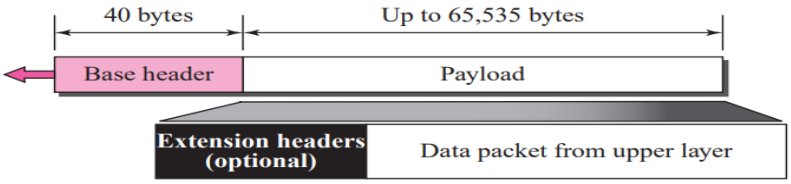
IPv6 Protocol:

IPv6 protocol responds to the above issues using the following main changes in the protocol:

- **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.

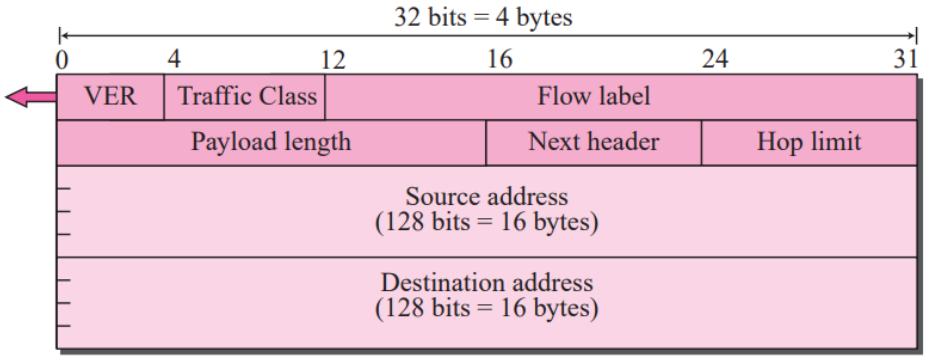
PACKET Format

Figure 27.1 *IPv6 datagram*



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.

Figure 27.2 *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. Each extension header also contains this field. Table 27.1 shows the values of next headers. Note that this field in version 4 is called the protocol.

❑ 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 connection-oriented protocol.

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

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 224 – 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.

Comparison between IPv4 and IPv6 Headers

The following shows the comparison between IPv4 and IPv6 headers.

❑ The **header length** field is eliminated in IPv6 because the length of the header is fixed in this version.

❑ The **service type field** is eliminated in IPv6. The traffic class and flow label fields together take over the function of the service type field.

❑ The **total length field** is eliminated in IPv6 and replaced by the payload length field.

❑ The **identification, flag, and offset fields** are eliminated from the base header in IPv6. They are included in the fragmentation extension header.

❑ The **TTL field** is called hop limit in IPv6.

❑ The **protocol field** is replaced by the next header field.

❑ The **header checksum** is eliminated because the checksum is provided by upper layer protocols; it is therefore not needed at this level.

❑ The **option fields in IPv4** are implemented as extension headers in IPv6.

Extension Headers

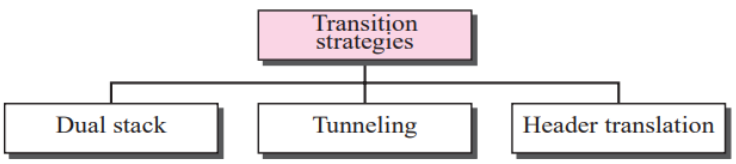
The length of the base header is fixed at 40 bytes. However, to give more functionality to the IP datagram, the base header can be followed by up to six extension headers. Many of these headers are options in IPv4. Figure 27.3 shows the extension header format. Six types of extension headers have been defined. These are hop-by-hop option, source routing, fragmentation, authentication, encrypted security payload, and destination option.

1. **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.
2. **Destination Option** The destination option is used when the source needs to pass information to the destination only.
3. **Source Routing** The source routing extension header combines the concepts of the strict source route and the loose source route options of IPv4.
4. **Fragmentation** 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.
5. **Authentication** The authentication extension header has a dual purpose: it validates the message sender and ensures the integrity of data.
6. **Encrypted Security Payload** The encrypted security payload (ESP) is an extension that provides confidentiality and guards against eavesdropping.

Translation from IPv4 to IPv6

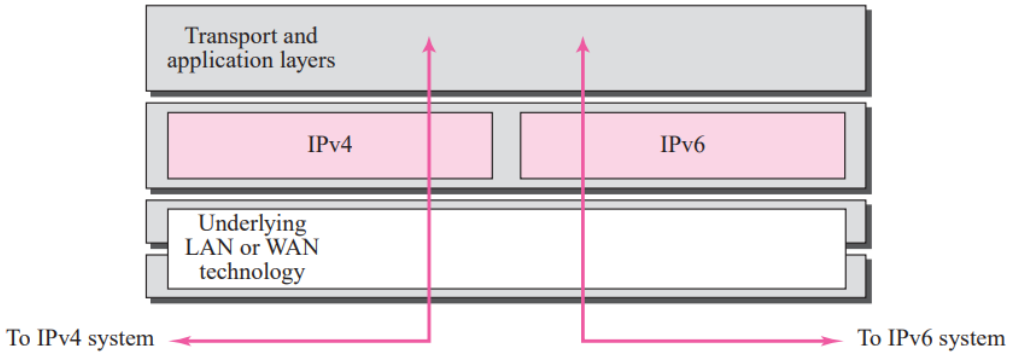
Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly. It will take a considerable amount of time before every system in the Internet can move from IPv4 to IPv6.

Figure 27.16 *Three transition strategies*



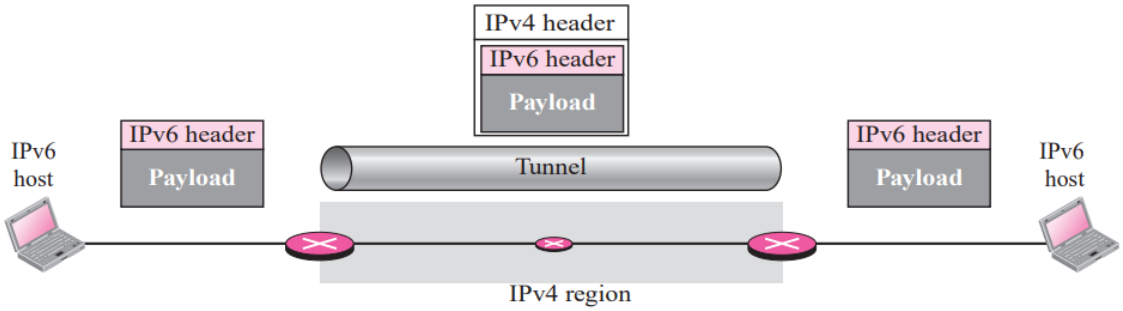
Dual Stack: A station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.

Figure 27.17 *Dual stack*



Tunneling: Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4**.**

Figure 27.18 *Tunneling strategy*



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 use 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 totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header.

Figure 27.19 *Header translation strategy*