INTERNET PROTOCOL (IP)

- NETWORK LAYER PROTOCOL
- IP — unreliable, connectionless protocol.
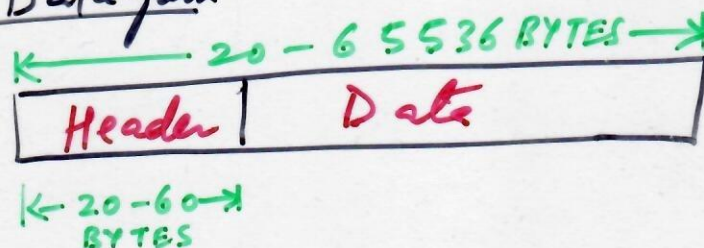- IP is best effort delivery service — No error checking

IP must be combined with TCP (reliable protocol) if reliability is important.

  Datagrams — different route to destination.
  Datagrams — could be out of order, could be lost or corrupted during transmission.

DATAGRAM   IP layer packets are called datagrams.

IP Datagram

$$\xleftarrow{\hspace{1cm}} 20 - 65536 \text{ BYTES} \longrightarrow$$

Header	Data

$\xleftarrow{} 20-60 \xrightarrow{}$ BYTES

HEADER

VER 4 bits	HLEN 4 bits	DS 8 bits		Total bits Length 16 bits	
Identification 16 bit			Flags 3 bits	Fragmentation offset 13 bits	
Time to Live 8 bits		Protocol 8 bits	Header Checksum 16 bits		
Source IP Address					
Destination IP Address					
Option					

VERSION (VER) version of IP protocol.
Header Length length of datagram header in 4 byte words. Header = 20-60 bytes. when no options then header length = 20 bytes & value of this field = 5 (∵ 5×4 = 20). when option field is at maximum size the value of field = 15 (∵ 15×4 = 60).

Differentiated Services (DS). This field was previously called service type.

			D	T	R	C		

D: Minimize Delay   R: Maximize Reliability
T: Maximize Throughput   C: Minimize Cost

PRECEDENCE   TOS Bits

SERVICE TYPE

CODE POINT
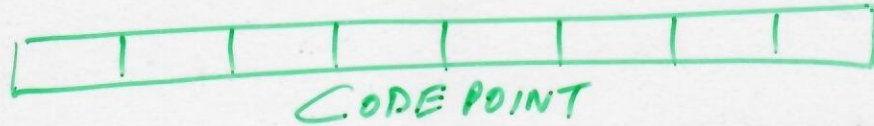
DIFFERENTIATED SERVICES

SERVICE TYPE   First 3 bits = precedence bits
Next 4 bits = TOS bits
LAST BIT → Not used

a **Precedence**   0(000) to 7(111). These bits define priority of datagram in issues such as congestion. Datagrams of lowest precedence are discarded first.

b **TOS Bits**

TOS BITS	DESCRIPTION
0000	NORMAL (DEFAULT)
0001	MINIMIZE COST
0010	MAXIMIZE RELIABILITY
0100	THROUGHPUT
1000	MINIMIZE DELAY

DIFFERENTIATED SERVICES   1st six bits = code field
next 2 bits → Not used

~~Codefield~~ Codepoint subfield can he used in 2 ways

a. when 3 rightmost bits are 0s, the 3 left most bits are interpreted the same as the precedence bits in the service type interpretation.

b. when 3 right most bits are not all 0s, 6 bits define 64 Services based on priority assignment by Internet or local authorities according to table below

Values for Codepoints

Category	Code point	Assigning Authority
1	XXXXX0	Internet
2	XXXX11	Local
3	XXXX01	Temporary or experimental

First Category = 32 service types
second " = 16 " "
Third " = 16 " "

First Category (nos 2, 4, ---- 62) assigned by Internet Authorities
IInd " (" 3, 7, 11, 15--- 63) can be used by Local "
IIIrd " (" 1, 5, 9 ---- 61) is temporary & can he used
for experimental purposes.

TOTAL LENGTH of IP datagram in bytes.

Length of data = Total Length — Header Length

Header Length = 4× value in HLEN field.

Total length field = 16 bits $\therefore$ IP datagram length = 65535 bytes
$(2^{16} - 1)$.

Fragmentation of ~~datagram~~ necessary for passing this N/Ws.
· Ethernet frame = 46 - 1500 bytes. If < 46 bytes, then some padding is used.

Identification the field used in fragmentation

Flag field used in fragmentation.

Fragmentation offset : used in fragmentation.

Time to Live field mostly used for controlling maximum nos of hops visited by the datagram.

Protocol higher level protocol that uses services of IP layer.

value	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

CHECKSUM

Source Address IP address of source, must remain same till packets reaches destination.

Destination Address must remain unchanged during IP datagram travels from both source host to dest host.

FRAGMENTATION

MAXIMUM TRANSFER UNIT (MTU)

• Each data link layer protocol has its own frame format in most protocols

• One of field in format is maximum size of data field i.e size of datagram must be less than this max size which depends upon H/w & S/w used in N/w.

IP Datagram

↓

Header	Max Length of data that can be encapsulated in a frame	Trailer

MTU

FRAME

MTUs for some N/Ws

PROTOCOL	MTU
HYPERCHANNEL	65 535
TOKEN RING (16 Mbps)	17 914
TOKEN RING (4 Mbps)	4 464
FDDI	4 352
ETHERNET	1500
X.25	576
PPP	296

To make IP independent of physical N/W, designers decided to make max length of IP datagram = 65535 bytes.

Fragmentation is reqd so that datagram passes thro' various N/Ws. Each fragment has its own header. A datagram can be fragmented several times before it reaches the final destination.

Dest host does re-assembly of fragments, though fragments can reach destination thro' different routes.

FIELDS RELATED TO FRAGMENTATION

Identification 16 bit field identifies a datagram originating from source host.

Identification + Source IP Address → uniquely defines datagram.
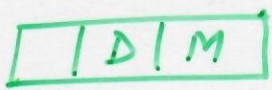
For uniqueness, labelling is done thro' counters.

Counter → set to tive value which is given to datagram

Next datagram → next value of counter.

All fragments of datagram → same value of identification number, which helps at re-assembly.

Flags 3 bit field.   1st bit ⟶ Reserved
                      2nd bit ⟶ Do not fragment (D)
                      3rd bit ⟶ More fragments (M)

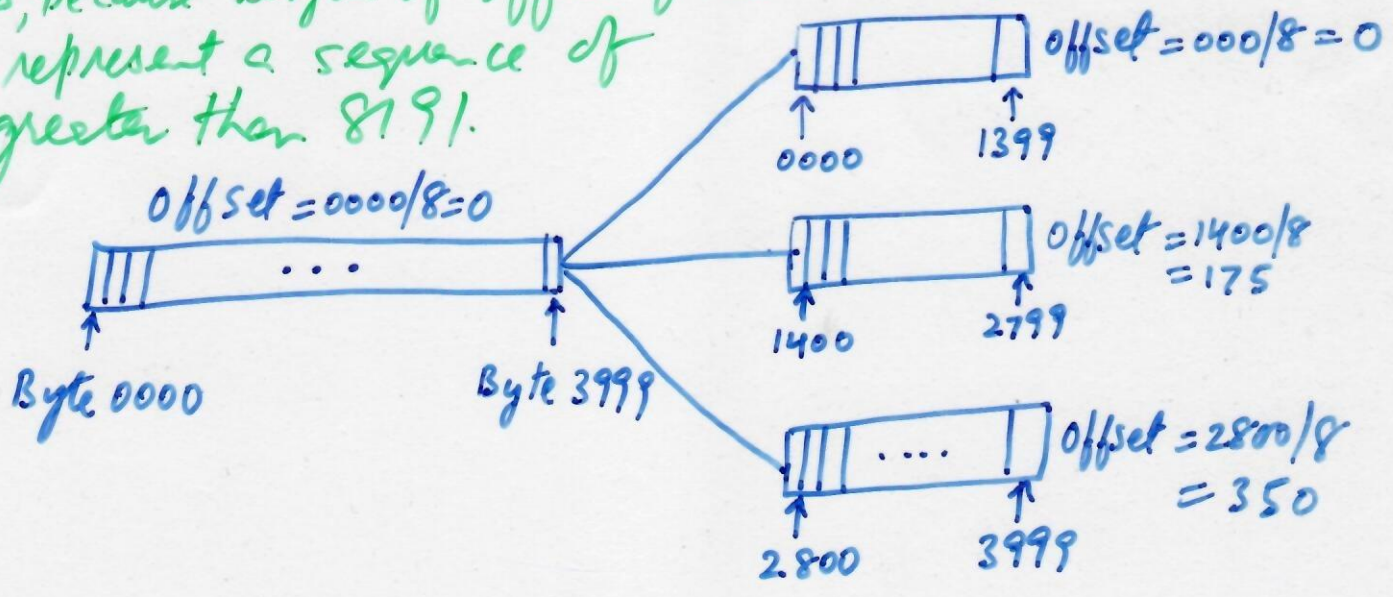|	D	M

D=1, m/c must not fragment. If doesn't pass thró a N/w
         then N/w discards it.
D=0, datagram can be
         fragmented.

M=1, datagram is not the last fragment, i.e more
         fragments after this one.

M=0   this is last or only fragment.

FRAGMENTATION OFFSET   13 bit field shows relative
position of this fragment w.r.t whole datagram.

    OFFSET of data in original datagram measured in units of
8 bytes, because length of offset field is only 13 bits long &
can't represent a sequence of
bytes greater than 8191.

Offset=0000/8=0   offset=000/8=0

Byte 0000   Byte 3999   ↑   ↑
                                   0000   1399

                                         Offset=1400/8
                                               =175
                                   ↑   ↑
                                  1400   2799

                                         Offset=2800/8
                                               =350
                                   ↑   ↑
                                  2.800   3999

BYTES 0000-3999
ORIGINAL DATAGRAM

BYTES 0000-1399
FRAGMENT 1

BYTES 1400-2799
FRAGMENT 2

BYTES 1400-2199
FRAGMENT 2.1

BYTES 2200-2799
Fragment 2.2

BYTES 2800-3999
FRAGMENT 3
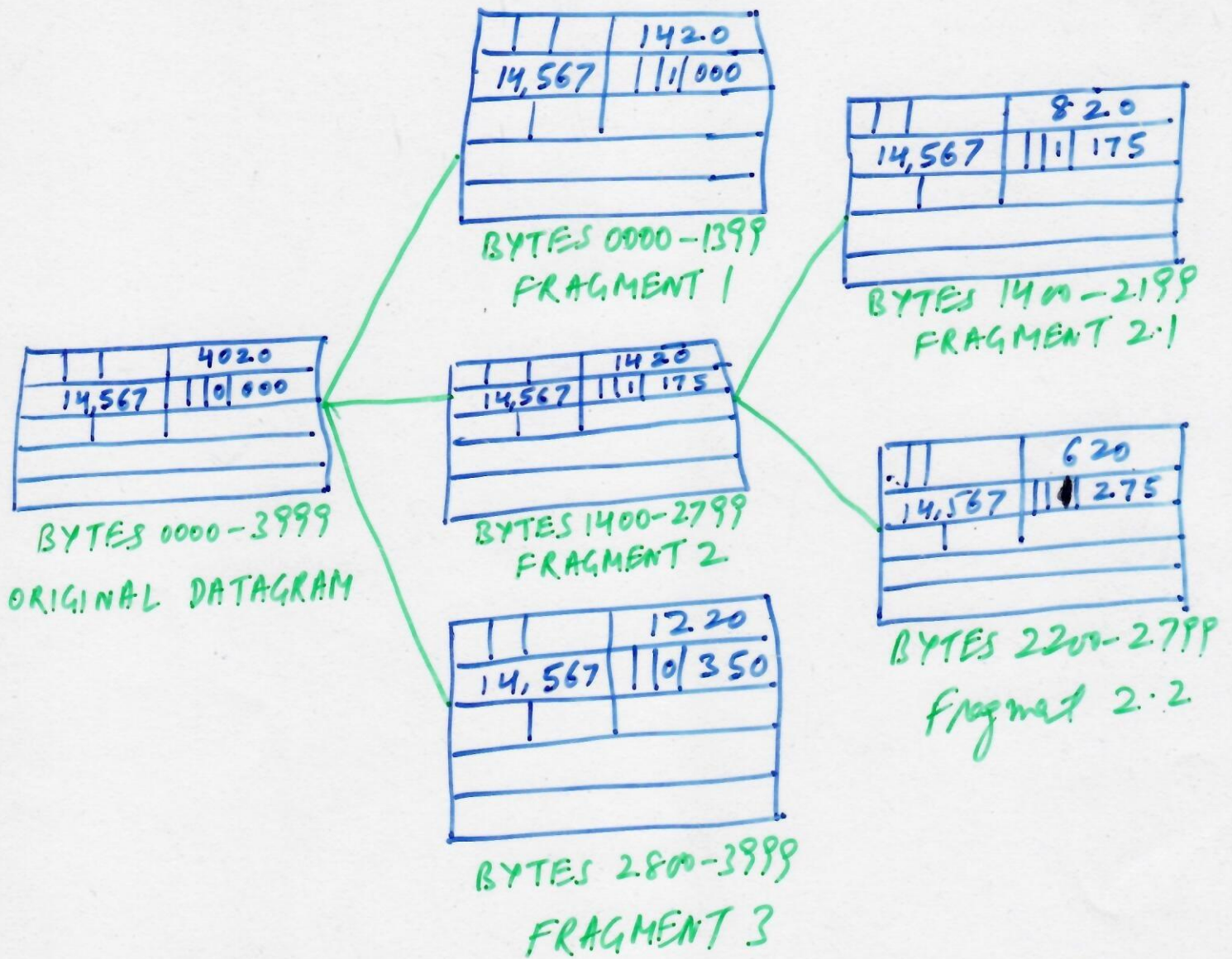
OPTIONS

variable part of header consists of OPTIONS that can be max. of 40 bytes.

Options used for N/W Testing & Debugging. reqd

Options — not part of IP header.

FORMAT

CODE 8 BITS	LENGTH 8 BITS	DATA VARIABLE LENGTH

COPY 1BIT	CLASS 2 BITS	NUMBER 5 BITS

COPY 0 COPY ONLY IN 1st FRAGMENT
      1 COPY INTO ALL FRAGMENTS

CLASS 00 DATAGRAM CONTROL
      01 RESERVED
      10 DEBUGGING & MGMT
      11 RESERVED
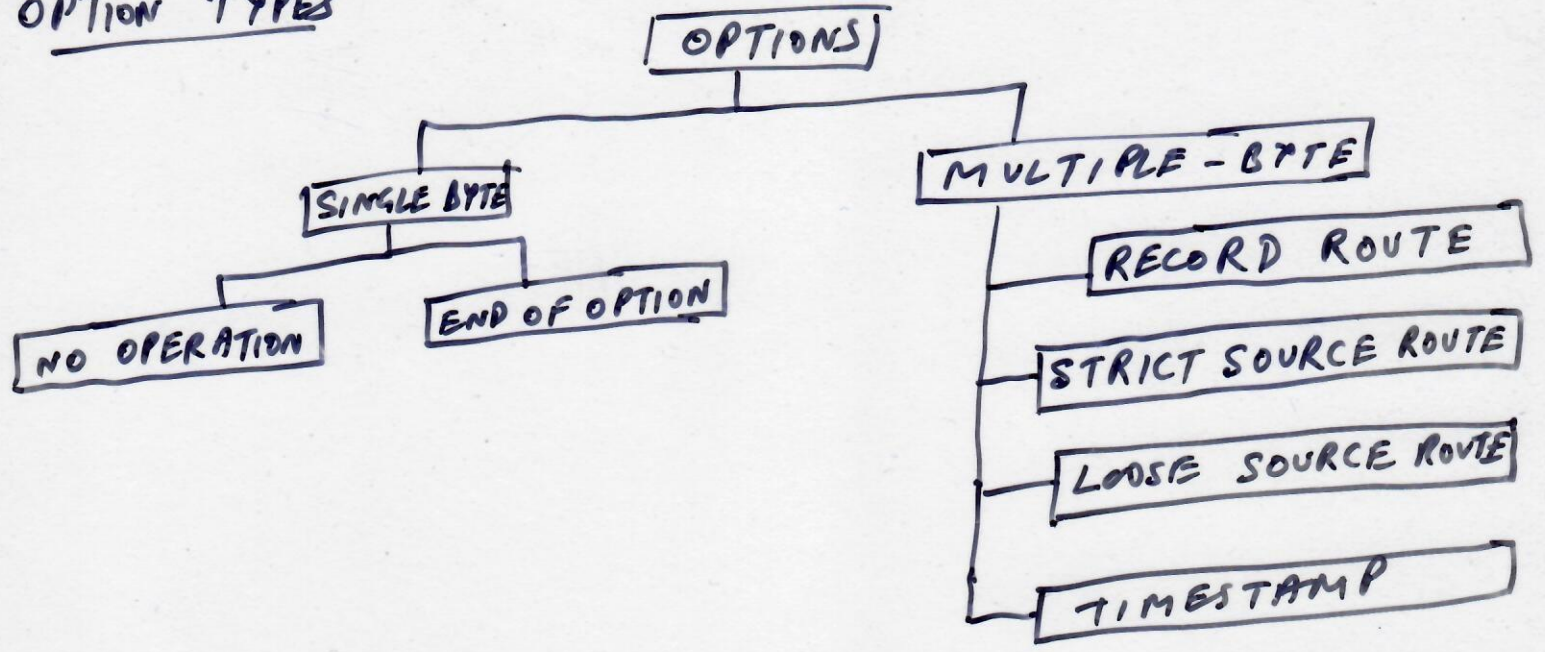
NUMBER (TYPE OF OPTION)

00000 END OF OPTION
00001 NO OPERATION
00011 LOOSE SOURCE ROUTE
00100 TIMESTAMP
00111 RECORD ROUTE
01001 STRICT SOURCE ROUTE

LENGTH defines total length of option

DATA data field contains data that specific options require.

OPTION TYPES

```
                    ┌─────────┐
                    │ OPTIONS │
                    └─────────┘
           ┌───────────────┴──────────────────┐
    ┌─────────────┐                    ┌──────────────────┐
    │ SINGLE BYTE │                    │ MULTIPLE - BYTE  │
    └─────────────┘                    └──────────────────┘
      ┌─────┴───────┐                  │  ┌──────────────────┐
┌──────────────┐ ┌────────────────┐    ├──│  RECORD  ROUTE   │
│ NO OPERATION │ │ END OF OPTION  │    │  └──────────────────┘
└──────────────┘ └────────────────┘    │  ┌──────────────────────┐
                                        ├──│ STRICT SOURCE ROUTE  │
                                        │  └──────────────────────┘
                                        │  ┌──────────────────────┐
                                        ├──│ LOOSE  SOURCE ROUTE  │
                                        │  └──────────────────────┘
                                        │  ┌──────────────────────┐
                                        └──│    TIMESTAMP         │
                                           └──────────────────────┘
```

NO OPERATION   used as a filler between options or used in
(Code1: 00000001)   beginning of an option.

END OF OPTION   padding at end of option field. After this
receiver looks for date
    (CODE0: 00000000)

RECORD ROUTE   record the internet routers that handle the
datagram.

STRICT SOURCE ROUTE: used by source to predetermine a route
for the datagram as it travels thro' the Internet. Router
addresses are filled in option field at start of journey.

LOOSE SOURCE ROUTE: similar to STRICT SOURCE ROUTE. Each route
in the list must be visited, but other routers can be visited.

TIMESTAMP   record the time of datagram processing by a
router. Time can be estimated of datagram movement from
one router to other.