Introduction and IPv4 Datagram Header

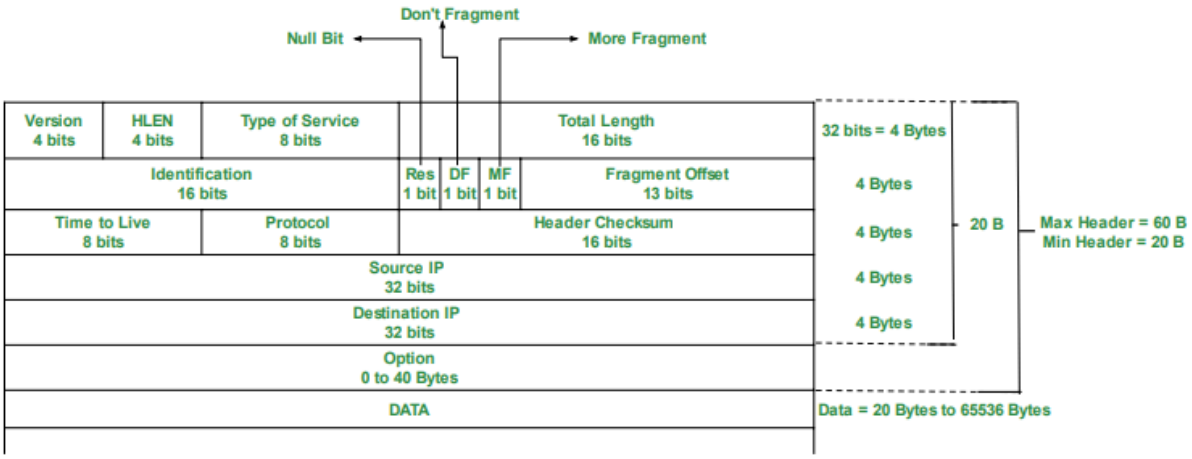
The network layer is the third layer (from bottom) in the OSI Model. The network layer is concerned with the delivery of a packet across multiple networks. The network layer is considered the backbone of the OSI Model. It selects and manages the best logical path for data transfer between nodes. This 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 multicasting, while class E addresses are reserved for military purposes. IPv4 uses 32-bit (4-byte) addressing, which gives 2^{32} 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.



IPv4 Datagram Header

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).

Below questions have been asked in previous GATE exam on above topics. GATE | GATE CS 2006 | Question 5 GATE | GATE-CS-2010 | Question 15 GATE | GATE-CS-2014 Set 3 | Question 35 GATE | GATE CS 2015 Set 1| Question 65

Last Updated : 20 Jun, 2023

80