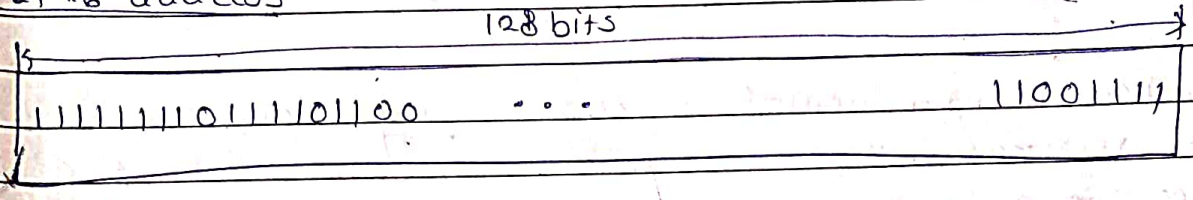
Next generation IPv6 ICMPv6

DATE /

IPv6

It is 128 bits or 16 bytes (octet) long as shown in fig. The address length in IPv6 is four times of the length address in IPv4

IPv6 address

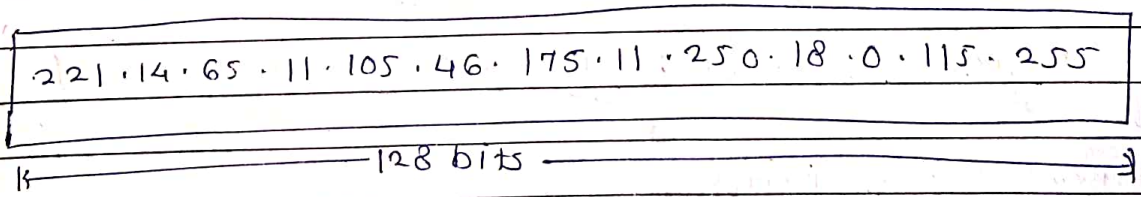


Notations

Computer stores address in binary but in the IPV6 address is 128 bits, cannot easily handled by human. Several notations have been proposed to represent IPv6 addresses.

1) Dotted Decimal Notation
2) Colon Hexadecimal Notation
3) Mixed Representation

1) Dotted Decimal Notation



In IPv6 address length is 128 bits, 128 bits are represent in Dotted Decimal with dotted format.

2) Colon hexadecimal Notation

To make addresses more readable IPv6 specifies colon hexadecimal notation. In this section notation 128 bits are divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal notation require four hexadecimal digits. so here 32 hexadecimal digits consist; with every four digits separated by a colon digi

Fig. shows an IPv6 address in colon hexadecimal notation

FDEC : ABA8 : 1245 : 3210 : ADFE : BBFF : 2922 : FFFF

fig - colon hexadecimal notation

In hexadecimal format address is long, many of the digits are zeros. In this case, we can abbreviate the address. The leading zeros of a section can be omitted. Using this form of abbreviation 0074 can be written as 74 & 000f as f & 0000 as 0. Note that 210 can't be abbreviated. this is called as zero compression if there are consecutive sections consisting of zeros only, we can remove all the zeros to altogether & replace them with double semicolon.

zero compression

FDEC : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF - original address

↓

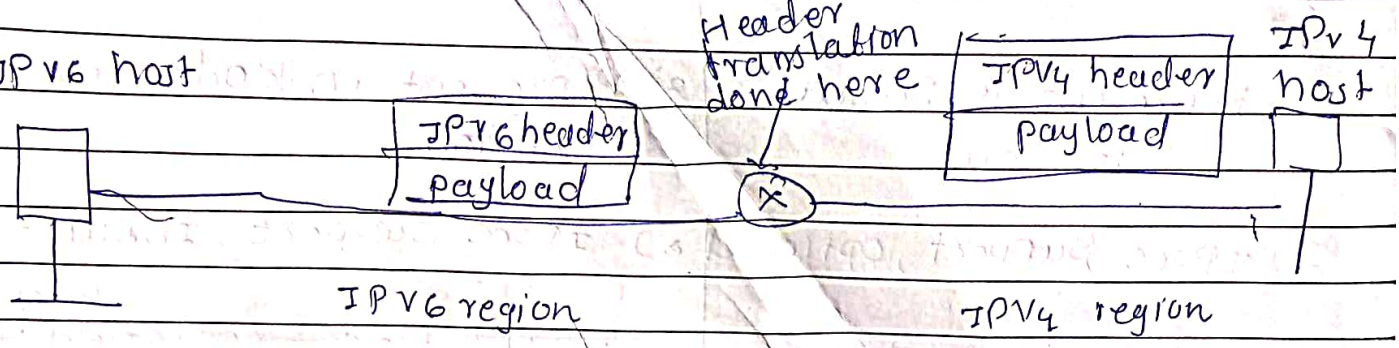
FDEC : : BBFF : 0 : FFFF - zero compressed

③ Mixed Representation

Mixed means combines colon hex, dotted decimal notation. This is appropriate during the transition period in which IPv4 address is embedded in an IPv6 address. we can use the colon hex notation for the left most six section & four bytes dotted decimal notation instead of rightmost two section

FDEC : 14AB : 2811 : BBFF : AAAA : BBBB : 130.24.24.18

The header of the IPv6 packet is converted to an IPv4 header.



Fig→ header translation

- It uses the mapped address to translate an IPv6 address to an IPv4 address.
- Some rules for used in transforming IPv6 packet header to an IPv4 packet header.

i) The IPv6 mapped address is changed to an IPv4 address by exacting the right most 32 bits
ii) The ~~value~~ type of service field in IPv4 is set to zero
iii) The value of the IPv6 priority field is discarded.
iv) The checksum for IPv4 is calculated & inserted in the corresponding field.
v) The IPv6 flow label is ignored.
vi) Compatible extension headers are converted to options & inserted in the IPv4 header. Some may have to be dropped
vii) The length of IPv4 header is calculated & inserted into corresponding field.
viii) The total length of the IPv4 packet is calculated & inserted in the corresponding field.

flow label → ignored
Type of service → set 0

TEJ MY BRAIN
DATE / /

IPV4	IPV6
1) Length of address 32 bit	1) 128 bit
2) Represent in Decimal Notation	2) Represent in Hexadecimal Notation
3) IPsec support, optional	3) IPsec support, Inbuilt
4) Packet flow indication → None	4) Packet flow - Yes, field present Label Req
5) checksum field → Yes	5) checksum field → None
6) Option field - Yes	6) Option field - None, Extension header
7) Address to MAC → ARP	7) Replaced by → ND
8) Broad cast message; Yes	8) special type of multicast address.
9) Total No. of address = 2^{32}	9) 2^{128}.

DATE / /

However, this happens when all or most of the rightmost sections of the IPv6 address are 0.s

::130.24.24.18

4) CIDR Notation

IPv6 uses hierarchical addressing, for this reason, IPv6 allows classless addressing & CIDR notation.

e.g → fig shows how we can define a prefix of 60 bits using CIDR.

CIDR address

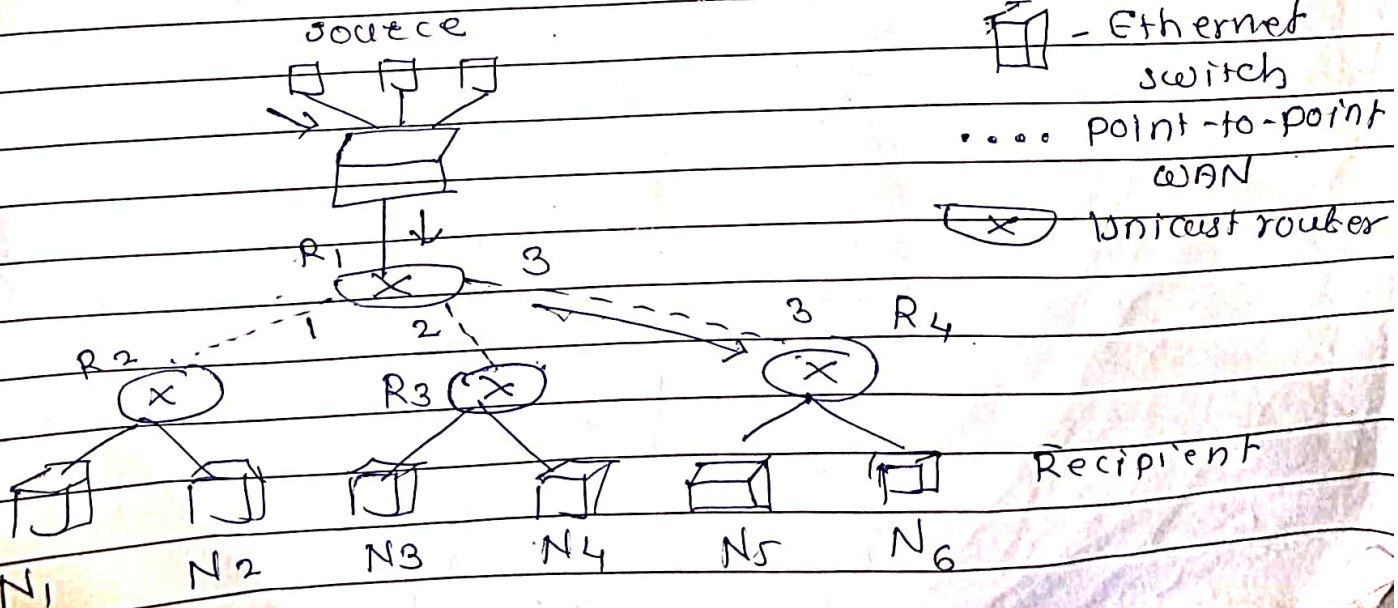
FDEC::BBFF:0:FFFF/60

Address Type

1) Unicast
2) Anycast
3) multicast

1) Unicast

A unicast address defines a ~~group~~ single interface. The packet sent to a unicast address will be routed to the intended recipient. In unicast, there is one source & one destination network. The relationship between source & destination network is one to one.



TEJ
MY BRAIN
DATE / /

2) Multicast

In multicasting there is one source & group of destinations. The relationship is one to many. In this type of source address is a unicast address but the destination address is group address.

DATE / /

IPv6 Packet format

It is is Internet Protocol version 6 (IPv6)

1) Larger address space → An IPv6 address is 128 bits long compared with the 32-bit address of IPv4 this is huge (2^96 times) increase in the address space.

2) Better header format → IPv6 uses a new header format in which options are separated from the base header & inserted, when needed, between the base header & upper layer data. This simplifies & speeds up the routing process because most of the options do not need to be checked by routers.

3) New options → IPv6 has new options to allow for additional functionalities.

4) Allowance for extension → In IPv6 designed to allow the extension of protocol if required by new technologies or applications.

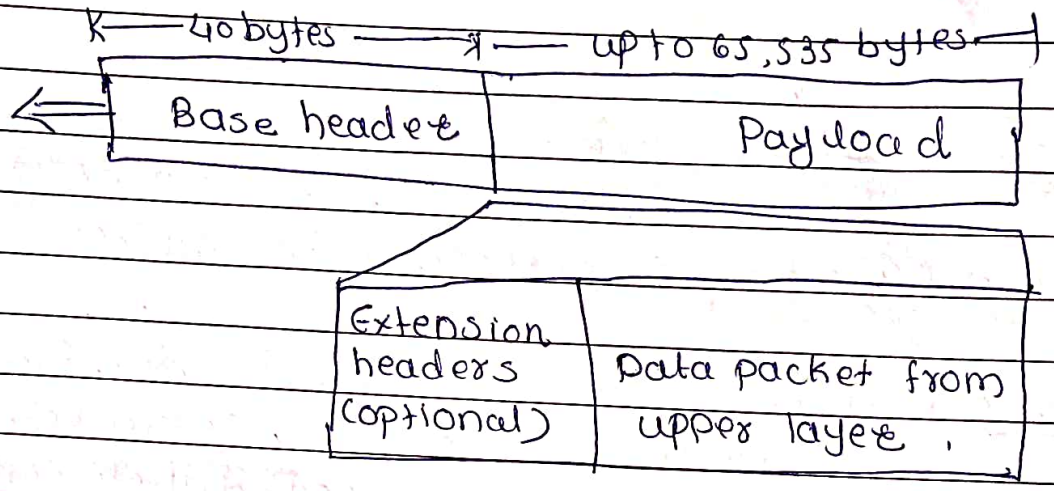
5) Support for resource allocation →
In IPv6, the type of service field has been removed but two new fields, traffic class & flow label have been added to enable the source to request special handling of the packet. It used to support traffic such as real-time audio & video.

6) Support for more security →
The encryption & authentication option in IPv6 provid confidentiality & integrity of the packet.

Packet format

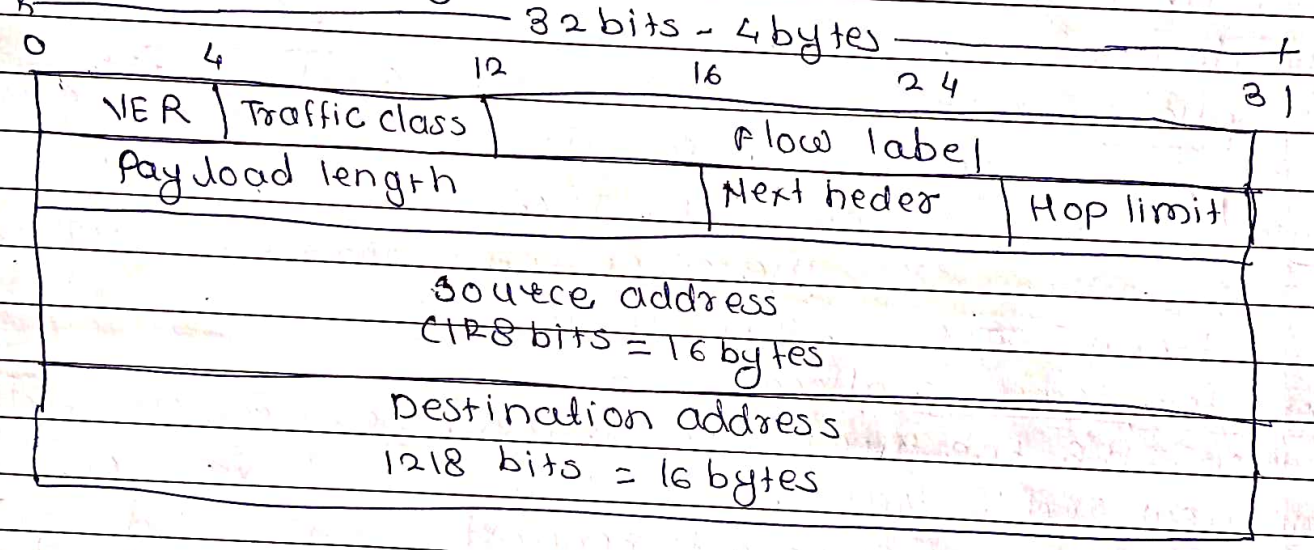
Each packet is composed of mandatory base header followed by the payload. The payload consists of two parts
i) Optional (Extension headers)
ii) Data from an upper layer.
The base header occupies 40 bytes, whereas the extension headers & data from upper layer contain up to 65,535 bytes information.

IPV6 datagram



Base header

It has a eight fields.



Fields

1) Version → This 4-bit field defines the version number of the IP. For IPV6 the value is 6.
2) Traffic class → This 8-bit field is used to distinguish different payloads with different delivery requirements. It replace the service class field in IPV4
It describe packets class or priority
3) Flow label → It is a 20-bit that is designed to provide special handling for a particular flow of data.
4) Payload length → The 2 byte payload length field defines the length of IP datagram excluding the base header.
5) Next header → It 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. Each extension header also contains this field. Table shows the values of next headers.

Next header codes.

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
43	source routing	60	Destination option.

6) Hop limit → This is 8-bit hop limit field serves the same purpose as TTL field. It indicates max. no. of routers the packet is capable of passing

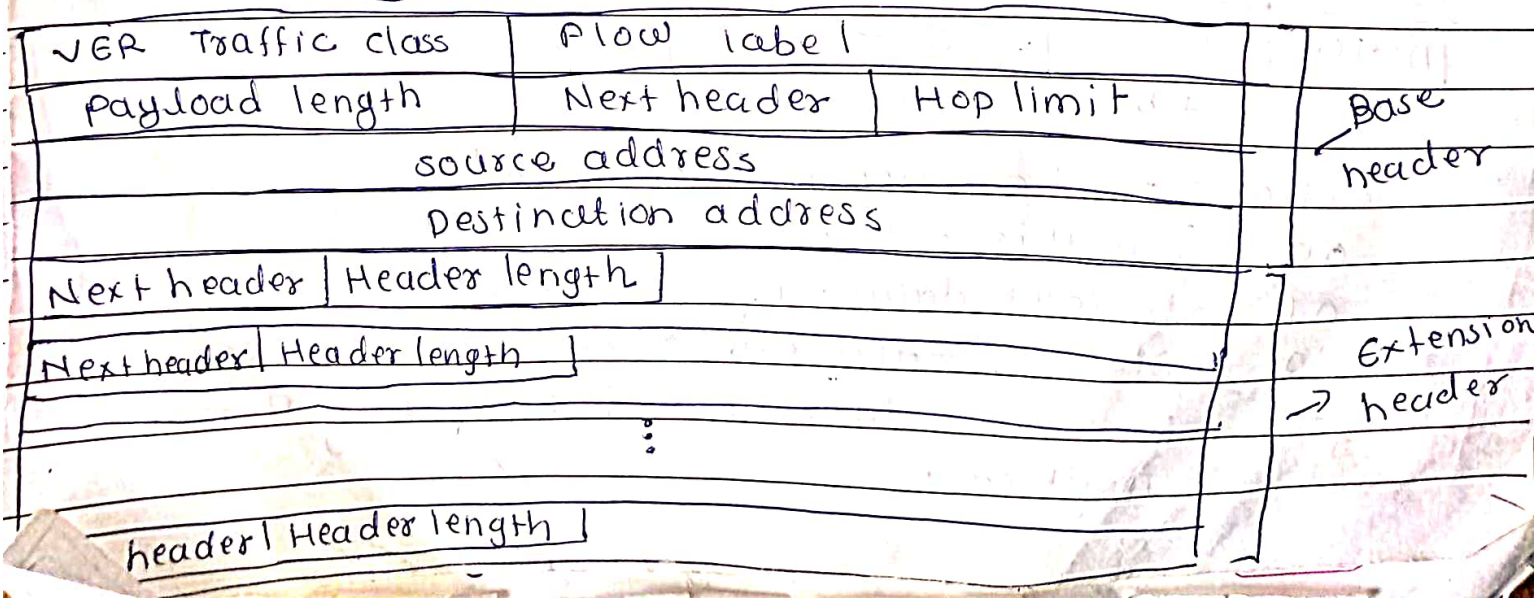
7) Source address → The source address field is a 16-byte Internet address that identifies the original source of datagram.

8) Destination address → It is a 16 byte Internet address that usually identifies the final destination of the datagram. If source routing is used this field contains the address of the next router.

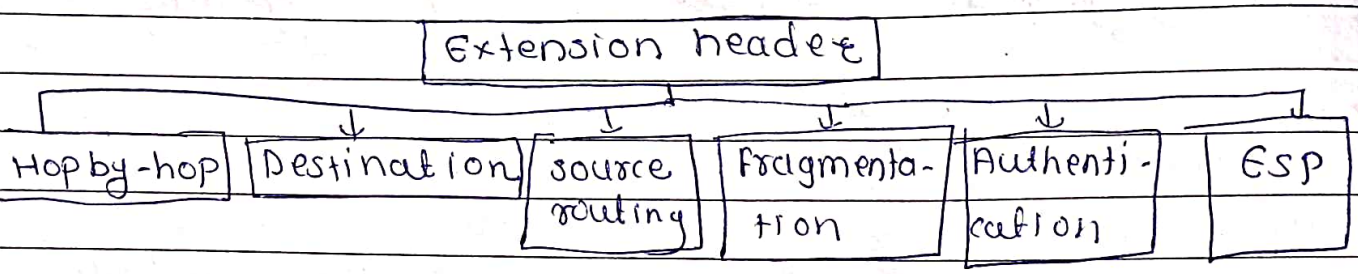
* Extension header

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 upto six extension headers.

Extension header format



Types of extension header



1)

- It is used to specify delivery parameters at each hop on the path to the destination
- It is identified by the value of 0 in IPv6 headers next header field.

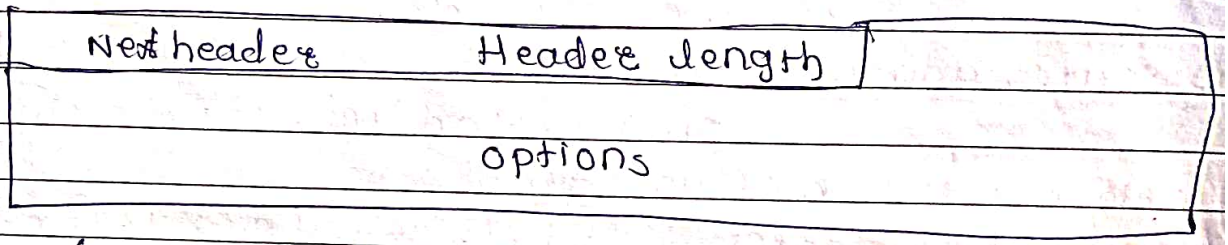
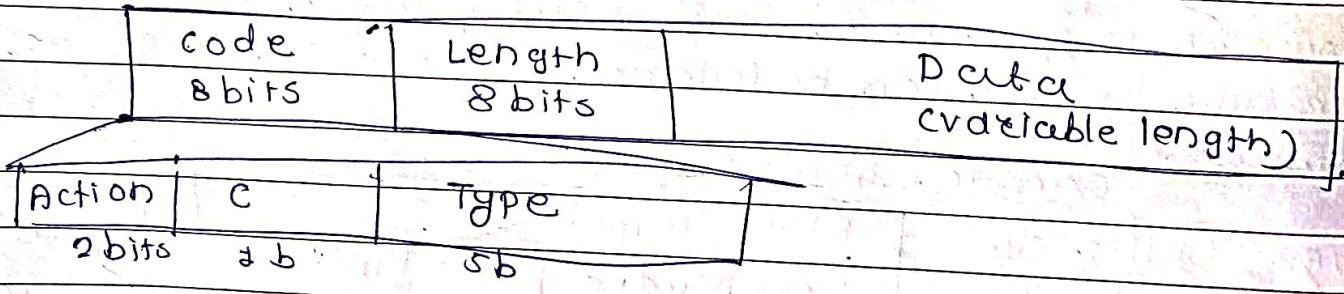


fig → hop by hop option header format

- There are 8 options have been defined
  i) Pad 1, ii) Pad N & iii) jumbo payload

i) Pad 1 → It is 1 byte long & is designed for alignment purpose.



Action: If the option not recognized
- 00 skip this option
- 01 Discard datagram, no more action
- 10 Discard datagram & send ICMP message
- 11 Discard datagram send ICMP msg if not multicast.

Date:

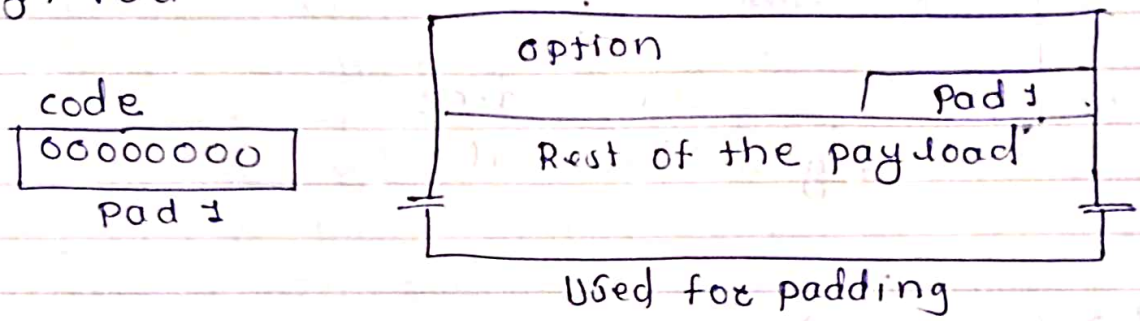
C : Change in option value

0 - Does not change in transit
1 - May be changed in transit

Type

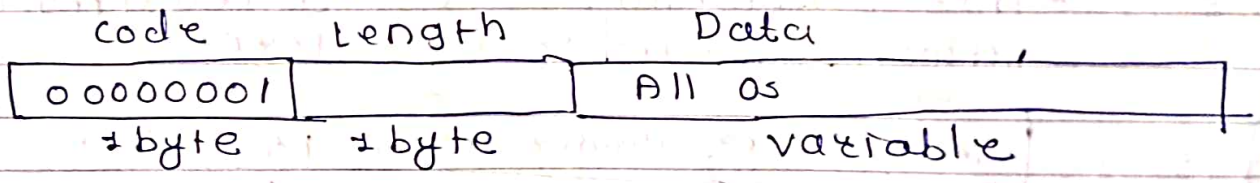
00000	pad 1
00001	Pad N
00010	Jumbo Payload

Fig → Pad 1



ii) Pad N

- similar to Pad 1
- Difference is that Pad N is used when 2 or more bytes are needed for alignment
- 1 byte long
- option code is 00000001



iii) Jumbo payload

- length of the payload in the IP datagram can be a maximum of 65,535 bytes so for any reason longer payload is required so we can use the jumbo payload option to define this longer length
- It start at a multiple of 4 bytes plus 2 from the begining of the extension headers.
- It starts at the (4n+2) byte where n is small integer

Sulekha

2) Destination

- It is used when the source needs to pass info. to the destination only.
- Immediate routers are not permitted access to this info.

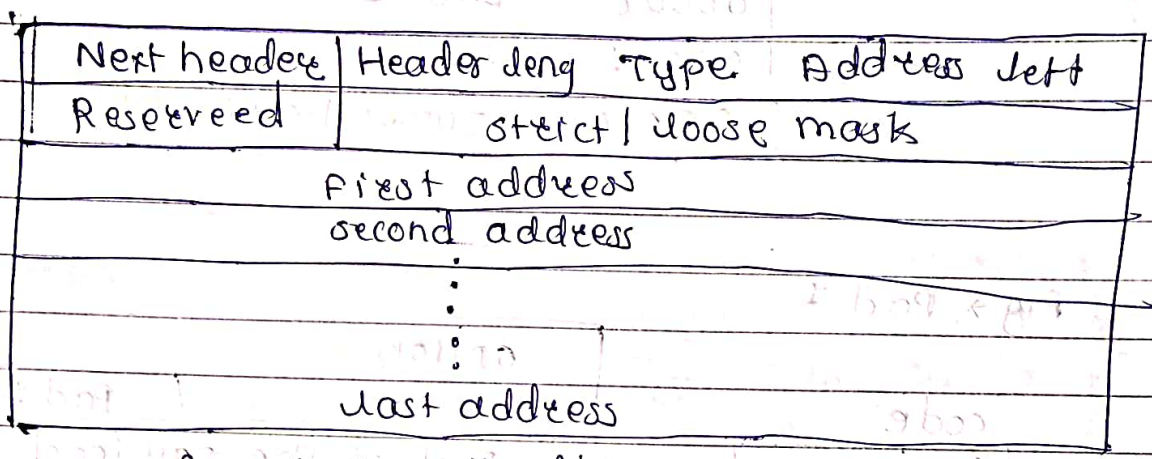


fig. source routing

3) Fragment

- In IPv6 original source can fragment
- source must use path MTU Discovery technique to find the smallest MTU supported by any n/w on the path.
- If the source does not use path MTU Discovery technique, it fragments the datagram to a size of 1,280 bytes or smaller.
- This is minimum size of MTU required for each network connected to the Internet

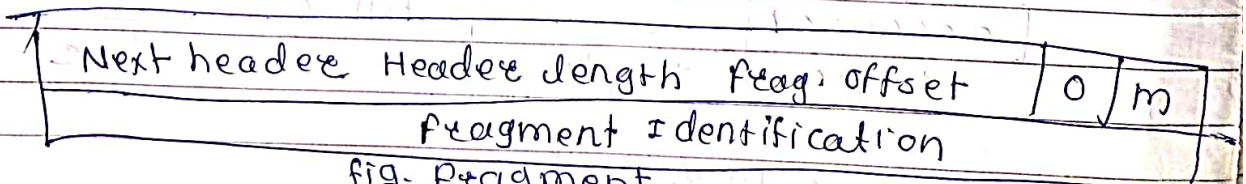


fig. Fragment

4) Encrypted Security Payload

i) It is an extension that provides confidentiality & guards against eavesdropping.

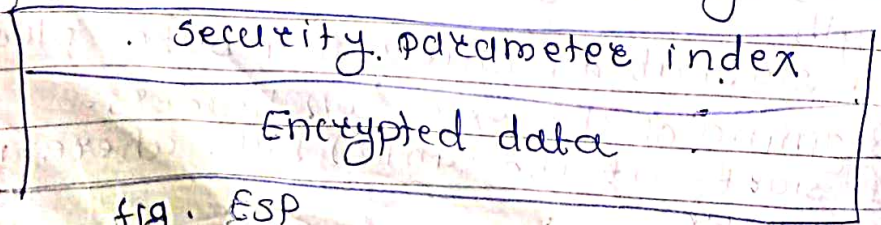
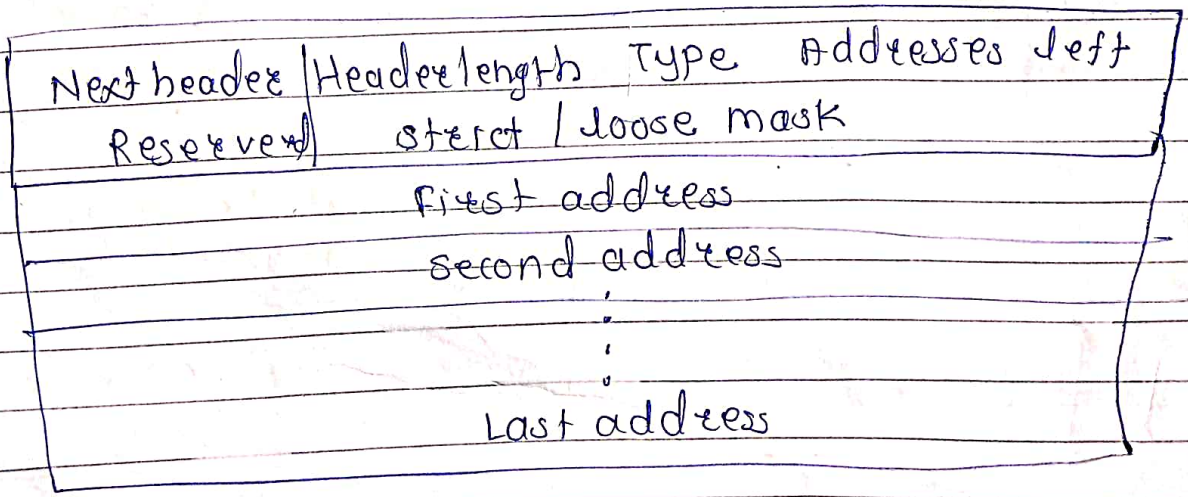


fig. ESP

ii) The security parameter index field is 32-bit word that defines the type of encryption/decryption used.
iii) The other field contains the encrypted data along with any extra parameters needed by the algorithm.
iii) Encryption can be implemented in two way
a) transport mode & tunnel mode.

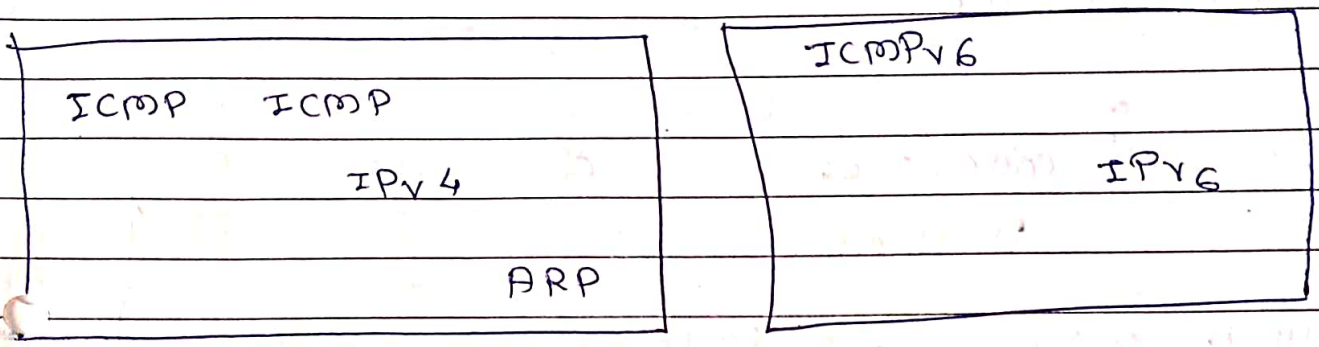
6) Source Routing
i) It combines strict source route & loose source route options of IPv4
ii) source routing header contains a minimum of seven fields. the 1st two fields, next header & header length are identical to that of the hop by hop extension header. Type of field defines loose/strict routing. The addresses left field determines the rigidity of routing. If set to strict, routing must follow exactly as indicated by the source, if instead mask is loose, other routers may be visited.



ICMPv6

It is a Internet Control message protocol version 6
It is more complicated than ICMPv4, some new messages added into it to make it more useful.

comparison of ICMPv4 & ICMPv6

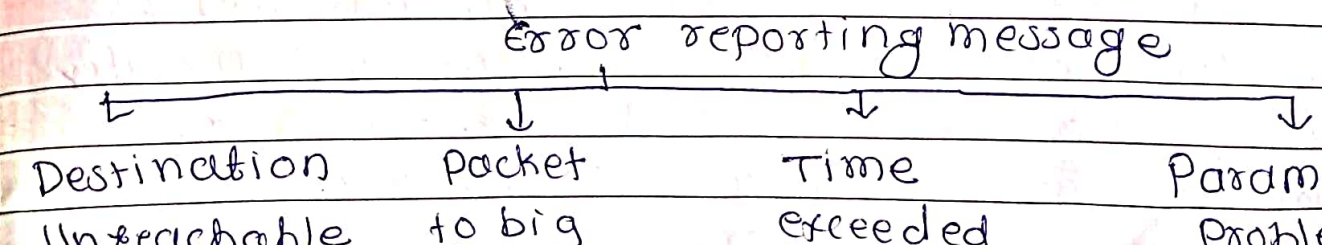


- ICMPv6 is message oriented, it uses messages to report errors, to get information, probe a neighbour or manage multicast communication.

Types

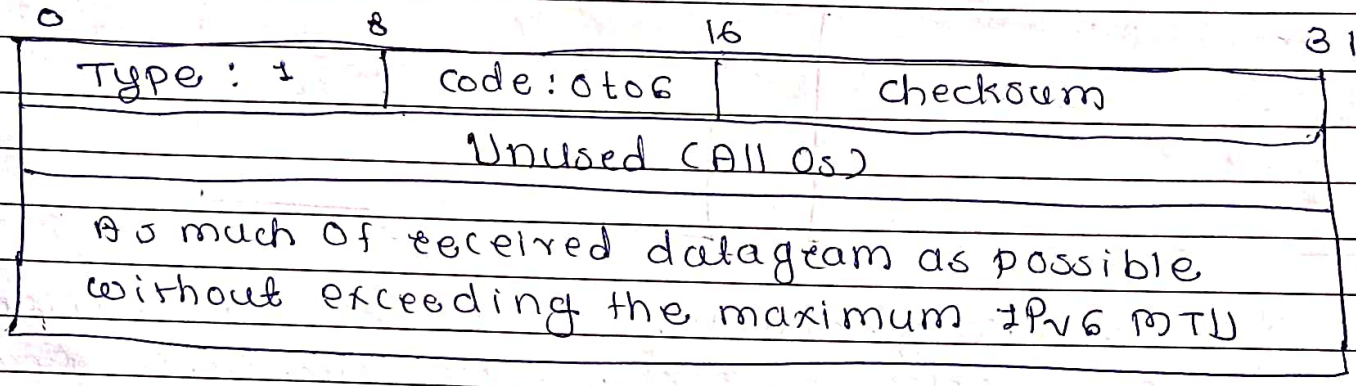
(1) Error message

main function of error message is to report the errors. There are four types of error messages.



1) Destination-Unreachable Message

When router cannot forward a datagram or a host cannot deliver content of the datagram to the upper layer protocol, the router or host discards the datagram & sends destination-unreachable error message to the source host. Fig. @ shows the format of the destination unreachable message.



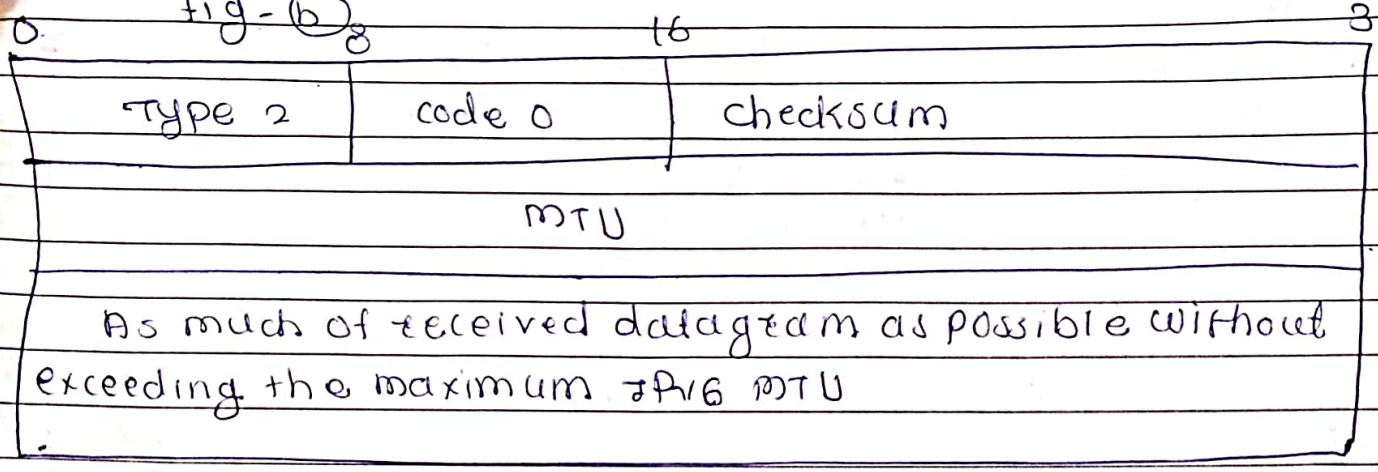
The code field for this type specifies the reason for discarding the datagram & explains exactly what has failed.

code 0 → No path to destination
code 1 → Communication with the destination is administratively prohibited.
code 2 → Beyond the scope of source address
code 3 → Destination address is unreachable
code 4 → Port unreachable
code 5 → Source address failed
code 6 → Reject route to destination

(2) Packet-Too-Big Message

- This is new type of message added to version 6.
- IPv6 does not fragment at the routers 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, two things are happen
  - i) Router discard the datagram
  - ii) ICMP error packet send message to the source, message is, a packet is too big message

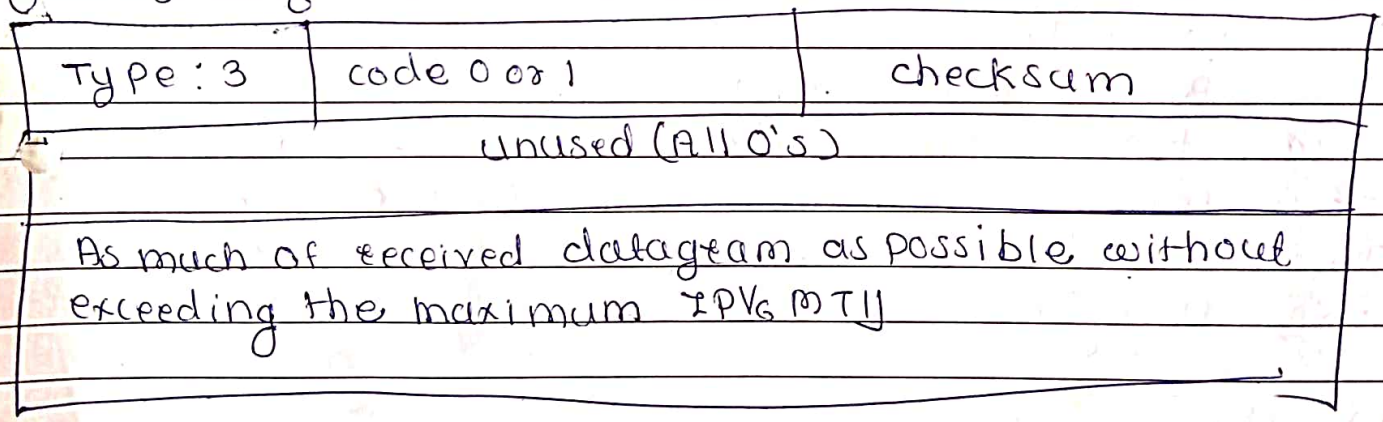
fig - (b)



(3) Time Exceeded Message

It is generated in two cases when the time to live value becomes zero & when not all fragments of a datagram have arrived in the time limit. format of the time exceeded message are same as to IPv4, only type value is changed.

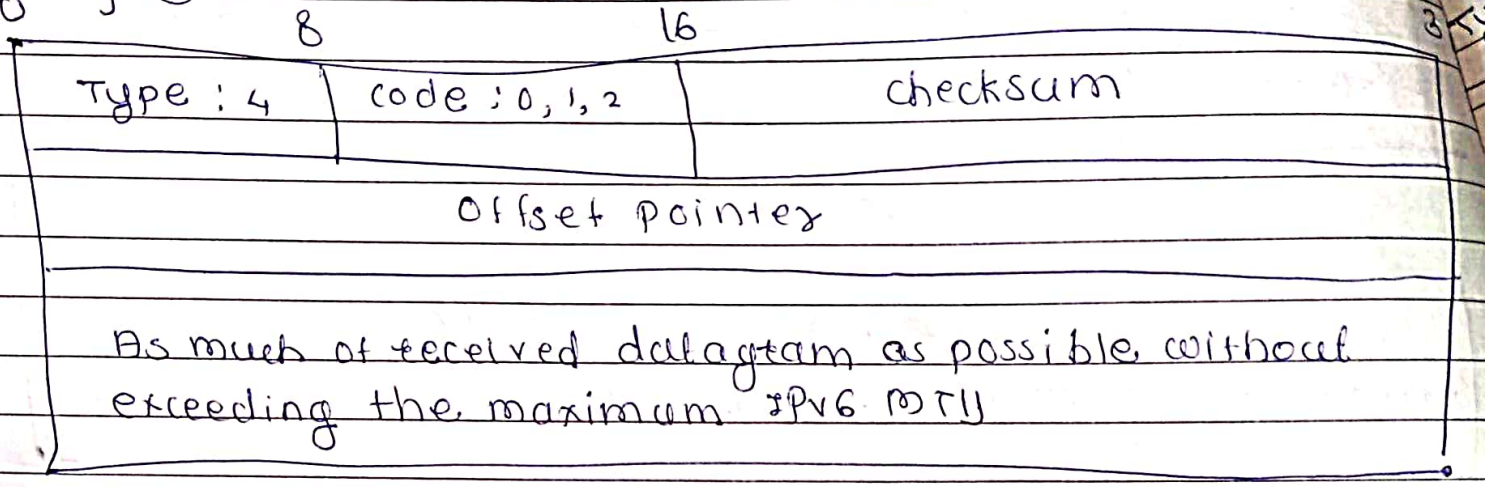
fig. (c)



(4) Parameter Problem Message

If router or the destination has discover any ambiguous or missing value in any field it discard the datagram & sends a parameter problem message to the source. The message in ICMPv6 is similar to IPv4 only the type value is changed & offset pointer field has been increased to 4 bytes. There are also 3 different codes.

fig. (a)



code 0 → Erroneous header field
code 1 → Unrecognized next header type
code 2 → Unrecognized IPv6 option.

II) Information Message

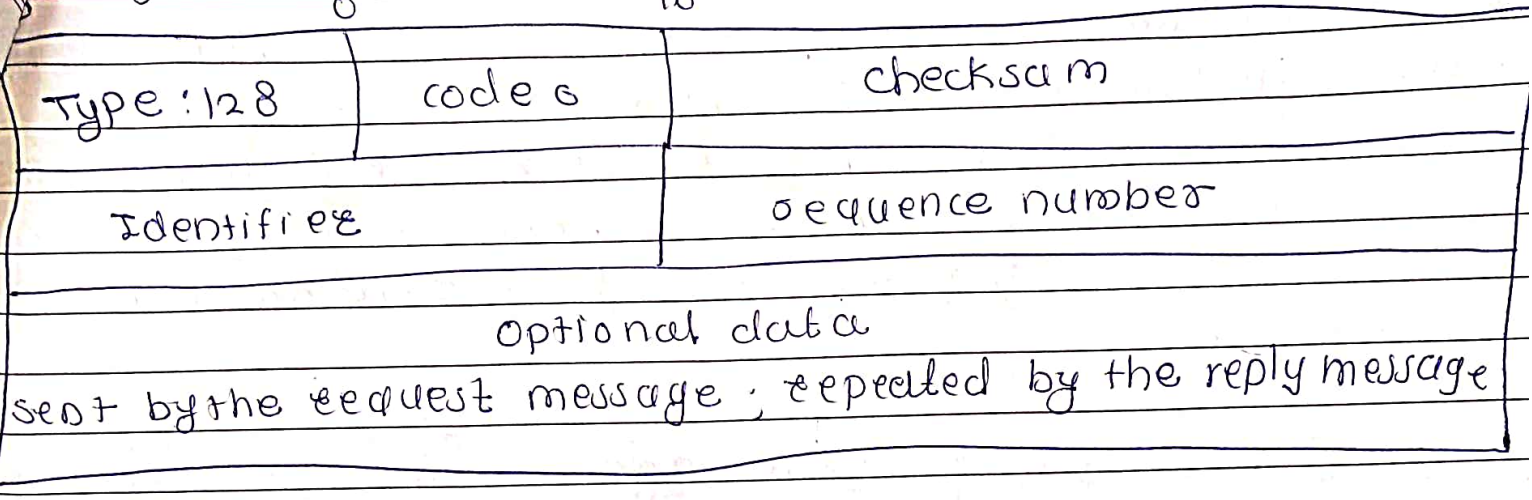
There are two types of information message
i) echo request
ii) echo reply

Both are designed to check if two devices in the Internet can communicate with each other. 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.

i) Echo-Request message

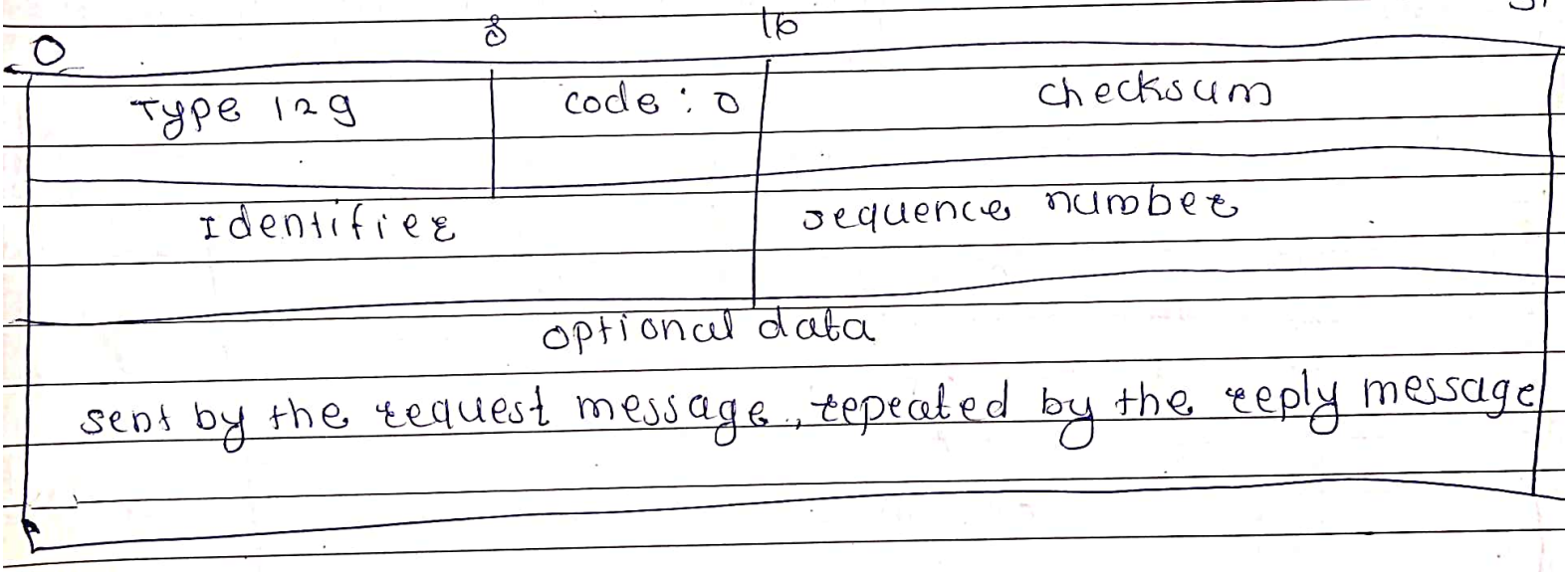
It is same as the one in version 4. The only type value is changed.

fig. (e)



ii) Echo reply message

4.



III) Neighbor - discovery Messages.

ICMPv6 message used to handle the issues of neighbor discovery. The most important issue is the definition of two new protocol that clearly define the functionality of these group messages, the Neighbor-Discovery (ND) protocol & the Inverse Neighbor-Discovery (IND) Protocol. These two protocol are used by nodes (hosts & routers) on the same link for 3 main purpose

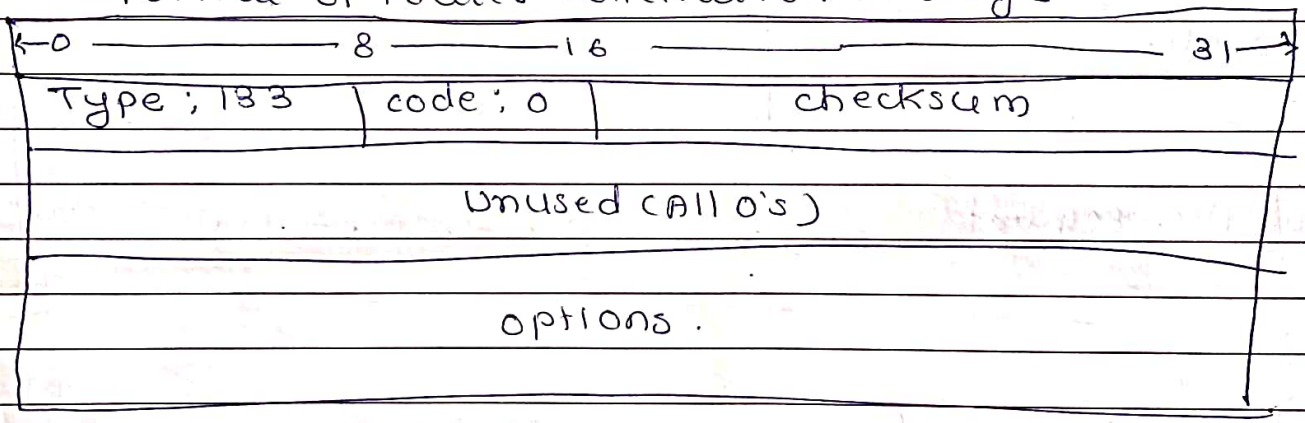
DATE / /

1. Hosts use the ND protocol to find routers in the neighbor that will forward packets for them.
2. Nodes use the ND protocol to find the link layer address of neighbors (Nodes attached to the same network)
3. Nodes use the ND protocol to find the IPv6 addresses of neighbor.

1) Router - solicitation Message

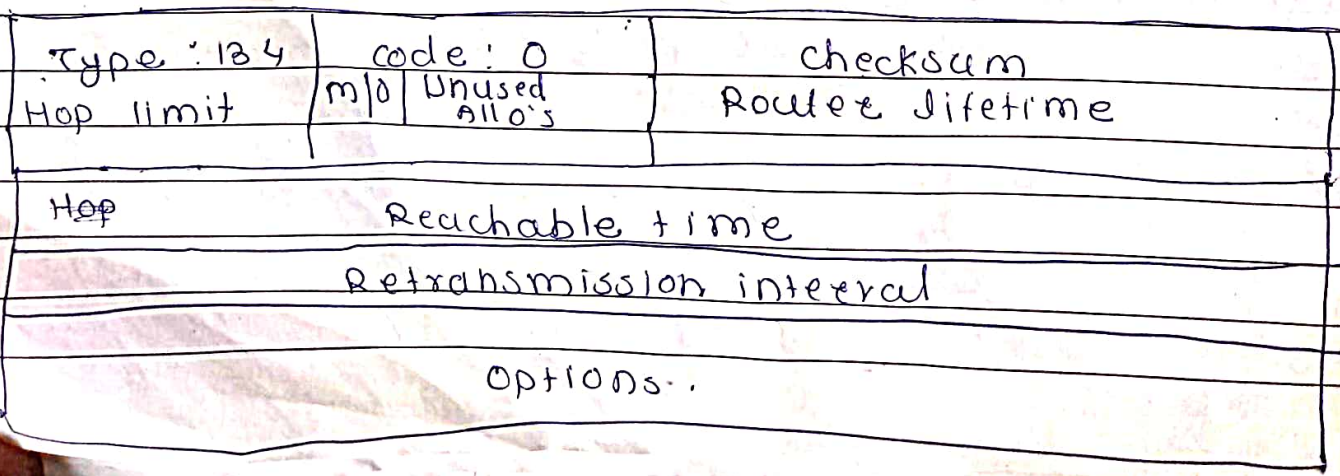
It is same as in version 4. A host uses the router - solicitation message to find a router in the network that can forward an IPv6 datagram for the host. The only option i.e so far defined for this message in the inclusion of physical (data link layer) address of the host to make the response easier for the router.

Format of Router solicitation message



(2) Router - Advertisement Message

The router - advertisement message is sent by a router solicitation message. Fig. shows format of router advertisement



Fields

1) Hop limit → This is 8-bit field limits the no. of hops that the requestor should use as the hop limit in it's IPv6 datagram.

2) M → This is 1-bit field is the "manage address configuration" field. When this bit is set to 1, the host needs to use the administration configuration.

3) O → This is 1 bit field is the "other address configuration" field. When this bit is set to 1, the host needs use the appropriate protocol for configuration.

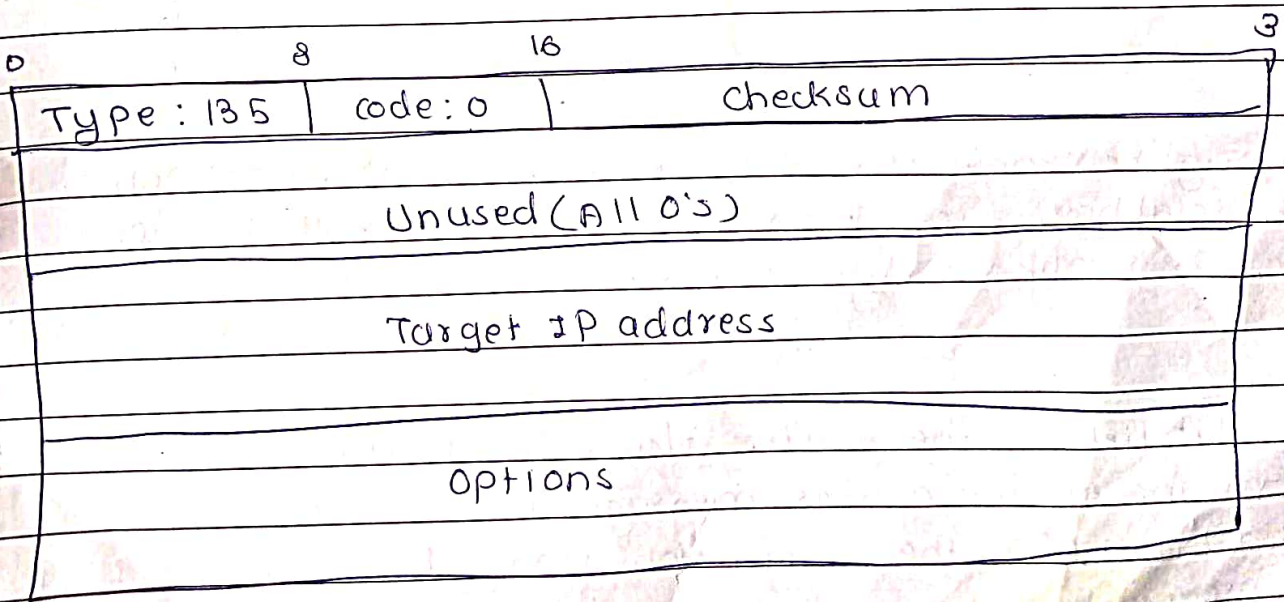
4) Router Lifetime → This 16-bit field defines the lifetime of the router as default router. When the value of this field is 0, it means that the router is not default router.

5) Reachable Time → This 32-bit field defines the time that the router is reachable.

6) Retransmission Interval → This 32-bit field defines the retransmission interval.

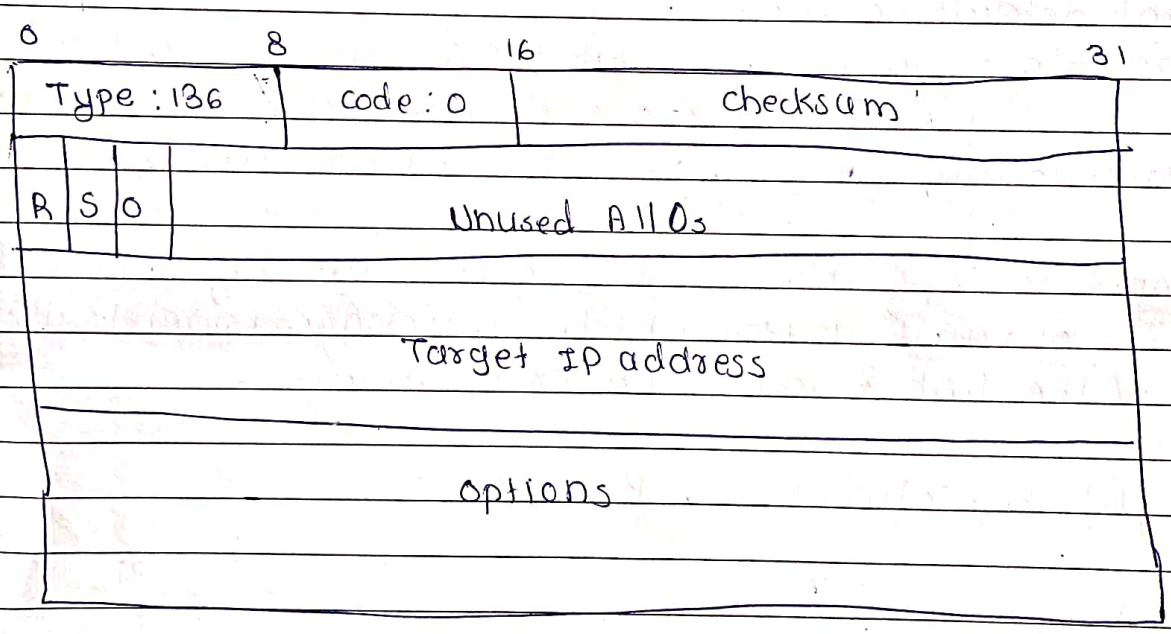
7) Option → some possible options are the link layer address of the link from which the message is sent, the MTU of the link & address prefix information.

3) Neighbor-solicitation Message



The neighbor solicitation message has the same data as the ARP request message. This message is sent when a host or router has message to send link address of the receiver. ~~The data link address is needed for the IP datagram~~ 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 receive can use the sender data link address to use a unicast response.

4) Neighbor - Advertisement Message



The neighbor-advertisement message is sent in response to the neighbor solicitation message. This is equivalent to the ARP reply message in IPv4.

Fields

R → 1 bit field is the router flag. When it is set to 1, it means sender of this message is a router

S → 1 bit field is the "solicitation" flag. When it is set 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.

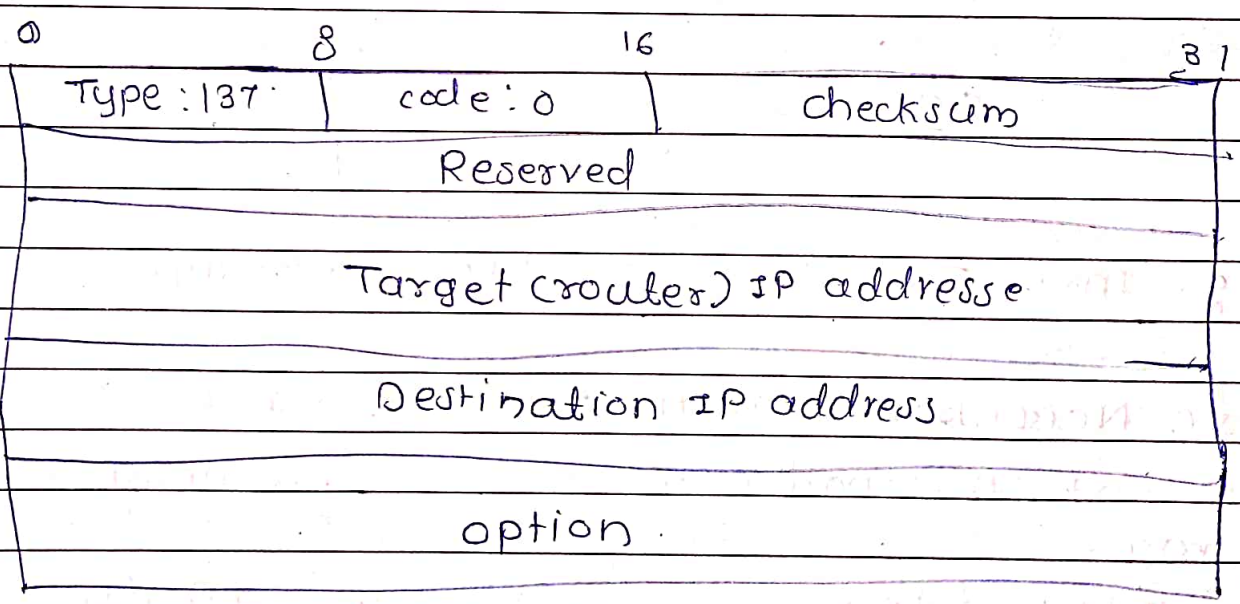
O → 1 bit field is the "override" flag when it is set, it means that the advertisement should override existing information in the cache.

Option → The only possible option is the link layer address of advertiser

⑤ Redirect Message

same as for version ~~IPv4~~.

- The redirection message is considered an error-reporting message, it is different from other error message.
- The router does not discard the datagram in this case, it is sent to the appropriate router.



* Redirect message

- ~~The~~ The possible option is the inclusion of the sender data link address & part of the redirect IP ctd header as long as the total size of msg does not exceed the MTU.

6) Inverse - Neighbor - solicitation Message

- It is sent by node that knows the link layer address of neighbor but not the neighbor's IP address.
- The msg is encapsulated in an IPv6 datagram using an all node multicast address.
- The sender must send the two pieces of information in the option field it's link layer address & the link layer address of the target node.
- The sender can also include it's IP address & the MTU value for the link.

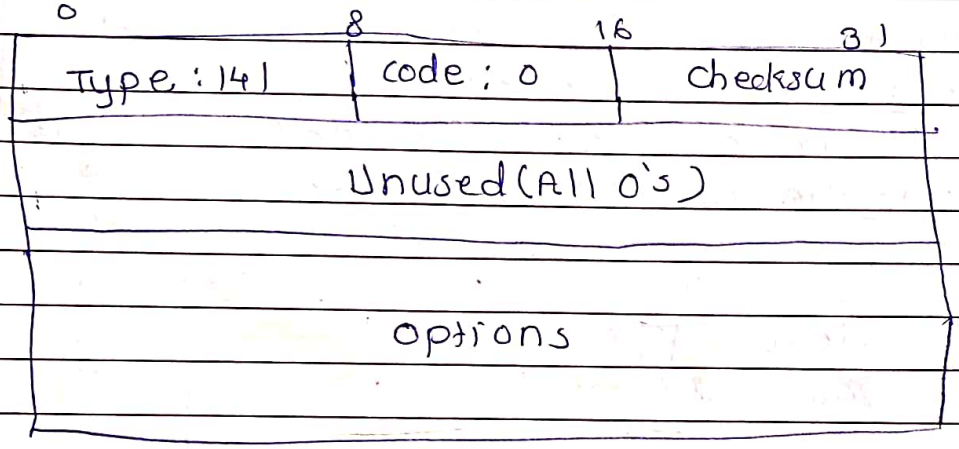


Fig. Inverse - neighbor - solicitation message

7) Inverse Neighbor - Advertisement Message

- It is sent in response to the inverse-neighbor discovery msg.
- The sender of this message must include link layer address of the sender & link layer address of the target node in the option section.

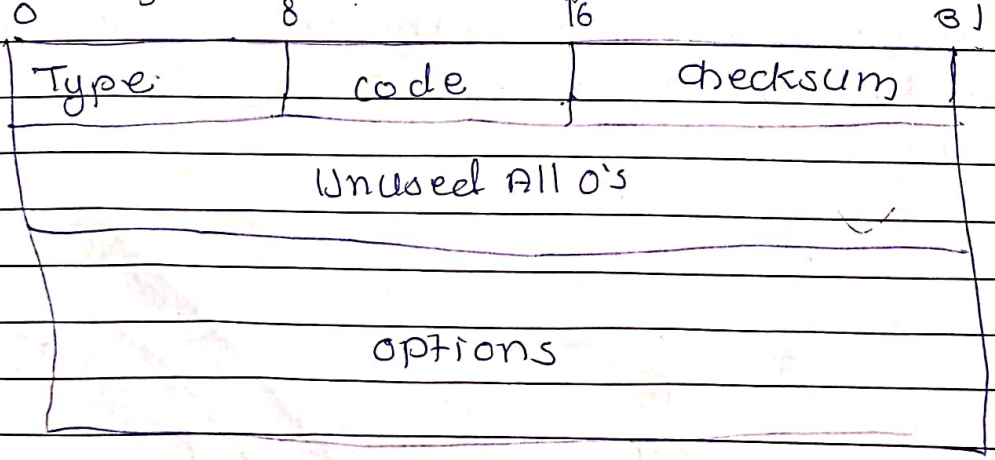


Fig → Inverse neighbor - advertisement message

DATE / /

Group Membership Message

i) membership-query message

membership report message

1) membership - Query message

- It is sent by a router to find active group members in the network

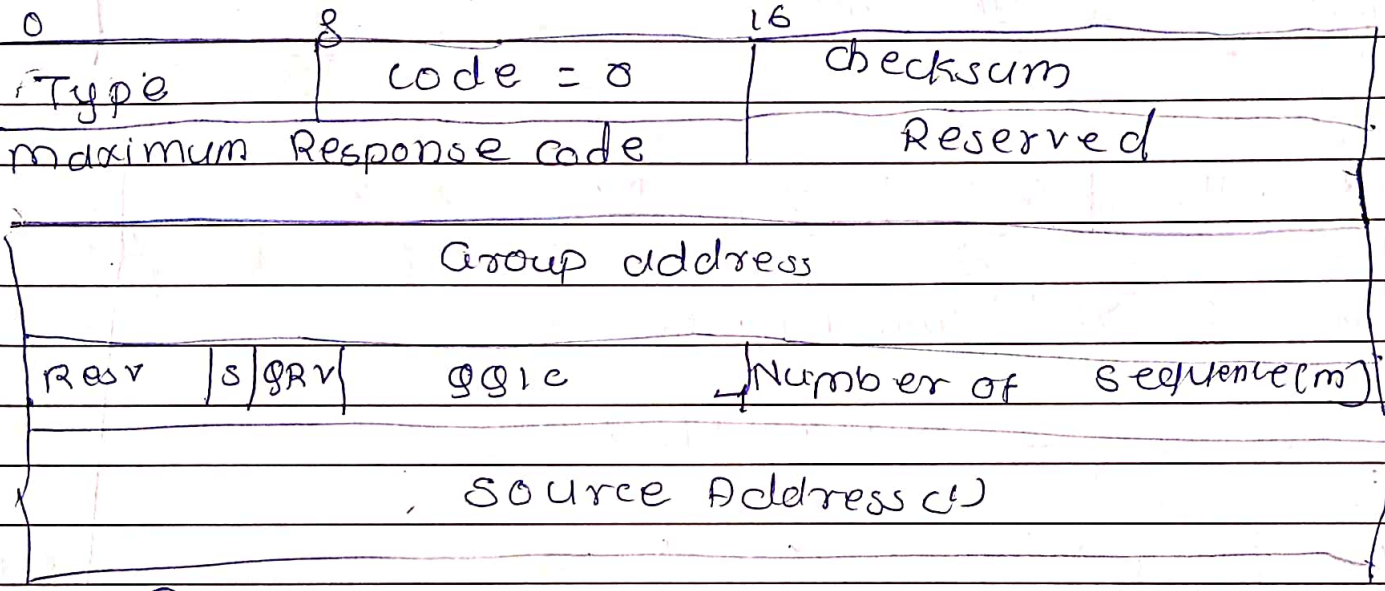
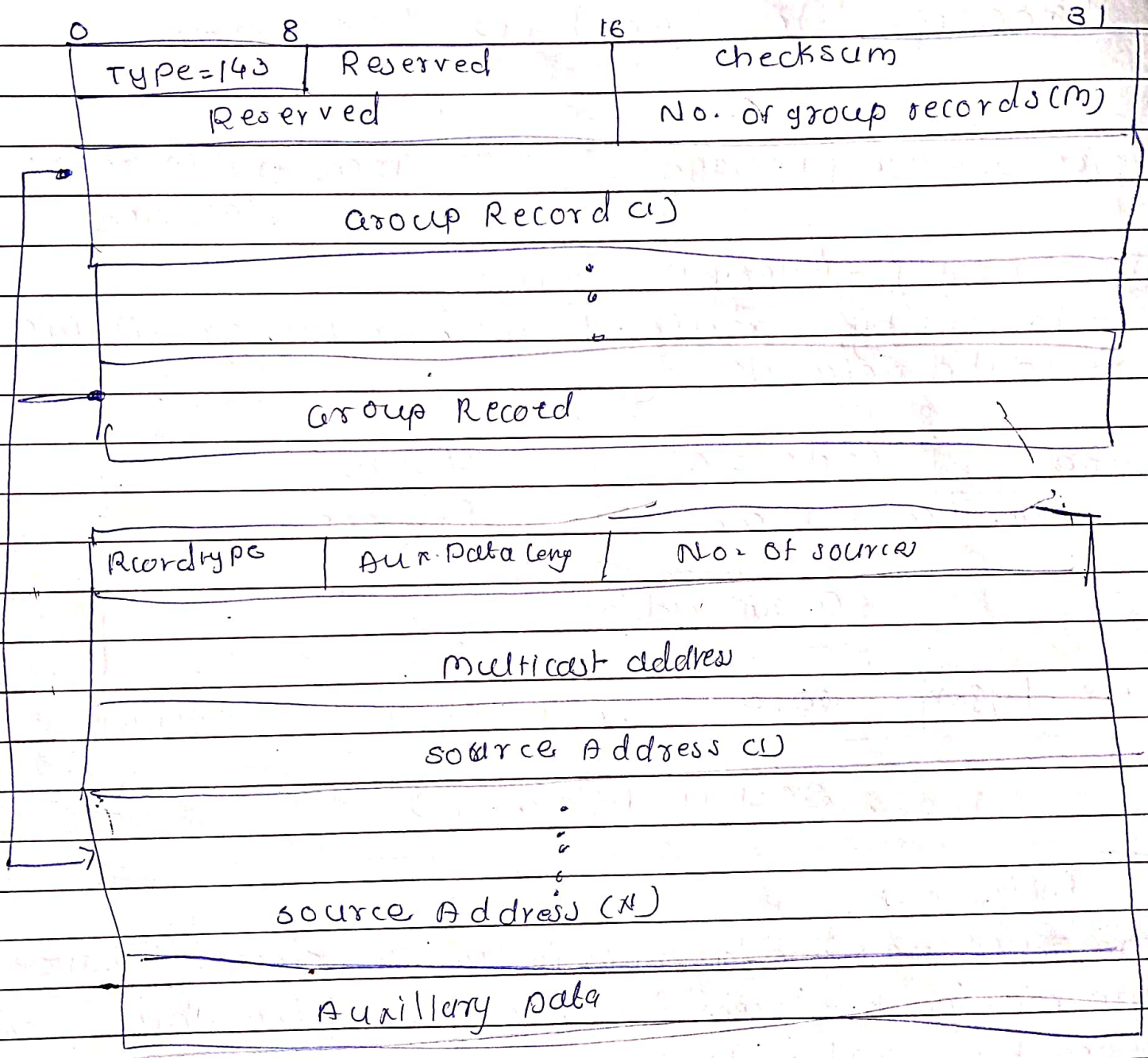


Fig:

- The fields are same as ones in IGMPv3 except the size of the multicast address & the source address has been changed from 32 bits to 128 bits.
- Another change in the field size is in the maximum response code field, in which size has been changed from 8 bits to 16 bits.

2) membership - Report Message

- Format of the membership report in MLDv2 is exactly same as one in IGMPv3 except that the sizes of the fields are changed because of the address size.


0
8
16
31
Type=143
Reserved
checksum
Reserved
No. of group records (M)
Group Record (1)
Group Record
RecordType
Aux Data Len
No. of sources
Multicast address
source Address (1)
source Address (N)
Auxiliary Data

If the DNS returns an IPv6 address, the source host sends an IPv6

② Tunneling → IPv6 client — IPv4 — IPv6 server (IPv4 encapsulate; IPv6 packet is encapsulated in an IPv4 packet when it enters the IPv4 region; tunnel)

- It is a strategy used when two computers using IPv6 want to communicate with each other & the packet must pass through a region that uses IPv4.
- To pass through this region, the packet must have an IPv4 address.
- So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region & it leaves its capsule when it exists the region.
- If the IPv6 packet goes through a tunnel at one end & emerges at other end. To make it clear that the IPv4 packet is carrying an IPv6 packet as data, the protocol value is set to 41

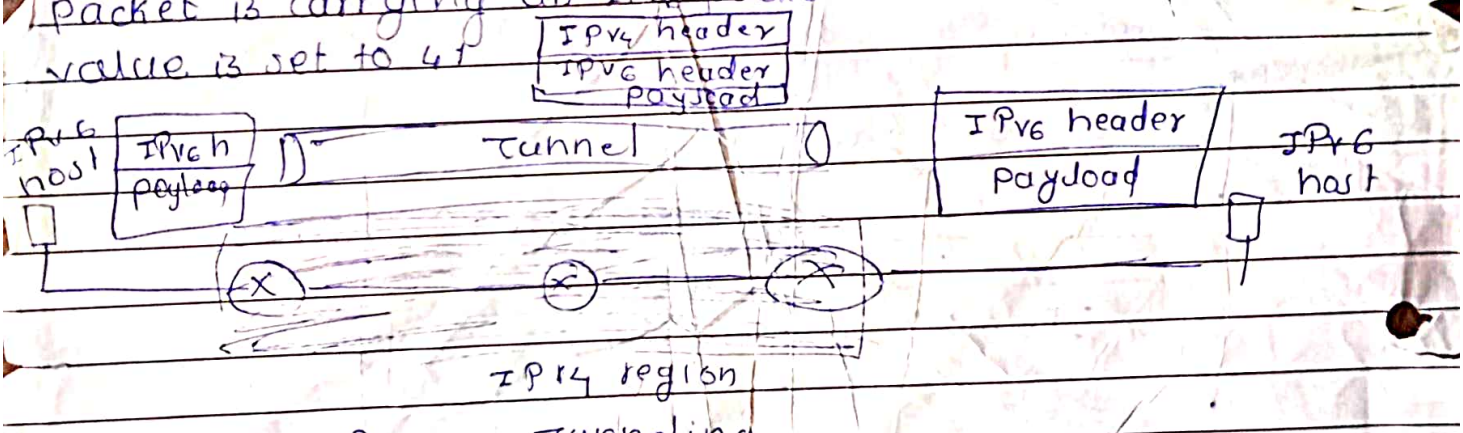


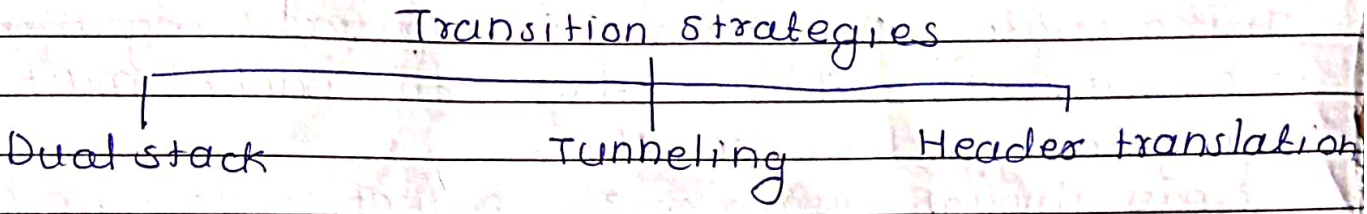
Fig. → Tunneling

③ Header translation

- It is necessary when the majority of the internet has moved to IPv6 but some systems still use IPv4.
- The sender wants to use IPv6, but receiver does not understand IPv6.
- Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver.
- In this case, the header format must totally changed through header translation.

Transition from IPv4 TO IPv6

- Transition from IPv4 to IPv6 can't happen suddenly because of the huge no. of systems on the internet.
- There are 3 strategies are used for transition from IPv4 to IPv6.



1) Dual stack

- It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocol.
- Station must run IPv4 & IPv6 simultaneously until all the internet uses IPv6.

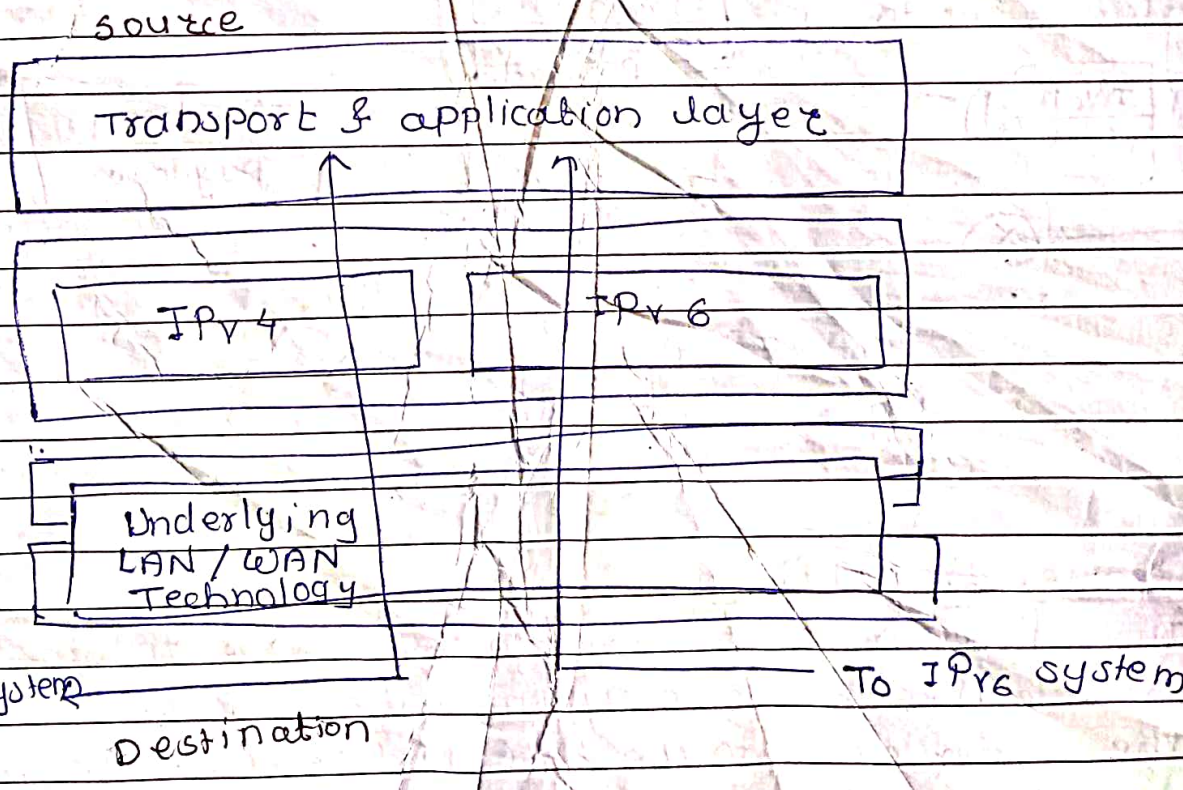


fig → Dual stack

- To determine which version to use when sending packet to a destination, the source host queries the DNS
- If the DNS returns an IPv4 address, the source host sends an IPv4 packet.