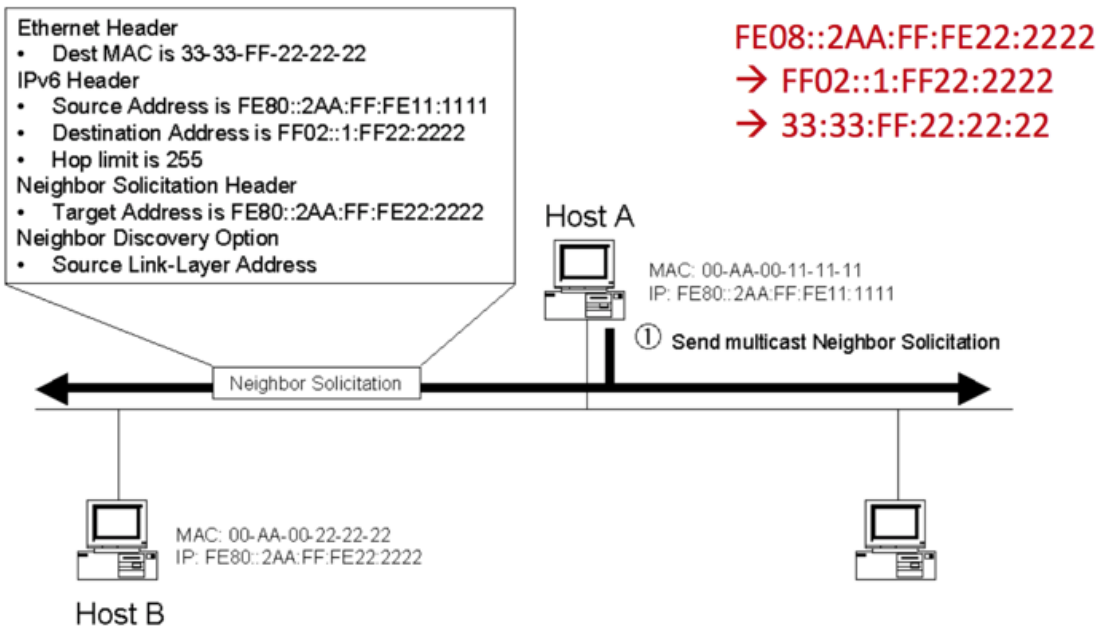
IPv6 NDP uses ICMPv6 control messages for various purposes:

1. ***RS- Router Solicitation* Messages (ICMPv6 Type 133)**
   - Sent by hosts to request that any local routers send a *Router Advertisement* message so they don't have to wait for the next regular advertisement message.
2. ***RA - Router Advertisement Messages (ICMPv6 Type 134)***
   - Sent regularly by routers to tell hosts that they exist and provide important prefix and parameter information to them.
3. ***NS - Neighbor Solicitation Messages (ICMPv6 Type 135)***
   - Sent to verify the existence of another host and to ask it to transmit a Neighbor Advertisement.
4. ***NA - Neighbor Advertisement* Messages (ICMPv6 Type 136)**
   - Sent by hosts to indicate the existence of the host and provide information about it.
5. ***Redirect* Messages (ICMPv6 Type 137)**
   - Sent by a router to tell a host of a better method to route data to a particular destination.

https://youtu.be/A3LFt7CHpgs

Example - Address Resolution

The multicast Neighbor Solicitation for address resolution



The unicast Neighbor Advertisement for address resolution