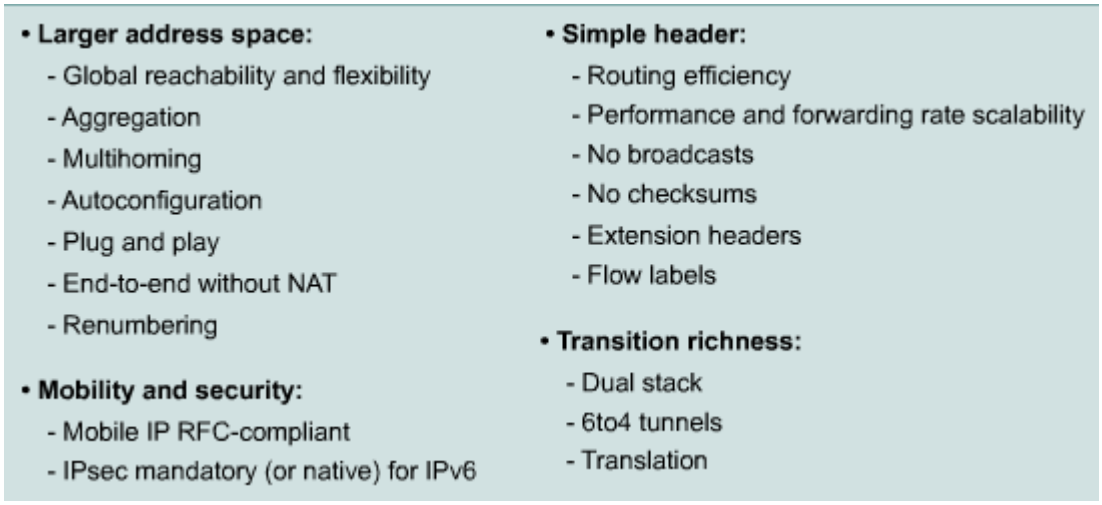
IPV6 AND ITS COMPARISON WITH IPV4

Features of IPV6:



- **Larger address space** Offers improved global reachability and flexibility; the aggregation of prefixes that are announced in routing tables; multihoming to several Internet service providers (ISPs) auto configuration that can include link-layer addresses in the address space; plug-and-play options; public-to private readdressing end to end without address translation; and simplified mechanisms for address renumbering and modification.

- **Simpler header:** Provides better routing efficiency; no broadcasts and thus no potential threat of broadcast storms; no requirement for processing checksums; simpler and more efficient extension header mechanisms; and flow labels for per-flow processing with no need to open the transport inner packet to identify the various traffic flows.

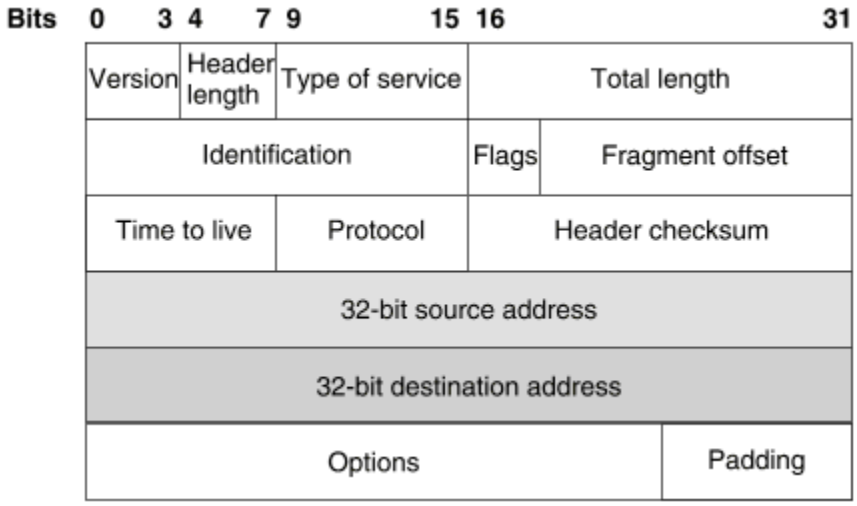
- **Mobility and security:** Ensures compliance with mobile IP and IPsec standards functionality; mobility is built in, so any IPv6 node can use it when necessary; and enables people to move around in networks with mobile network devices—with many having wireless connectivity.

  Mobile IP is an Internet Engineering Task Force (IETF) standard available for both IPv4 and IPv6. The standard enables mobile devices to move without breaks in established network connections. Because IPv4 does not automatically provide this kind of mobility, you must add it with additional configurations.

  IPsec is the IETF standard for IP network security, available for both IPv4 and IPv6. Although the functionalities are essentially identical in both environments, IPsec is mandatory in IPv6. IPsec is enabled on every IPv6 node and is available for use. The availability of IPsec on all nodes makes the IPv6 Internet more secure. IPsec also requires keys for each party, which implies a global key deployment and distribution.

- **Transition richness:** You can incorporate existing IPv4 capabilities in IPv6 in the following ways:
  - Configure a dual stack with both IPv4 and IPv6 on the interface of a network device.
  - Use the technique IPv6 over IPv4 (also called 6to4 tunneling), which uses an IPv4 tunnel to carry IPv6 traffic. This method (RFC 3056) replaces IPv4-compatible tunneling (RFC 2893). Cisco IOS Software Release 12.3(2)T (and later) also allows protocol translation (NAT-PT) between IPv6 and IPv4. This translation allows direct communication between hosts speaking different protocols.

IPv4 VS IPv6



An IPv4 header contains the following fields:
version The IP version number, 4.
lengthThe length of the datagram header in 32-bit words.
type of service Contains five subfields that specify the precedence, delay, throughput, reliability, and cost desired for a packet. (The Internet does not guarantee this request.) This field is not widely used on the Internet.
total length The length of the datagram in bytes including the header, options, and the appended transport protocol segment or packet.
Identification An integer that identifies the datagram.
Flags: Controls datagram fragmentation together with the identification field. The flags indicate whether the datagram may be fragmented, whether the datagram is fragmented, and whether the current fragment is the final one.
fragment offset The relative position of this fragment measured from the beginning of the original datagram in units of 8 bytes.
time to live How many routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagrams from remaining on the Internet forever.
Protocol The high-level protocol type.

header checksum A number that is computed to ensure the integrity of the header values.
source address The 32-bit IPv4 address of the sending host.
destination address The 32-bit IPv4 address of the receiving host.
Options A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.
Padding Null bytes which are added to make the header length an integral multiple of 32 bytes as required by the header length field.

Ipv6 header:

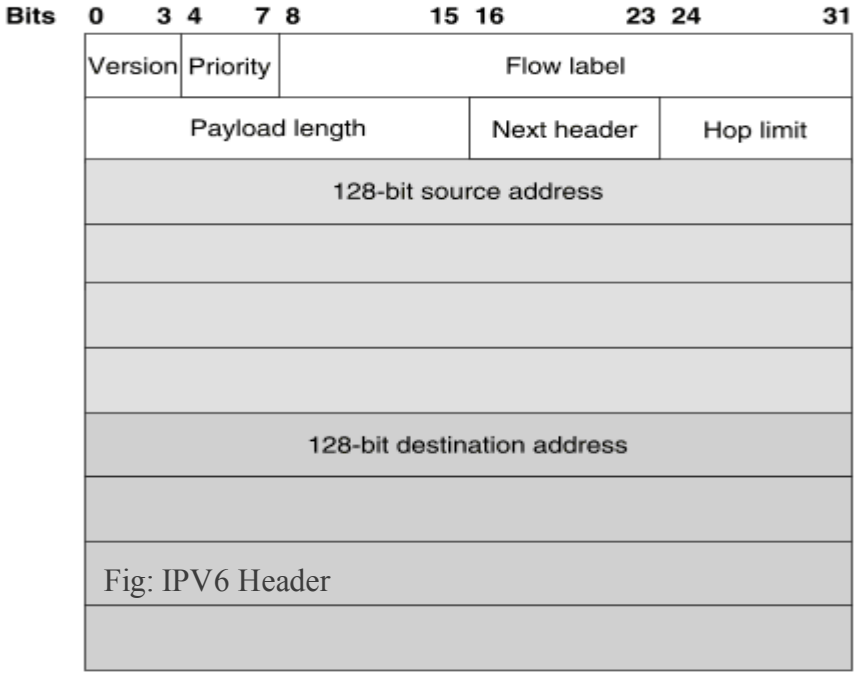


Fig: IPV6 Header

Specifically, IPv6 omits the following fields in its header.

- header length (the length is constant)
- identification
- flags

- fragment offset (this is moved into fragmentation extension headers)
- header checksum (the upper-layer protocol or security extension header handles data integrity)

IPv6 options improve over IPv4 by being placed in separate extension headers that are located between the IPv6 header and the transport-layer header in a packet. Most extension headers are not examined or processed by any router along a packet's delivery path until it arrives at its final destination. This mechanism improves router performance for packets containing options. In IPv4, the presence of any options requires the router to examine all options.

Another improvement is that IPv6 extension headers, unlike IPv4 options, can be of arbitrary length and the total amount of options that a packet carries is not limited to 40 bytes. This feature, and the manner in which it is processed, permit IPv6 options to be used for functions that were not practical in IPv4, such as the IPv6 Authentication and Security Encapsulation options.

By using extension headers, instead of a protocol specifier and options fields, newly defined extensions can be integrated more easily into IPv6.

IPV6 Addressing:

Address Representation:
Represented by breaking 128 bit into Eight 16-bit segments (Each 4 Hex character each)
Each segment is written in Hexadecimal separated by colons.
Hex digit are not case sensitive.
Rule 1:
Drop leading zeros:
2001:0050:0000:0235:0ab4:3456:456b:e560
2001:050:0:235:ab4:3456:456b:e560
Rule2:
Successive fields of zeros can be represented as "::" , But double colon appear only once in the address.
FF01:0:0:0:0:0:0:1
FF01::1
Note : An address parser identifies the number of missing zeros by separating the two parts and entering 0 until the 128 bits are complete. If two "::" notations are placed in the address, there is no way to identify the size of each block of zeros.
Ipv4 vs ipv6

IPV4	IPV6
1. source and destination addresses are 32 bits.)	1. Source and destination addresses are 128 bits.
2. ipv4 support small address space.	2. Supports a very large address space sufficeint for each and every people on earth.
3. ipv4 header includes checksum.	3. ipv6 header doesn't includes the checksum. (the upper-layer protocol or security extension header handles data integrity)
4. addresses are represented in dotted decimal format. (Eg. 192.168.5.1)	4. Addresses are represented in 16-bit segments Each segment is written in Hexadecimal separated by colons. (Eg. 2001:0050:020c:0235:0ab4:3456:456b:e560
5. Header includes options.	All optional data is moved to IPV6 extension header..
6. Broadcast address are used to send traffic to all	6. There is no IPV6 broadcast address. Instead a link