Network Layer | Introduction and IPv4 Datagram Header

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

**Fragmentation of data packets:** Splitting of data packets that are too large to be transmitted on the network

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.

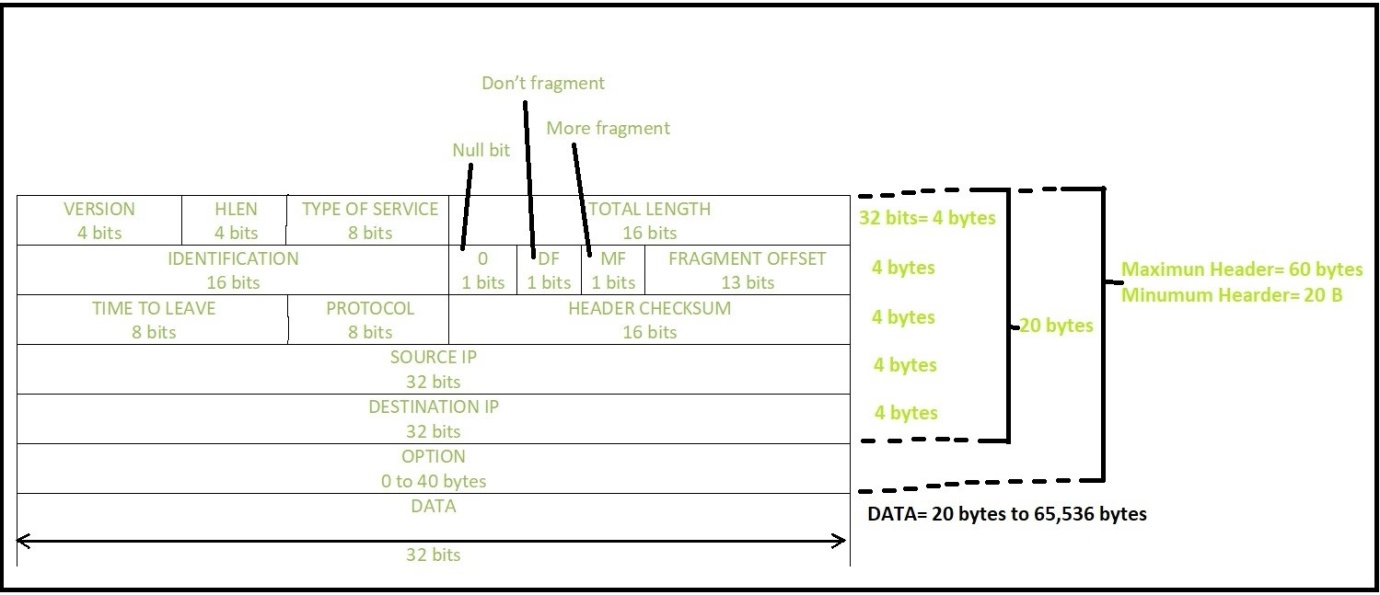
The packet switching is further subdivided into Virtual circuits and Datagram.

**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*

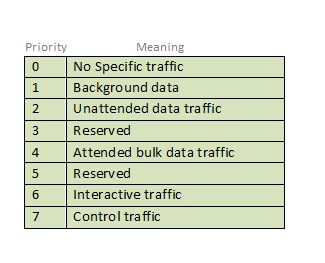
***Option:****Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.*

Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).

**Ipv6**

**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 priority of the packet. If congestion occurs on router then packets with least priority will be discarded.  
As of now only 4-bits are being used (and 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.  
Source node is allowed to set the priorities but on the way routers can change it. Therefore, destination should not expect same priority which was set by source node.

**Flow Label (20-bits) :**Flow Label field is used by 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, intermediate router can use source address, 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 do 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, source is also supposed to specify the lifetime of flow.

**Payload Length (16-bits) :** It is a 16-bit (unsigned integer) field, indicates total size of the payload which tells routers about amount of information a particular packet contains in its payload. Payload Length field includes extension headers(if any) and upper layer packet. In case length of 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 jumbo payload option is used in the Hop-by-Hop options extension header.

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

**Hop Limit (8-bits) :** Hop Limit field is 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 packet is discarded if value decrements to 0. This is used to discard the packets that are stuck in infinite loop because of some routing error.

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

**Destination Address (128-bits) :** 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 *IPv4 Option Field*, Extension Headers are introduced in IPversion 6. The extension header mechanism is very important part of the IPv6 architecture. 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.