**IPv4 Datagram**

The network layer is the third layer (from bottom) in the OSI Model. The network layer is concerned with the delivery of a packet across multiple networks. The network layer is considered the backbone of the OSI Model. It selects and manages the best logical path for data transfer between nodes. This layer contains hardware devices such as routers, bridges, firewalls, and switches, but it actually creates a logical image of the most efficient communication route and implements it with a physical medium. Network layer protocols exist in every host or router. The router examines the header fields of all the IP packets that pass through it. Internet Protocol and Netware IPX/SPX are the most common protocols associated with the network layer.  
In the OSI model, the network layer responds to requests from the layer above it (transport layer) and issues requests to the layer below it (data link layer).

**Responsibilities of Network Layer:**

***Packet forwarding/Routing of packets:****Relaying of data packets from one network segment to another by nodes in a computer network*

***Connectionless communication (IP):****A data transmission method used in packet-switched networks in which each data unit is separately addressed and routed based on information carried by it*

There are two types of network transmission techniques, circuit switched network and packet switched network.  
**Circuit Switch vs Packet Switch**  
In circuit switched network, a single path is designated for transmission of all the data packets. Whereas in case of a packet-switched network, each packet may be sent through a different path to reach the destination.

In a circuit switched network, the data packets are received in order whereas in a packet switched network, the data packets may be received out of order.

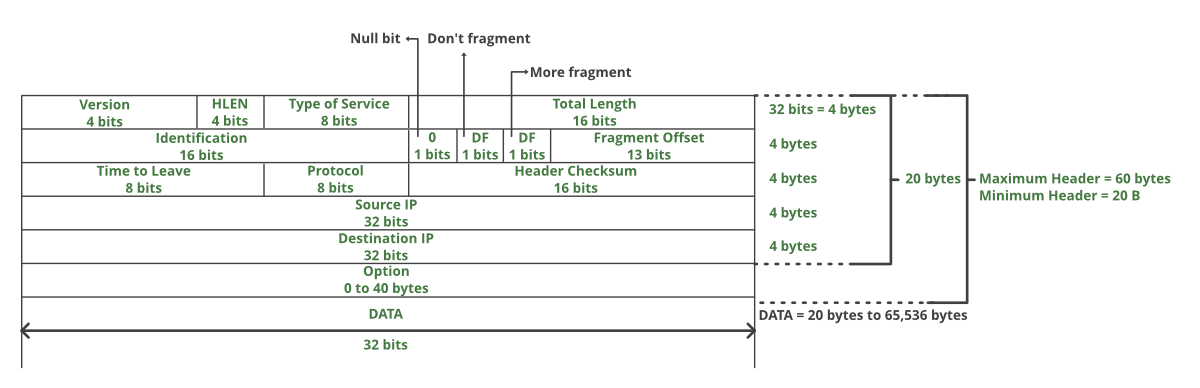
The packet switching is further subdivided into Virtual circuits and Datagram.

**IPv4:**  
IPv4 is a connectionless protocol used for packet-switched networks. It operates on a best effort delivery model, in which neither delivery is guaranteed, nor proper sequencing or avoidance of duplicate delivery is assured. Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type.

IPv4 is defined and specified in IETF publication RFC 791.  
IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E. Classes A, B and C have a different bit length for addressing the network host. Class D addresses are reserved for military purposes, while class E addresses are reserved for future use.

IPv4 uses 32-bit (4 byte) addressing, which gives 232 addresses. IPv4 addresses are written in the dot-decimal notation, which comprises of four octets of the address expressed individually in decimal and separated by periods, for instance, 192.168.1.5.

**IPv4 Datagram Header**  
Size of the header is 20 to 60 bytes.



***VERSION:****Version of the IP protocol (4 bits), which is 4 for IPv4*

***HLEN:****IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.*

***Type of service:*** *Low Delay, High Throughput, Reliability (8 bits)*

***Total Length:****Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.*

***Identification:****Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)*

***Flags:****3 flags of 1 bit each: reserved bit (must be zero), do not fragment flag, more fragments flag (same order)*

***Fragment Offset:****Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.*

***Time to live:****Datagram’s lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.*

***Protocol:****Name of the protocol to which the data is to be passed (8 bits)*

***Header Checksum:****16 bits header checksum for checking errors in the datagram header*

***Source IP address:****32 bits IP address of the sender*

***Destination IP address:****32 bits IP address of the receiver*

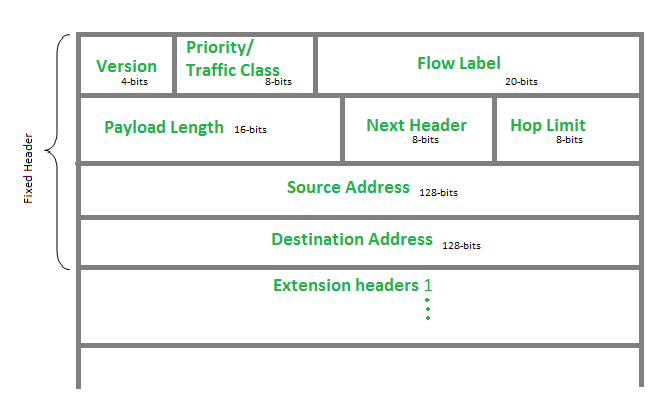
***Option:****Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.*

# Internet Protocol version 6 (IPv6) Header

Prerequisite: [Introduction to Internet Protocol version 6](https://www.geeksforgeeks.org/internet-protocol-v6-ipv6/)

IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Let’s look at the header of IP version 6 and understand how it is different from the IPv4 header.

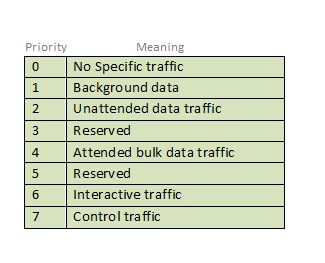
**IP version 6 Header Format:** 



**Version (4-bits):** Indicates version of Internet Protocol which contains bit sequence 0110.

**Traffic Class (8-bits):** The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded.   
As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.

Priority assignment of Congestion controlled traffic : 



Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to uncontrolled data traffic.   
The source node is allowed to set the priorities but on the way, routers can change it. Therefore, the destination should not expect the same priority which was set by the source node.

**Flow Label (20-bits):**Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service. In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets. Between a source and destination, multiple flows may exist because many processes might be running at the same time. Routers or Host that does not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, the source is also supposed to specify the lifetime of the flow.

**Payload Length (16-bits):** It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers(if any) and an upper-layer packet. In case the length of the payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and the jumbo payload option is used in the Hop-by-Hop options extension header.

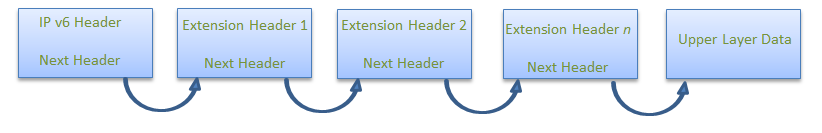
**Next Header (8-bits):** Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.

**Hop Limit (8-bits):** Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.

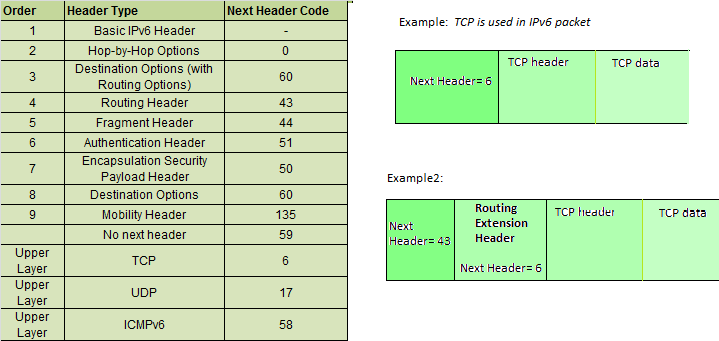
**Source Address (128-bits):** Source Address is the 128-bit IPv6 address of the original source of the packet.

**Destination Address (128-bits):** The destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

**Extension Headers:** In order to rectify the limitations of the *IPv4 Option Field*, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.



IPv6 packet may contain zero, one or more extension headers but these should be present in their recommended order:



**Rule:** Hop-by-Hop options header (if present) should always be placed after the IPv6 base header.

# IPv4 vs IPv6

## **What is IP?**

An IP stands for internet protocol. An IP address is assigned to each device connected to a network. Each device uses an IP address for communication. It also behaves as an identifier as this address is used to identify the device on a network. It defines the technical format of the packets. Mainly, both the networks, i.e., IP and TCP, are combined together, so together, they are referred to as a [TCP/IP](https://www.javatpoint.com/tcp-ip-full-form). It creates a virtual connection between the source and the destination.

We can also define an IP address as a numeric address assigned to each device on a network. An IP address is assigned to each device so that the device on a network can be identified uniquely. To facilitate the routing of packets, TCP/IP protocol uses a 32-bit logical address known as IPv4(Internet Protocol version 4).

An [IP](https://www.javatpoint.com/ip-full-form) address consists of two parts, i.e., the first one is a network address, and the other one is a host address.

There are two types of IP addresses:

* IPv4
* IPv6

### **What is IPv4?**

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.

For example, **66.94.29.13**

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

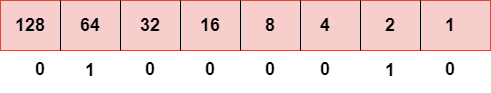
**Representation of 8 Bit Octet**

IPv4 vs IPv6

The above representation shows the structure of 8- bit octet.

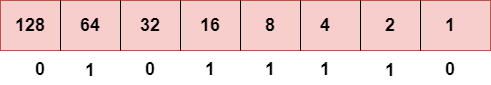
Now, we will see how to obtain the binary representation of the above IP address, i.e., 66.94.29.13

**Step 1: First, we find the binary number of 66.**



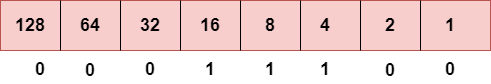
To obtain 66, we put 1 under 64 and 2 as the sum of 64 and 2 is equal to 66 (64+2=66), and the remaining bits will be zero, as shown above. Therefore, the binary bit version of 66 is 01000010.

**Step 2: Now, we calculate the binary number of 94.**



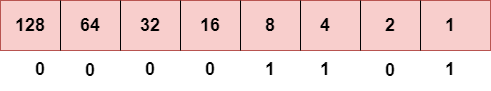
To obtain 94, we put 1 under 64, 16, 8, 4, and 2 as the sum of these numbers is equal to 94, and the remaining bits will be zero. Therefore, the binary bit version of 94 is 01011110.

**Step 3: The next number is 29.**



To obtain 29, we put 1 under 16, 8, 4, and 1 as the sum of these numbers is equal to 29, and the remaining bits will be zero. Therefore, the binary bit version of 29 is 00011101.

**Step 4: The last number is 13.**



To obtain 13, we put 1 under 8, 4, and 1 as the sum of these numbers is equal to 13, and the remaining bits will be zero. Therefore, the binary bit version of 13 is 00001101.

### **Drawback of IPv4**

Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet. Although the various techniques were invented, such as variable- length mask, network address translation, port address translation, classes, inter-domain translation, to conserve the bandwidth of IP address and slow down the depletion of an IP address. In these techniques, public IP is converted into a private IP due to which the user having public IP can also use the internet. But still, this was not so efficient, so it gave rise to the development of the next generation of IP addresses, i.e., IPv6.

### **What is IPv6?**

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

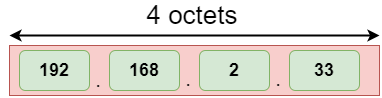
* **Dual stacking:** It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.
* **Tunneling:** In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.
* **Network Address Translation:** The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion (3.4\*1038) addresses.

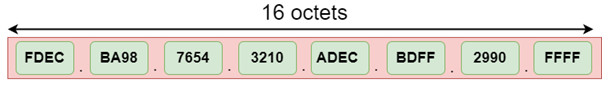
IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time

### **Address format**

**The address format of IPv4:**



**The address format of IPv6:**



The above diagram shows the address format of IPv4 and IPv6. An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255. Whereas an IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

### **Differences between IPv4 and IPv6**

|  |  |  |
| --- | --- | --- |
|  | **Ipv4** | **Ipv6** |
| **Address length** | IPv4 is a 32-bit address. | IPv6 is a 128-bit address. |
| **Fields** | IPv4 is a numeric address that consists of 4 fields which are separated by dot (.). | IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon. |
| **Classes** | IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E. | IPv6 does not contain classes of IP addresses. |
| **Number of IP address** | IPv4 has a limited number of IP addresses. | IPv6 has a large number of IP addresses. |
| **VLSM** | It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes. | It does not support VLSM. |
| **Address configuration** | It supports manual and DHCP configuration. | It supports manual, DHCP, auto-configuration, and renumbering. |
| **Address space** | It generates 4 billion unique addresses | It generates 340 undecillion unique addresses. |
| **End-to-end connection integrity** | In IPv4, end-to-end connection integrity is unachievable. | In the case of IPv6, end-to-end connection integrity is achievable. |
| **Security features** | In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind. | In IPv6, IPSEC is developed for security purposes. |
| **Address representation** | In IPv4, the IP address is represented in decimal. | In IPv6, the representation of the IP address in hexadecimal. |
| **Fragmentation** | Fragmentation is done by the senders and the forwarding routers. | Fragmentation is done by the senders only. |
| **Packet flow identification** | It does not provide any mechanism for packet flow identification. | It uses flow label field in the header for the packet flow identification. |
| **Checksum field** | The checksum field is available in IPv4. | The checksum field is not available in IPv6. |
| **Transmission scheme** | IPv4 is broadcasting. | On the other hand, IPv6 is multicasting, which provides efficient network operations. |
| **Encryption and Authentication** | It does not provide encryption and authentication. | It provides encryption and authentication. |
| **Number of octets** | It consists of 4 octets. | It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16. |