Internet protocol Ipv4 and Ipv6

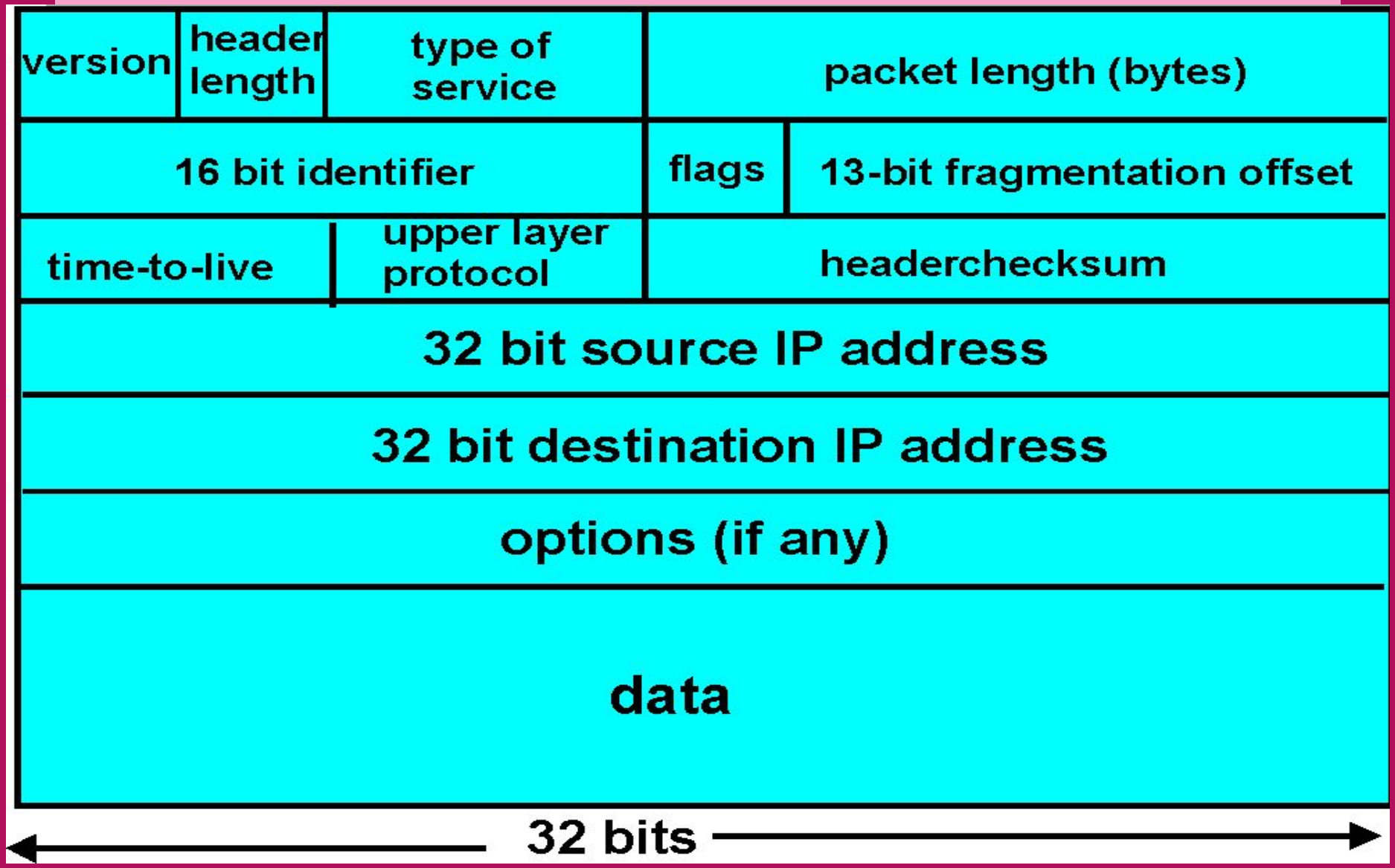
The Internet Protocol (IP): Forwarding and Addressing in the Internet

- The Internet's network layer has three major components
  - **IP protocol**
  - **Routing component**, which determines the path a datagram follows from source to destination. Routing protocols compute the forwarding tables that are used to forward packets through the network.
  - The **facility to report errors in datagrams** and respond to requests for certain network-layer information.

Datagram Format

- A network-layer packet is referred to as a *datagram.*

IPv4 datagram format



The key fields in the IPv4 datagram are the following:

- **Version Number:**
- These 4 bits specify the IP protocol version of the datagram.
- The router uses the version number to determine how to interpret the remainder of the IP datagram.
- Different versions of IP use different datagram formats.

- **Header Length:**
- The 4-bit header length (HLEN) field defines the total length of the datagram header.
- The IPv4 datagram has a variable-length header.
- When a device receives a datagram, it needs to know when the header stops and the data, which is encapsulated in the packet, starts.

- **Options:**
- There are a number of optional parameters that may be present in an IPV4 datagram.
- They typically configure a number of behaviours like
  - The method to be used during source routing,
  - Some control and probing facilities
  - A number of experimental features

- **Type of service (TOS):**
- It is included in the IPv4 header to allow different "types" of IP datagrams to be distinguished from each other so that they could be handled differently in times of overload.

- **Datagram Length:**
- This is the total length of the IP datagram (header plus data) measured in bytes.
- Since this field is 16 bits long, the theoretical maximum size of the IP datagram to 65,535 bytes.
- However, datagrams are rarely greater than 1500 bytes, and are often limited in size to 576 bytes.
- **Identifier, Flags, Fragmentation Offset:**
- These three fields have to do with so-called IP fragmentation. The new version of IP, IPv6 does not allow for fragmentation

- **Time-to-live:**
- It is included to insure that datagrams do not circulate in the network.
- This field is decremented by one each time the datagram is processed by a router.
- If the TTL field reaches 0, the datagram must be dropped.

- **Protocol:**
- This field is only used when an IP datagram reaches its final destination. The value of this field indicates the transport-layer protocol at the destination to which the data portion of this IP datagram will be passed.
- For example, a value of **6** indicates that the data portion is passed to **TCP,** while a value of **17** indicates that the data is passed to **UDP.**

- **Header Checksum:**
- The header checksum aids a router in detecting bit errors in a received IP datagram.
- Routers typically discard datagrams for which an error has been detected.

- **Source and Destination IP Address:**
- These fields carry the 32 bit IP address of the source and final destination for this IP datagram.

- **Data (payload):**
- The data field of the IP datagram contains the transport-layer segment (TCP or UDP) to be delivered to the destination.
- However, the data field can carry other types of data.

IP Fragmentation and Reassembly

- Not all link layer protocols can carry packets of the same size.
- The maximum amount of data that a link-layer packet can carry is called the **MTU (maximum transfer unit)**.
- Each IP datagram is encapsulated within the link-layer packet for transport from one router to the next router .

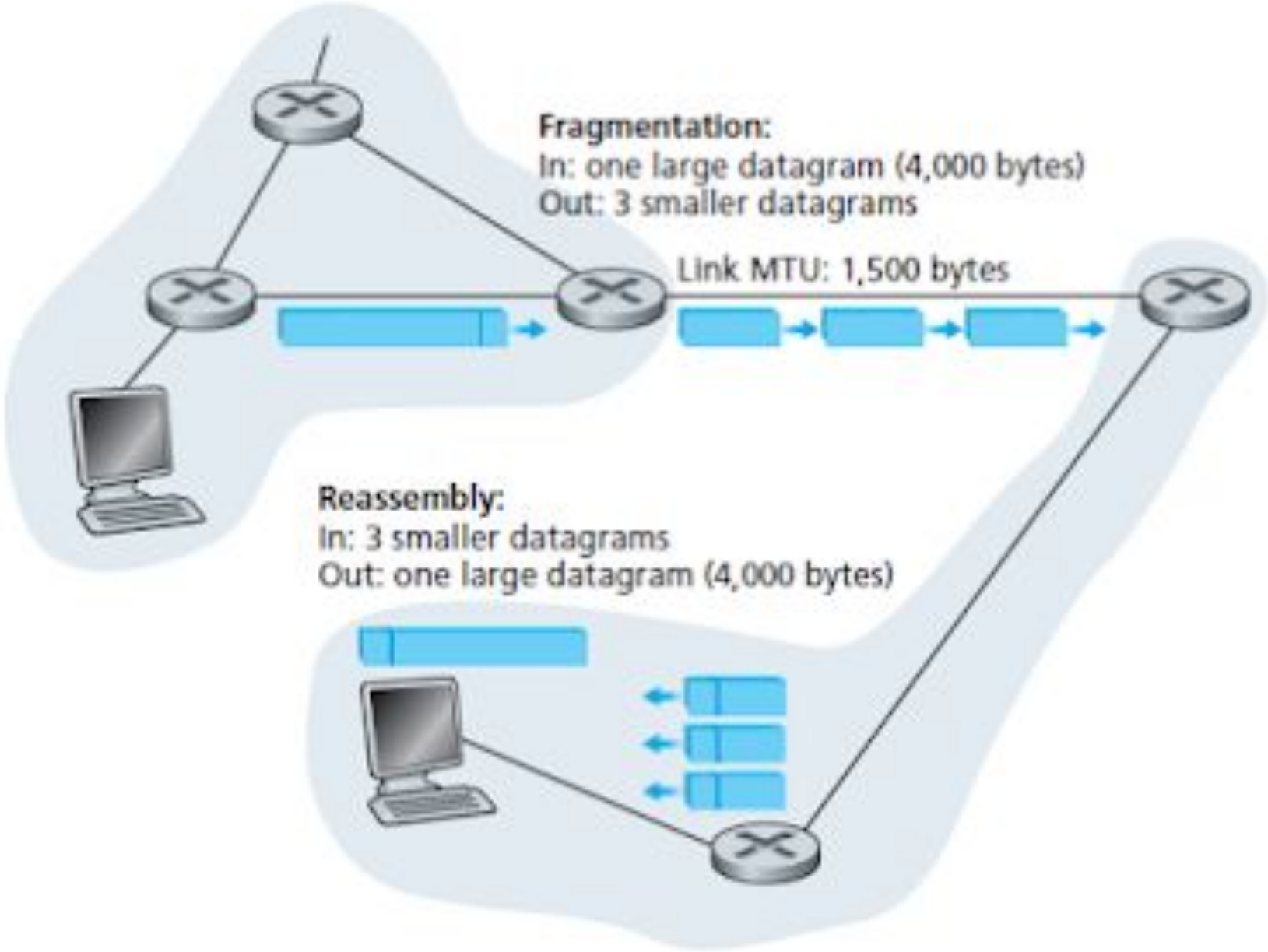
- The MTU of the link-layer protocol places a hard limit on the length of an IP datagram.

- The solution to this problem is to "fragment" the data in the IP datagram among two or more smaller IP datagrams, and then send these smaller datagrams over the outgoing link. Each of these smaller datagrams is referred to as a **fragment**.

- The host or router that fragments a datagram must change the values of three fields:
  - **Flags**
  - **Fragmentation offset**
  - **Total length.**

- **Identification.** This **16-bit field identifies a datagram originating from the source host.** When a datagram is fragmented, the value in the **identification field is copied to all fragments**. The identification number helps the destination in reassembling the datagram.

- **Flags.**
  - This is a 3-bit field.
    1. 1st bit is **reserved**. (future use and always set to 0)
    2. 2nd bit called the **do not fragment** bit.
       - 1 : machine **must not fragment**
       - **0 :** machine **can fragment if needed**
    3. 3rd bit specify **more fragment**
       - **0** : **it's the last fragment**
       - **1 : more fragment.**
- **Fragmentation offset.** This 13-bit field shows the relative position of this fragment with respect to the whole datagram.


Fragmentation:
In: one large datagram (4,000 bytes)
Out: 3 smaller datagrams
Link MTU: 1,500 bytes
Reassembly:
In: 3 smaller datagrams
Out: one large datagram (4,000 bytes)

IPV6

The most important changes introduced in Ipv6 are evident in the packet format:

- Expanded addressing capabilities
- A streamlined 40 byte header
- Flow labeling and priority

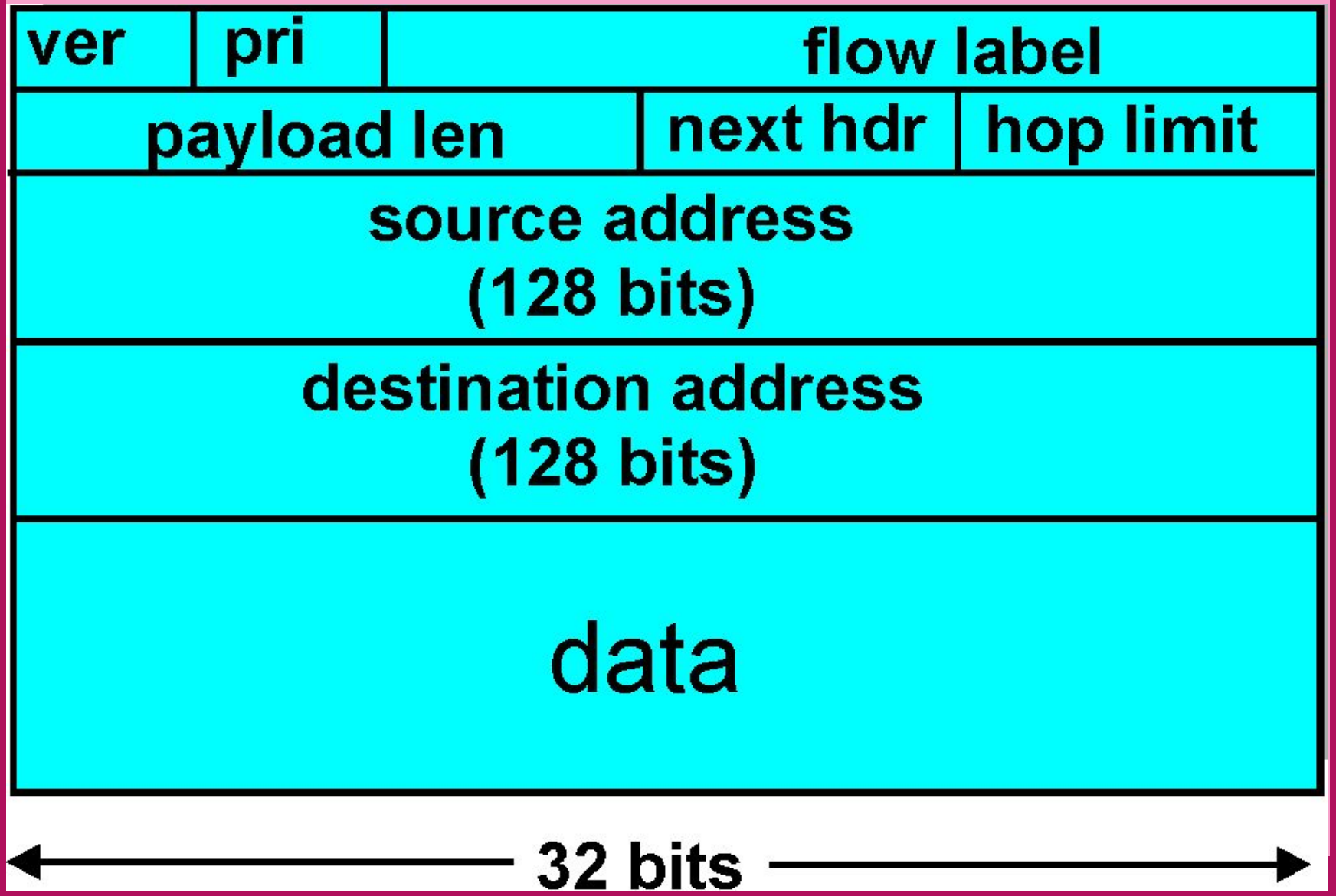
- **Expanded addressing capabilities.**
- IPv6 increases the size of the IP address from 32 to 128 bits.
- In addition to unicast and multicast addresses, a new type of address, called an **anycast address**, has also been introduced, which allows a packet addressed to an anycast address to be delivered to any one of a group of hosts.

- **A streamlined 40 byte header.**
- A number of IPv4 fields have been dropped or made optional.
- The resulting 40-byte fixed-length header allows for faster processing of the IP packet.
- A new encoding of options allows for more flexible options processing.

- **Flow labeling and priority.**
- IPv6 allows "labeling of packets belonging to particular flows for which the sender requests special handling, such as a non-default quality of service or real-time service."
  - For example, audio and video transmission might likely be treated as a flow. On the other hand, the more traditional applications, such as file transfer and email might not be treated as flows.

- The IPv6 header also has a 4-bit **priority** field.
  - Gives priority to certain packets within a flow, or it can be used to give priority to datagrams from certain applications over packets from other applications.

IPV6 Packet Format



- **version.** This four bit field identifies the IP version number. Not surprisingly, IPv6 carries a value of "6" in this field.

- **priority.** This four bit field is similar in spirit to the ToS field in IPV4.
  - 0 - 7 for priority among traffic that is congestion -controlled (packets would back off)
  - 8 - 15 for non-congestion controlled traffic, such as constant bit rate real-time traffic (Packets would not back off)

- **flow label**. Used to identify a "flow" of packets.

- **payload length.** This 16-bit value is treated as an unsigned integer given **the number of bytes in the IPv6 packet following the fixed length**, 40 byte packet header.

- **next header.** This field identifies the **protocol to which the contents (data field) of this packet will be delivered** (e.g., to TCP or UDP). The field uses the same values as the Protocol field in the IPv4 header.

- **hop limit.** The contents of this field are **decremented by one by each router that forward the packet. If the hop limit count reaches zero, the packet is discarded**.

- **source and destination address.** An IPv6 address has the following structure:

- **data.** This is the payload portion of the IPv6 packet. When the packet reaches its destination, the payload will be removed from the IP packet and passed on to the protocol specified in the nexheader field.

- **Fragmentation/Reassembly.**
  - **IPv6 does not provide for fragmentation and reassembly**.
  - If the packet received by a router is too large to be forwarded over the outgoing link, the **router simply drops the packet and sends a "Packet Too Big" ICMP error message back to the sender.**
  - The sender can **then resend the data, using a smaller IP packet size.**
  - Fragmentation and reassembly is a time-consuming operation; **removing this functionality from the routers and placing it squarely in the end systems considerably speeds up IP forwarding within the network.**

- **Checksum.**
  - Because the transport layer (e.g, TCP and UDP) and data link (e.g., Ethernet) protocols in the Internet layers perform checksumming, the designers of IP probably felt that **this functionality was sufficiently redundant in the network layer that it could be removed.**
  - Once again**, fast processing** of IP packets was a central concern.

- **Options.** The options **field is one of the possible "next headers"** pointed to from within the IPv6 header. That is, just as TCP or UDP protocol headers can be the next header within an IP packet, so too can an options field. The removal of the options filed results in a fixed length, 40 byte IP header.