IPv6 ADDRESSING

IPv4 has the small size of the address space.

An IPv6 address is 128 bits or 16 bytes(octets) long, four times the address length in IPv4.

IPv6 address, in hexadecimal format, is very long, many of the digits are zeros.

In this case, the leading zeros of a section canbe omitted. Using this form of abbreviation, 0074 can be written as 74, 000F as F, and 0000 as 0.

Address Space

The address space of IPv6 contains 2128 addresses. This address space is 296 times the IPv4 address—definitely no address depletion—as shown, the size of the space is

340, 282, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456.

Three Address Types

In IPv6, a destination address can be of three categories: unicast, anycast, and multicast.

Unicast Address

A unicast address defines a single interface (computer or router). The packet sent to aunicast address will be routed to the intended recipient (Receiver).

Anycast Address

An anycast address defines a group of computers that all share a single address. A packet with an anycast address is delivered to only one member of the group, the most reachable one.

An anycast communication is used, for example, when there are several servers that can respond to an inquiry. The request is sent to the one that is most reachable.

Multicast Address

A multicast address defines a group of computers.

Difference between any casting and multicasting.

In any casting, only one copy of the packet is sent to one of the members of the group; in multicasting each member of the group receives a copy.

Address Space Allocation

Like the address space of IPv4, the address space of IPv6 is divided into several blocks of varying size and each block is allocated for a special purpose. Most of the blocks are still unassigned and have been set aside for future use.

IPv6 Packet Format

The IPv6 packet is shown in Figure 3.5.1. Each packet has a base header followed by the payload. The base header occupies 40 bytes, payload is upto 65,535 bytes of information.

The description of fields follows.

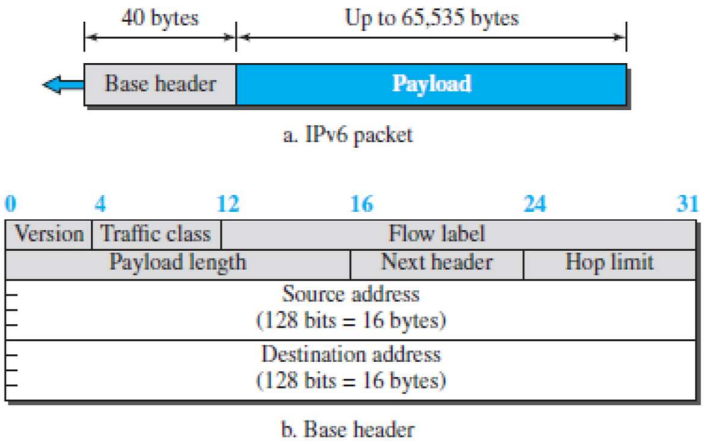

Fig3.5.1: IPv6 datagram.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-674]

Version. The 4-bit version field defines the version number of the IP. For IPv6, the value is 6.

Traffic class. The 8-bit traffic class field is used to distinguish different payloads with different delivery requirements. It replaces the type-of-service 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 header.

Note that IPv4 defines two fields related to the length: header length and total length.

In IPv6, the length of the base header is fixed (40 bytes); only the length of the payload needs to be defined.

Next header. The **next header** is an 8-bit field defining the type of the first extension header (if present) or the type of the data that follows the base header in the datagram.

Hop limit. The 8-bit hop limit field serves the same purpose as the TTL field in IPv4.

Source and destination addresses. The source address field is a 16-byte (128bit) internet address that identifies the original source of the datagram.

The destination address field is a 16-byte (128-bit) Internet address that identifies the destination of the datagram.

Payload. Compared to IPv4, the payload field in IPv6 has a different format and meaning, as shown in Figure .

Extension Header

An IPv6 packet is made of a base header and some extension headers. The length of the base header is fixed at 40 bytes.

To give more functionality to the IP datagram, the base header can be followed by up to six extension headers as shown in figure 3.5.2.

Six types of extension headers have been defined.

These are hop-by-hop option, source routing, fragmentation, authentication, encrypted security payload, and destination option (see Figure below).

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. For example, routers must be informed about certain management, debugging, or control functions.

Destination Option

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.

Fragmentation

The concept of fragmentation in IPv6 is the same as that in IPv4.

In IPv6, only the original source can fragment. A source must use a Path MTU.

Discovery technique to find the smallest MTU supported by any network on the path. The source then fragments using this knowledge.

If the source does not use a Path MTU Discovery technique, it fragments the datagram to a size of 1280 bytes or smaller. This is the minimum size of MTU required for each network connected to the Internet.

Authentication

The authentication extension header has a dual purpose:

It validates the message sender and ensures the integrity of data. It is needed so the receiver can be sure that a message is from the genuine sender and not others.

Encrypted Security Payload

The encrypted security payload (ESP) is an extension that provides confidentiality and guards against eavesdropping.

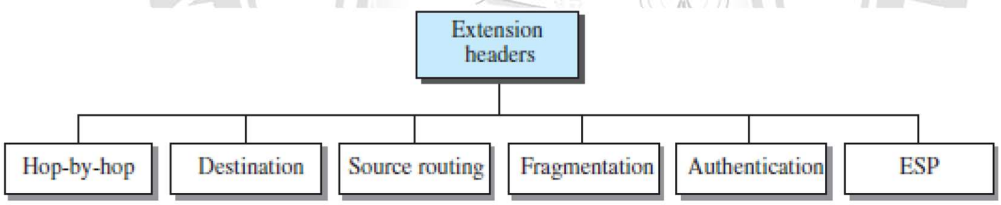

Fig3.5.2: Extension header types.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-677]