Unit - V

UNIT – V: Internet Protocol Version 6

Introduction - Advantages of IPv6 - IPv6 addressing format - IPv6 header - IPv6 extension headers - ICMPv6

IPv6 - Introduction

- ✓ Several reasons for the need of a new protocol, Internet Protocol version 6 (IPv6).
  - The main reason was the address depletion.
  - Other reasons are related to the slowness of the process due to some unnecessary processing, the need for new options, support for multimedia, and the desperate need for security.

Comparison between IPv4 and IPv6 Headers

IPv4	IPv6
Source and destination address are 32bits or 4Bytes Example: 192.168.0.1	Source and destination address are 128bits or 16Bytes Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
Header contains checksum	Header does not contains checksum
Header contains options	All optional data in moved to IPv6 extension headers
Broadcast addresses are used to send packets to all nodes on a subnet.	No Broadcast addresses, Instead link local scope all nodes multicast address is used.
Manual or DHCP based IP configuration.	Nodes are capable of auto configuration.
Fragmentation is done by sending host and also router which slows down the process.	Fragmentation is done only by the sender of the packet.
IPSec header support is optional	IPSec header support is required.
No identification of packet flow in IP header.	Flow label field is used to identify the packet flow and prioritized delivery
ARP is used to find link-layer address for IPv4 address.	ARP request is replace with multicast Neighbor Solicitation messages.
IGMP is used to manage local subnet group membership	IGMP is replaced with Multicast Listener Discovery (MLD)

Advantages of IPv6

- ✓ **Larger address space:** An IPv6 address is 128 bits long. Compared with the 32-bit address of IPv4, this is a huge (296 times) increase in the address space.
- ✓ **Better header format:** IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
- ✓ **New options:** IPv6 has new options to allow for additional functionalities.
- ✓ **Allowance for extension:** IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
- ✓ **Support for resource allocation:** In IPv6, the type-of-service field has been removed, but two new fields, traffic class and flow label have been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.
- ✓ **Support for more security:** The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

IPv6 addressing format

- ✓ An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.
- ✓ For example, given below is a 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

0010000000000001 0000000000000000 0011001000111000 1101111111100001
0000000001100011 0000000000000000 0000000000000000 1111111011111011

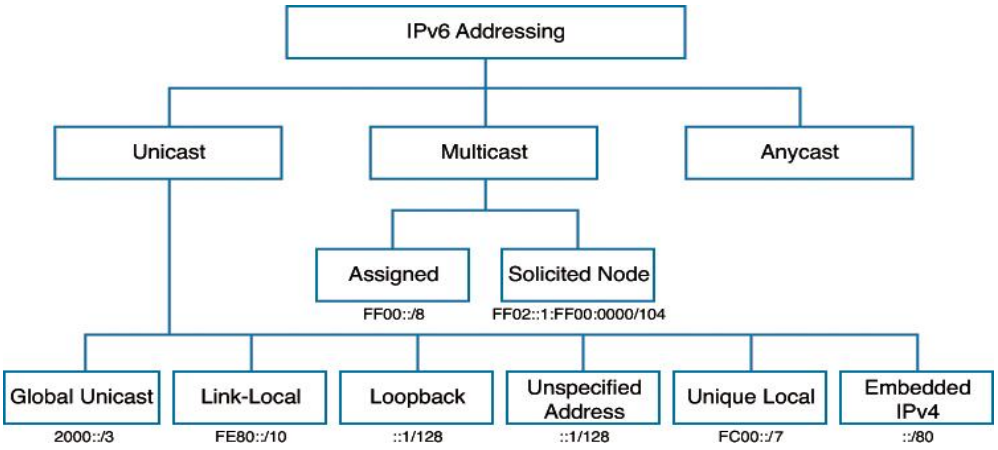
- ✓ Each block is then converted into Hexadecimal and separated by ':' symbol:

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

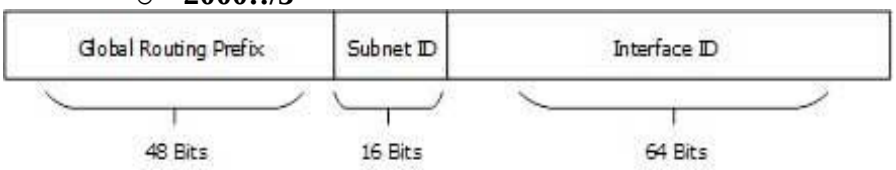
- ✓ Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:
  - Rule.1: Discard leading Zero(es):
    - In Block 6, 0036, the leading two 0s can be omitted, such as (6th block):
    - 2001:0000:3238:DFE1:1263:36:0000:FEFB
  - Rule.2: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):
    - 2001:0000:3238:DFE1:1263::FEFB
  - Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):
    - 2001:0:3238:DFE1:1263::FEFB
    -
- ✓ **IPv6 Address Types:**
  - IPv6 has three types of addresses, which can be categorized by type and scope:
    - **Unicast addresses:** A packet is delivered to one interface.
    - **Multicast addresses:** A packet is delivered to multiple interfaces.

- **Anycast addresses:** A packet is delivered to the nearest of multiple interfaces (in terms of routing distance).

- IPv6 does not use broadcast messages.

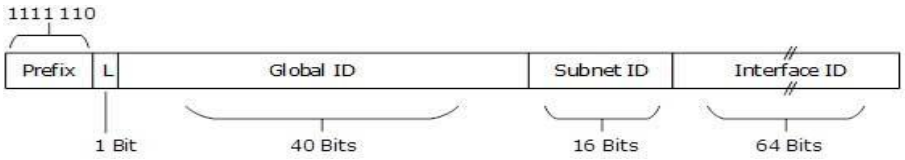


- **<u>Unicast addresses:</u>**
  - A single unique address identifying an IPv6 interface. Further classified into the following:
  - **Global Unicast Address**
    - This address type is equivalent to IPv4's public address. Global Unicast addresses in IPv6 are globally identifiable and uniquely addressable.
      - **2000::/3**



  - **Link-Local Address**
    - Auto-configured IPv6 address is known as Link-Local address. This address always starts with FE80. The first 16 bits of link-local address is always set to 1111 1110 1000 0000 (FE80). The next 48-bits are set to 0.
      - **FE80::/10**

  - **Unique-Local Address**
    - This type of IPv6 address is globally unique, but it should be used in local communication. The second half of this address contains Interface ID and the first half is divided among Prefix, Local Bit, Global ID and Subnet ID.
      - **FC00::/7**



- Prefix is always set to 1111 110. L bit, is set to 1 if the address is locally assigned. So far, the meaning of L bit to 0 is not defined. Therefore, Unique Local IPv6 address always starts with 'FD'.

- **Unspecified Address:**
  - An IPv6 address with all 128 bits set to zero is called the unspedified adddress (which correspond to 0.0.0.0 in IPv4). This address should not be assigned to any host and it should only be used as the source address by initializing host before it has learned of its own address. If a host listens for incoming connection on this address, it means that the host and/or its application is listening on all interfaces belong to that host.
    - **::/128**
- **Loopback Address:**
  - **::1/128**
  - It is the loopback address of the local host which is the equivalent of the 127.0.0.1 in IPv4. When an application in a specific host sends a data packet to this address, the TCIP/IP stack will loop the packet back on the same interface it was sent to so the packet never exits that host.
  - The first 127 bit of the loopback address is set to all 0's and the last bit set to 1 resulting an IP address that takes the form of 0:0:0:0:0:0:0:1:/128 or ::1/128 for short.

- **Multicast addresses:**
  - An identifier for a group of interfaces.
    - Usually belonging to more than one node .
    - Interfaces may belong to more than one multicast group.
    - Replaces broadcasts.
    - May not be used as a source address.
    - Some common IPv6 multicast addresses are the following:

Address	Description	Available Scopes
ff0X::1	All nodes address, identify the group of all IPv6 nodes	Available in scope 1 (interface-local) and 2 (link-local): • ff01::1 → All nodes in the interface-local • ff02::1 → All nodes in the link-local
ff0X::2	All routers	Available in scope 1 (interface-local), 2 (link-local) and 5 (site-local): • ff01::2 → All routers in the interface-local • ff02::2 → All routers in the link-local • ff05::2 → All routers in the site-local
ff02::5	OSPFIGP	2 (link-local)
ff02::6	OSPFIGP Designated Routers	2 (link-local)

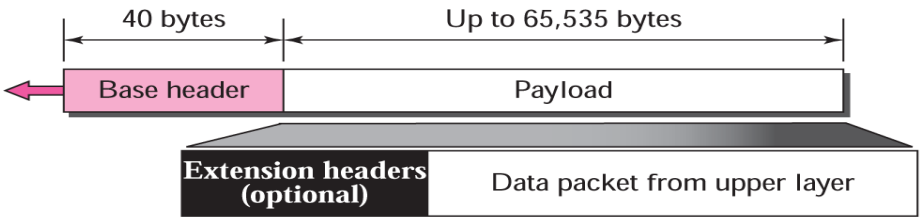
ff02::9	RIP Routers	2 (link-local)
ff02::a	EIGRP Routers	2 (link-local)
ff02::d	All PIM Routers	2 (link-local)
ff02::1a	All RPL Routers	2 (link-local)
ff0X::fb	mDNSv6	Available in all scopes
ff0X::101	All Network Time Protocol (NTP) servers	Available in all scopes
ff02::1:1	Link Name	2 (link-local)
ff02::1:2	All-dhcp-agents	2 (link-local)
ff02::1:3	Link-local Multicast Name Resolution	2 (link-local)
ff05::1:3	All-dhcp-servers	5 (site-local)
ff02::1:ff00:0/104	Solicited-node multicast address.	2 (link-local)
ff02::2:ff00:0/104	Node Information Queries	2 (link-local)

- **Anycast addresses:**
  - An IPv6 address that is assigned to more than one interface (typically more than one node).
    - Same as Unicast addresses
    - Derived from the same address space
    - Packets destined for anycast address are delivered to the "nearest" interface
    - Subnet router anycast address definition

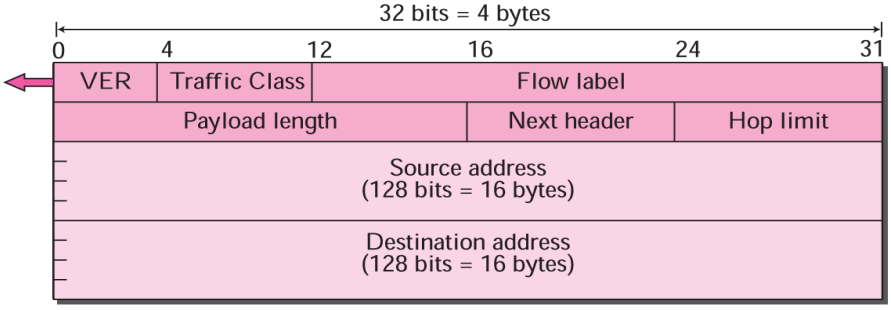
IPv6 Header

- ✓ The IPv6 packet is shown in below. Each packet is composed of a mandatory base header followed by the payload.
- ✓ The payload consists of two parts:
  - optional extension headers and
  - data from an upper layer.
- ✓ The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 bytes of information.

- ✓ IPv6 datagram



✓ Format of the base header



- These fields are as follows:
  - **Version:** This 4-bit field defines the version number of the IP. For IPv6, the value is 6.
  - **Traffic Class:** This 8-bit field is used to distinguish different payloads with different delivery requirements. It replaces the service class field in IPv4.
  - **Flow label:** The **flow label** is a 20-bit field that is designed to provide special handling for a particular flow of data.
  - **Payload length:** The 2-byte payload length field defines the length of the IP datagram excluding the base header.
  - **Next header:** The **next header** is an 8-bit field defining the header that follows the base header in the datagram. The next header is either one of the optional extension headers used by IP or the header of an encapsulated packet such as UDP or TCP.

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

  - **Hop limit:** This 8-bit **hop limit** field serves the same purpose as the TTL field in IPv4.
  - **Source address:** The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram.
  - **Destination address:** The destination address field is a 16-byte (128-bit) Internet address that usually identifies the final destination of the datagram. However, if source routing is used, this field contains the address of the next router.

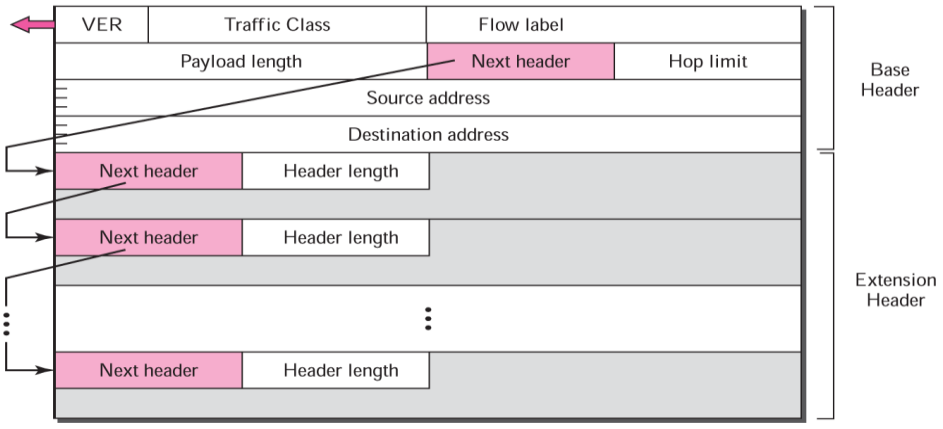
✓ **Flow Label:**
- In version 6, the flow label has been directly added to the format of the IPv6 datagram to allow us to use IPv6 as as connection-oriented protocol.
- To a router, a flow is a sequence of packets that share the same characteristics, such as traveling the same path, using the same resources, having the same kind of security, and so on. A router that supports the handling of flow labels has a flow label table.

- The table has an entry for each active flow label; each entry defines the services required by the corresponding flow label. When the router receives a packet, it consults its flow. It then provides the packet with the services mentioned in the entry.

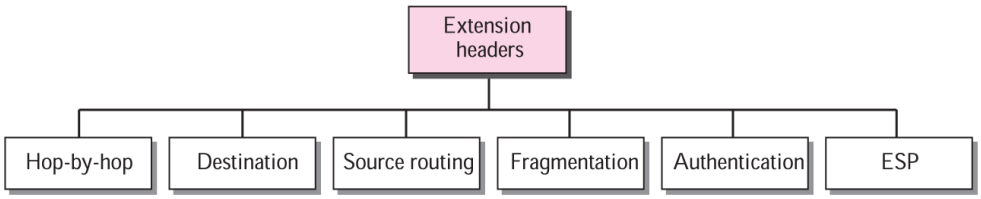
- In its simplest form, a flow label can be used to speed up the processing of a packet by a router. When a router receives a packet, instead of consulting the routing table and going through a routing algorithm to define the address of the next hop, it can easily look in a flow label table for the next hop label table to find the corresponding entry for the flow label value defined in the packet. It then provides the packet with the services mentioned in the entry.
- In its more sophisticated form, a flow label can be used to support the transmission of real-time audio and video. Real-time audio or video, particularly in digital form, requires resources such as high bandwidth, large buffers, long processing time, and so on.
- The use of real-time data and the reservation of these resources require other protocols such as Real-Time Protocol (RTP) and Resource Reservation Protocol (RSVP) in addition to IPv6.
- To allow the effective use of flow labels, three rules have been defined:
  1. The flow label is assigned to a packet by the source host. The label is a random number between 1 and 2^{24}– 1. A source must not reuse a flow label for a new flow while the existing flow is still alive.
  2. If a host does not support the flow label, it sets this field to zero. If a router does not support the flow label, it simply ignores it.
  3. All packets belonging to the same flow have the same source, same destination, same priority, and same options.

IPv6 extension headers

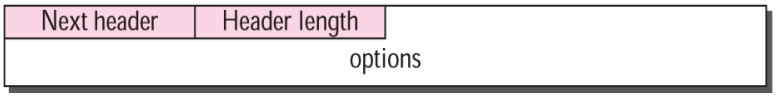
✓ The length of the base header is fixed at 40 bytes. However, to give more functionality to the IP datagram, the base header can be followed by up to six extension headers. Many of these headers are options in IPv4. Figure shows the extension header format.



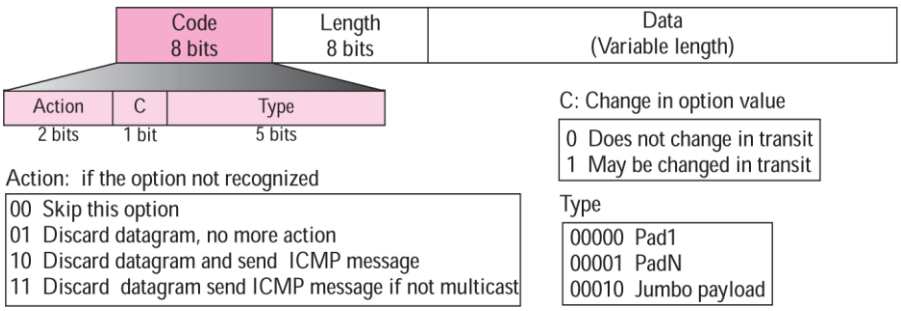
✓ Six types of extension headers have been defined. These are **hop-by-hop option, source routing, fragmentation, authentication, encrypted security payload, and destination option.**



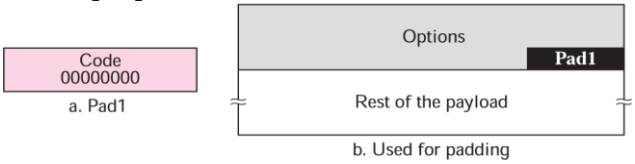
- **Hop-by-Hop Option:**
  - The hop-by-hop option is used when the source needs to pass information to all routers visited by the datagram.
  - The hop-by-hop options have a similar format, shown in Figure.
  - The 8-bit next header field identifies the next header that follows this extension header.
  - The 8-bit header extension length is the length of this extension header, in units of 8 bytes, but not including the first 8 bytes. For example, if this extension header occupies 8 bytes, then its header extension length is 0; if this extension header occupies 16 bytes, then its header extension length is 1, and so on.
  - These two headers are padded to be a multiple of 8 bytes with either the pad1 option or the padN option and Jumbo load option.



  - Figure shows the format of the hop-by-hop option header.
    - The first field defines the next header in the chain of headers.
    - The header length defines the number of bytes in the header (including the next header field).
    - The rest of the header contains different options.
  - The format of options in a hop-by-hop option header:

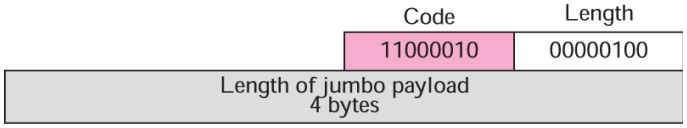


    - Figure shows the general format of the option. Three hop-by-hop options:
      - **Pad1:** This option is 1 byte long and is designed for alignment purposes.



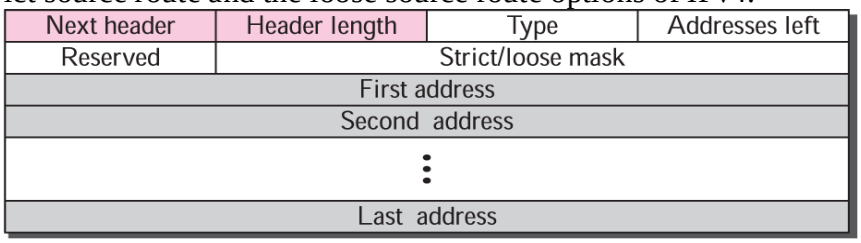
- **PadN:** PadN is similar in concept to Pad1. The difference is that PadN is used when 2 or more bytes are needed for alignment.

- **Jumbo payload:** The jumbo payload option to define this longer length.



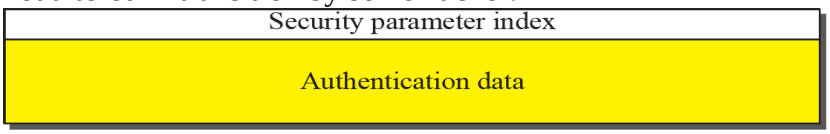
- **Destination Option:**
  - The header formats same as hop-by-hop header format.
  - The destination option is used when the source needs to pass information to the destination only. Intermediate routers are not permitted access to this information.

- **Source Routing:**
  - The source routing extension header combines the concepts of the strict source route and the loose source route options of IPv4.

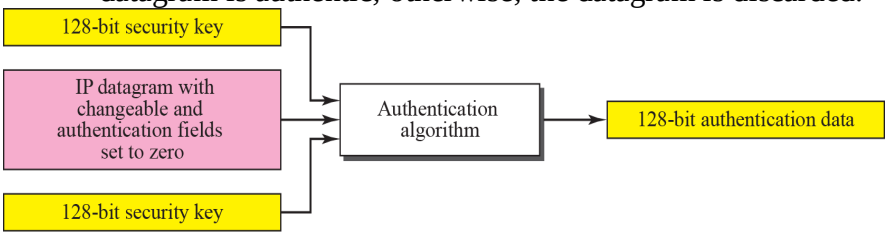


  - The source routing header contains a minimum of seven fields:
    - The first two fields, next header and header length, are identical to that of the hop-by-hop extension header.
    - The type field defines loose or strict routing.
    - The addresses left field indicates the number of hops still needed to reach the destination.
    - The strict/loose mask field determines the rigidity of routing. If set to strict, routing must follow exactly as indicated by the source.
- **Fragmentation**
  - Fragmentation EH is critical in support of communication using fragmented packets.

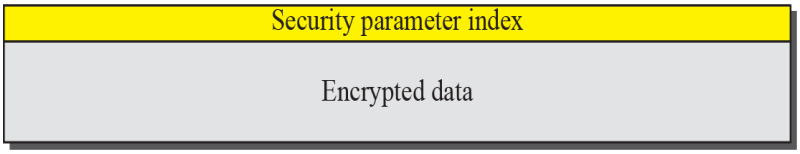
- **Authentication**
  - Authentication EH is similar in format and use to the IPv4 authentication header.
  - The authentication extension header has a dual purpose: it validates the message sender and ensures the integrity of data. The former is needed so the receiver can be sure that a message is from the genuine sender and not from an imposter. The latter is needed to check that the data is not altered in transition by some hacker.



  - Calculation of authentication data:
    - The sender passes a 128-bit security key, the entire IP datagram, and the 128-bit security key again to the algorithm. Those fields in the datagram with values that change during transmission are set to zero. The datagram passed to the algorithm includes the authentication header extension, with the authentication data field set to zero. The algorithm creates authentication data which is inserted into the extension header prior to datagram transmission.
    - The receiver functions in a similar manner. It takes the secret key and the received datagram (again, with changeable fields set to zero) and passes them to the authentication algorithm. If the result matches that in the authentication data field, the IP datagram is authentic; otherwise, the datagram is discarded.

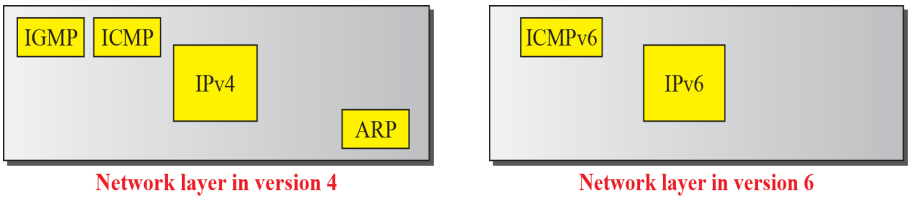


- **Encrypted security payload**
  - Encapsulating Security Payload EH is similar in format and use to the IPv4 ESP header.
  - The encrypted security payload (ESP) is an extension that provides confidentiality and guards against eavesdropping.
  - The security parameter index field is a 32-bit word that defines the type of encryption/decryption used. The other field contains the encrypted data along with any extra parameters needed by the algorithm.
  - Encryption can be implemented in two ways: transport mode or tunnel mode.

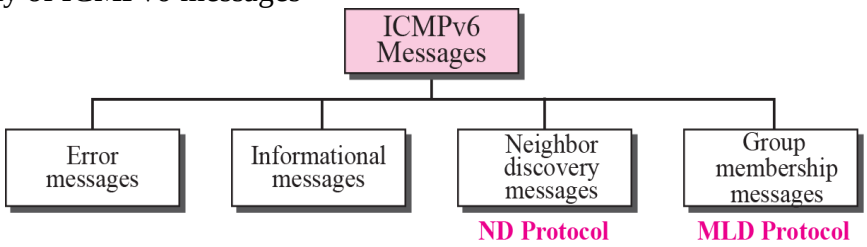


ICMPv6 – Introduction

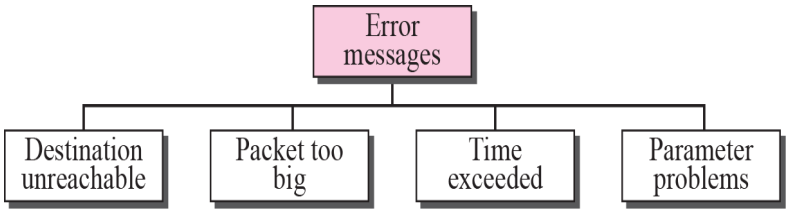
- ✓ This new version, Internet Control Message Protocol version 6 (ICMPv6), follows the same strategy and purposes of version 4
- ✓ ICMPv6, however, is more complicated than ICMPv4
  - Some protocols that were independent in version 4 are now part of ICMPv6
  - Some new messages have been added to make it more useful
- ✓ Comparison of network layers in version 4 and version 6



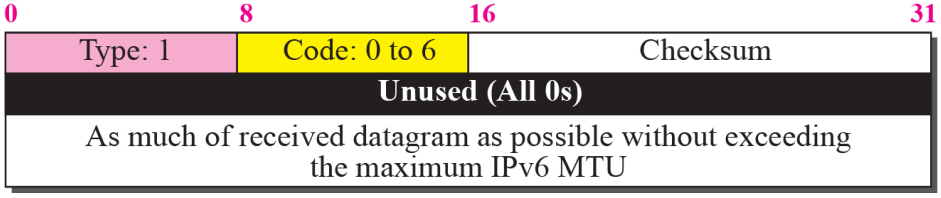
- ✓ Taxonomy of ICMPv6 messages



- **Error Messages**
  - One of the main responsibilities of ICMP is to report errors
  - Four types of errors are handled
    - Destination unreachable
    - Packet too big
    - Time exceeded
    - Parameter problems



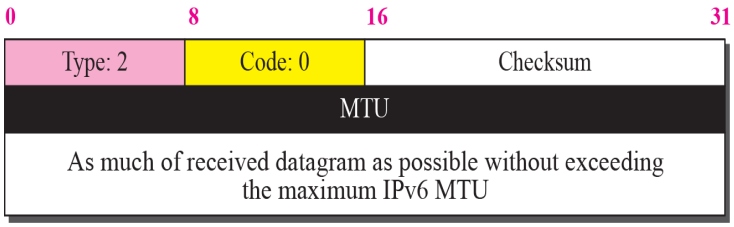
- **Destination unreachable message**
  - When a router cannot forward a datagram or a host cannot deliver the content of the datagram to the upper layer protocol, the router or the host discards the datagram and sends a destination-unreachable error message to the source host.



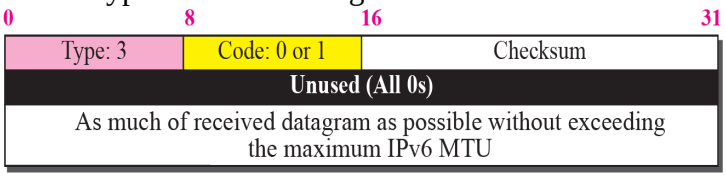
- Code 0 : No path to destination
- Code 1 : Communication is prohibited
- Code 2 : Beyond the scope of source address

- Code 3 : Destination address is unreachable
- Code 4 : Port unreachable
- Code 5 : Source address failed (filtering policy)
- Code 6 : Reject route to destination

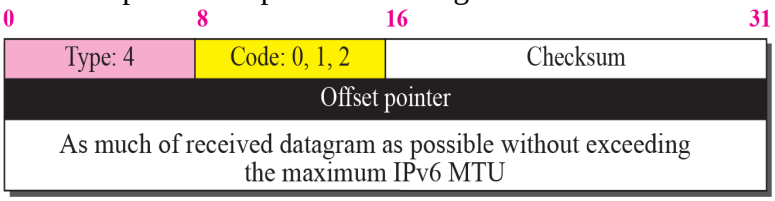
- **Packet-too-big message**



  - If a router receives a datagram that is larger than the maximum transmission unit (MTU) size of the network through which the datagram should pass.
    - Discarding the datagram
    - Then, sending an ICMP error packet to the source
  - MTU field : informing the sender of the maximum size packet accepted by the network
- **Time-exceeded message**
  - The format of the time-exceeded message in version 6 is similar to the one in version 4. The only difference is that the type value has changed to 3.



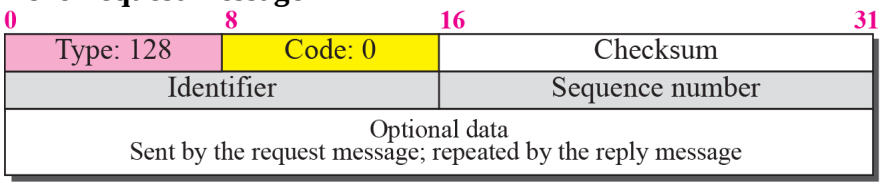
- **Parameter-problem message**
  - If a router or the destination host discovers any ambiguous or missing value in any field, it discards the datagram and sends a parameter-problem message to the source.



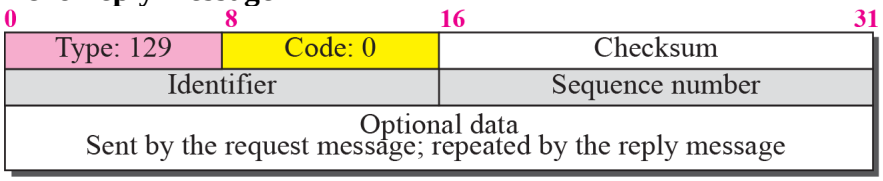
  - Offset pointer : 4 bytes
  - Code fields
    - Code 0 : Erroneous header field
    - Code 1 : Unrecognized next header type
    - Code 2 : Unrecognized IPv6 option

- **<u>Informational Messages</u>**
  - Two of the ICMPv6 messages can be categorized as informational messages
  - Echo request and echo reply messages

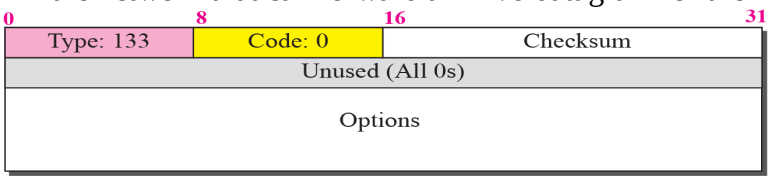
- A host or router can send an echo request message to another host; the receiving computer or router can reply using the echo response message
- **Echo-request message**



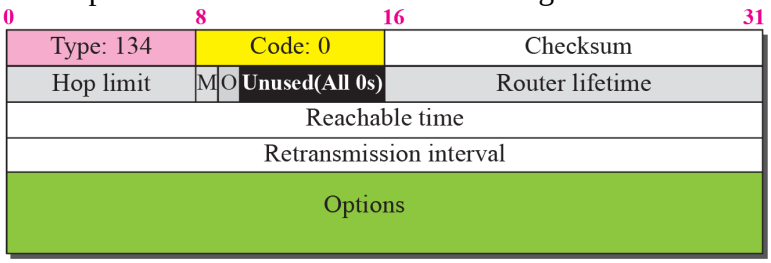
- **Echo-reply message**



- **<u>Neighbor-Discovery Message</u>**
  - Several messages in the ICMPv4 have been redefined in ICMPv6 to handle the issue of neighbor discovery
  - The most important issue is the definition of two new protocols that clearly define the functionality of these group messages
    - Neighbor-Discovery (ND) protocol
    - Inverse-Neighbor-Discovery (IND) protocol
  - Router Solicitation and Advertisement
  - An option is added to allow the host to announce its physical address to make it easier for the router to respond.
  - **Router-solicitation message**
    - A host uses the router-solicitation message to find a router in the network that can forward an IPv6 datagram for the host.



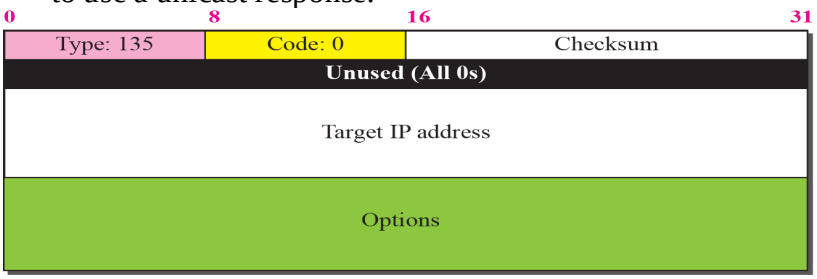
  - **Router-advertisement message**
    - The router-advertisement message is sent by a router in response to a router solicitation message.



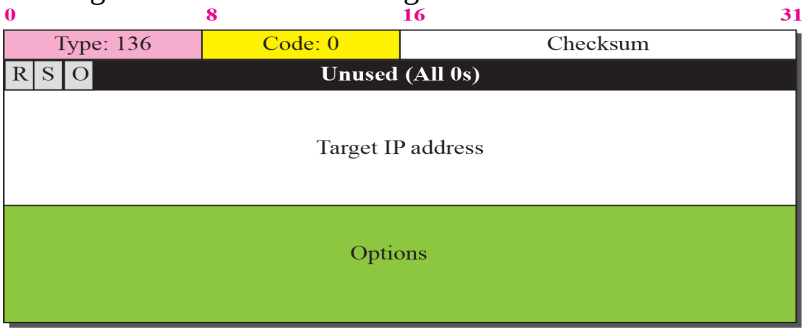
    - The fields are explained below:
      - Hop Limit: This 8-bit field limits the number of hops that the requestor should use as the hop limit in its IPv6 datagram.

- M: This 1-bit field is the "manage address configuration" field. When this bit is set to 1, the host needs to use the administration configuration.
- O: This 1-bit field is the "other address configuration" field. When this bit is set to 1, the host needs to use the appropriate protocol for configuration.
- Router Lifetime: This 16-bit field defines the lifetime (in units of seconds) of the router as the default router. When the value of this field is 0, it means that the router is not a default router.
- Reachable Time: This 32-bit field defines the time (in units of seconds) that the router is reachable.
- Retransmission Interval: This 32-bit field defines the retransmission interval (in units of seconds).
- Option: Some possible options are the link layer address of the link from which the message is sent, the MTU of the link, and address prefix information.

- **Neighbor-solicitation message**
  - The neighbor solicitation message has the same duty as the ARP request message. This message is sent when a host or router has a message to send to a neighbor. The sender knows the IP address of the receiver, but needs the data link address of the receiver. The data link address is needed for the IP datagram to be encapsulated in a frame. The only option announces the sender data link address for the convenience of the receiver. The receiver can use the sender data link address to use a unicast response.



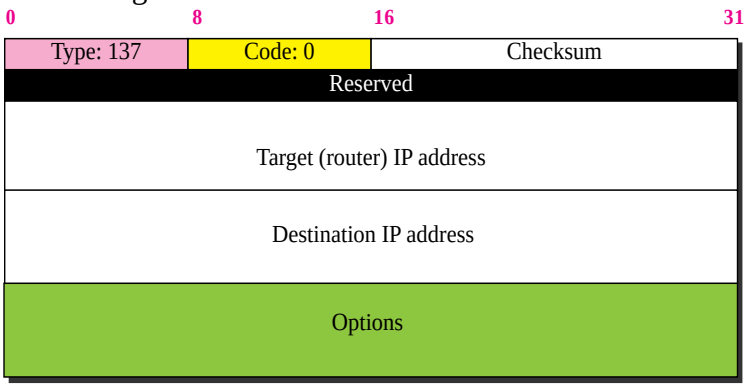
- **Neighbor advertisement message**
  - The neighbor-advertisement message is sent in response to the neighbor-solicitation message.



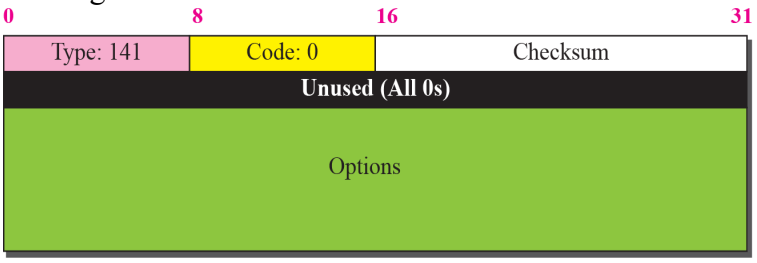
  - The fields are explained below:
    - R: This 1-bit field is the "router" flag. When it is set to 1, it means the sender of this message is a router.

- S: This 1-bit field is the "solicitation" flag. When it is set to 1, it means that the sender is sending this advertisement in response to a neighbor solicitation. An advertisement can be sent by a host or router without solicitation.
- O: This 1-bit field is the "override" flag. When it is set, it means that the advertisement should override existing information in the cache.
- Option: The only possible option is the link layer address of the advertiser.

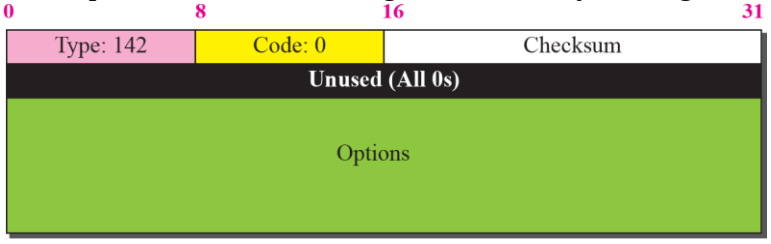
- **Redirection message**
  - An option is added to let the host know the physical address of the target router



- **Inverse-neighbor-solicitation message**
  - The inverse-neighbor-solicitation message is sent by a node that knows the link layer address of a neighbor, but not the neighbor's IP address.

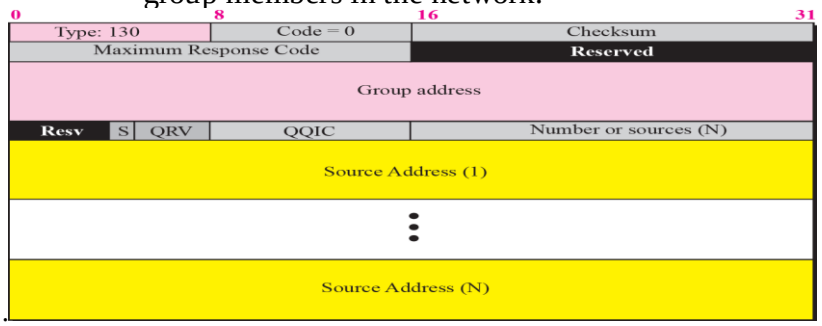


- **Inverse-neighbor-advertisement message**
  - The inverse-neighbor-advertisement message is sent in response to the inverseneighbor-discovery message.



- **Group Membership Message**
  - The management of multicast delivery handling in IPv4 is given to the IGMPv3 protocol
  - In IPv6, this responsibility is given to the Multicast Listener Delivery protocol
    - MLDv1 is the counterpart to IGMPv2; MLDv2 is the counterpart to IGMPv3
    - The idea is the same as in IGMPv3, but the sizes and formats of the messages have been changed to fit the larger multicast address size in IPv6.

  - **Membership query message format**
    - A membership-query message is sent by a router to find active group members in the network.



  - Membership-report message format