An undertaking of Bhaktapur Municipality

Khwopa College of Engineering

Affiliated to Tribhuvan Univeristy

Libali, Bhaktapur, Nepal

A
Note
on
Computer Network

Compiled By

Er. Dinesh Ghemosu

Table of Contents

The unexamined life is not worth living.

Socrates

7

Introductin of IPV6

7.1 Introduction

- Internet Protocol version 6 (IPv6) was developed to overcome the shortcomings of IPv4 and meet the future needs for internet.
  - Internet has grown exponentially and address space allowed by IPv4 is saturating.
  - IPv4 on its own does not provide any security features.
    - data has to be encrypted with some other security application before being sent on the internet.
  - Data prioritization in IPv4 is not up-do-date.
    - Though IPv4 has a few bits reserved for service type, but they do ot provide much functionality such as for real-time data.
  - IPv4 lacks authentication and privacy of data, and support for QoS.
  - IPv4 does not provide route aggregation, jumbo frames delivery and auto configuration.

7.2 Benefits of IPv6

- **Expanded Address Space** : 128 bits long, 3.1 x 10^{38} addresses.
- **Simplification of header** : only 7 fields; This change allows routers to process packets faster and speed up routing . This further improves throughout and delay.
- **Better support for option** : extended header speeds up packet processing time.
- **Security** : encryption and authentication, IPsec
- **Quality of Service**: real-time traffic such as for multimedia.
- **Stateful and Stateless auto-configuration**: allows devices on a network to address themselves with a link-local unicast address as well as with a global unicast address.

7.3 IPv6 Address

- IPv6 address are 128 bits in length. (16 bytes) Address space =$2^{128} = 3.4 \times 10^{38}$ possible addressable nodes.
- It uses hexadecimal colon notation.
- In this notation 128 bits is divided into eight sections. Each section is 2 bytes long.
- Two bytes in hexadecimal notation require four hexadecimal digits. Thus, the address consists of 32 hexadecimal digits, with every four digits separated by a colon.

We can write IPv6 in abbreviated form (Figure 7.2):
- This can be done by omitting the leading zeros of a section (four digits between two colons).
- In such a form, only leading zero can be omitted and not the trailing zeros.

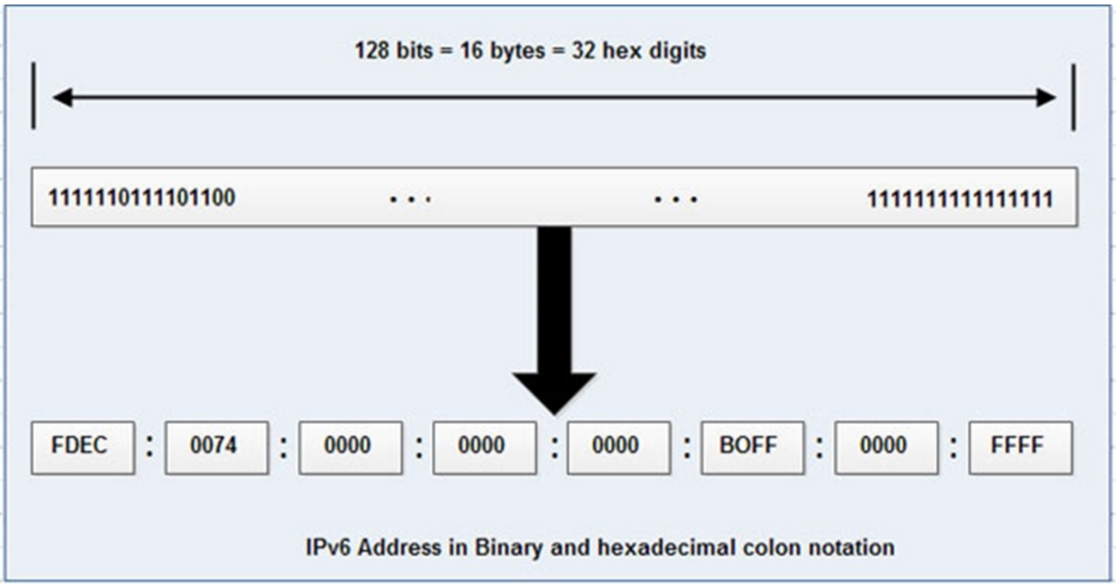
128 bits = 16 bytes = 32 hex digits
1111110111101100
• • •
• • •
1111111111111111
FDEC : 0074 : 0000 : 0000 : 0000 : BOFF : 0000 : FFFF
IPv6 Address in Binary and hexadecimal colon notation

Figure 7.1: IPv6 Notation

- Using this form of abbreviation, 0074 can be written as 74, 000F as F, and 0000 as 0.Note 3210 cannot be abbreviated.
- Further abbreviations are also possible if there are consecutive sections consisting of zeros only. Using this scheme, zeros can be removed altogether and can be replaced with a double colon.

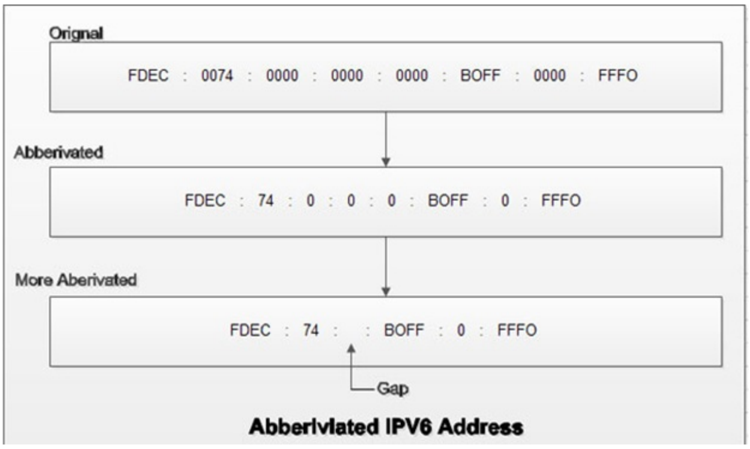
Orignal
FDEC : 0074 : 0000 : 0000 : 0000 : BOFF : 0000 : FFFO
Abberivated
FDEC : 74 : 0 : 0 : 0 : BOFF : 0 : FFFO
More Aberivated
FDEC : 74 : : BOFF : 0 : FFFO
Gap
Abberiviated IPV6 Address

Figure 7.2: Abbreviated IPv6 Address.

7.4 Part of IPv6 Address

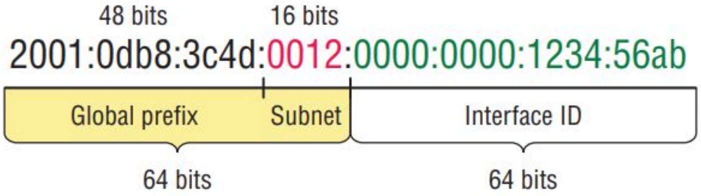

Figure 7.3: IPv6 address example.

Prefixes in IPv6

- The leftmost fields of the IPv6 address contain the prefix, which is used for routing IPv6 packets. IPv6 prefixes have the following format:

$$prefix/lengthinbits$$

- Prefix length is stated in classless inter-domain routing (CIDR) notation. CIDR notation is a slash at the end of the address that is followed by the prefix length in bits.

7.5 IPv6 Address Types

There are three types of addresses.

i. Unicast
   - An address for a single interface.
   - Types:
     - Global Unicast Address: These are your typical publicly routable addresses and they're the same as in IPv4. Global addresses start at 2000::/3.
     - Link-local address: These are like the Automatic Private IP Address (APIPA) addresses that are not meant to be routed. They start with FE80::/10.

ii. Multicast
   - An address for a set of interfaces and is delivered to all interfaces identified by that address. Packets that are sent to the multicast address go to all members of the multicast group. Muticast address start with FF00::/8.

iii. Anycast
   - An address for a set of interfaces and is delivered to one of the interfaces identified by that address. Packets that are sent to the anycast address go to the anycast group member node that is physically closest to the sender.

Note: There is no broadcast address in IPv6.

7.6 IPv6 Header

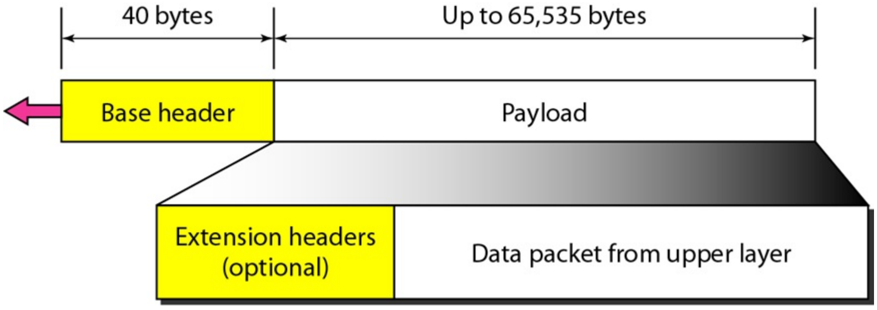

Figure 7.4: IPv6 datagram header and payload.

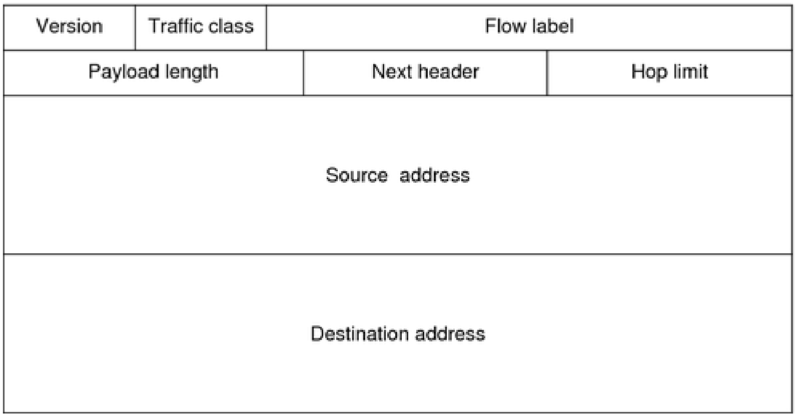

Figure 7.5: IPv6 datagram header format.

- **Version (4 bits)**
  - Identifies the version of IP protocol.

- Version field is always 6 for IPv6.

- **Traffic Class (8 bits)**
  - Identifies and distinguish between different classes or priorities of IPv6 packets.

- **Flow Label (20 bits)**
  - Used to maintain the sequential flow of packets. - Host label those packets for which it is requesting special handling by routers in the networks.
  - A flow is uniquely identified by the combination of a source address, destination address, and a nonzero 20-bit flow label. Thus, all packets that are to be part of the same flow are assigned the same flow label by the source. Helps avoid re-ordering of data packets.
  - Designed for streaming/real-time media.

- **Payload Length (16 bits)**
  - Specify the length of the payload in bytes.
  - Payload is composed of Extension Headers and Upper Layer data.

- **Next Header**
  - Identifies the type of extension header immediately following the IPv6 header

- **Hop Limit (8 bits)**
  -Specifies the maximum number of hop an IPv7 packet can be forwarded.
  - Decremented by 1 by each node that forwards the packet.
- **Source Address (128 bits)**
  Indicates the address of originator of the packet.

- **Destination Address (128 bits)**
  Indicates the intended portion of the packet.

7.7 Comparison between IPv4 and IPv6

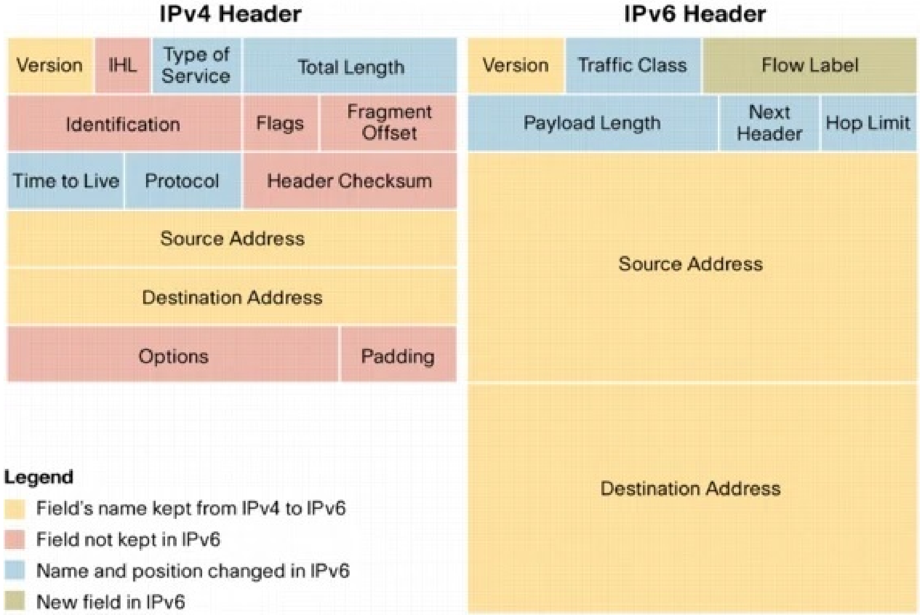

Figure 7.6: Ipv4 and IPv6 header comparision.

Key Difference:

- IPv4 is 32-Bit IP address whereas IPv6 is a 128-Bit IP address.
- IPv4 is a numeric addressing method whereas IPv6 is an alphanumeric addressing method.
- IPv4 binary bits are separated by a dot(.) whereas IPv6 binary bits are separated by a colon(:).

- IPv4 offers 12 header fields whereas IPv6 offers 8 header fields.
- IPv4 supports broadcast whereas IPv6 doesn't support broadcast.
- IPv4 has checksum fields while IPv6 doesn't have checksum fields
- When we compare IPv4 and IPv6, IPv4 supports VLSM (Variable Length Subnet Mask) whereas IPv6 doesn't support VLSM.
- IPv4 uses ARP (Address Resolution Protocol) to map to MAC address whereas IPv6 uses NDP (Neighbour Discovery Protocol) to map to MAC address.

Issues	**IPv4**	**IPv6**
Size of IP address	32 bit	128 bit
Addressing Method	IPv4 is a numeric address, and its binary bits are separated by a dot (.)	IPv6 is an alphanumeric address whose binary bits are separated by a colon (:). It also contains hexadecimal.
Number of header fields	18	8
Length of header filed	20 - 60 bytes	40 bytes fixed
Checksum	Yes	No filed for it.
Examle	172.2345.24	2001:0db8:0000:0000:0000:ff00:0042:7879
Types of address	Unicast, broadcast, and multicast.	Unicast, multicast, and anycast.
Number of classes	IPv4 offers five different classes of IP Address. Class A to E.	lPv6 allows storing an unlimited number of IP Address.
Configuration	You have to configure a newly installed system before it can communicate with other systems.	In IPv6, the configuration is optional, depending upon on functions needed.
VLSM Support	Supports	Does not support.
Fragmentation	Fragmentation is done by sending and forwarding routes.	Fragmentation is done by the sender.
RIP	RIP is a routing protocol supported by the routed daemon.	RIP does not support IPv6. It uses static routes.
Network Configuration	Networks need to be configured either manually or with DHCP. IPv4 had several overlays to handle Internet growth, which require more maintenance efforts.	IPv6 support autoconfiguration capabilities.
Best Feature	Widespread use of NAT (Network address translation) devices which allows single NAT address can mask thousands of non-routable addresses, making end-to-end integrity achievable.	It allows direct addressing because of vast address Space.
Address Mask	Use for the designated network from host portion.	Not used.
SNMP	SNMP is a protocol used for system management.	SNMP doesnot support IPv6.
Mobility and Interoperability	Relatively constrained network topologies to which move restrict mobility and interoperability capabilities.	IPv6 provides interoperability and mobility capabilities which are embedded in network devices.
Security	Security is dependent on applications - IPv4 was not designed with security in mind.	IPSec(Internet Protocol Security) is built into the IPv6 protocol, usable with a proper key infrastructure.
Address Configuration	Manual ofr DHCP	Stateless address autoconfiguration using Internet Control Message Protocol version 6 (ICMPv6) or DHCPv6 .
IP to MAC resolution	Broadcast ARP	Multicast Neighbour Solicitation.
Local subnet Group management	Internet Group Management Protocol GMP)	Multicast Listener Discovery (MLD)

Optional Fields	Has optional field.	Does not have optional fields. But Extension headers are available.
Dynamic host configuration Server	Clients have approach DHCS (Dynamic Host Configuration server) whenever they want to connect to a network.	A Client does not have to approach any such server as they are given permanent addresses.
Mapping	Uses ARP(Address Resolution Protocol) to map to MAC address	Uses NDP(Neighbour Discovery Protocol) to map to MAC address

Table 7.1: Differences between IPv4 and IPv6.

7.8 Extension Header

- Some of the missing IPv4 fields are occasionally still needed, so IPv6 introduced the concept of extension headers.
- These headers can be supplied to provide extra information, but encoded in an efficient way.
- Fixed header contains only necessary information
  - Avoiding information which is either not required or is rarely used.
  - All such information is put between the Fixed Header and the upper layer header in the form of extension headers.
  - Each extension header is identified by a distinct value.
- When extension header are used,
  - IPv6 Fixed Header's Next Header field points to the first Extension Header.
  - If there is one more Extension Header, then the first Extension Header's 'Next Header' field points to the second one, and so on.
  - The last Extension Header's 'Next-Header' field points to the Upper Layer Header.

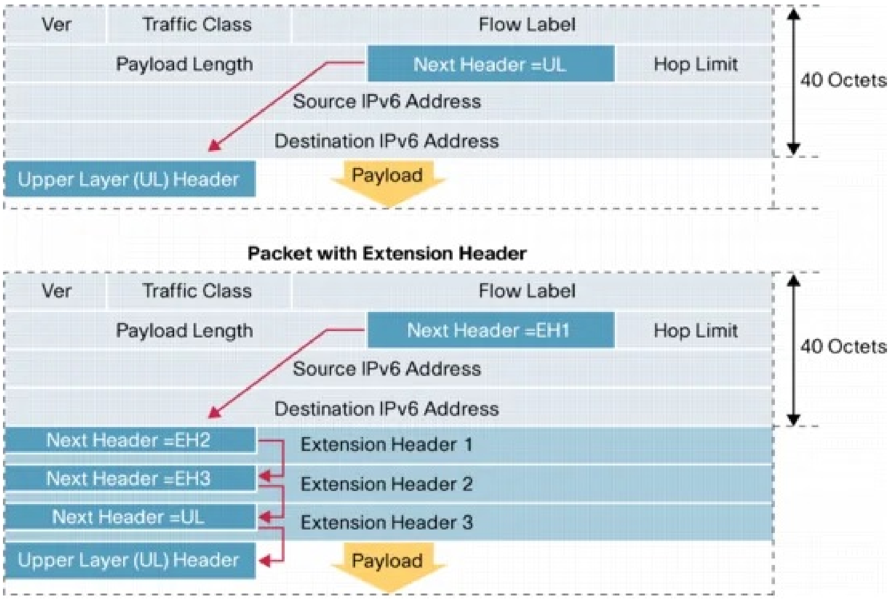

Figure 7.7: Chaining extension headers in IPv6.

Note: The only MUST requirement is that the Hop-by-Hop EH has to be the first one.

IPv6 Extension Headers and their Recommended Order in a Packet

Hop-by-Hop Option Header

- Must be the first header extension.
- If present, must be examined by every router along the path.

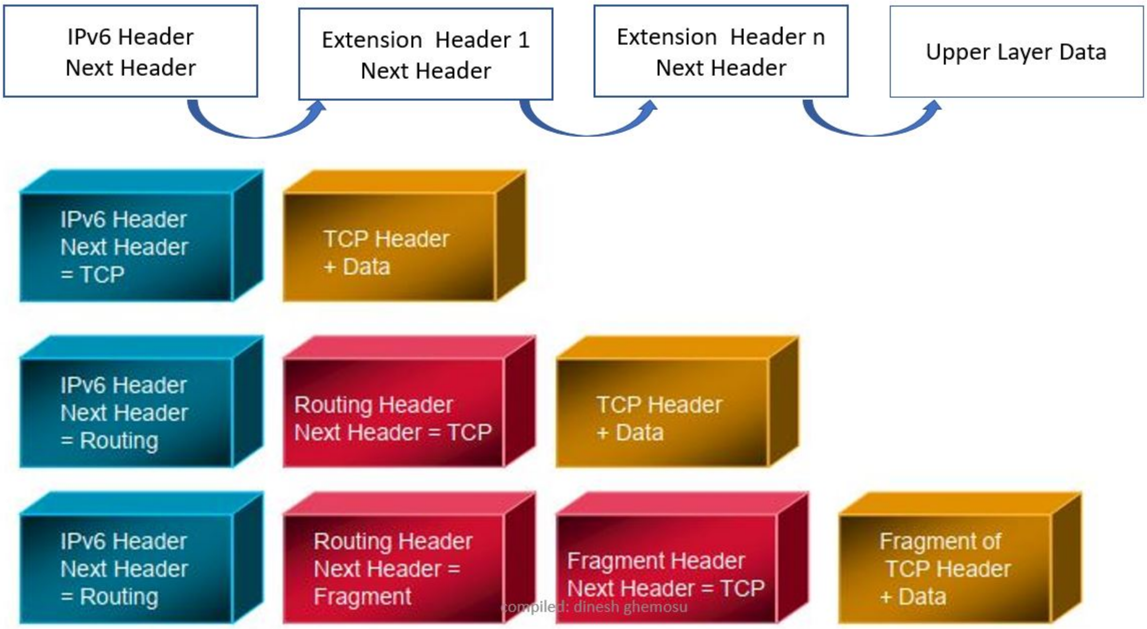

Figure 7.8: Extension header chaining example.

Table 7.2: Extension header types and next header code.

Order	Header Type	Next Header Code
1	Basic IPv6 Header	-
2	Hop-by-Hop Header	0
3	Destination Option (with Rouging Option)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
•	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

- Used for the support of Jumbo-grams or, with the Router Alert option.
- It is identified by the value of 0 in the IPv6 header's Next Header field.
- Consists of a *Next Header field*, a *Header Extension Length field*, and an *Options field* that contains one or more options.
- The value of the Header Extension Length field is 0. - An option is a set of fields that either describes a specific characteristic of the packet delivery or provides padding. Each option is encoded in the type-length-value (TLV) format.

Destination Option Header
- Used to specify packet delivery parameters for either intermediate destinations or the final destination.
- This header is identified by the value of 60 in the previous header's Next Header field.
- Format of header is same as that of hop-by-hop option header.

Routing Header
- List one or more routers that must be visited on the way to the packet's destination. - The Routing header is identified by the value of 43 in the previous header's Next Header field. - The Routing header consists of

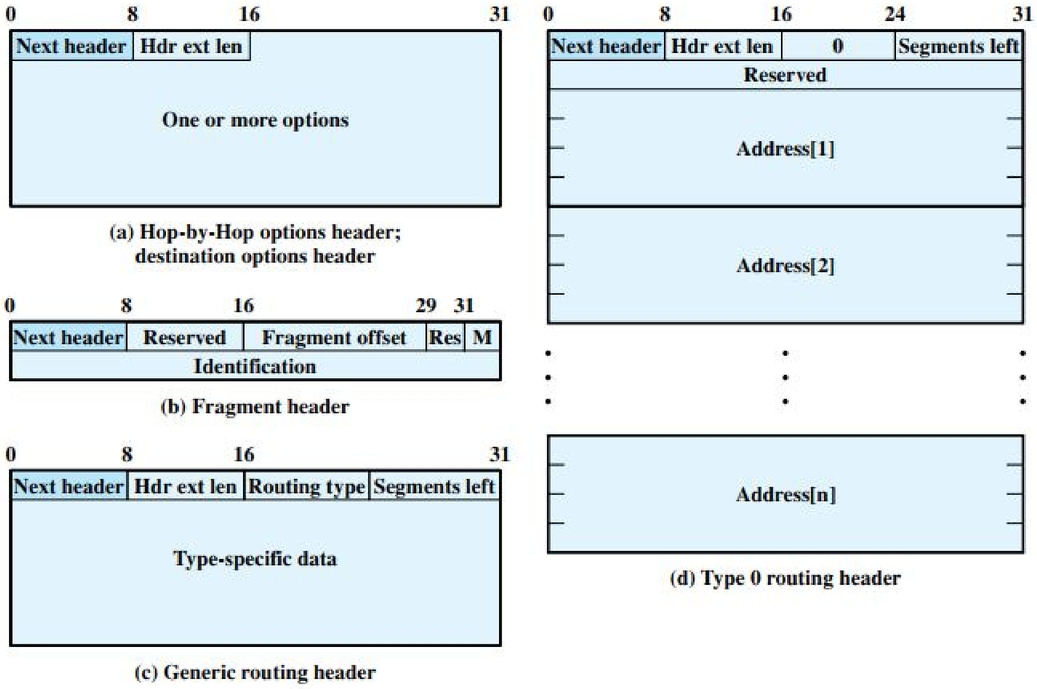

Figure 7.9: Extension headers format.

- a Next Header field,
- a Header Extension Length field (defined in the same way as the Hop-by-Hop Options extension header),
- a Routing Type field,
- a Segments Left field that indicates the number of intermediate destinations that are still to be visited, and
- routing type-specific data.

Fragment Header
- The Fragment header is used for IPv6 fragmentation and reassembly services.
- This header is identified by the value of 44 in the previous header's Next Header field.
- The Fragment header includes a Next Header field, a 13-bit Fragment Offset field, a More Fragments flag, and a 32-bit Identification field. The Fragment Offset, More Fragments flag, and Identification fields are used in the same way as the corresponding fields in the IPv4 header.
- In IPv6, only source nodes can fragment payloads. An IPv6 router will never fragment an IPv6 packet being forwarded.

Authentication Header
The Authentication header provides:
- data authentication (verification of the node that sent the packet),
- data integrity (verification that the data was not modified in transit), and
- anti-replay protection (assurance that captured packets cannot be retransmitted and accepted as valid data)
for the IPv6 packet, including the fields in the IPv6 header that do not change in transit across an IPv6 internetwork.
The Authentication header is identified by the value of 51 in the previous header's Next Header field.

Note:
- The Authentication header does not provide data confidentiality services for the upper-layer PDU by encrypting the data so that it cannot be viewed without the encryption key.
- To obtain data authentication and data integrity for the entire IPv6 packet and data confidentiality for the upper-layer PDU, you can use both the Authentication header and the Encapsulating Security Payload header

and trailer.

Encapsulating Security Payload
- The Encapsulating Security Payload (ESP) header and trailer provide data confidentiality, data authentication, data integrity, and replay protection services to the encapsulated payload.
- The ESP header provides no security services for the IPv6 header or extension headers that occur before the ESP header.
- The ESP header and trailer are identified by the value of 50 in the previous header's Next Header field.

Extension Header References:
`https://www.microsoftpressstore.com/articles/article.aspx?p=2225063&seqNum=4`
`https://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d`
`html`

7.9 IPv6 Multicasting

- Multicasting is the process of sending packets from a host to the multiple number of member hosts of a multicast group.
- IPv6 supports the use of multicast addresses. The multicast address identifies a multicast group, which is a group of interfaces, usually on different nodes. An interface can belong to any number of multicast groups. If the first 16 bits of an IPv6 address is FF00, the address is a multicast address. **FF00::/8** indicates that multicast address follows.
- Multicast addresses are used for sending information or services to all interfaces that are defined as members of the multicast group. For example, one use of multicast addresses is to communicate with all IPv6 nodes on the local link.
- When an interface's IPv6 unicast address is created, the kernel automatically makes the interface a member of certain multicast groups. For example, the kernel makes each node a member of the Solicited Node multicast group, which is used by the Neighbor Discovery protocol to detect reachability. The kernel also automatically makes a node a member of the All-Nodes or All Routers multicast groups.

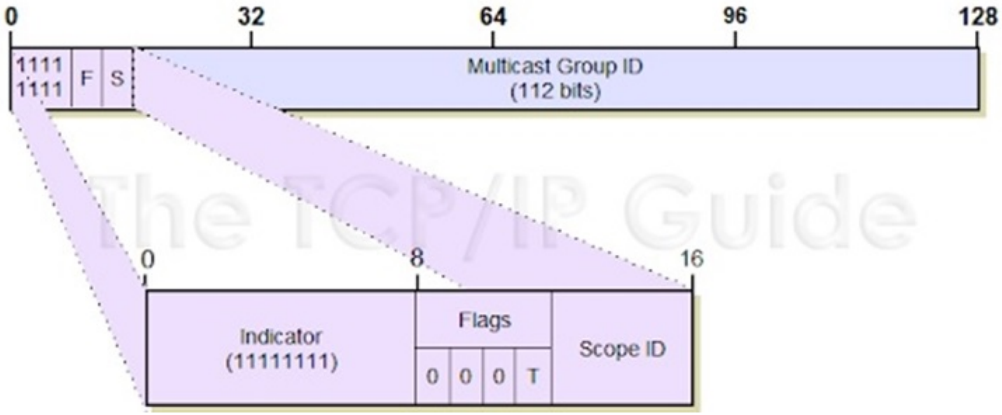

Figure 7.10: General Multicast address format for IPv6.

- IPv6 multicast address are in the range of FF00::/8 - Flag field: 000T values.
    - *T = 0*, for permanent address defined by IANA (Internet Assigned Numbers Authority)
    - *T = 1*, for transient addresses.
- Scope field: the domain in which the multicast packet should be propagated.

7.10 Overview of IPv4 to IPv6 Transition Mechanism

- Three strategies have been devised for transitions (figure 7.11):

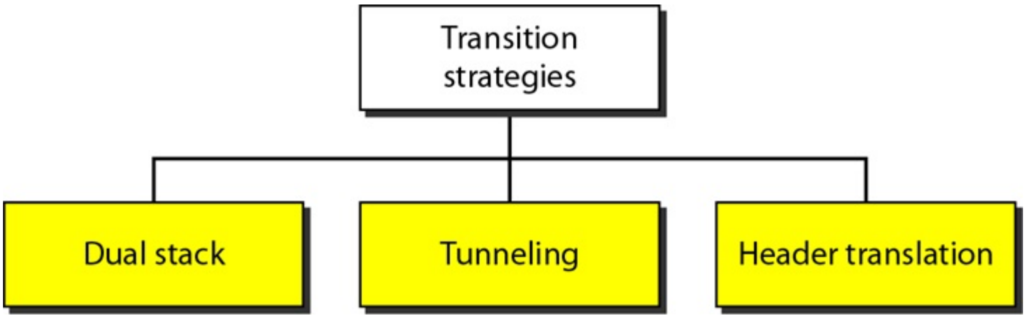

Figure 7.11: IPv4 to IPv6 transition strategies.

7.10.1 Dual Stack

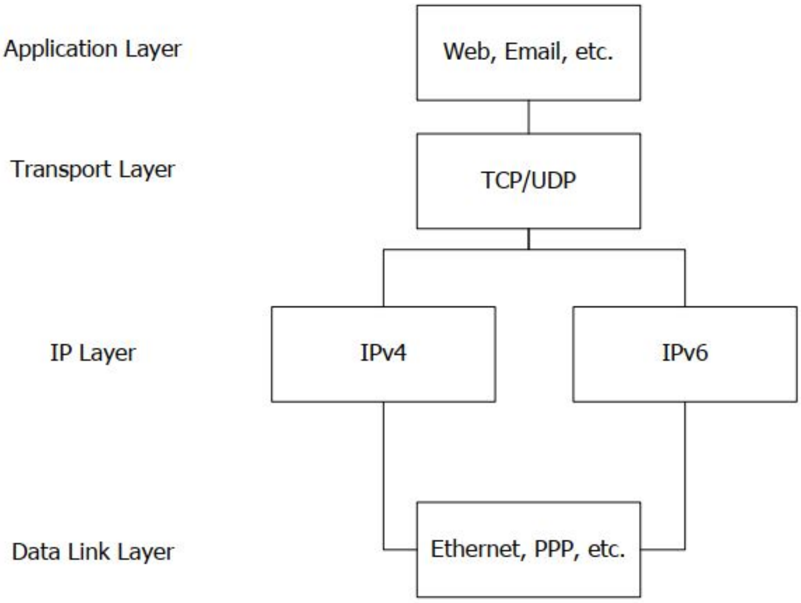

Figure 7.12: Dual stack.

- It is recommended that all nodes (i.e stations, intermediate network devices), before migrating completely to version 6, have a dual stack of protocols during the transition, i.e. a node must run IPv4 and IPv6 simultaneously until the Internet uses IPv6.
- If both the end stations support IPv6, they can communicate with IPv6, otherwise they will communicate with IPv4.
- To determine which version to use when sending a packet to destination, the source host queries the DNS; if the DNS returns an IPv4 address, the source host sends an IPv4 packet, else IPv6 packet.

7.10.2 Tunneling

- When different IP versions exist on intermediate path or transit networks, tunneling provides a better solution where user's data can pass through non-supported IP version.
- Figure 7.14 and 7.13 depicts the communication through tunnel.

Tunneling IPv6 via IPv4 Network

- Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass 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 as it enters the region, and leaves it capsule when it exits the region.
- During this, IPv4 is carrying an IPv6 packet as data, and the protocol is set to 41.
- Figure 7.13 depicts the encapsulation process of IPv6 header when transit through IPv4 network.

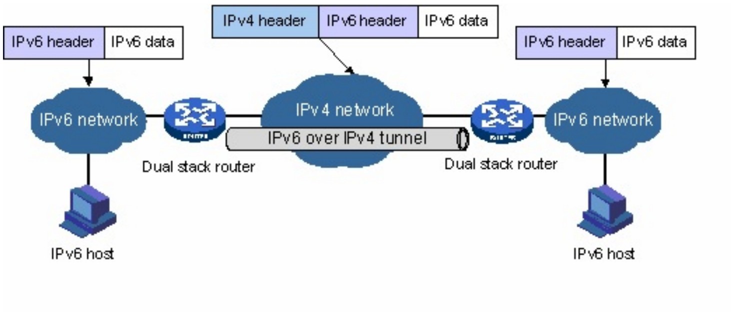

Figure 7.13: Tunneling IPv6 via IPv4.

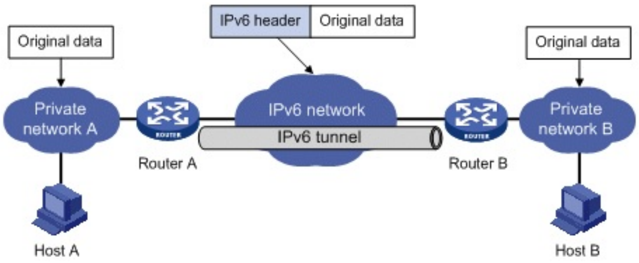

Figure 7.14: Tunneling IPv4 via IPv6.

Automatic Tunneling Mechanisms: 6to4 Overview
- The most widely used mechanism.
- In its basic configuration, 6to4 is used to connect two IPv6 hosts across an IPv4 network.
- Use special trick for the **2002::/16** IPv6 prefix that is reserved for 6to4 use.
- Next 32 bits of the prefix are the 32 bits of the IPv4 address of the 6to4 router.
- For example, a 6to4 router on 192.168.10.10 would use an IPv6 prefix of 2002:C0A8:0A0A::/48 for its site network.

- When a 6to4 router seeks a packet with destination prefix 2002::/16, it knows to tunnel the packet in IPv4 towards the IPv4 address indicated in the next 32 bits.
- Thus, any site with single unicast IPv4 address can transmit to the IPv6 network using the 2002::/16 prefix.

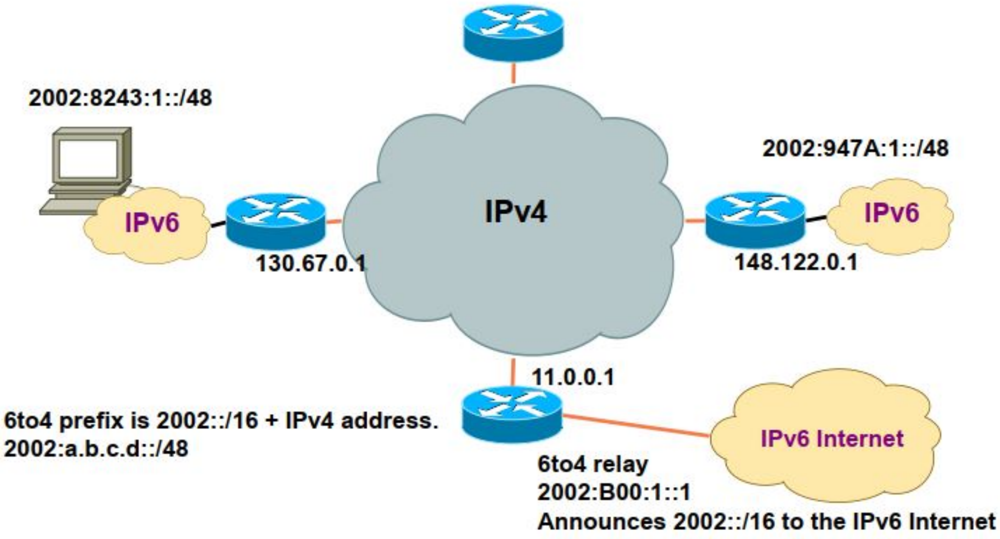

Figure 7.15: An example of 6to4 tunnel.

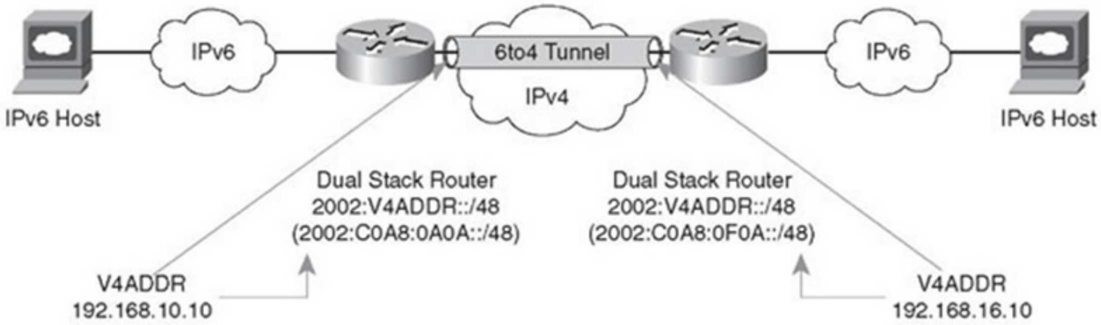

Figure 7.16: An example of 6to4 tunnel.

7.10.3 Header Translation

- Header Translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4. The sender wants to used IPv6, but the 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 be completely changed through header translation.
- The NAT-PT router translate IPv6 packets into IPv4 packets by doing address and port translation and vice-versa.

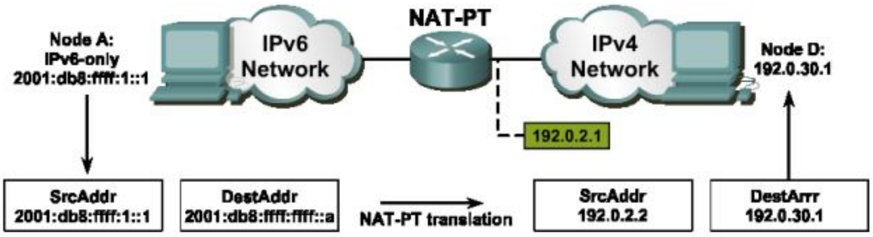

Figure 7.17: IPv6-IPv4 translation.

`https://en.wikipedia.org/wiki/IPv6`