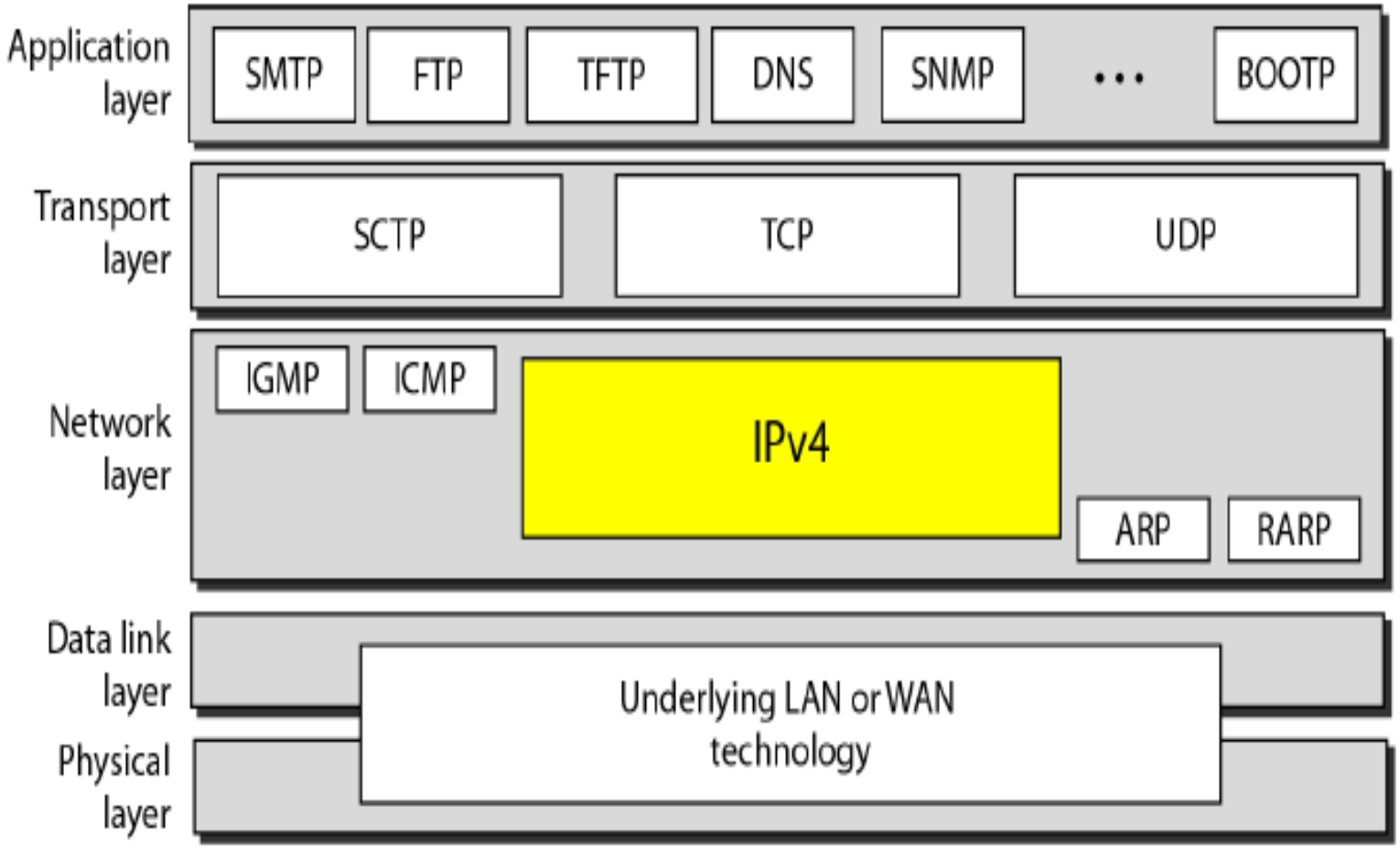
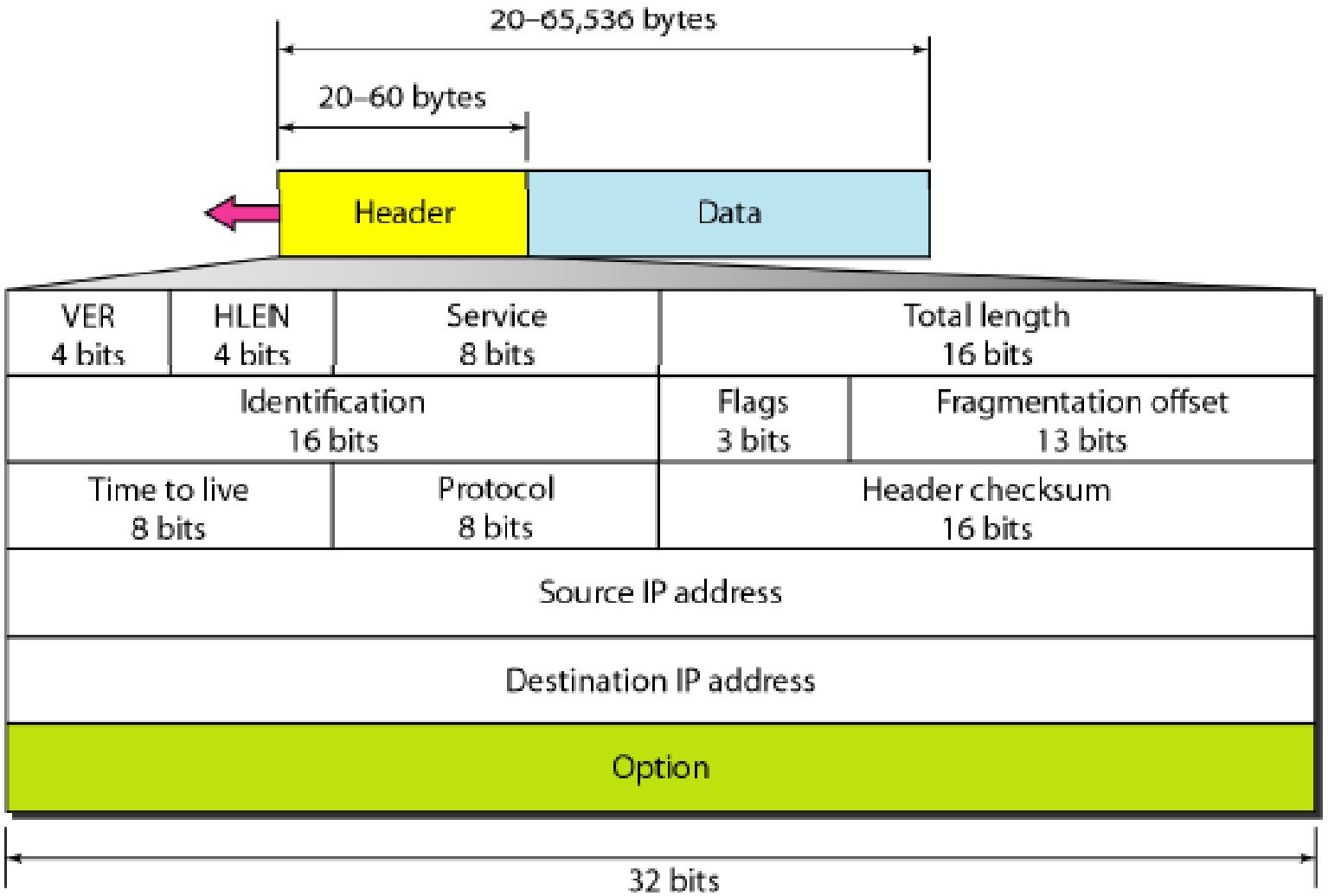
The Internet Protocol IP

The Internet Protocol IP

- The **Internet Protocol Version 4 (IPv4)** is the delivery mechanism used by the TCP/IP protocols.
- IPv4 is an unreliable and connectionless datagram protocol.
- The following figure shows the position of IPv4 in the suite


Application layer
SMTP
FTP
TFTP
DNS
SNMP
• • •
BOOTP
Transport layer
SCTP
TCP
UDP
Network layer
IGMP
ICMP
IPv4
ARP
RARP
Data link layer
Underlying LAN or WAN technology
Physical layer

Datagram

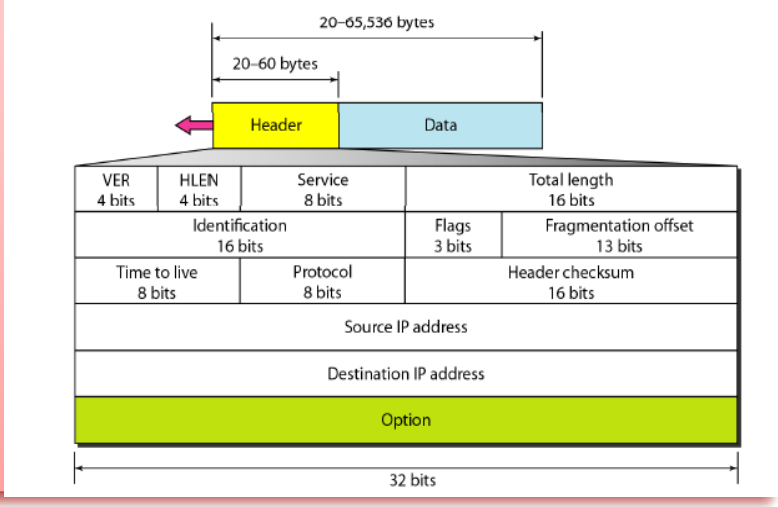

20–65,536 bytes
20–60 bytes
Header
Data
VER
4 bits
HLEN
4 bits
Service
8 bits
Total length
16 bits
Identification
16 bits
Flags
3 bits
Fragmentation offset
13 bits
Time to live
8 bits
Protocol
8 bits
Header checksum
16 bits
Source IP address
Destination IP address
Option
32 bits

- A datagram is a variable-length packet consisting of two parts:
  - Header
  - Data

  The header is 20 to 60 byte in length and contains information essential to routing and delivery.

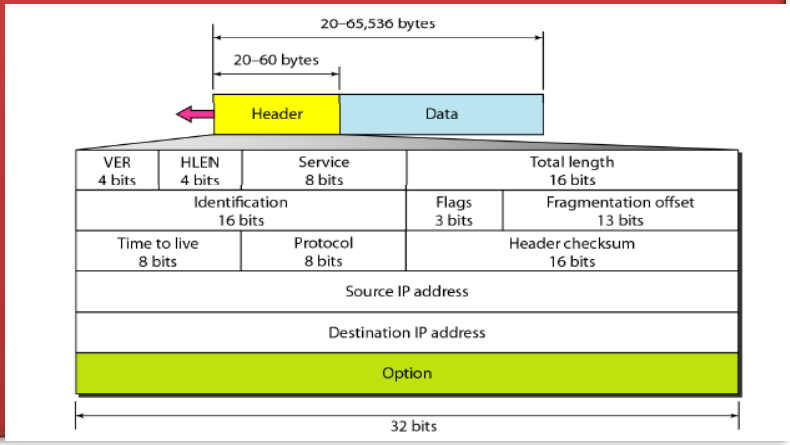
Version: (VER)

- this 4-bit field defines the version of the IP protocol.
- This field tells the IPv4 software running in the processing machine that datagram has the format of version 4.



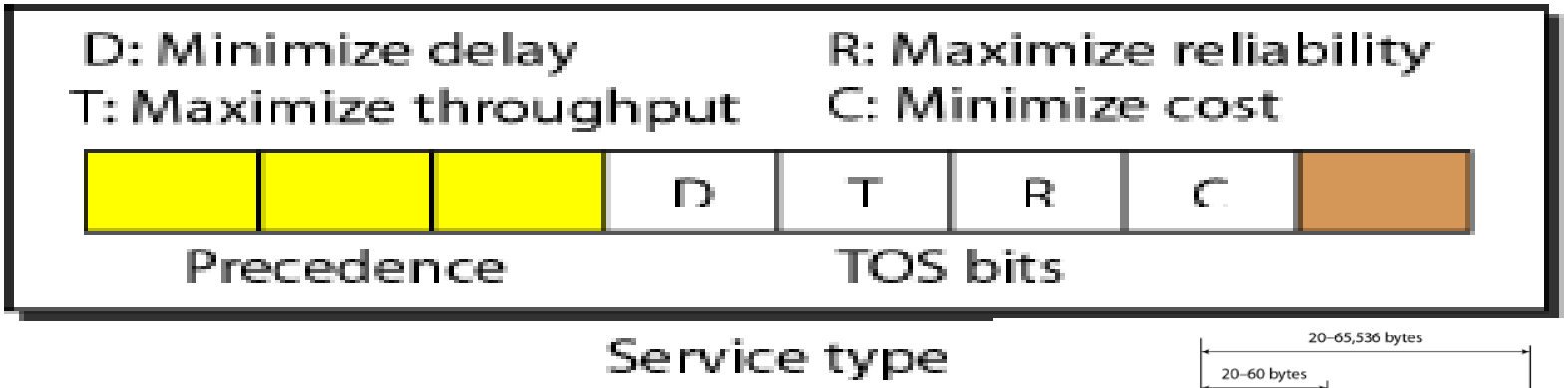
Header Length (HLEN)

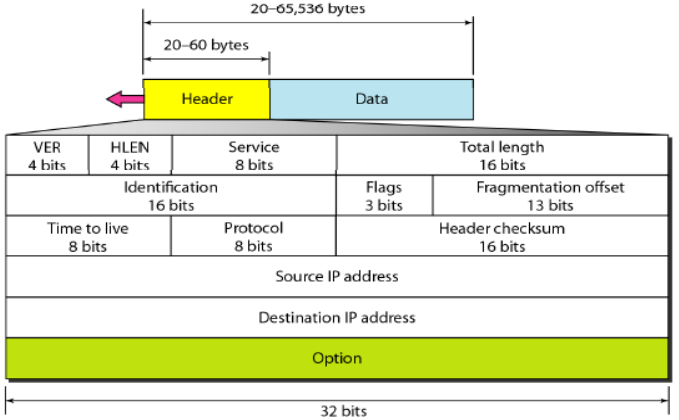
- this 4-bit field defines the total length f the datagram header in 4-byte words.
- This field is needed because the length of the header is variable (between 20 to 60 bytes).
- When there are no options, the header length is 20 bytes, and the value of this field is 5: (5 x 4 =20).
- When the option is at maximum size, the value of this field is 15 (15 x 4 = 60)



Services.

The first 3 bits are called precedence bits.
The next 4 bits are called Type of service (TOS) bits.
And the last bit is not used.





Precedence

- is 3 bits subfield: from 000 to 111 (0 to 7). These bits defines the priority of the datagram in issues such as congestion.
- For example: if a router is congested and needs to discard some datagram, those of lowest precedence are discarded first. Network management has upper precedence.

TOS bits (type of service)

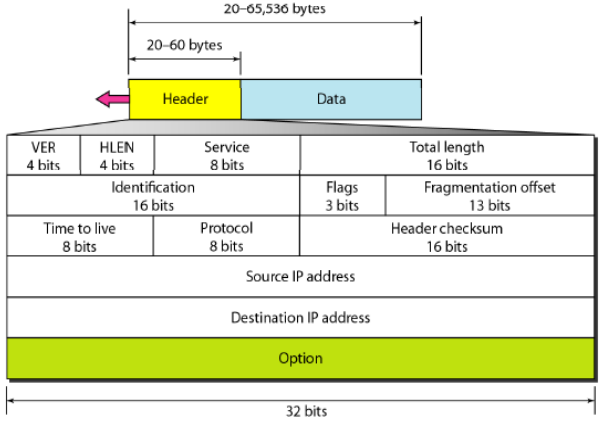
- TOS is a 4 bits subfield

TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

Protocol	*TOS Bits*	*Description*
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

Total length

- this is a 16-bit field that defines the total length (header + data) if the IPv4 datagram in byte.
- Since the field length is 16 bits, the total length of the IPv4 datagram is limited to 2^{16} -1 = 65535 bytes, of which (20 to 60) bytes are the header and the rest is data from the upper layer.
- But, some physical networks are not able to encapsulate a datagram of 65535 bytes in their frames. So, the datagram must be fragmented to be able to pass through those network.



Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

Identification

- this field is used in fragmentation

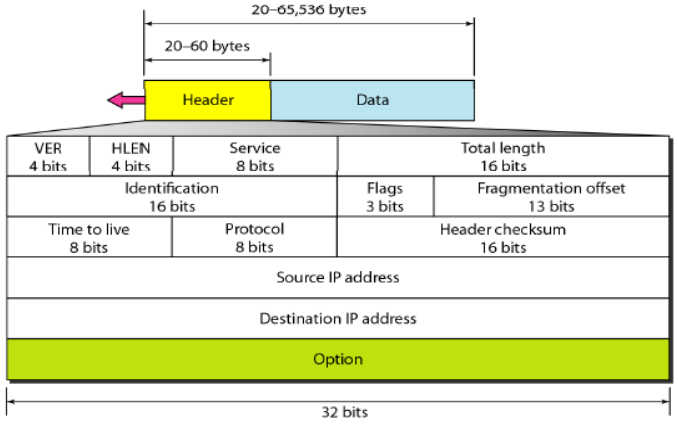
Flags

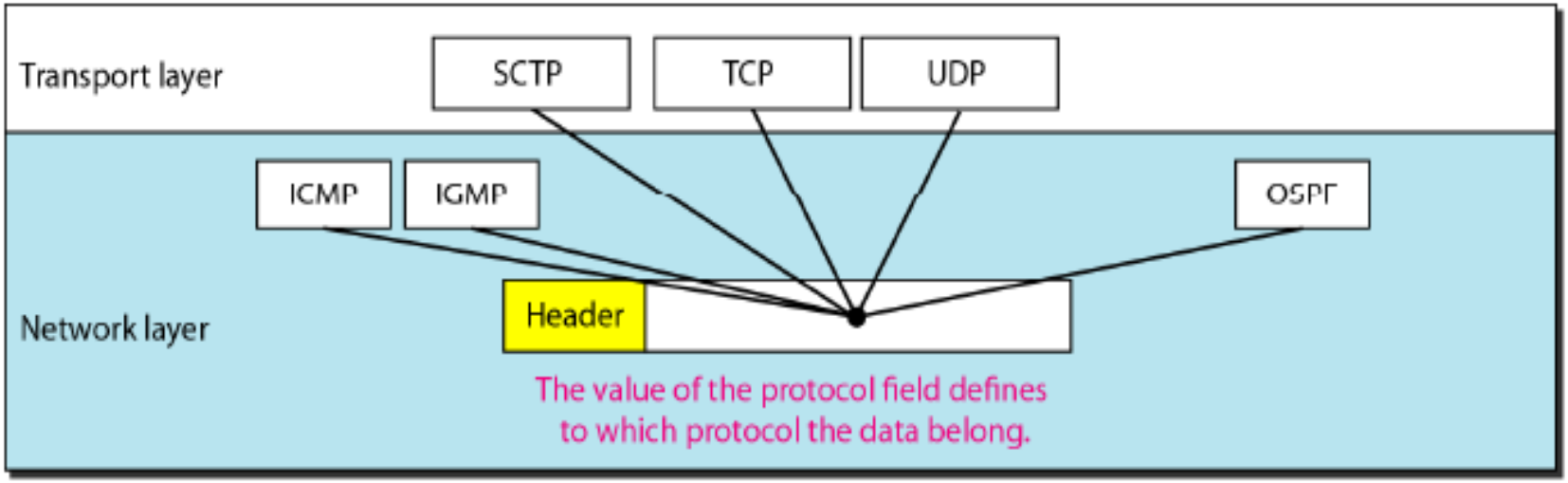
- this field is used in fragmentation

Time to live:

Protocol

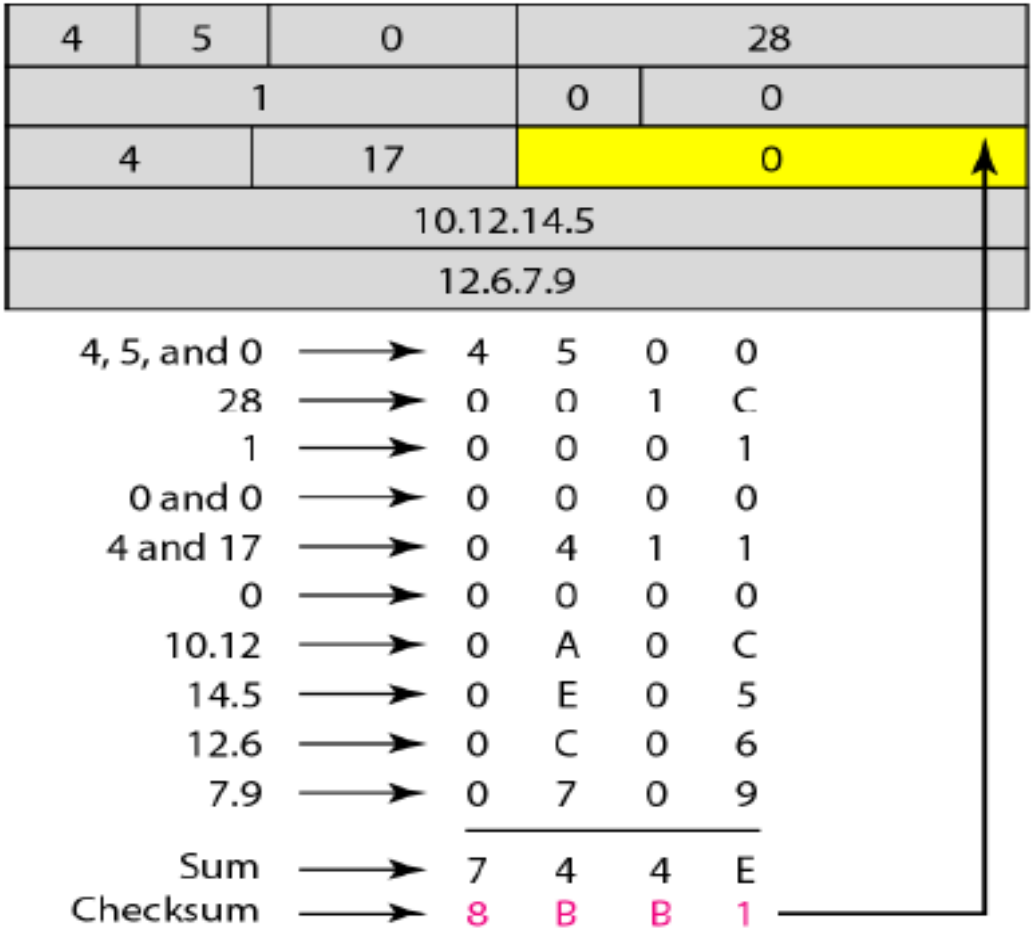
- this 8-bit field defines the higher level protocol that uses the services of IPv4 layer.
- An IPv4 datagram can encapsulate data from several higher level protocols such as TCP, UDP, ICMP.
- This field defines the final destination protocol to which the IPv4 datagram is delivered.
- (i.e. the value of this field helps the receiving network layer know to which protocol the data belong.





Value	*Protocol*
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

Checksum


4
5
0
28
1
0
0
4
17
0
10.12.14.5
12.6.7.9
4, 5, and 0 → 4 5 0 0
28 → 0 0 1 C
1 → 0 0 0 1
0 and 0 → 0 0 0 0
4 and 17 → 0 4 1 1
0 → 0 0 0 0
10.12 → 0 A 0 C
14.5 → 0 E 0 5
12.6 → 0 C 0 6
7.9 → 0 7 0 9
Sum → 7 4 4 E
Checksum → 8 B B 1

Source address

Destination address

Example

- ***An IPv4 packet has arrived with the first 8 bits as shown:***

01000010

- ***The receiver discards the packet. Why?***

Solution

- *There is an error in this packet.*
- *The 4 leftmost bits (0100)show the version, which is correct.*
- *The next 4 bits (0010)show an invalid header length (2 × 4 = 8).*
- *The minimum number of bytes in the header must be 20.*
- *The packet has been corrupted in transmission.*

Example

- ***In an IPv4 packet, the value of HLEN is 1000 in binary.***
- ***How many bytes of options are being carried by this packet?***

Solution

- ***The HLEN value is 8, which means the total number of bytes in the header is 8 × 4, or 32 bytes.***
- ***The first 20 bytes are the base header, the next 12 bytes are the options.***

Example

- ***In an IPv4 packet, the value of HLEN is 5, and the value of the total length field is 0x0028.***
- ***How many bytes of data are being carried by this packet?***

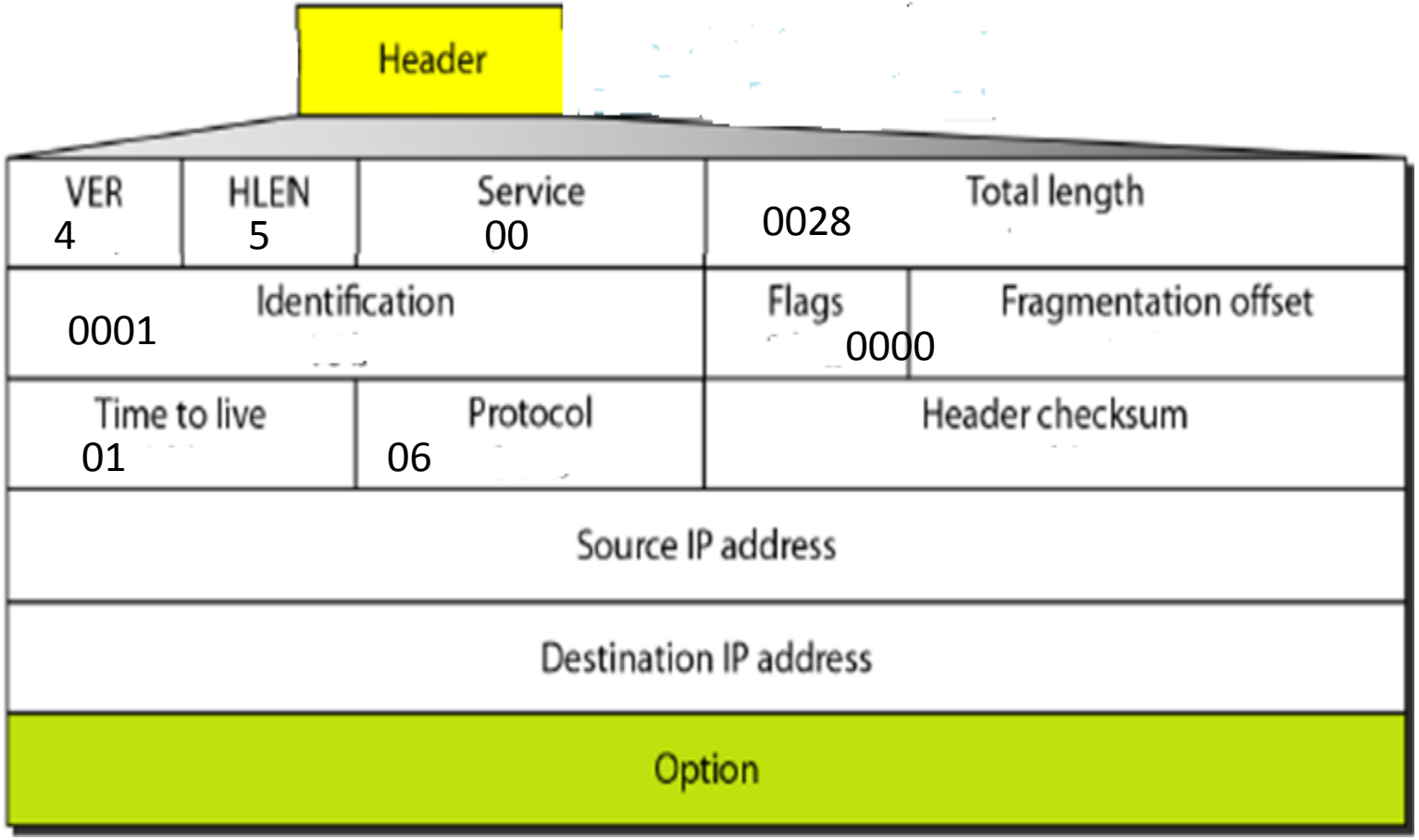
Solution

- ***The HLEN value is 5, which means the total number of bytes in the header is 5 × 4, or 20 bytes (no options).***
- ***The total length is 40 bytes, which means the packet is carrying 20 bytes of data (40 – 20).***

Example

- ***An IPv4 packet has arrived with the first few hexadecimal digits as shown.***
    - ***0x450000280001000000106 . . .***
- ***How many hops can this packet travel before being dropped? The data belong to what upper-layer protocol?***

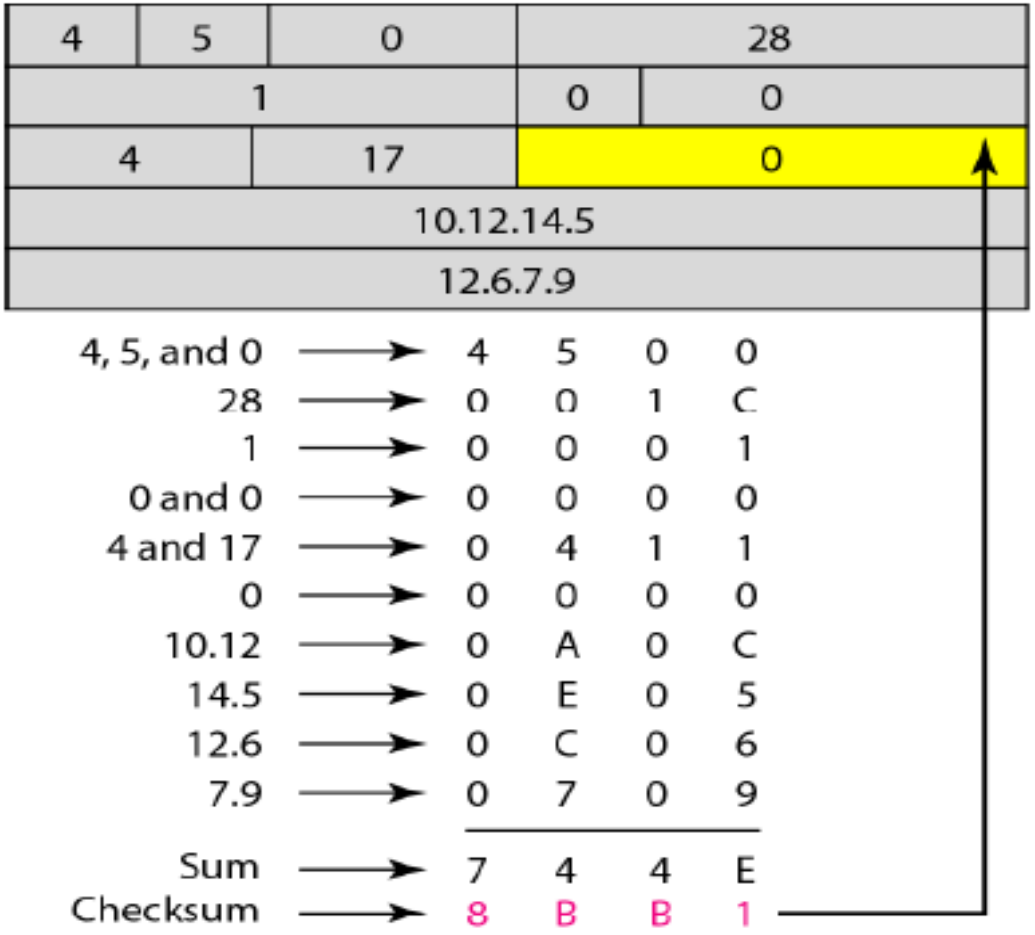
0x45000028000100000106 . . .



Solution

- *To find the time-to-live field, we skip 8 bytes.*
- *The time-to-live field is the ninth byte, which is 01.*
- *This means the packet can travel only one hop.*
- *The protocol field is the next byte (06), which means that the upper-layer protocol TCP*

Example of checksum calculation in IPv4



FRAGMENTATION

- A datagram can travel through different networks. Each router decapsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates in another frame. For example, if a router connects a LAN to a WAN, it receives a frame in the LAN format and sends a frame in the WAN format.

Maximum Transfer Unit: MTU

- To make the IPv4 protocol independent of the physical network, the designers decides to make the maximum length of the IPv4 datagram equal to 65535 bytes.
- This makes transmission more efficient if we use a protocol with an MTU of this size.
- However, for other physical networks, we must divide the datagram to make it possible to pass through these networks.
- This called **fragmentation**

- The value of the MTU depends on the physical network protocol.
- The table shows the values for some protocols:

Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

- When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but with some changed.
- A fragmented datagram may itself be fragmented if it encounters a network with an even smaller MTU.
- In other words, a datagram can be fragmented several times before it reaches the final destination.

- In IPv4, a datagram can be fragmented by the source host or any router in the path.
- The reassembly of the datagram is done only by the destination host.
- Whereas the fragmented datagram can travel through different routers.
- When a datagram is fragmented, required parts of the header must be copied by all fragments.

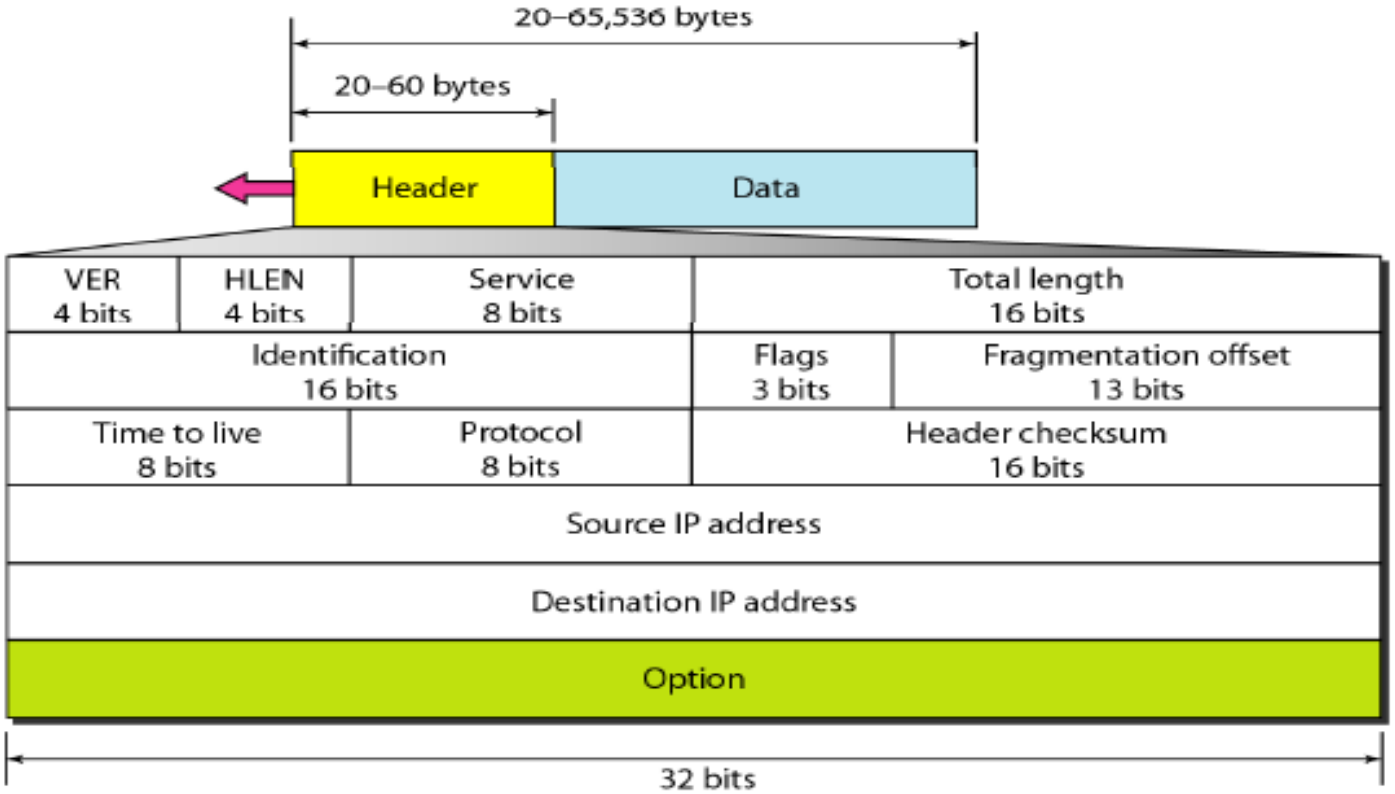
- The host or router that fragments a datagram must change the value of three fields:
- Flags
- Fragmentation offset
- Total length

- The rest of the fields must be copied.
- The values of checksum must be recalculated.

Fields Related to Fragmentation

- Identification
- Flags
- Fragmentation offset

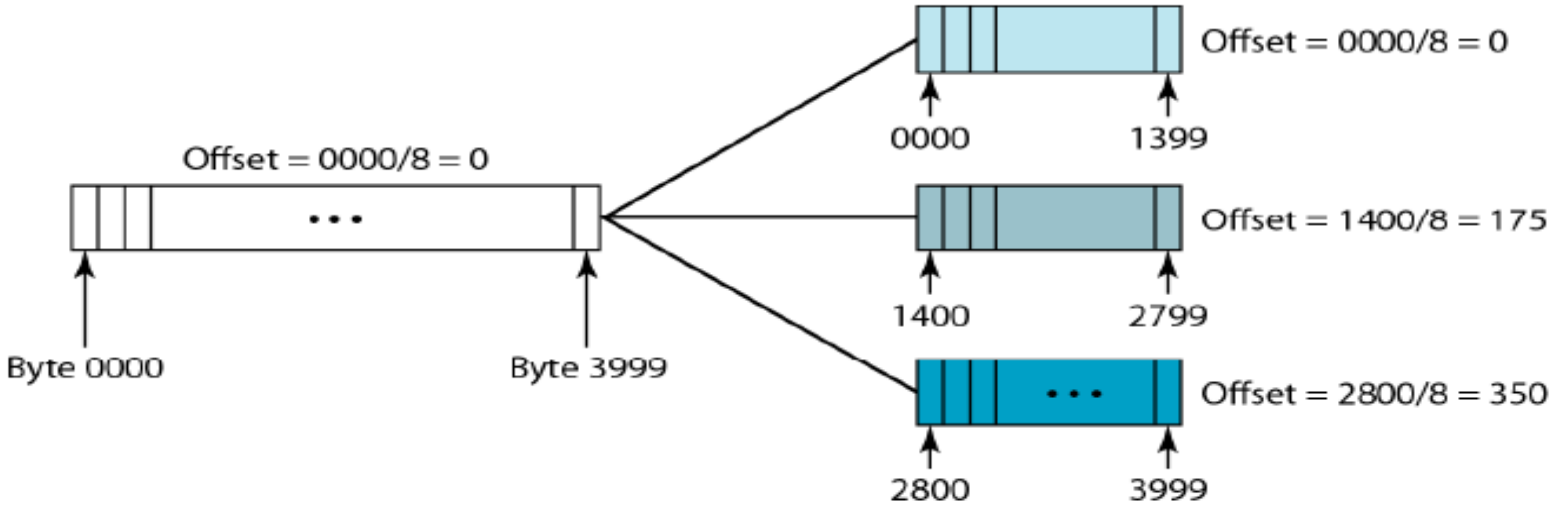
Flags used in fragmentation



- Flags: this is a 3-bit field:
- The first bit is reserved
- The second bit is called the "" do not fragment"" bit " D":
  - If " D=1", the machine must not fragment the datagram.
  - If " D=0 " the datagram can be fragmented.
- The third bit is called the ""more fragment "" bit :"M"
  - If " M=1" it means the datagram is not the last fragment; there are more.
  - If " M=0" it means this the last or only fragment

Fragmentation offset

- this 13-bit field shows the relative position of this fragment with respect to the whole datagram.



Example

- ***A packet has arrived with an M bit value of 0.***
- ***Is this the first fragment, the last fragment, or a middle fragment?***
- ***Do we know if the packet was fragmented?***

Solution:
while the M bit is 0, it means that there are no more fragments; the fragment is the last one.
However, we cannot say if the original packet was fragmented or not.
A non-fragmented packet is considered the last fragment.

Example

- ***A packet has arrived with an M bit value of 1.***
- ***Is this the first fragment, the last fragment, or a middle fragment?***
- ***Do we know if the packet was fragmented?***

Solution

While the M bit is 1, it means that there is at least one more fragment.

This fragment can be the first one or a middle one, but not the last one.

We don't know if it is the first one or a middle one; we need more information (the value of the fragmentation offset)

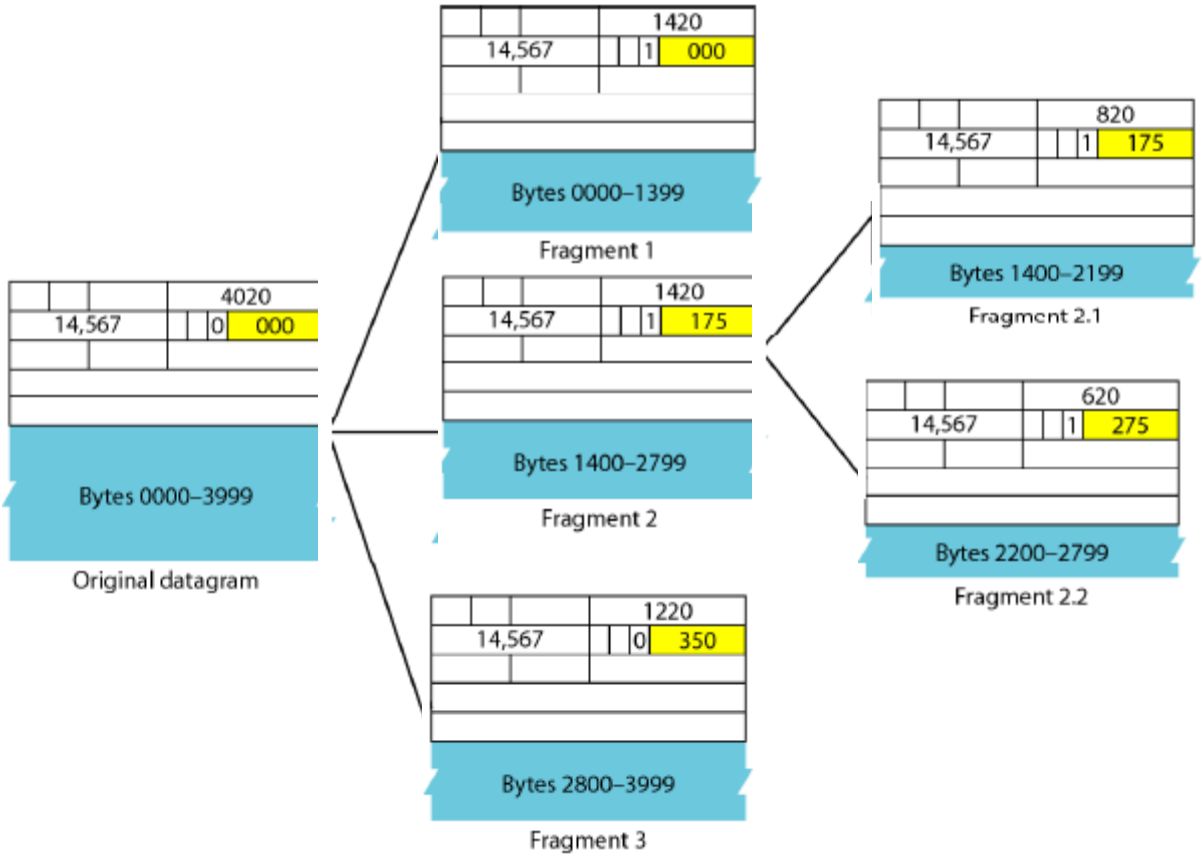
Example

- ***A packet has arrived with an M bit value of 1 and a fragmentation offset value of 0.***
- ***Is this the first fragment, the last fragment, or a middle fragment?***

Solution

Because the M bit is 1, it is either the first fragment or a middle one. Because the offset value is 0, it is the first fragment

Fragmentation example



D: Do not fragment
M: More fragments

Priority

- If one of two consecutive datagram must be discarded due to the congestion, the datagram with lower packet priority will be discarded.
- IPv6 divides traffic into two categories :
- 1- congestion controlled traffic
- 2- non-congestion controlled traffic

1- congestion controlled traffic

Priority	*Meaning*
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

1-No specific traffic

- A priority of 0 is assigned to packet when the process does not define a priority

2- Background data

- Delivery of the news is a good example

3- reserved

4-Unattended data traffic

- E- mail belongs to this group

5- Attended bulk data traffic

- A protocol that transfers data while the user is waiting to receive the data (delay) is given priority 4. TFTP and HTTP belongs to this group

6- Interactive traffic

- Protocol such as TELNET that need user interaction are assigned to the second highest priority 6 in this group

7- Control traffic

- Routing protocol such as OSPF and RIP and SNMP protocols have this priority

2- non- congestion controlled traffic

Priority	*Meaning*
8	Data with greatest redundancy
. . .	. . .
15	Data with least redundancy