



IPv6 Protocol Overview

An IPv6 packet has three parts: an IPv6 basic header, one or more IPv6 extension headers, and an upper-layer protocol data unit (PDU).

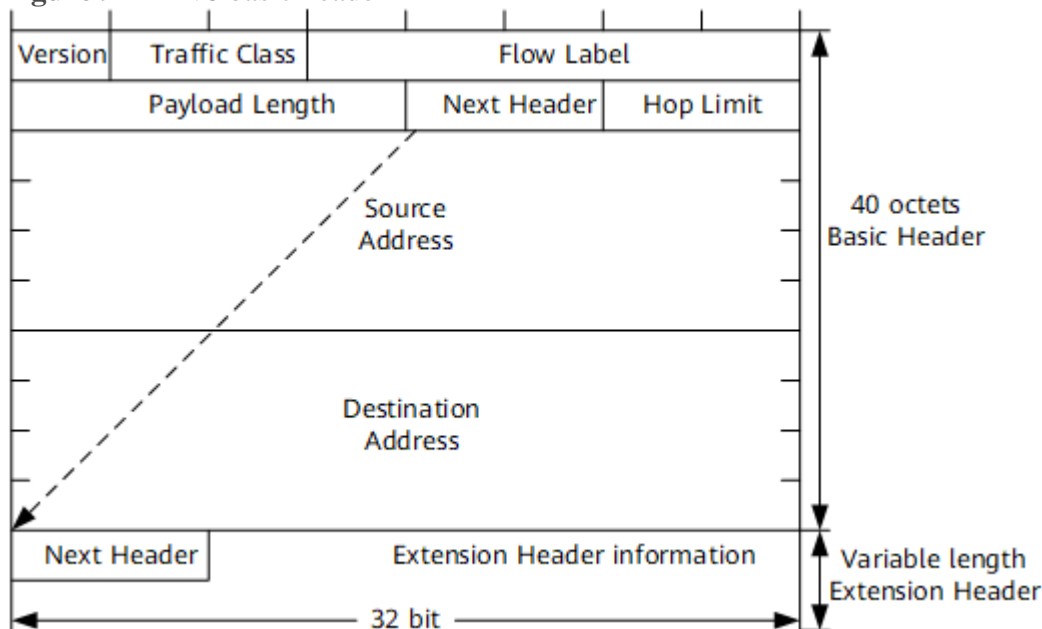
An upper-layer PDU is composed of the upper-layer protocol header and its payload, which maybe an ICMPv6 packet, a TCP packet, or a UDP packet.

IPv6 Basic Header

An IPv6 basic header is fixed as 40 bytes long and has eight fields. Each IPv6 packet must have an IPv6 basic header that provides basic packet forwarding information, and which all devices parse on the forwarding path.

[Figure 9-7](#) shows the IPv6 basic header.

Figure 9-7 IPv6 basic header



An IPv6 basic header contains the following fields:

- Version: 4 bits long. In IPv6, the value of the Version field is set to 6.
- Traffic Class: 8 bits long. This field indicates the class or priority of an IPv6 packet. The Traffic Class field is similar to the TOS field in an IPv4 packet and is mainly used in QoS control.
- Flow Label: 20 bits long. This field was added in IPv6 to differentiate traffic. A flow label and source IP address identify a data flow. Intermediate network devices can effectively differentiate data flows based on this field.
- Payload Length: 16 bits long. This field indicates the length of the IPv6 payload in bytes. The payload is the part of the IPv6 packet following the IPv6 basic header, including the extension header and upper-layer PDU. This field has a maximum value of 65535. If the payload length exceeds 65535 bytes, the field is set to 0, and the Jumbo Payload option in the Hop-by-Hop Options header is used to express the actual payload length.



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

- Next Header: 8 bits long. This field identifies the type of the first extension header that follows the IPv6 basic header or the protocol type in the upper-layer PDU.
- Hop Limit: 8 bits long. This field is similar to the Time to Live field in an IPv4 packet, defining the maximum number of hops that an IP packet can pass through. Each device that forwards the packet decrements the field value by 1. If the field value is reduced to 0, the packet is discarded.
- Source Address: 128 bits long. This field indicates the address of the packet originator.
- Destination Address: 128 bits long. This field indicates the address of the packet recipient.

Unlike the IPv4 packet header, the IPv6 packet header does not carry IHL, identifier, flag, fragment offset, header checksum, option, or padding fields, but it carries the flow label field. This facilitates IPv6 packet processing and improves processing efficiency. To support various options without changing the existing packet format, the Extension Header information field is added to the IPv6 packet header, improving flexibility. The following paragraphs describe IPv6 extension headers.

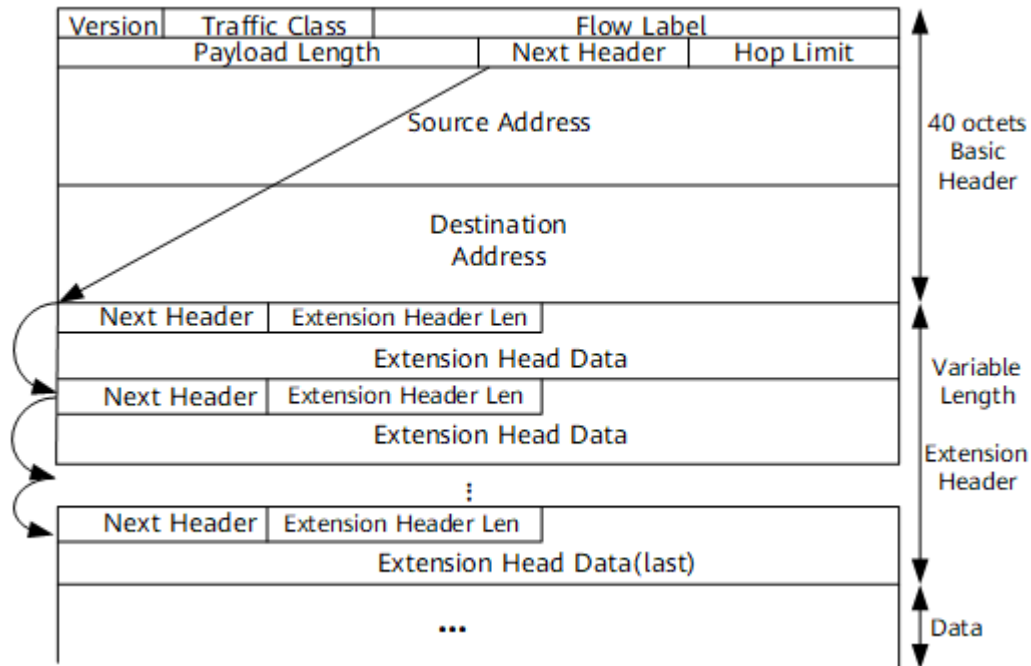
IPv6 Extension Header

An IPv4 packet header has an optional field (Options), which includes security, timestamp, and record route options. The variable length of the Options field makes the IPv4 packet header length range from 20 bytes to 60 bytes. When devices forward IPv4 packets with the Options field, many resources need to be used. Therefore, these IPv4 packets are rarely used in practice.

To improve packet processing efficiency, IPv6 uses extension headers to replace the Options field in the IPv4 header. Extension headers are placed between the IPv6 basic header and upper-layer PDU. An IPv6 packet may carry zero or more extension headers. The sender of a packet adds one or more extension headers to the packet only when the sender requests the destination device or other devices to perform special handling. Unlike IPv4, IPv6 has variable-length extension headers, which are not limited to 40 bytes. This facilitates further extension. To improve extension header processing efficiency and transport protocol performance, IPv6 requires that the extension header length be an integer multiple of 8 bytes.

When multiple extension headers are used, the Next Header field of an extension header indicates the type of the next header following this extension header. The Next Header field in the IPv6 basic header indicates the type of the first extension header, and the Next Header field in the first extension header indicates the type of the next extension header. If there are no extension headers following the current one, the Next Header field indicates the upper-layer protocol type. [Figure 9-8](#) shows the IPv6 extension header format.

Figure 9-8 IPv6 extension header format



An IPv6 extension header contains the following fields:

- Next Header: 8 bits long. This is similar to the Next Header field in the IPv6 basic header, indicating the type of the next extension header (if any) or the upper-layer protocol type.
- Extension Header Len: 8 bits long. This indicates the extension header length excluding the Next Header field.
- Extension Head Data: Variable length. This includes a series of options and the padding field.

RFC 2460 defines six IPv6 extension headers: Hop-by-Hop Options header, Destination Options header, Routing header, Fragment header, Authentication header, and Encapsulating Security Payload header.

Table 9-2 IPv6 extension headers

Header Type	Next Header Field Value	Description
Hop-by-Hop Options header	0	This header carries information that every node must examine along the delivery path of a packet. This header is used in the following applications: <ul style="list-style-type: none"> • Jumbo payload (if the payload length exceeds 65535 bytes) • Prompting devices to check this option before the devices forward packets. • Resource Reservation Protocol (RSVP)
Destination Options	60	This header carries information that only the destination node of a packet examines. Currently, this header is used in mobile IPv6.



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Header Type	Next Header Field Value	Description
header		
Routing header	43	An IPv6 source node uses this header to specify the intermediate nodes that a packet must pass through on the way to its destination. This option is similar to the Loose Source and Record Route option in IPv4.
Fragment header	44	Like IPv4 packets, the length of IPv6 packets to be forwarded cannot exceed the maximum transmission unit (MTU). When the packet length exceeds the MTU, the packet needs to be fragmented. In IPv6, the Fragment header is used by an IPv6 source node to send a packet larger than the MTU.
Authentication header	51	IPSec uses this header to provide data origin authentication, data integrity check, and packet anti-replay functions. It also protects some fields in the IPv6 basic header.
Encapsulating Security Payload header	50	This header provides the same functions as the Authentication header plus IPv6 packet encryption.

Conventions for IPv6 extension headers

When a single packet uses more than one extension header, the headers must be listed in the following order:

- IPv6 basic header
- Hop-by-Hop Options header
- Destination Options header
- Routing header
- Fragment header
- Authentication header
- Encapsulating Security Payload header
- Destination Options header
- Upper-layer header

Intermediate devices determine whether to process extension headers based on the Next Header field value in the IPv6 basic header. The intermediate devices do not need to examine or process all extension headers.

Each extension header can only occur once in an IPv6 packet, except for the Destination Options header which may occur twice (once before a Routing header and once before the upper-layer header).



SNS COLLEGE OF TECHNOLOGY, COIMBATORE –35
(An Autonomous Institution)
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

