IP addresses

An IP address is a number identifying of a computer or another device on the Internet.
IP addresses uniquely identify the source and destination of data transmitted with the Internet Protocol.

IPv4 addresses

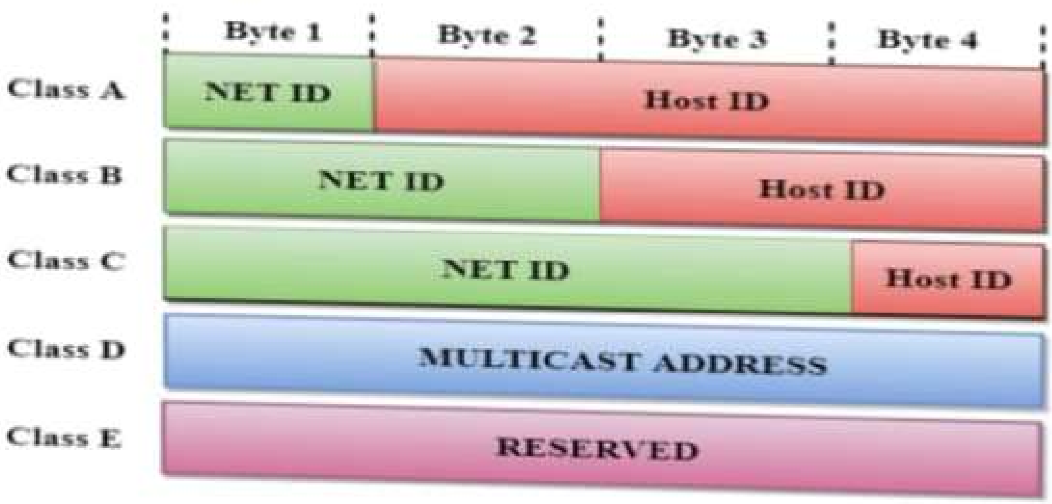
IPv4 addresses are 32 bits long (four bytes).

With an IPv4 IP address, there are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used.

Every IPv4 address is broken down into four octets (which is another name for bytes), and translated into binary to represent the actual IP address.

An ip address is divided into two parts:

- **Network ID:** It represents the number of networks.
- **Host ID:** It represents the number of hosts.



Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address

Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

- The Network ID is 16 bits long.
- The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet are always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 2^{14} = 16384 network address

The total number of hosts in Class B = 2^{16} - 2 = 65534 host address

Class C

In Class C, an IP address is assigned to only small-sized networks.

- The Network ID is 24 bits long.
- The host ID is 8 bits long.

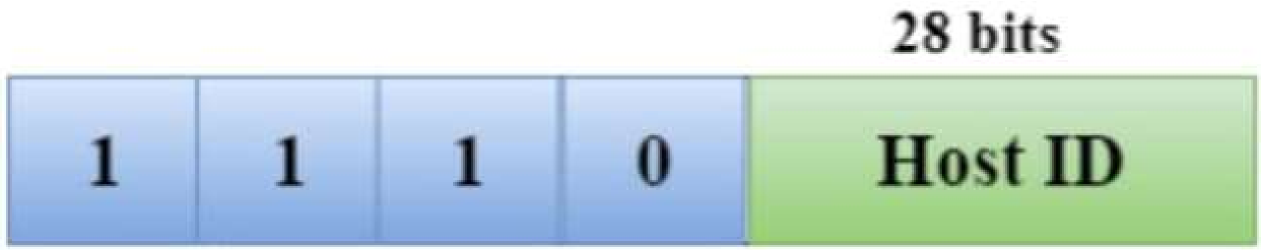
In Class C, the higher order bits of the first octet are always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks = 2^{21} = 2097152 network address

The total number of hosts = 2^{8} - 2 = 254 host address

Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet are always set to 1110, and the remaining bits determine the host ID in any network.

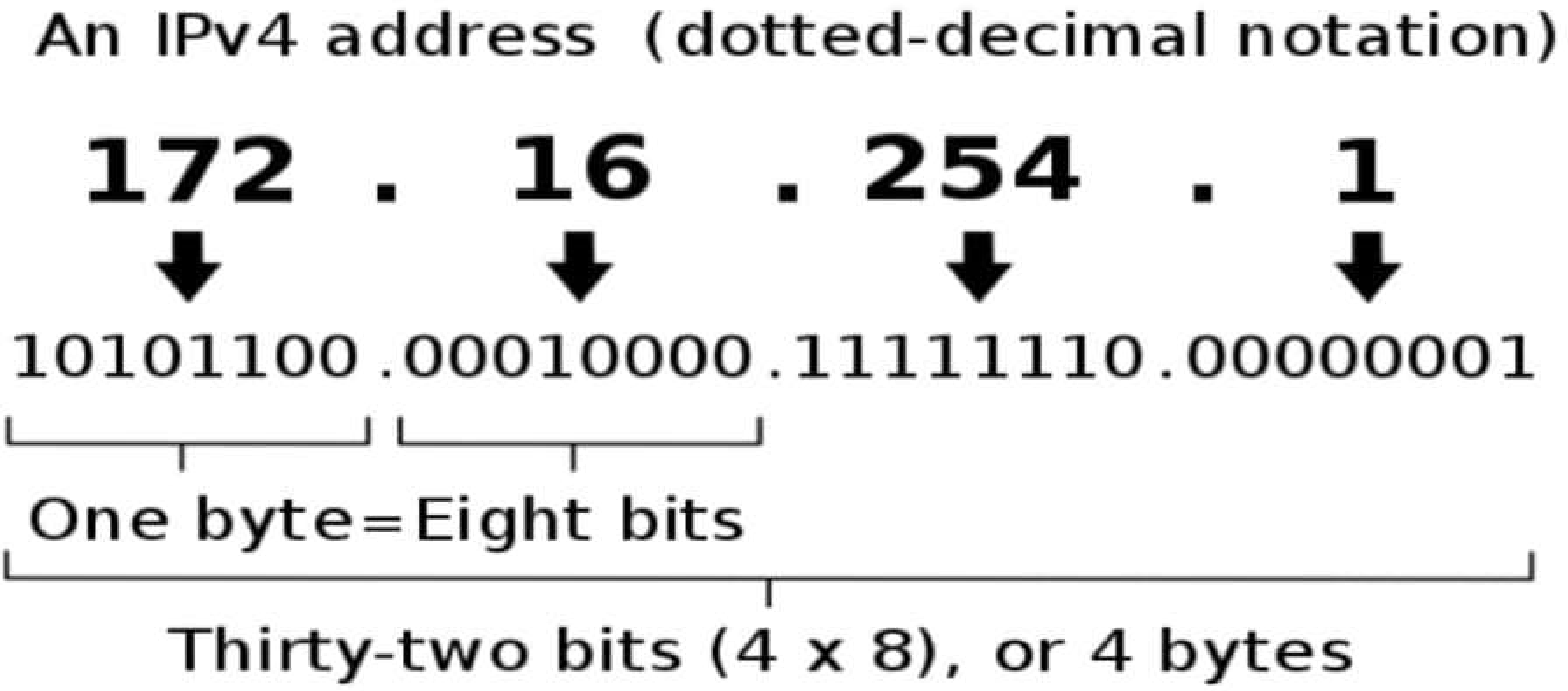


Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet are always set to 1111, and the remaining bits determine the host ID in any network.

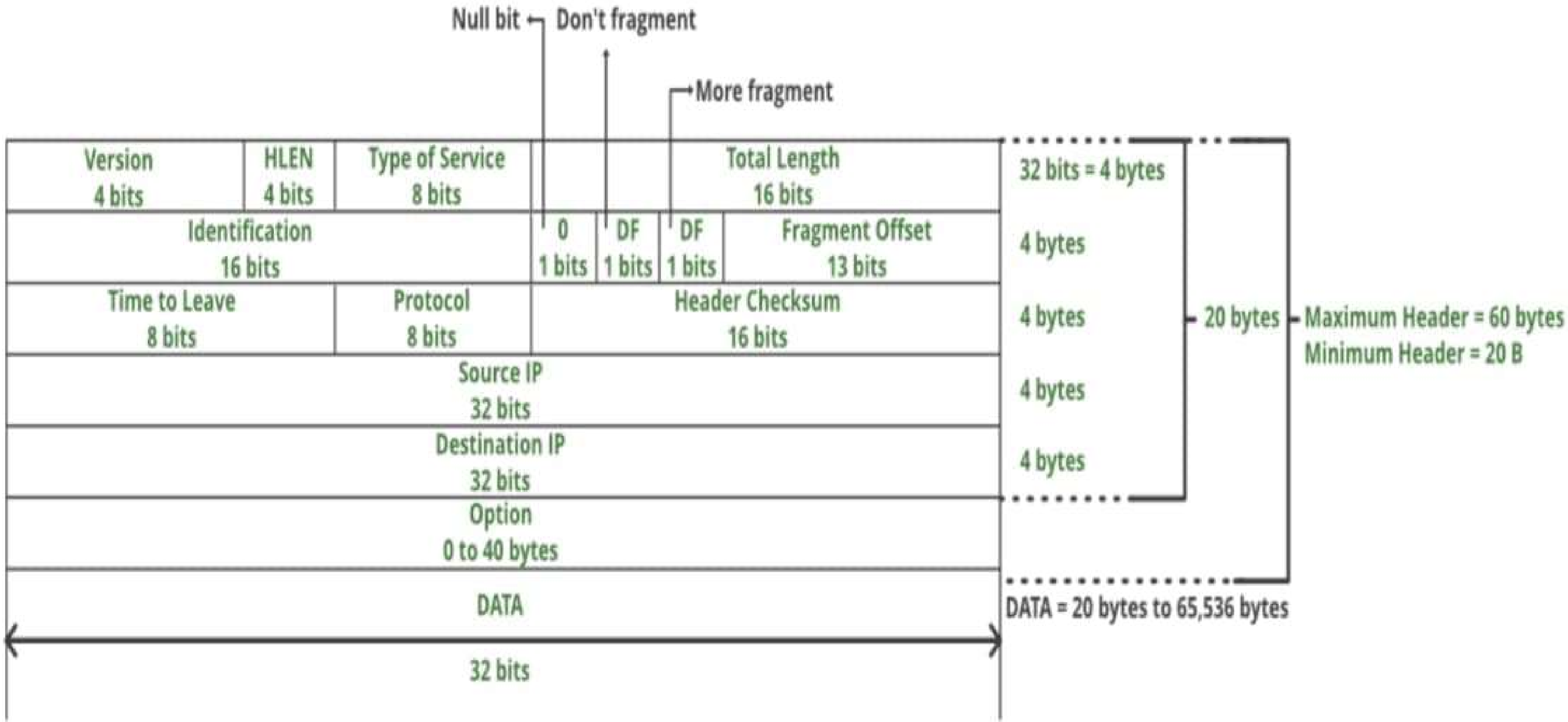
SUMMARY of IPv4 addresses in the form of TABLE:

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255


An IPv4 address (dotted-decimal notation)
172 . 16 . 254 . 1
10101100.00010000.11111110.00000001
One byte=Eight bits
Thirty-two bits (4 x 8), or 4 bytes

IPv4 Datagram Header

Size of the header is 20 to 60 bytes.



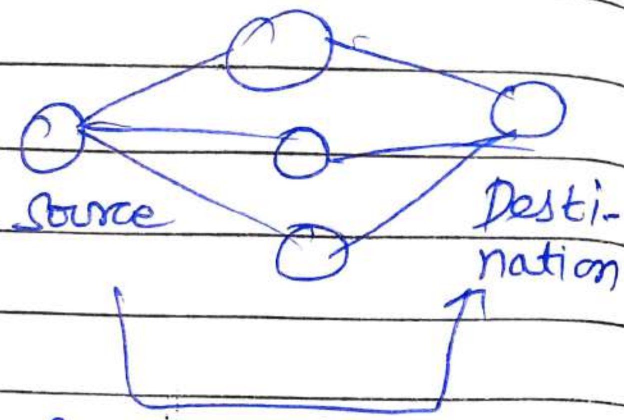
IPv4 header

↓

connectionless & datagram service

↓

no need to establish any connection for sending the packets



Packet can follow any route to reach destination.

IPv4 header →

Minimum: 20 bytes to 60 bytes :Maximum

Datagram = Header + Payload

Payload ↓ pure data

जो upper layer (transport layer) से आ रहा है।

Date

Length of Payload

↳ 0 to 65515 bytes

0 → कोई भी data नहीं आ रहा।

65515 bytes → Maximum size of data

Total value →

65515 + 20 bytes = 65535 = 2^{16}

65515 → Max. payload (data)

20 bytes → Min. header

2^{16} → पूरा datagram

VER → version of IP

Its value is 0100 in IPv4 (4 bits).

0100 → It is equal to 4

Header length (HLEN) → defines the length of datagram header.

Page No.
Date

It's value can be from
(4 bits) 0000 to 1111

Its value is multiplied by 4 to get the length in bytes.

Example - value length

~~0000 → 0 = 0X4 = 0~~

~~0001 → 1X4 = 4 bytes~~

1111 → 15 X 4 = 60 bytes

Maximum value. Maximum length.

but it's not possible 0, 1, 2, 3, 4 are invalid.

~~Its minimum value is 5~~

i.e. 5X4 = 20 bytes → Minimum length of header.

Type of Service (8 bits) →
(DSCP)
(Differentiated Services Code Point)

Date

Reserved for future use.

P	P	P	D	T	R	C	O

P P P → defines Precedence of the Packet

C → **Cost** (follow shortest path) → if cost to be spent is min. then, set it to 1.

D → **Delay** → this value is 1 if the delay in service is not accepted

eg in Whatsapp Calling (Call करते time delay नहीं होना चाहिए)

T → **Throughput** → rate of transfer ज्यादा होना चाहिए तो bit is set to 1, otherwise 0.

R → **Reliability** → packet must be transmitted reliably & packet should not be dropped then bit set to 1.

future use →

DSCP	ECN

0 … 5 6 … 7

DSCP ↑

ECN → Explicit Congestion Notification → (2 bits)

ECN → Its value 11 defines there is congestion in the network. But do not drop packet

Total length (16 bits) -
↓
max. denotes 2^{16} → total length of data

Time to live (8 bits) →
It is a 8 bit field which controls the maximum number of routers visited by the datagram.

(कई बार Packet loop में फंस जाता है & so it will create congestion)

because of wrong information or any other problem

$2^8 = 256$ → maximum value
(0 to 255)

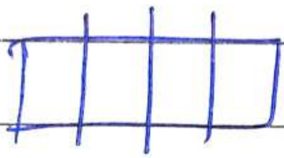
packet will start transmitting & visit routers one by one. Its value will start decreasing & when it will reach 0 the packet will be dropped.

Fragmentation →

Identification (16 bits)	Flag (3)	fragment offset (13 bits)

Identification:

Datagram is divided into small units & each unit can be transmitted through different routes.



When these units reach destination, then how will the destination know that all these units belong to one packet only.

Its max. value is 2^{16}

Flag:

Res 0	DF	MF

Res → Reserved & fixed

DF → Do not fragment bit

MF → More fragment bit

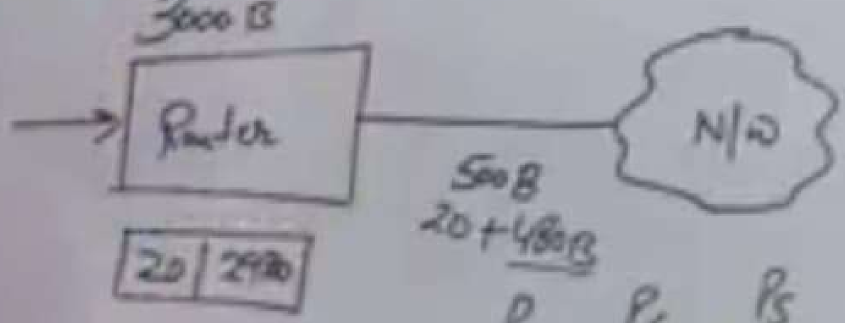
Do not fragment bit	More fragment bit
0	0
0	1
1	0
1	1

(DF = 0) → fragment किया हुआ है (रास्ते में भी packet को divide कर सकते हैं)

(DF = 1) → There is no fragmentation allowed

A datagram of 3000 B (20 B of IP header + 2980 B IP Payload) reached at Router and must be forward to link with MTU of 500 B. How many fragments will be generated and also write MF, offset, Total length value for all

$$\left\lceil \frac{2980\,B}{480\,B} \right\rceil = 7$$



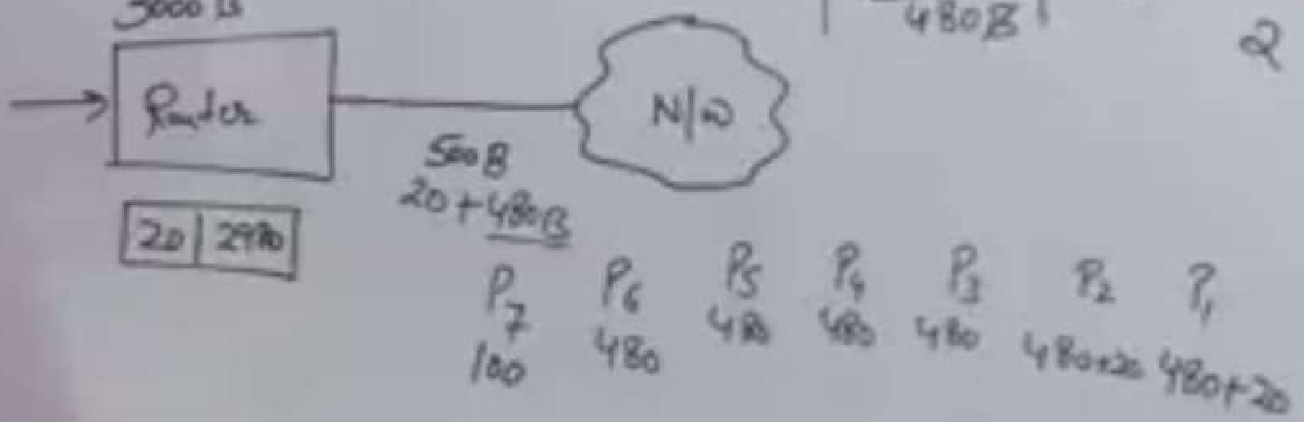
P_7 P_6 P_5 P_4 P_3 P_2 P_1

7 480 480 480 480 480+20 480+20

A datagram of 3000 B (20 B of IP header + 2980 B IP Payload) reached at Router and must be forward to link with MTU of 500 B. How many fragments will be generated and also write MF, offset, Total length value for all

$\left\lceil \frac{2980\,B}{480\,B} \right\rceil = 7$ $\qquad 480 \times 6 = 2880$

2



P_7	P_6	P_5	P_4	P_3	P_2	P_1
7	480	480	480	480	480+20	480+20
100+20	5ms	5ms	5ms	5ms	500	500
120						

Total length -

	P_7	P_6	P_5	P_4	P_3	P_2	P_1
	120	500	500	500	500	500	500
MF	0	1	1	1	1	1	1

P_7 (MF = 0): This is the last packet (इसके बाद कोई packet नहीं है).

P_1 (MF = 1): It tells that there is one more packet after this.

Offset: How many number of databytes are there ahead of you? It tells this.

P_7	P_6	P_5	P_4	P_3	P_2	P_1
$\frac{480\times6}{8}$	$\frac{480\times5}{8}$	$\frac{480\times4}{8}$	$\frac{480\times3}{8}$	$\frac{480\times2}{8}$	480	0

Scale of 8 is used here.

Sender → $\frac{480}{8} = 60$ bytes

480 → P_2 से आगे इतने 480 Byte का data है जो travel कर रहा है।

P_7	P_6	P_5	P_4	P_3	P_2	P_1
360	300	240	180	120	60	0

P_7 → 360: इससे आगे कितना data है?

P_2 → 60: Receiver

$60 \times 8 = 480$ bytes

$360 \times 8 = 2880$ bytes

का data इसके आगे है।

4.11. INTERNET PROTOCOL (IP) (MDU, Sem. Exam. (ECE), 05) (10 marks)

This is a host to host network layer delivery protocol designed for the internet. IP is a connectionless datagram protocol with no guarantee of reliability. It is an unreliable protocol because it does not provide any error control or flow control. IP can only detect the error and discards the packet which is corrupted. If IP is to be made more reliable, then it must be paired with a reliable protocol such as TCP at the transport layer. Each IP datagram is handled independently and each one can follow a different route to the destination. So there is a possibility of receiving out of order packets at the destination. Some packets may even be lost or corrupted. IP relies on a higher-level protocol to take care of all these problems.

4.11.1. Datagram

Packets in IP layer are called datagrams. Figure 4.23 shows the IP datagram format. A datagram is a variable length packet with two parts namely the header and data. The header is 20 to 60 bytes in length. It contains the information essential for routing and delivery. The other part of the datagram is the data field which is of variable length.

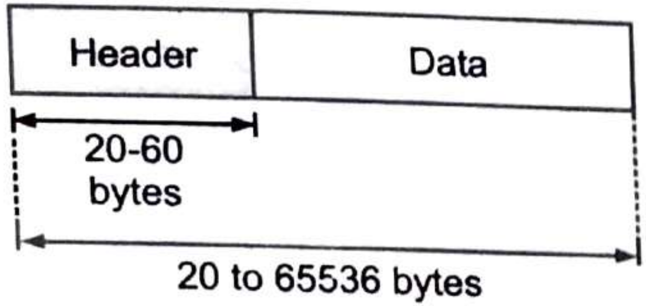
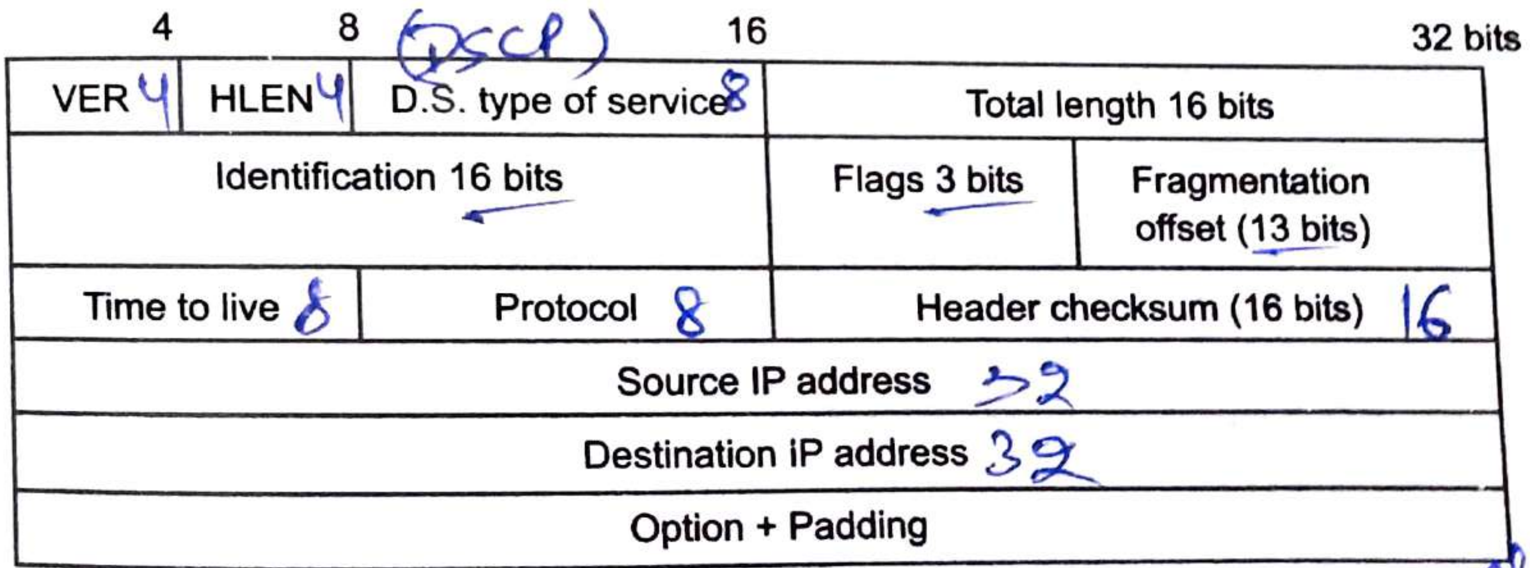


Fig. 4.23 *IP datagram format*

4.11.2. Structure of IP Frame Header

The IP frame header contains routing information and control information associated with datagram delivery. The IP header structure has been shown in figure 4.24.



Various field in the IP header are as follows :

1. VER (version)

This field defines the version of IP. Current version of IP is IPv4 and the latest version of IP is IPv6. It is a four bit long field.

2. HLEN (Header length)

This field defines the length of the datagram header in 4-byte word. Its value must be multiplied by 4 to give the length in bytes.

3. Differential Services (DS)

This field defines the class of the datagram for quality of service purpose.

Networks may offer service precedence, meaning that they accept traffic only above certain precedence at times of load. There is a three way trade off between low delay, high reliability and throughput.

4. Total Length

This field defines the total length of the IP datagram. The total length includes the length of header as well as the data field.

The field length of this field is 15 bits so the total length of the IP datagram is restricted to $(2^{16} - 1) = 65535$ bytes of which 20 to 60 bytes are the header and the remaining are data. The field allows the length of a datagram to be upto 65, 535 bytes, although such long datagrams are impractical for most hosts and networks. All hosts must be prepared to accept datagram of upto 576 bytes, regardless of whether they arrive whole or in fragments. It is recommended that hosts send datagram larger then 576 bytes only if the destination is prepared to accept larger datagram.

5. Identification, Flag and Offset

Identification

This field identifies the datagram originating from the source host. When a datagram is fragrmented, the value in the identification field is copied into all fragments. The identification number helps the destination in reassembling the fragments of the datagram.

Flag

This is a three bit field. The 3 bits are as shown in figure 4.25

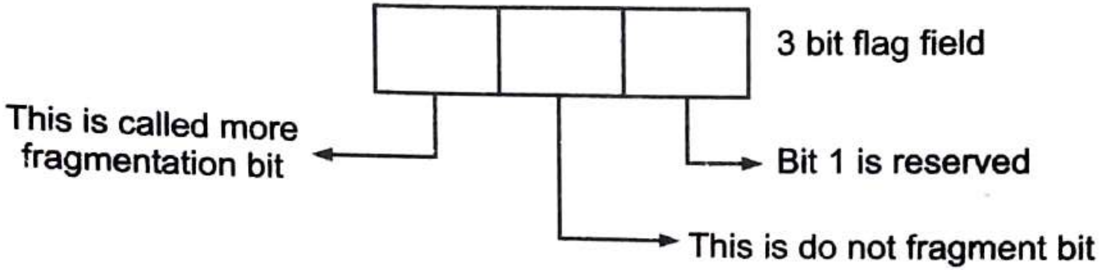


Fig. 4.25 Flag bits

First bit reserved, and it should be 0. The second bit is called *Do not Fragment* bit. If this bit is "I" then machine should not fragment the datagram. But if the value of this bit is 0 then the machine should fragment the datagram if only if necessary. The third bit is called as "More Fragment Bit". If it is 1 it means that the datagram is not the last fragment but if its value is 0 it shows that this is the last or the only fragment.

Fragmentation Offset

This is a 13 bit field which shows the relative positions of this fragmented with respect to the whole datagram. It is the offset of the data in the original datagram measured in units of 8 bytes. To understand this refer figure 4.26. This original IP packet (datagram) contains 4000 bytes numbered from 0 to 3999. It is fragmented into three fragments.

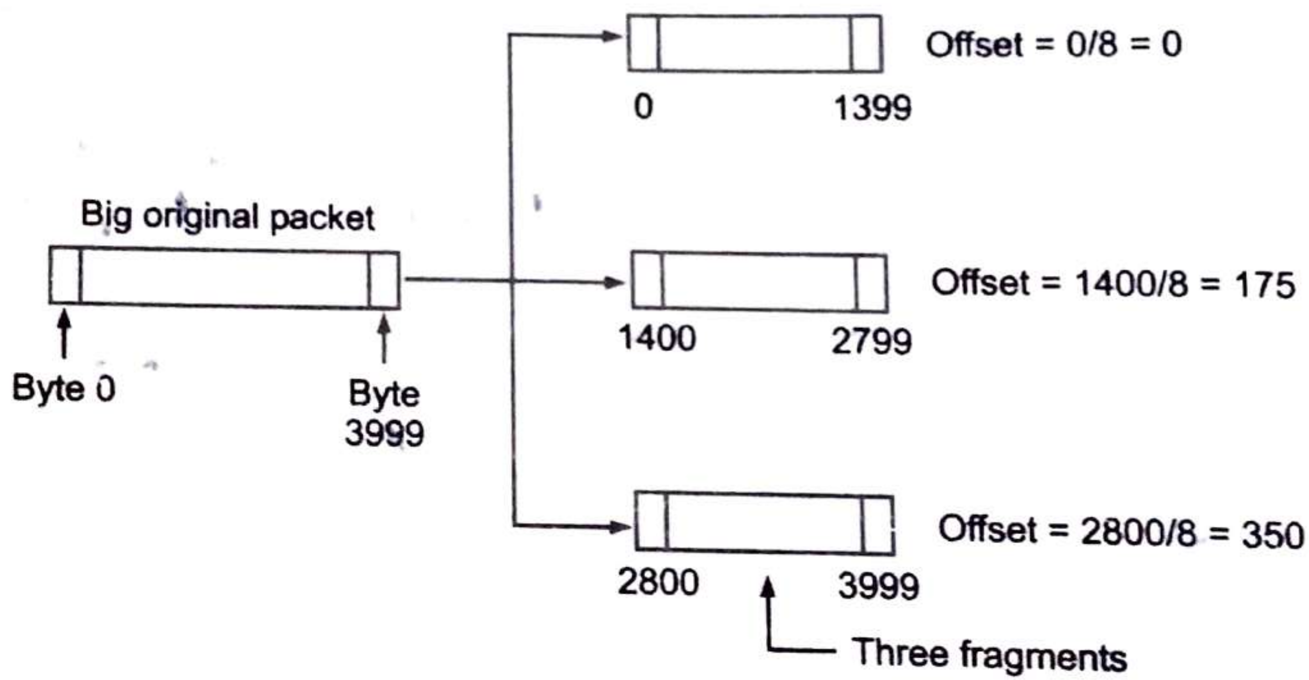


Fig. 4.26 Example of fragmentation

The first fragment contains 1400 bytes numbered from 0 to 1399. The offset for this fragment is 0/8 = 0. Similarly the offsets for the other two fragments are 1400/8 = 175 and 2800/8 = 350 respectively as shown in figure 4.27. The offset is measured in unit of 8 bytes. Because the length of the offset field is 13 bits. Hence, the fragments should be of size such that first byte number is divisible by 8.

6. Time to live

This is a 8 bit log field which controls the maximum number of routers visited by the datagram.

7. Protocol

This field defines the higher-level protocol which uses the services of the IP layer. An IP datagram can encapsulate data from various higher level protocols such as TCP, DUP, ICMP and IGMP. The protocol field specifies the final destination protocol to which the IP datagram should be delivered. Since IP multiplexes and demultiplexes data from different higher level protocols, the value of protocol field helps in demultiplexing at the final destination.

8. Header checksum

A checksum in IP packet covers on the header only. Since some header fields change, this field is recomputed and verified at each point that the Internet header is processed.

9. Source address

This field is used for defining the IP address of the source.

10. Destination Address

This field is used for defining the IP address of the destination.

11. Options

Options are not required for every datagram. They are used for network testing and debugging. IP provides several optional features, allowing a packet's sender to set requirements on the path it takes through the network (source routing), trace the route a packet takes (record route), and label packets with security features.

4.11.3. Services Provided

IP provides the following services:

Addressing

IP headers contain 32-bit addresses which identify the sending and receiving hosts. These addresses are used by intermediate routers to select a path through the network for the packet.

Fragmentation

IP packets may be split, or fragmented, into smaller packets. This permits a large packet to travel across a network which can only handle smaller packets. IP fragments and reassembles packets transparently.

Packet time out

Each IP packet contains a Time to Live (TTL) field, which is decremented every time a router handles the packet. If TTL reaches zero, the packet is discarded, preventing packets from running in circles forever and flooding a network.