Network layer

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).

NETWORK-LAYER SERVICES

- **Logical addressing**: If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems, i.e logical addresses of the sender and receiver.

- **Routing**: When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.

- One of the functions of the network layer is to provide this mechanism. Network layer is responsible for routing the packet from its source to the destination.

- There is more than one route from the source to the destination. The network layer is responsible for finding the best one routes using routing protocols.

- **Packetizing:** Encapsulating the payload (data received from upper layer) in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination.

- Adds a header that contains the source and destination addresses and some other information that is required by the network-layer protocol and delivers the packet to the data-link layer.

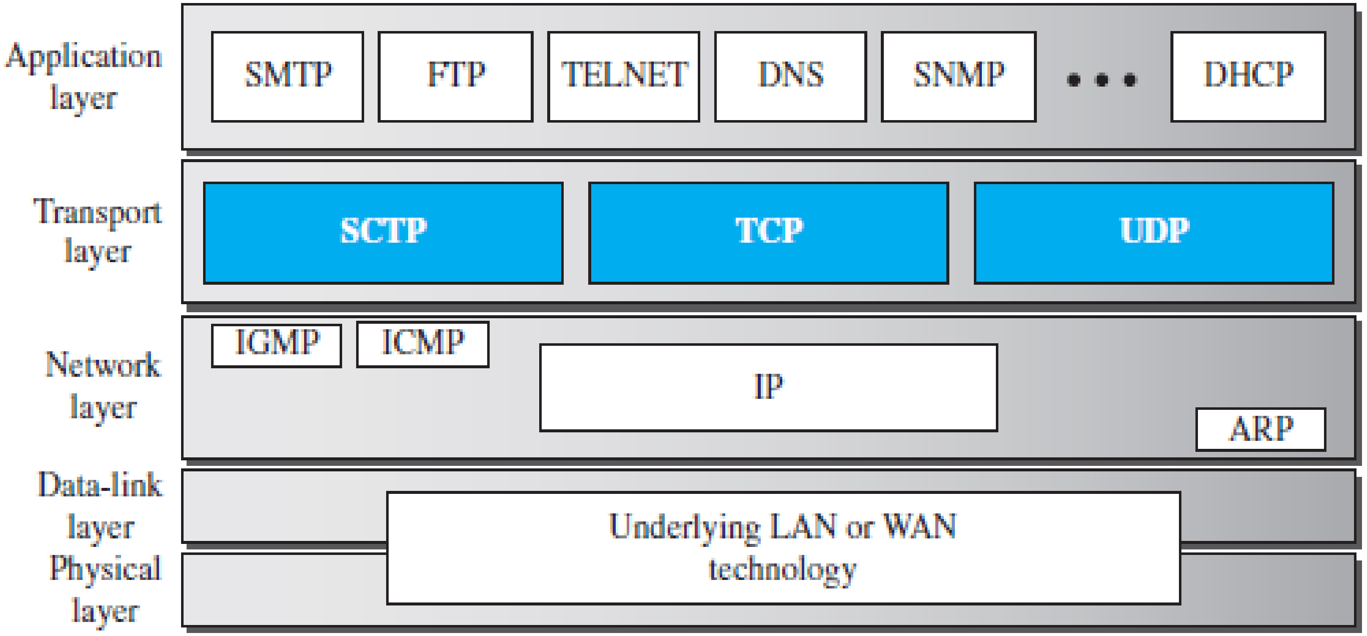
- The source is not allowed to change the content of the payload unless it is too large for delivery and needs to be fragmented.

- The routers in the path are not allowed to decapsulate the packets they received unless the packets need to be fragmented.

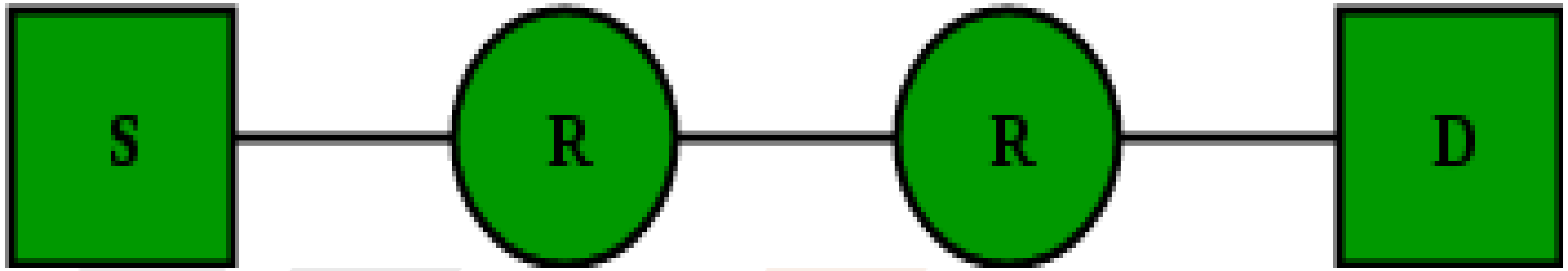
- **Error Control:** Error control is not directly provided in the Network layer, but checksum is added in datagram to control any corruption in header, but not in whole datagram. Although we use a protocol ICMP which provides some level of error control.

- **Flow Control:** Network Layer does not directly provide any flow control, the job of the network layer at the receiver is so simple that it may rarely be overwhelmed.

- **Congestion Control:** Congestion in the network layer is a situation in which too many datagrams are present in an area of the Internet. Congestion may occur if the number of datagrams sent by source computers is beyond the capacity of the network or routers.



Q Assume that source S and destination D are connected through two intermediate routers labelled R. Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D. **(GATE-2013) (1 Marks)**

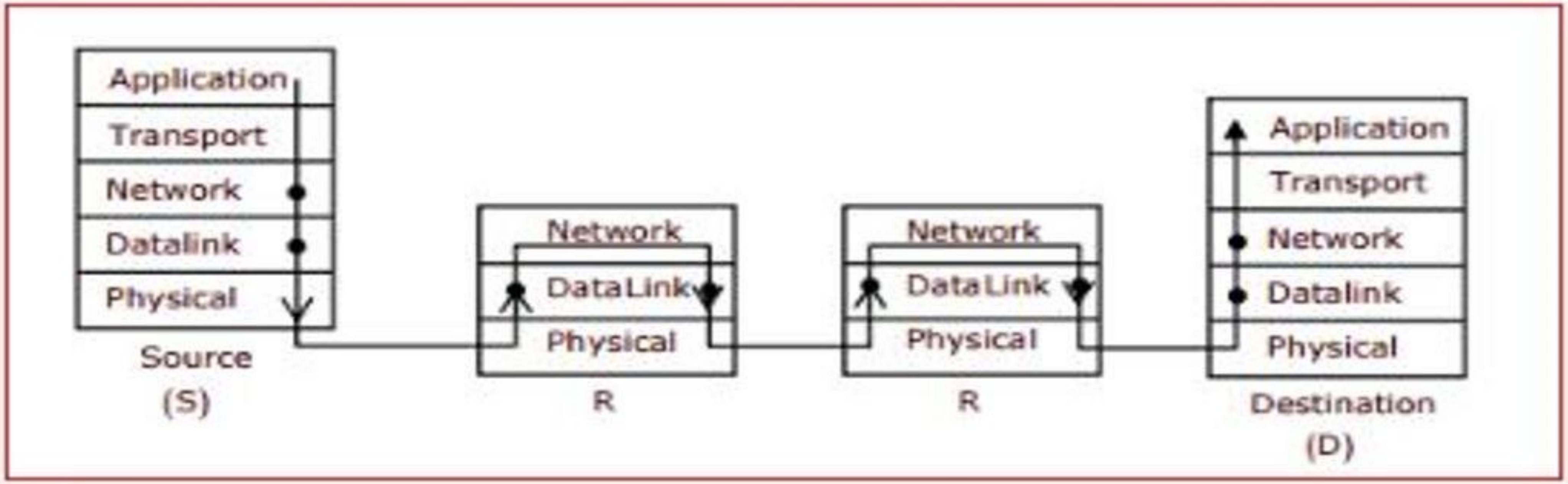


(A) Network layer – 4 times and Data link layer – 4 times

(B) Network layer – 4 times and Data link layer – 3 times

(C) Network layer – 4 times and Data link layer – 6 times

(D) Network layer – 2 times and Data link layer – 6 times


Application
Transport
Network
Datalink
Physical
Source
(S)
Network
DataLink
Physical
R
Network
DataLink
Physical
R
Application
Transport
Network
Datalink
Physical
Destination
(D)

Q Which one of the following statements is FALSE? **(GATE-2004) (1 Marks)**

(A) Packet switching leads to better utilization of bandwidth resources than circuit switching.

(B) Packet switching results in less variation in delay than circuit switching.

(C) Packet switching requires more per packet processing than circuit switching

(D) Packet switching can lead to reordering unlike in circuit switching

Break

IPv4

- IPv4 is an ***unreliable connectionless datagram protocol***—a best-effort delivery service.

- The term *best-effort* means that IPv4 packets can be corrupted, be lost, arrive out of order, or be delayed, and may create congestion for the network.

- ***datagram*** approach means Each datagram is handled independently, and each datagram can follow a different route to the destination.

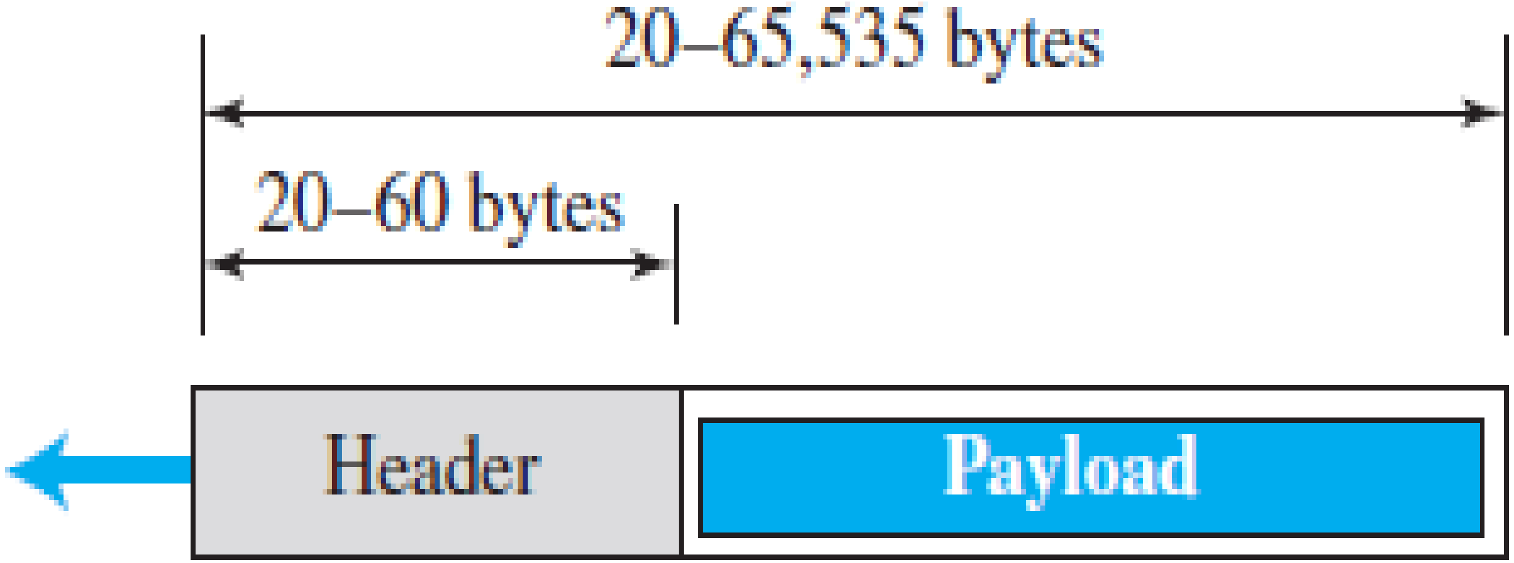
- If reliability is important, IPv4 must be paired with a reliable protocol such as TCP, so the delivery mechanism used is TCP/IP protocols.

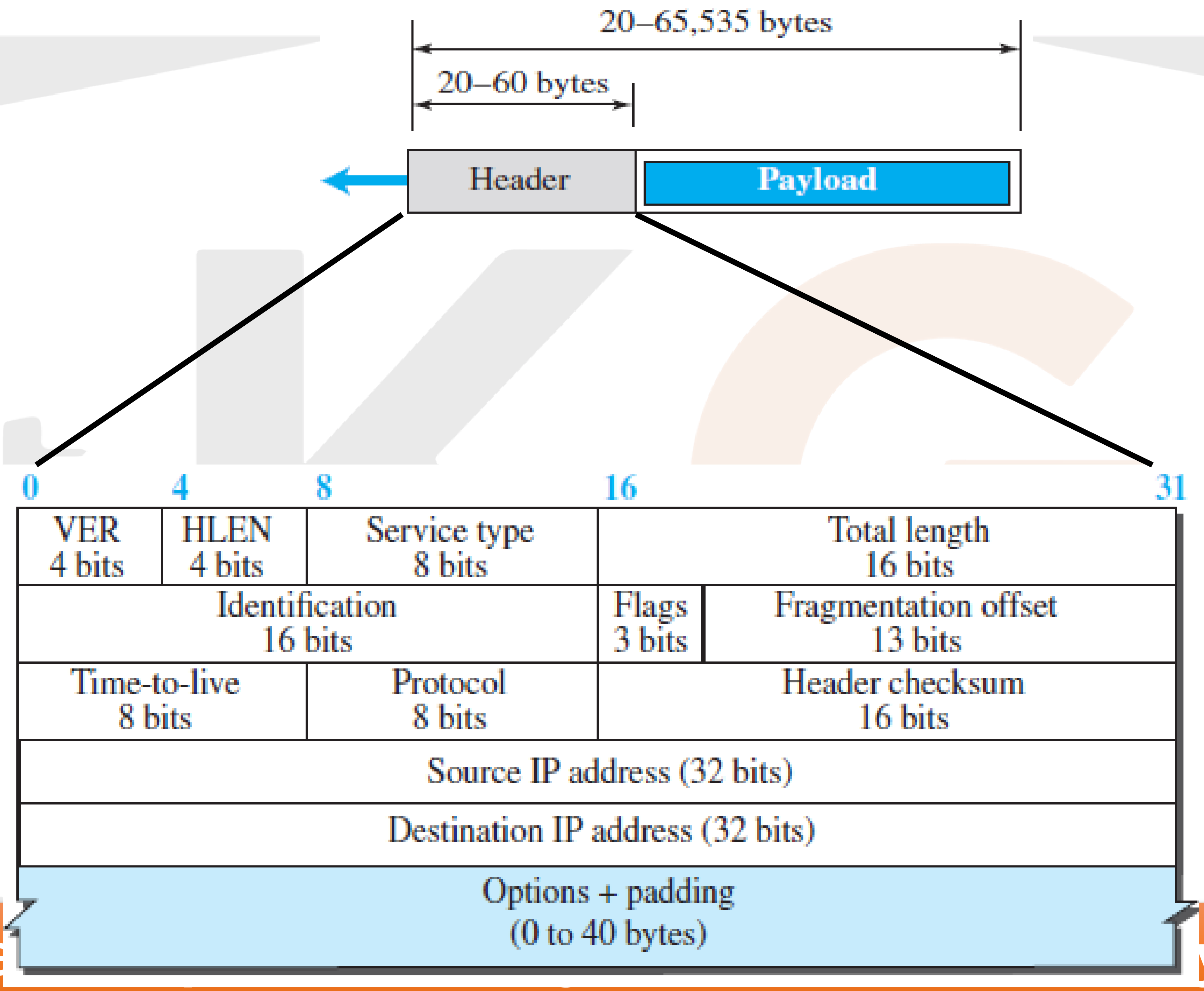
Datagram Format

- Packets used by the IP are called ***datagrams*.**

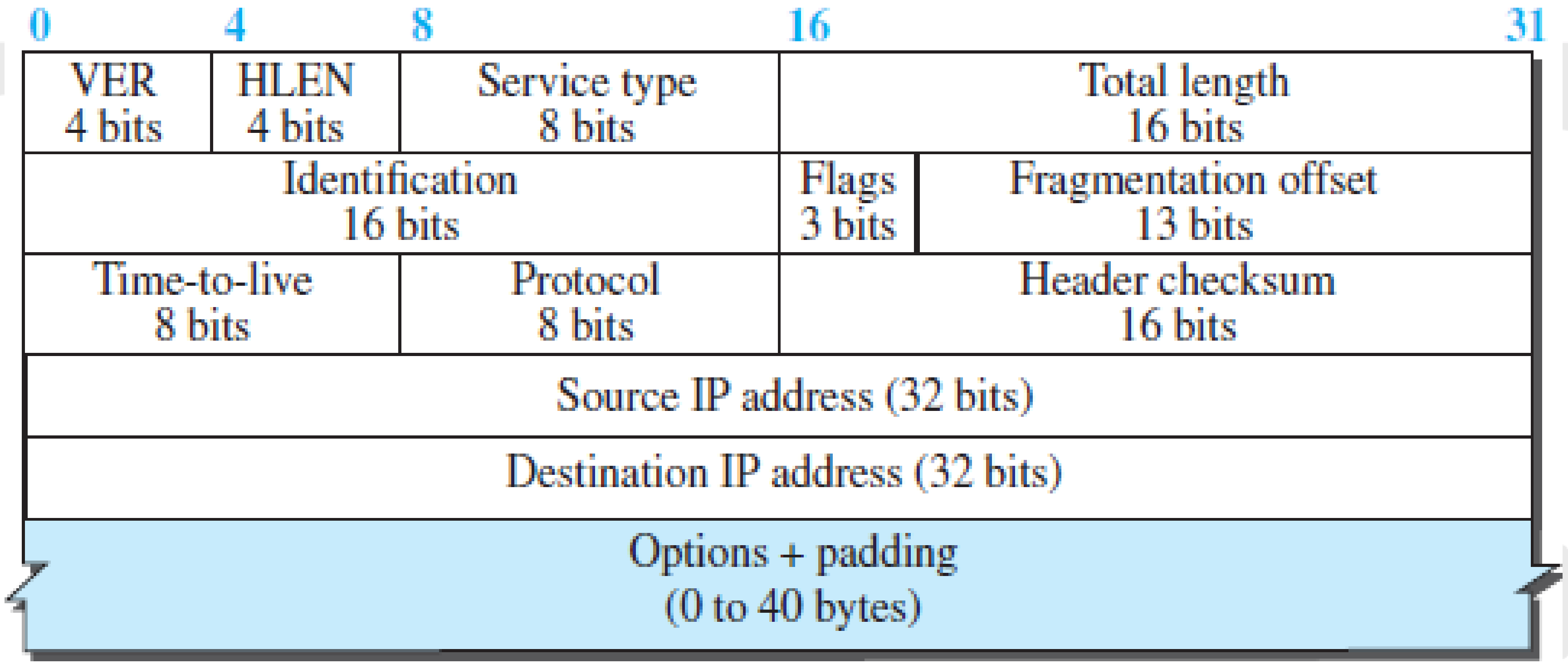
- A datagram is a variable-length packet consisting of two parts: header and payload (data).

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





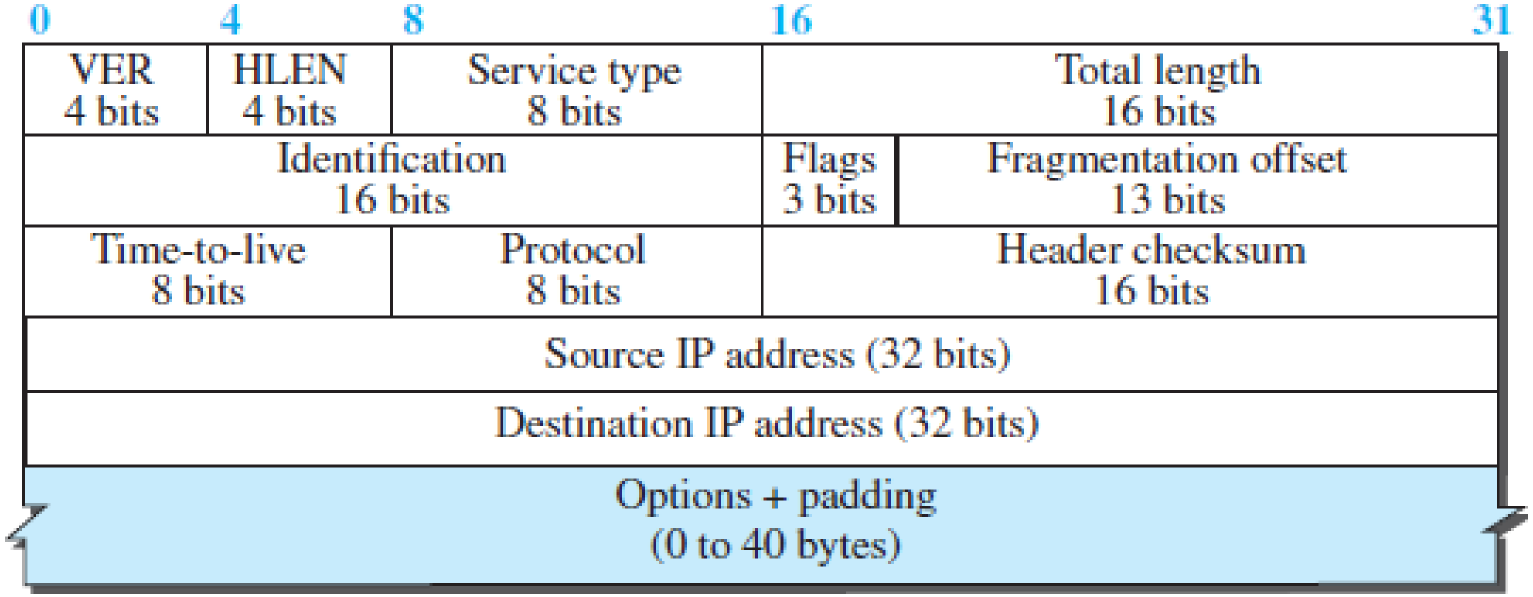
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				



0	4	8	16	31
VER 4 bits	HLEN 4 bits	Service type 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 (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

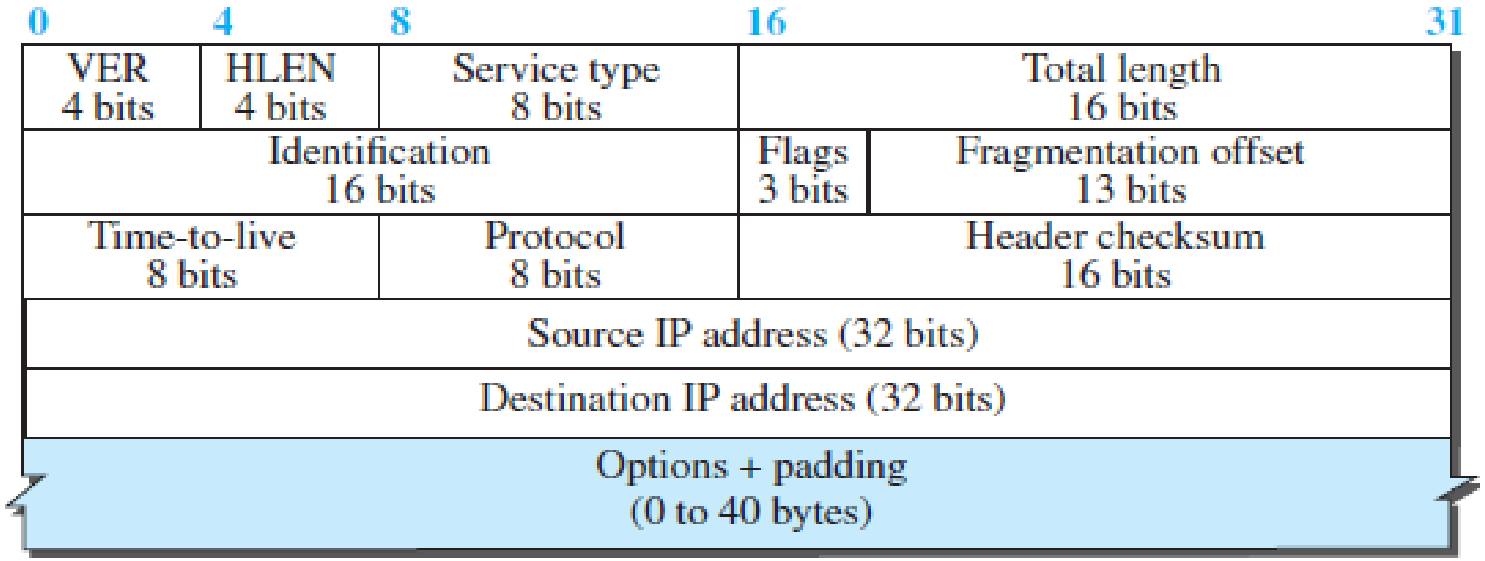
- ***Version Number.*** The 4-bit version number (VER) field defines the version of the IPv4 protocol, which, has the value of 4.

- **Header Length.** The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words. The IPv4 datagram has a variable-length header.
- **Scaling Factor:**
  - To make the value of the header length (number of bytes) fit in a 4-bit header length, the total length of the header is calculated as 4-byte words.
  - The total length is divided by 4 and the value is inserted in the field.
  - The receiver needs to multiply the value of this field by 4 to find the total length.
  - Example: If header length field contains decimal value 5 (represented as 0101), then Header length = 5 x 4 = 20 bytes



0	4	8	16	31
VER 4 bits	HLEN 4 bits	Service type 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 (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

- **<u>Point to Note</u>**
  - The length of IP header always lies in the range of [20 bytes, 60 bytes]
  - The initial 5 rows of the IP header are always used. So, ***minimum length of IP header*** = 5 x 4 bytes = 20 bytes.
  - The size of Options field can go up to 40 bytes. So, ***maximum length of IP header*** = 20 bytes + 40 bytes = 60 bytes.
  - The range of header length field value is always [5, 15] as [20/4 = 5, 60/4 = 15]
  - The range of header length is always [20, 60].



0 4 8 16 31

VER 4 bits | HLEN 4 bits | Service type 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

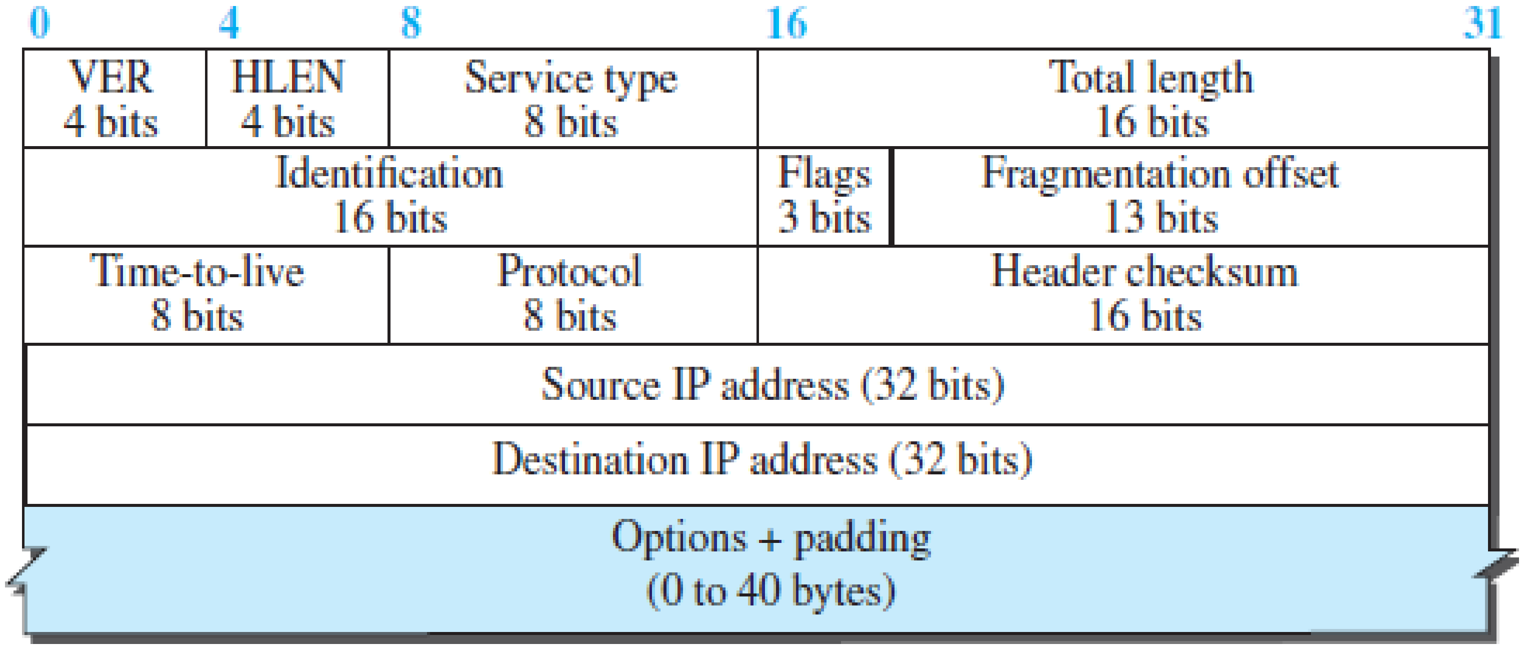
Source IP address (32 bits)

Destination IP address (32 bits)

Options + padding (0 to 40 bytes)

- **Services** - IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.

- Precedence is a 3-bit subfield ranging from 0 (000 in binary) to 7 (111 in binary). The precedence defines the priority of the datagram in issues such as congestion. If a router is congested and needs to discard some datagrams, those datagrams with lowest precedence are discarded first.



0 4 8 16 31

VER 4 bits | HLEN 4 bits | Service type 8 bits | Total length 16 bits

Identification 16 bits | Flags 3 bits | Fragmentation offset 13 bits

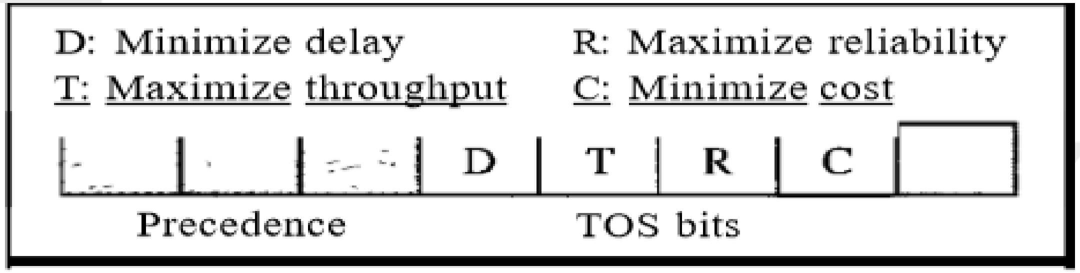
Time-to-live 8 bits | Protocol 8 bits | Header checksum 16 bits

Source IP address (32 bits)

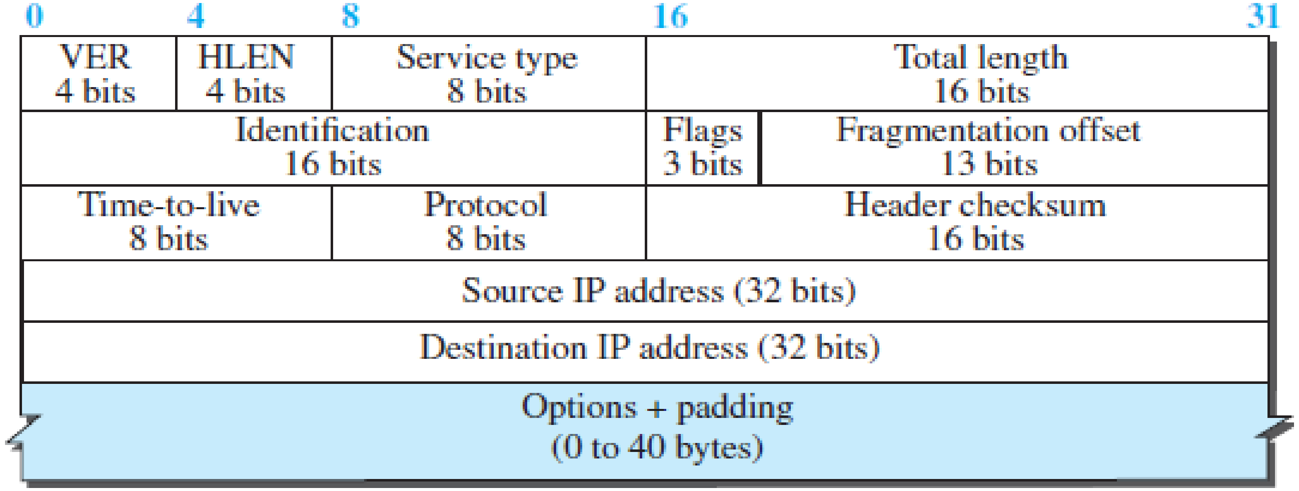
Destination IP address (32 bits)

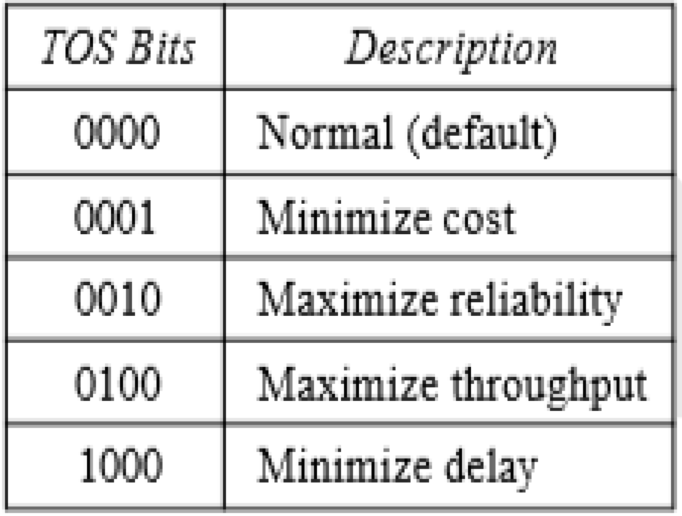
Options + padding (0 to 40 bytes)

- ***Service Type*.** It defines how the datagram should be handled. Service type is an 8-bit field that is used for Quality of Service (QoS).



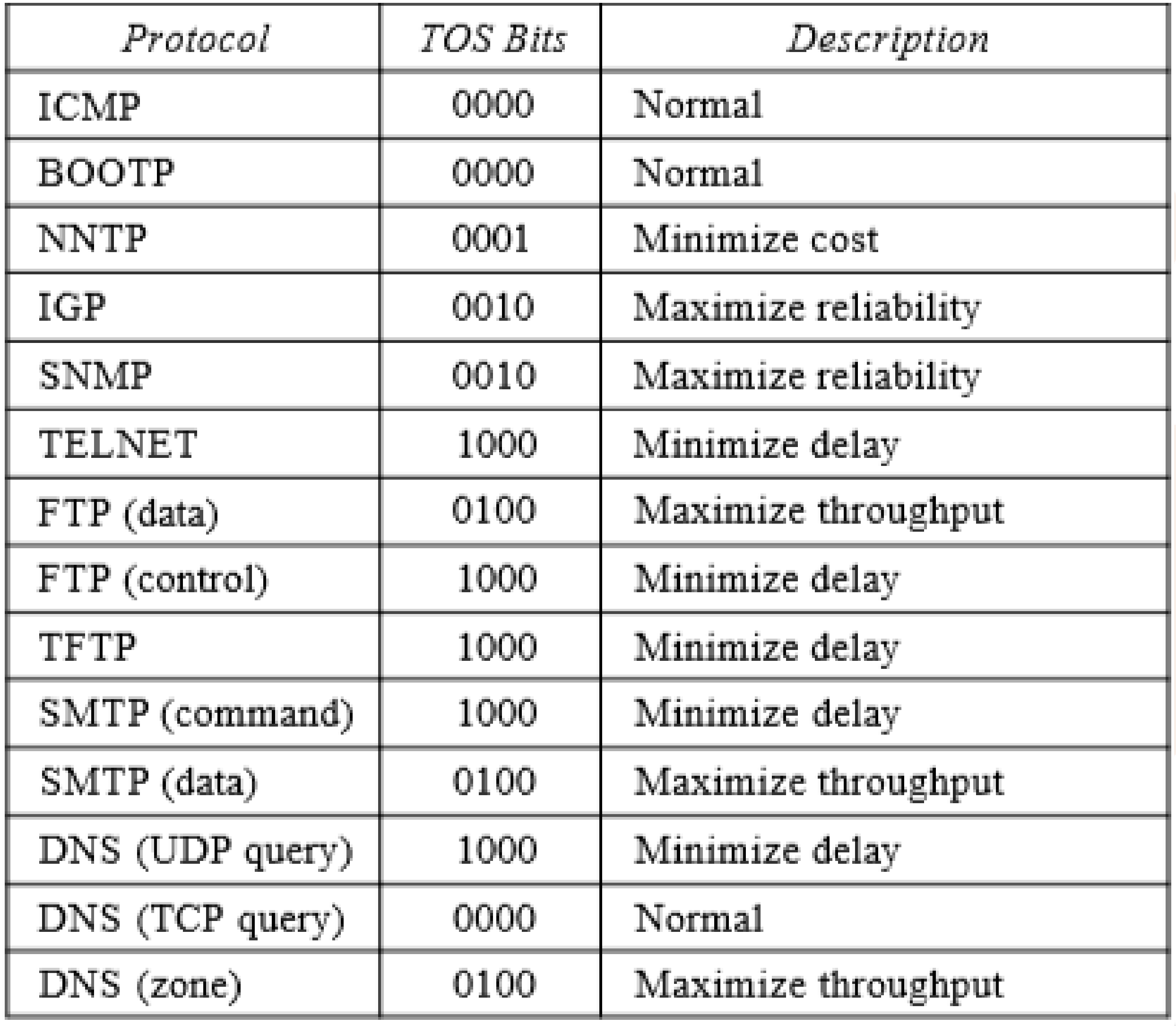
Service type





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

- TOS bits is a 4-bit subfield with each bit having a special meaning. Although a bit can be either 0 or 1, one and only one of the bits can have the value of 1 in each datagram



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

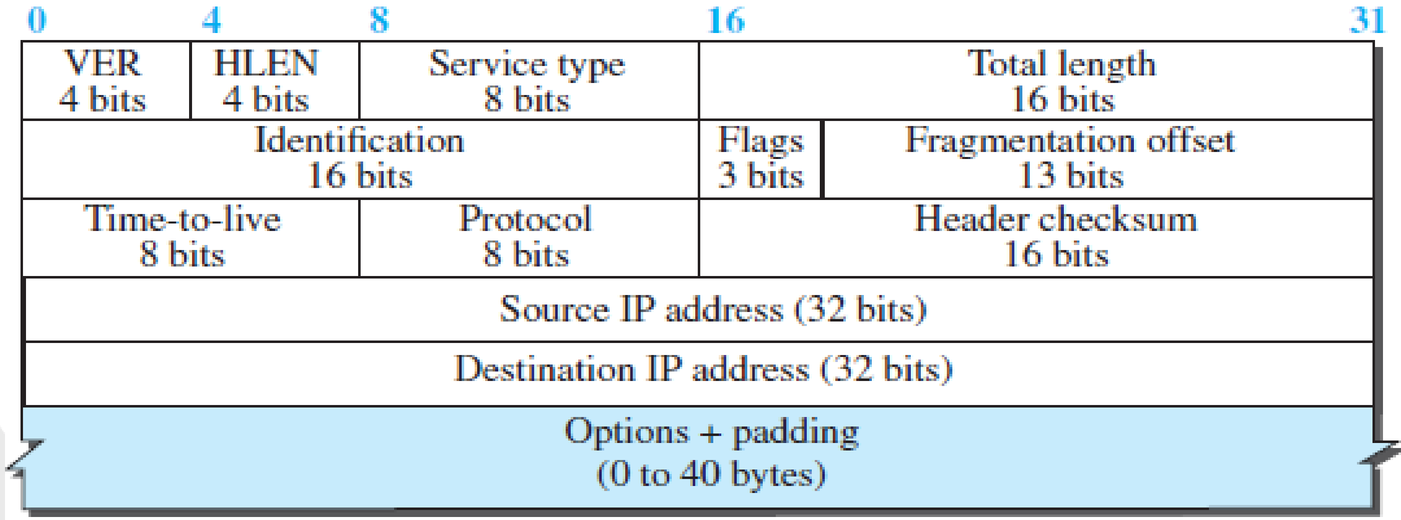
- ***Total Length.*** It defines the total length (header plus data) of the IP datagram in bytes. This field helps the receiving device to know when the packet has completely arrived.

- **Minimum total length of datagram** = 20 bytes (20 bytes header + 0 bytes data)

- **Maximum total length of datagram** = Maximum value of 16-bit word = 65535 bytes

- To find the length of the data coming from the upper layer, subtract the header length from the total length.

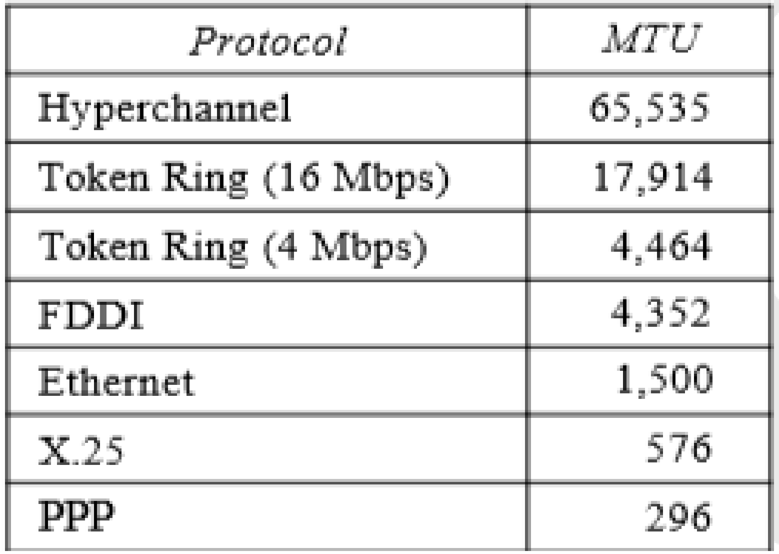
- ***Length of data = total length − (HLEN) × 4***



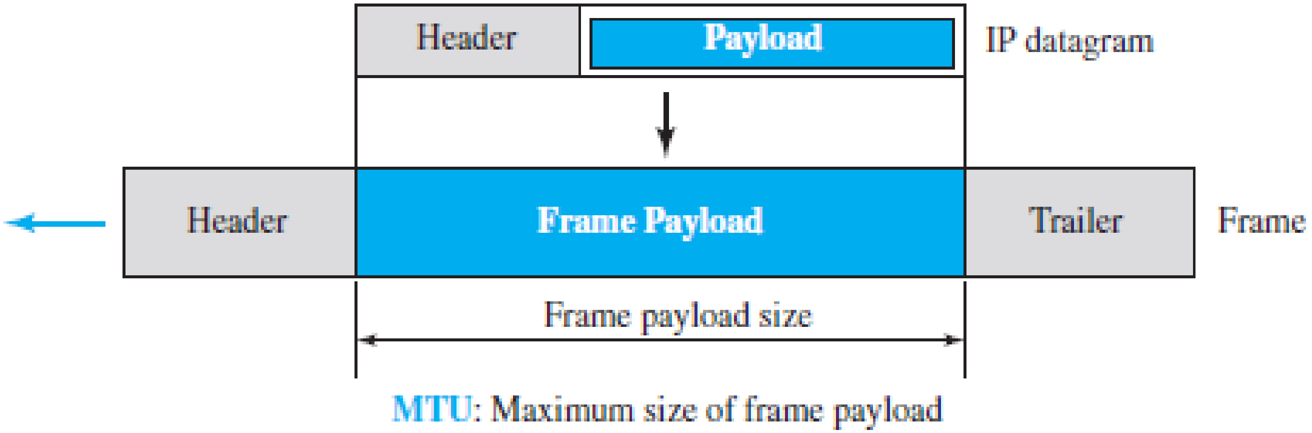
0	4	8	16	31
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

Maximum Transfer Unit (MTU)

- Each link-layer protocol has its own frame format.
- One of the features of each format is the maximum size of the payload that can be encapsulated.
- In other words, when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size.



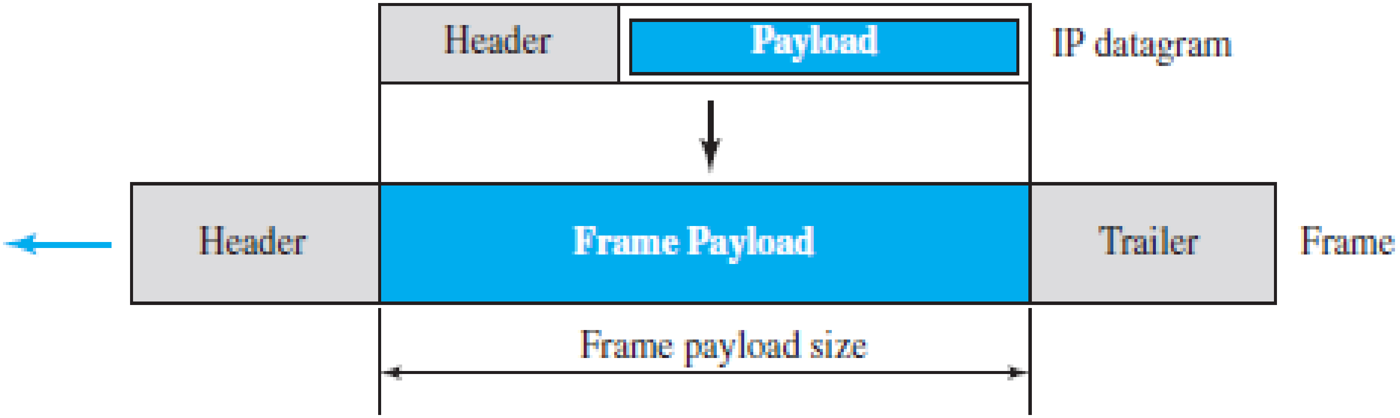
Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296



- ***The value of the MTU differs from one physical network protocol to another.*** For example, the value for a LAN is normally 1500 bytes, but for a WAN it can be larger or smaller.

- When a datagram is fragmented it means that the payload of the IP datagram is fragmented and each fragment has its own header with most of the fields repeated, but some have been changed such as flags, fragmentation offset, and total length and checksum is recalculated at each point.

- A fragmented datagram may itself be fragmented if it encounters a network with an even smaller MTU. Thus, ***datagram may be fragmented several times before it reaches the final destination.***



MTU: Maximum size of frame payload

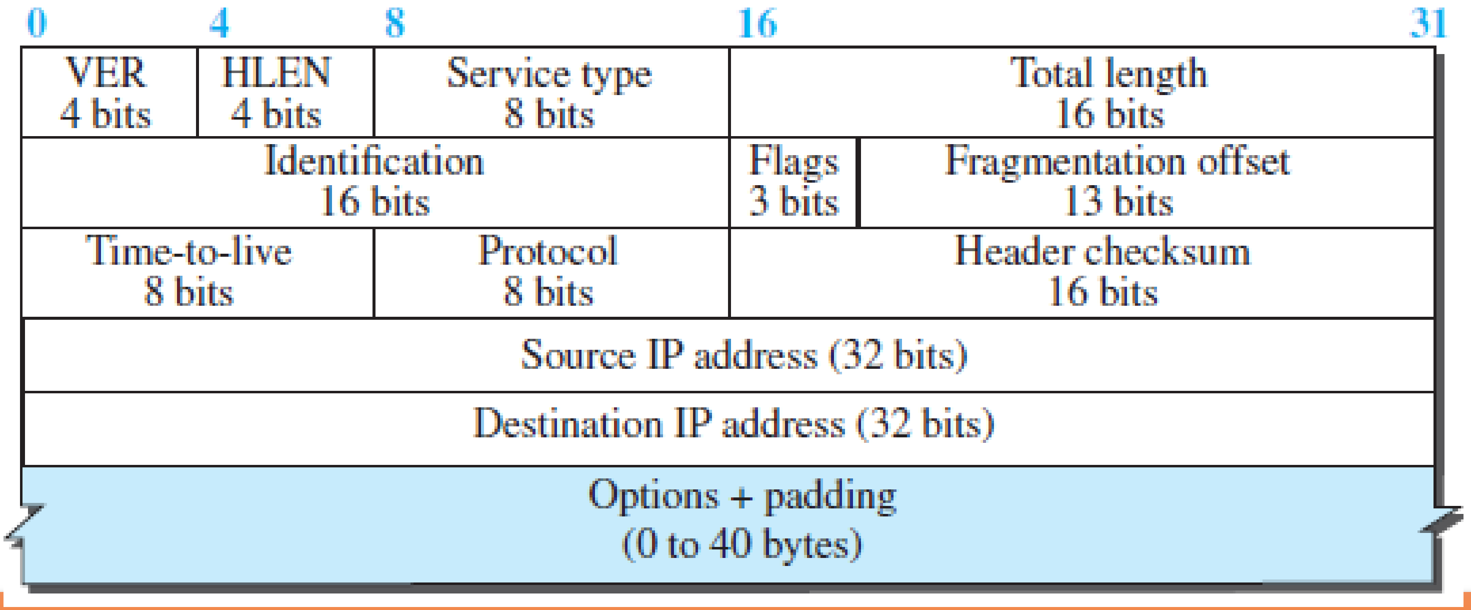
Break

- **Identification**: 16-bit *identification field* identifies a datagram originating from the source host. To guarantee uniqueness, IP protocol uses a counter to label the datagrams.

- The counter is initialized to a positive number. When the IP protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by one.

- When a datagram is fragmented, the value in the identification field is copied into all fragments so used for the identification of the fragments of an original IP datagram.

- The identification number helps the destination in reassembling the datagram.



0 4 8 16 31

VER 4 bits

HLEN 4 bits

Service type 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 (32 bits)

Destination IP address (32 bits)

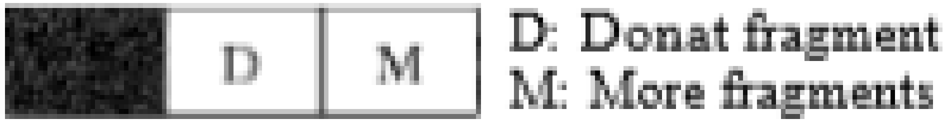
Options + padding (0 to 40 bytes)

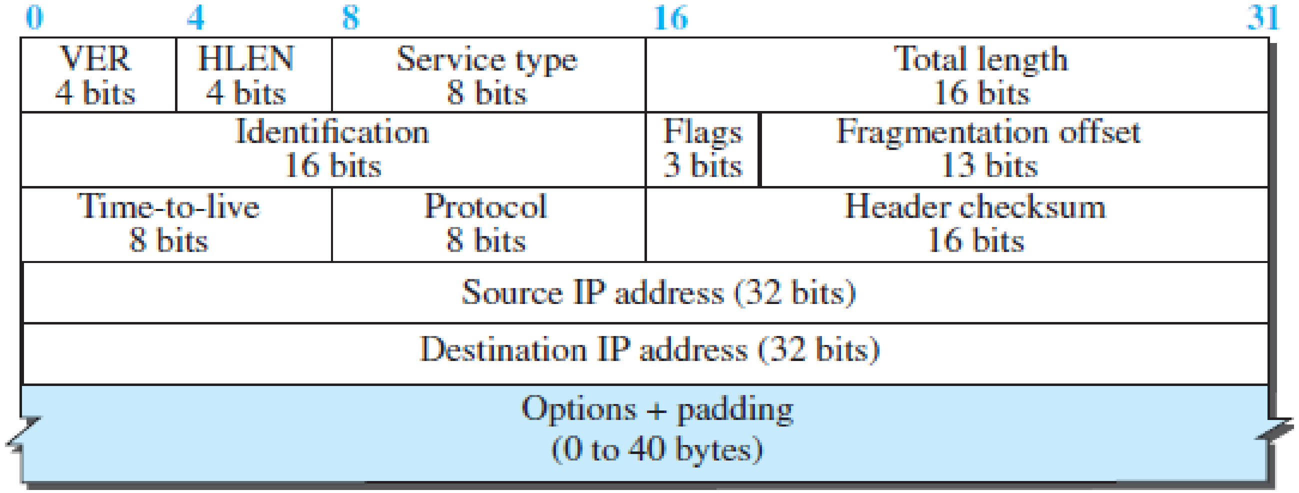
Break

Fragmentation

- Fragmentation is a process of dividing the datagram into fragments during its transmission.
- 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, because each fragment becomes an independent datagram.
- The fragmented datagram can travel through different routes.

- **Flag Field:** The 3-bit *flags field* defines three flags.
    - The leftmost bit is reserved (not used).
    - The second bit (D bit) is called the *do not fragment* bit.
        - If its value is 1, the machine must not fragment the datagram.
        - If its value is 0, the datagram can be fragmented if necessary.
    - The third bit (M bit) is called the *more fragment bit*.
        - If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one.
        - If its value is 0, it means this is the last or only fragment.





VER 4 bits | HLEN 4 bits | Service type 8 bits | Total length 16 bits

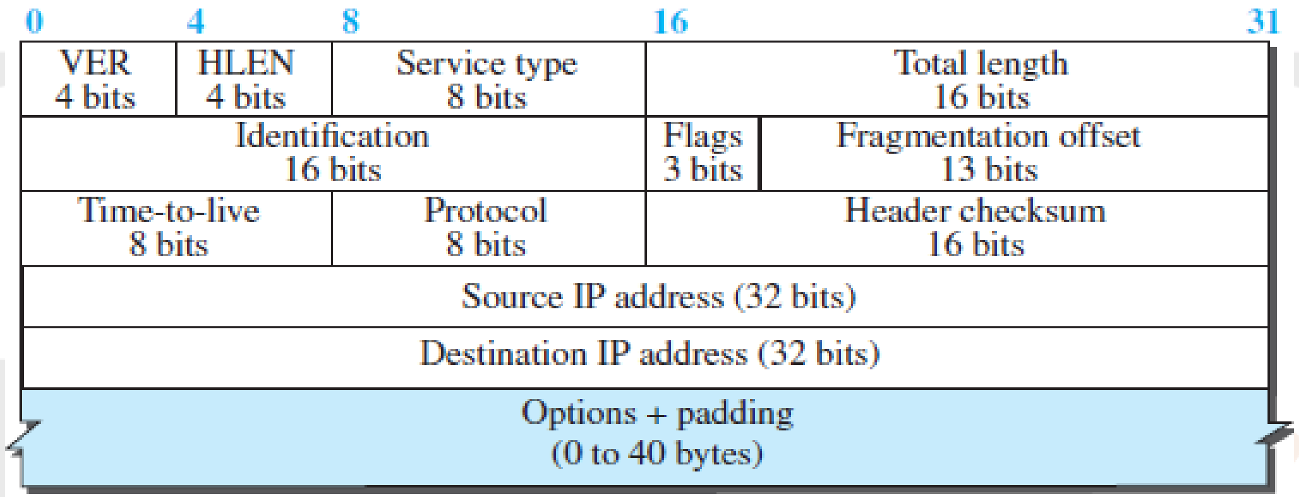
Identification 16 bits | Flags 3 bits | Fragmentation offset 13 bits

Time-to-live 8 bits | Protocol 8 bits | Header checksum 16 bits

Source IP address (32 bits)

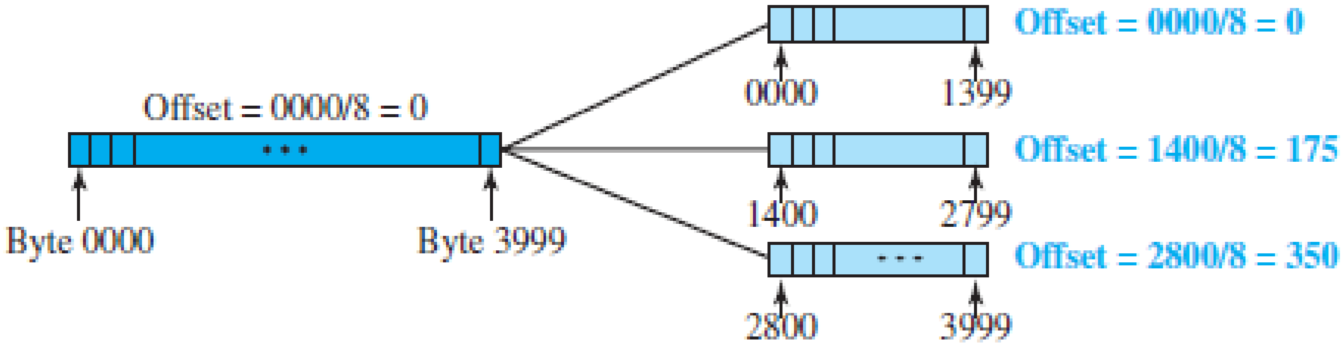
Destination IP address (32 bits)

Options + padding (0 to 40 bytes)



<table>
<tr><td>0</td><td>4</td><td>8</td><td>16</td><td>31</td></tr>
<tr><td>VER
4 bits</td><td>HLEN
4 bits</td><td>Service type
8 bits</td><td colspan="2">Total length
16 bits</td></tr>
<tr><td colspan="3">Identification
16 bits</td><td>Flags
3 bits</td><td>Fragmentation offset
13 bits</td></tr>
<tr><td colspan="2">Time-to-live
8 bits</td><td>Protocol
8 bits</td><td colspan="2">Header checksum
16 bits</td></tr>
<tr><td colspan="5">Source IP address (32 bits)</td></tr>
<tr><td colspan="5">Destination IP address (32 bits)</td></tr>
<tr><td colspan="5">Options + padding
(0 to 40 bytes)</td></tr>
</table>

- **Fragmentation Offset**: The 13-bit *fragmentation offset field* shows the relative position of this fragment with respect to the whole datagram.
- It is the offset of the data in the original datagram measured in units of 8 bytes.



- The bytes in the original datagram are numbered 0 to 3999.
- The first fragment carries bytes 0 to 1399. The offset value => 0/8 = 0.
- The second fragment carries bytes 1400 to 2799; the offset value => 1400/8 = 175.
- The third fragment carries bytes 2800 to 3999. The offset value => 2800/8 = 350.

Example: Consider host A is present in network X having MTU = 520 bytes. There is another host B present in network Y having MTU = 200 bytes. Now, host A wants to send a message to host B.

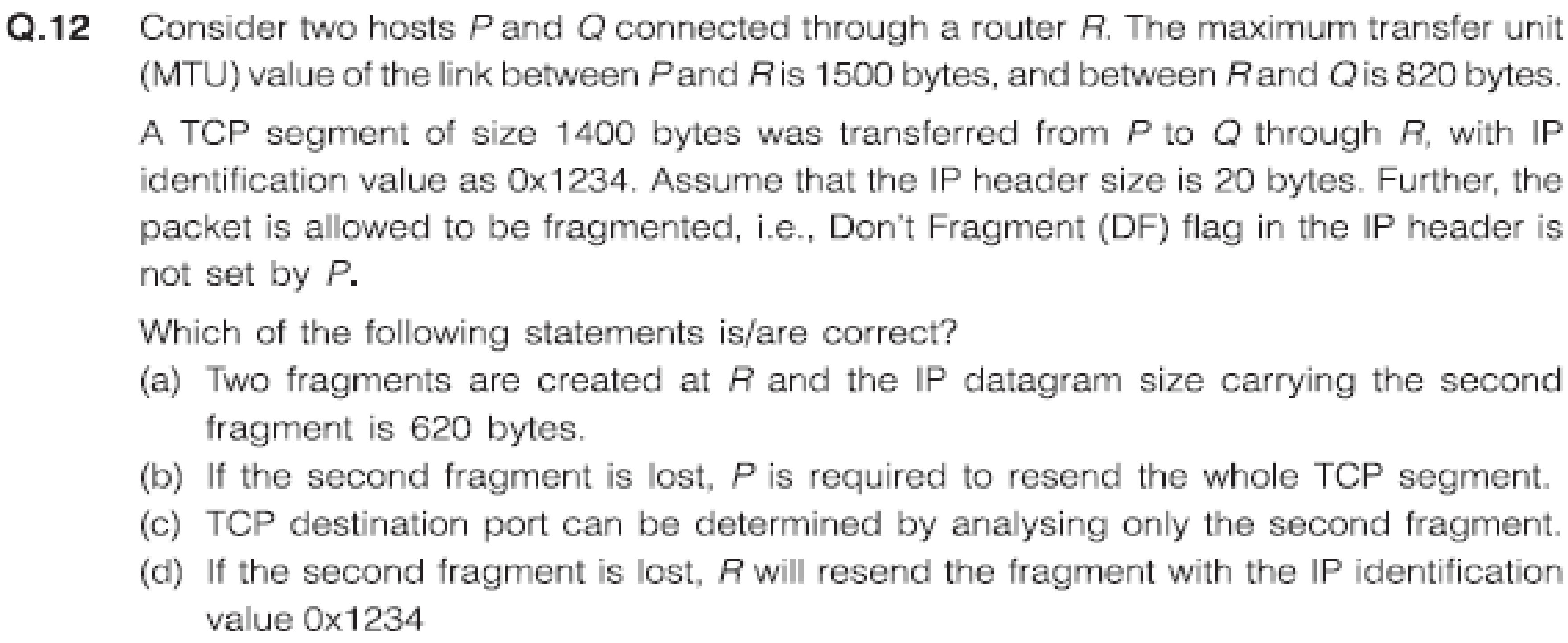
Example: A packet has arrived with an M bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

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?

Example: A packet has arrived in which the offset value is 100. What is the number of the first byte? Do we know the number of the last byte?

Example: A packet has arrived in which the offset value is 100, the value of HLEN is 5, and the value of the total length field is 100. What are the numbers of the first byte and the last byte?

(Gate-2021) (1 Marks)



Q.12 Consider two hosts *P* and *Q* connected through a router *R*. The maximum transfer unit (MTU) value of the link between *P* and *R* is 1500 bytes, and between *R* and *Q* is 820 bytes.

A TCP segment of size 1400 bytes was transferred from *P* to *Q* through *R*, with IP identification value as 0x1234. Assume that the IP header size is 20 bytes. Further, the packet is allowed to be fragmented, i.e., Don't Fragment (DF) flag in the IP header is not set by *P*.

Which of the following statements is/are correct?

(a) Two fragments are created at *R* and the IP datagram size carrying the second fragment is 620 bytes.

(b) If the second fragment is lost, *P* is required to resend the whole TCP segment.

(c) TCP destination port can be determined by analysing only the second fragment.

(d) If the second fragment is lost, *R* will resend the fragment with the IP identification value 0x1234

Q Consider an IP packet with a length of 4,500 bytes that includes a 20-byte IPv4 header and a 40-byte TCP header. The packet is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0. The fragmentation offset value stored in the third fragment is ___________. **(Gate-2018) (2 Marks)**

Q An IP datagram of size 1000 bytes arrives at a router. The router has to forward this packet on a link whose MTU (maximum transmission unit) is 100 bytes. Assume that the size of the IP header is 20 bytes. The number of fragments that the IP datagram will be divided into for transmission is __________. **(Gate-2016) (2 Marks)**

Q Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How may total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment? **(Gate-2015) (2 Marks)**

(A) 6 and 925

(B) 6 and 7400

(C) 7 and 1110

(D) 7 and 8880

Q An IP router with a Maximum Transmission Unit (MTU) of 1500 bytes has received an IP packet of size 4404 bytes with an IP header of length 20 bytes. The values of the relevant fields in the header of the third IP fragment generated by the router for this packet are **(Gate-2014) (2 Marks)**

(A) MF bit: 0, Datagram Length: 1444; Offset: 370

(B) MF bit: 1, Datagram Length: 1424; Offset: 185

(C) MF bit: 1, Datagram Length: 1500; Offset: 37

(D) MF bit: 0, Datagram Length: 1424; Offset: 2960

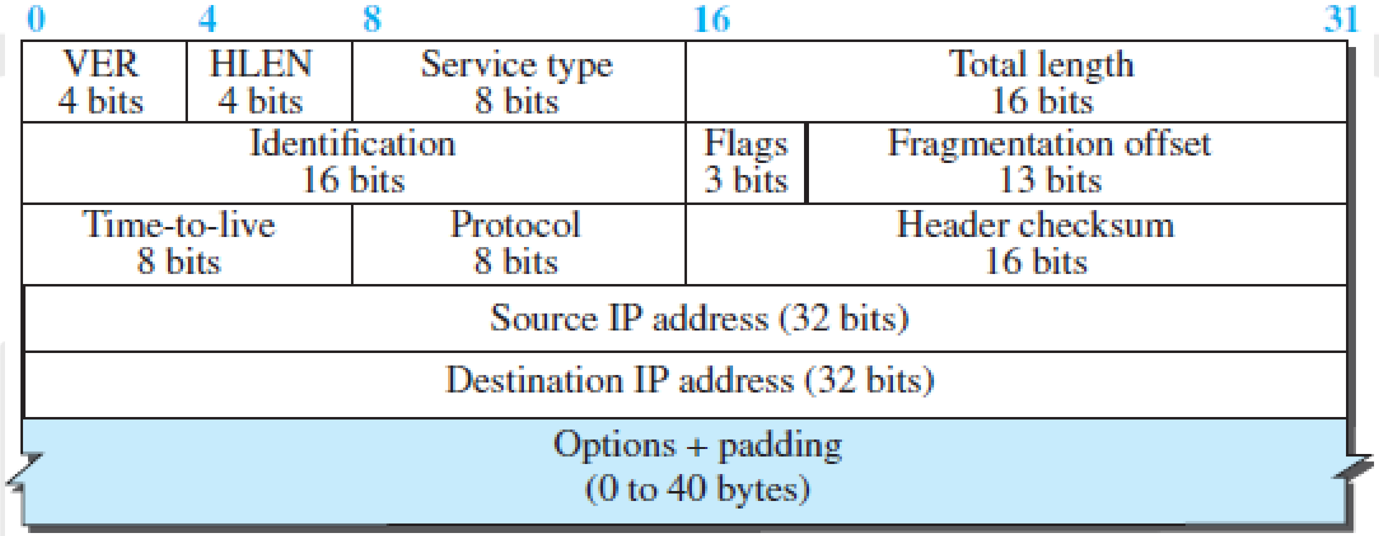
Q In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are **(Gate-2013) (2 Marks)**

(A) Last fragment, 2400 and 2789

(B) First fragment, 2400 and 2759

(C) Last fragment, 2400 and 2759

(D) Middle fragment, 300 and 689



0 4 8 16 31

VER 4 bits | HLEN 4 bits | Service type 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 (32 bits)

Destination IP address (32 bits)

Options + padding (0 to 40 bytes)

- **Time-to-live.** The time-to-live (TTL) field is used to control the maximum number of hops (routers) visited by the datagram.
- This value is approximately two times the maximum number of routers between any two hosts.
- Each router that processes the datagram decrements this number by one.
- If this value, after being decremented, is zero, the router discards the datagram.
- This field is needed because routing tables in the Internet can become corrupted. A datagram may travel between two or more routers for a long time without ever getting delivered to the destination host. This field limits the lifetime of a datagram.
- Another use of this field is to intentionally limit the journey of the packet. For example, if the source wants to confine the packet to the local network, it can store 1 in this field. When the packet arrives at the first router, this value is decremented to 0, and the datagram is discarded.

Q One of the header fields in an IP datagram is the Time to Live (TTL) field. Which of the following statements best explains the need for this field? **(Gate-2010) (1 Marks)**

(A) It can be used to prioritize packets

(B) It can be used to reduce delays

(C) It can be used to optimize throughput

(D) It can be used to prevent packet looping

Q For which one of the following reasons does Internet Protocol (IP) use the time-to-live (TTL) field in the IP datagram header **(Gate-2006) (1 Marks)**

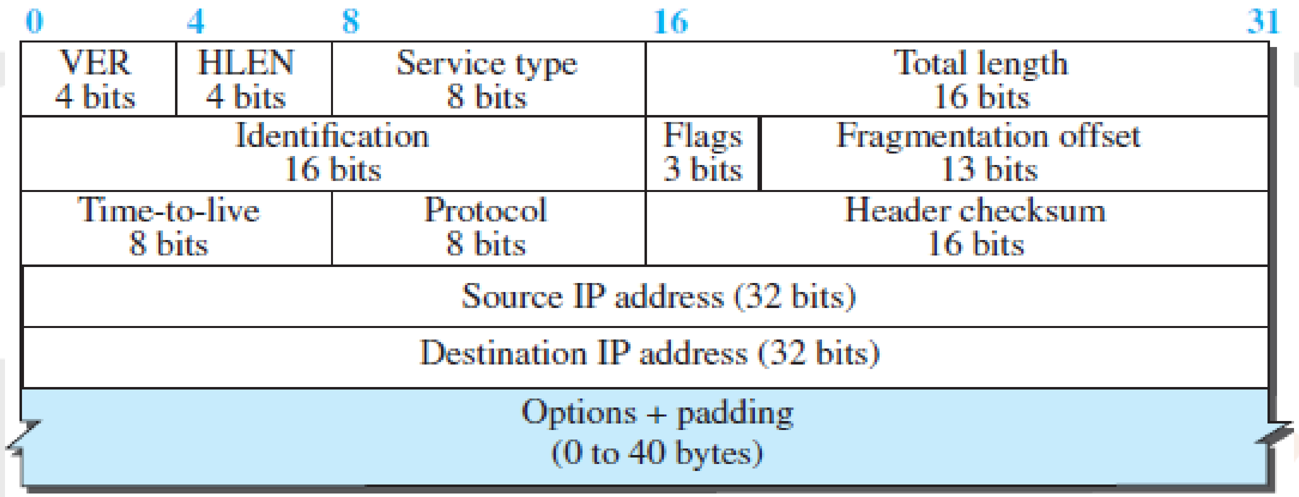
(A) Ensure packets reach destination within that time

(B) Discard packets that reach later than that time

(C) Prevent packets from looping indefinitely

(D) Limit the time for which a packet gets queued in intermediate routers.

Break


0 4 8 16 31

VER 4 bits | HLEN 4 bits | Service type 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

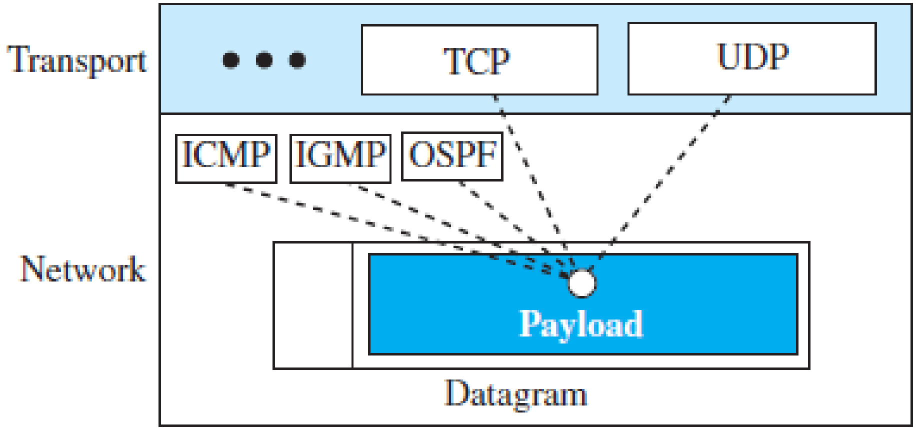
Source IP address (32 bits)

Destination IP address (32 bits)

Options + padding (0 to 40 bytes)

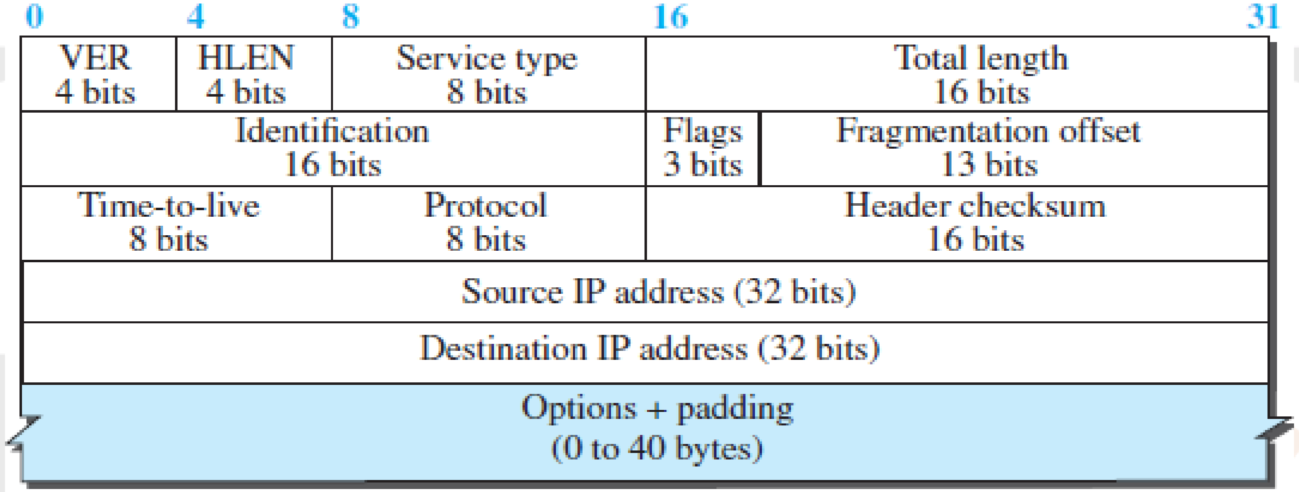
- **Protocol**. In TCP/IP, the data section of a packet, called the payload, carries the whole packet from another protocol. A datagram, for example, can carry a packet belonging to any transport-layer protocol such as UDP or TCP.

- When the datagram arrives at the destination, the value of this field helps to define to which protocol the payload should be delivered.



Some protocol values

ICMP	01
IGMP	02
TCP	06
UDP	17
OSPF	89



VER 4 bits	HLEN 4 bits	Service type 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 (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

- **Header checksum.** IP adds a header checksum field to check the header, but not the payload.
  - IP is not a reliable protocol; it does not check whether the payload carried by a datagram is corrupted during the transmission.
  - The datagram header, is added by IP, and its error-checking is the responsibility of IP.
  - Since the value of some fields, such as TTL, may change from router to router, the checksum needs to be recalculated at each router.
  - First, all higher-level protocols that encapsulate data in the IPv4 datagram have a checksum field that covers the whole packet. Therefore, the checksum for the IPv4 datagram does not have to check the encapsulated data.
  - Second, the header of the IPv4 packet changes with each visited router, but the data do not. So, the checksum includes only the part that has changed. If the data were included, each router must recalculate the checksum for the whole packet, which means an increase in processing time.

Q Host A (on TCP/IP v4 network A) sends an IP datagram D to host B (also on TCP/IP v4 network B). Assume that no error occurred during the transmission of D. When D reaches B, which of the following IP header field(s) may be different from that of the original datagram D? **(Gate-2014) (1 Marks)**

(i) TTL

(ii) Checksum

(iii) Fragment Offset

(A) (i) only

(B) (i) and (ii) only

(C) (ii) and (iii) only

(D) (i), (ii) and (iii)

Q Which of the following statements is TRUE? **(Gate-2006) (1 Marks)**

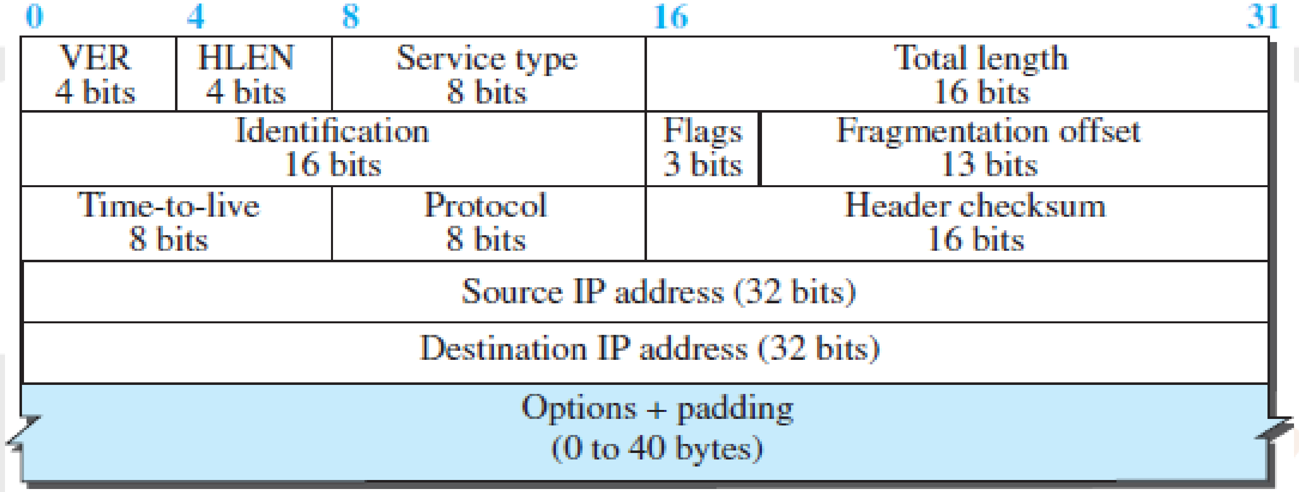
(A) Both Ethernet frame and IP packet include checksum fields

(B) Ethernet frame includes a checksum field and IP packet includes a CRC field

(C) Ethernet frame includes a CRC field and IP packet includes a checksum field

(D) Both Ethernet frame and IP packet include CRC fields

Break



0 4 8 16 31

VER 4 bits | HLEN 4 bits | Service type 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 (32 bits)

Destination IP address (32 bits)

Options + padding (0 to 40 bytes)

- **Source and Destination Addresses.** These 32-bit source and destination address fields define the IP address of the source and destination respectively.

- **Options.** A datagram header can have up to 40 bytes of options. Options can be used for network testing and debugging.
  - They are not a required part of the IP header

- **Payload.** Payload, or data, is the main reason for creating a datagram. Payload is the packet coming from other protocols that use the service of IP.
  - Payload is the content of the package; the header is only the information written on the package.

Example: An IPv4 packet has arrived with the first 8 bits as $(01000010)_2$. The receiver discards the packet. Why?

Example: In an IPv4 packet, the value of HLEN is 5, and the value of the total length field is $(0028)_{16}$. How many bytes of data are being carried by this packet?

Example: An IPv4 packet has arrived with the first few hexadecimal digits as shown.

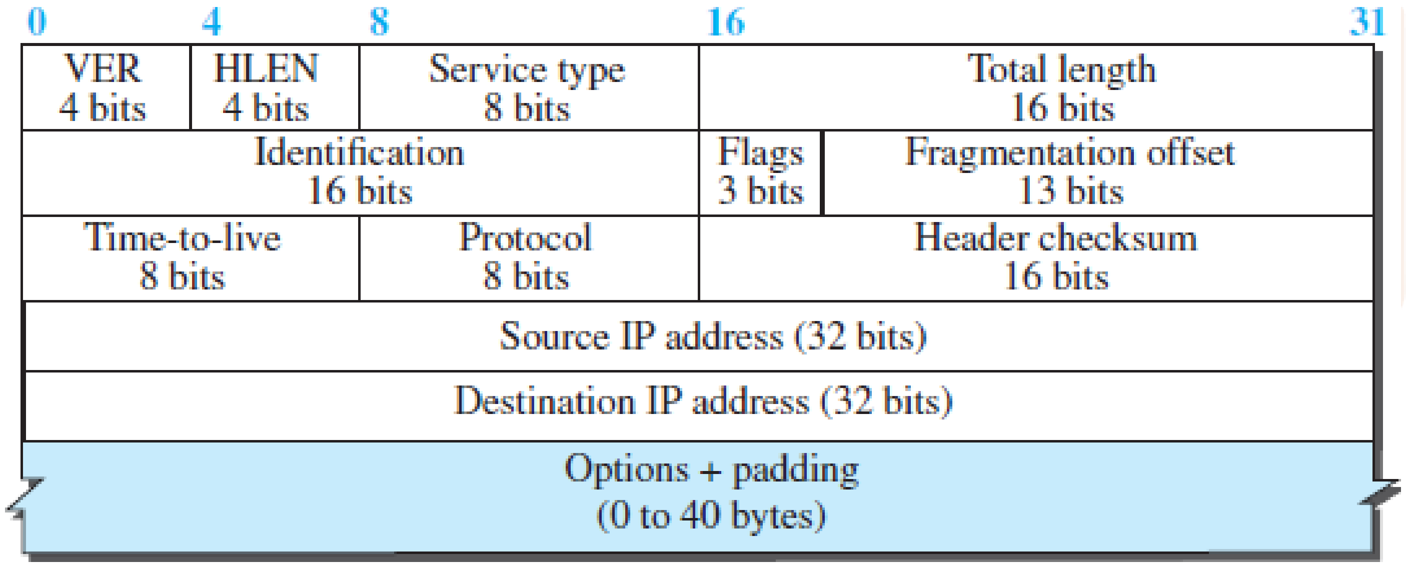
$(45000028000100000102\ldots)_{16}$

How many hops can this packet travel before being dropped?

Break

Variable part

- The header of the IPv4 datagram is made of two parts: a fixed part and a variable part.
- The fixed part is 20 bytes long and was discussed in the previous section.
- The variable part comprises the options that can be a maximum of 40 bytes. Options, as the name implies, are not required for a datagram.
- They can be used for network testing and debugging. Although options are not a required part of the IPv4 header, option processing is required of the IPv4 software.
- This means that all implementations must be able to handle options if they are present in the header.



0 4 8 16 31

VER 4 bits | HLEN 4 bits | Service type 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 (32 bits)

Destination IP address (32 bits)

Options + padding (0 to 40 bytes)

- **End of Option**
  - An end-of-option option is a 1-byte option used for padding at the end of the option field. It, however, can only be used as the last option.

- **Record Route**
  - A record route option is used to record the Internet routers that handle the datagram. It can list up to nine router addresses. It can be used for debugging and management purposes.

- **Strict Source Route**
  - A strict source route option is used by the source to predetermine a route for the datagram as it travels through the Internet. Dictation of a route by the source can be useful for several purposes.
  - The sender can choose a route with a specific type of service, such as minimum delay or maximum throughput.
  - Alternatively, it may choose a route that is safer or more reliable for the sender's purpose. For example, a sender can choose a route so that its datagram does not travel through a competitor's network.
  - If a datagram specifies a strict source route, all the routers defined in the option must be visited by the datagram. A router must not be visited if its IPv4 address is not listed in the datagram. If the datagram visits a router that is not on the list, the datagram is discarded and an error message is issued.
  - If the datagram arrives at the destination and some of the entries were not visited, it will also be discarded and an error message issued.

- **Loose Source Route**
  - A loose source route option is similar to the strict source route, but it is less rigid. Each router in the list must be visited, but the datagram can visit other routers as well.

- **Timestamp**
  - A timestamp option is used to record the time of datagram processing by a router. The time is expressed in milliseconds from midnight, Universal time or Greenwich mean time.
  - Knowing the time, a datagram is processed can help users and managers track the behaviour of the routers in the Internet. We can estimate the time it takes for a datagram to go from one router to another. We say estimate because, although all routers may use Universal time, their local clocks may not be synchronized.

Q The maximum number of IPv4 router addresses that can be listed in the record route (RR) option field of an IPv4 header is __________ **(Gate-2017) (1 Marks)**

Q Which one of the following fields of an IP header is NOT modified by a typical IP router? **(Gate-2015) (1 Marks)**

(A) Checksum

(B) Source address

(C) Time to Live (TTL)

(D) Length

Q Which of the following assertions is FALSE about the Internet Protocol (IP)? **(Gate-2003) (1 Marks)**

(A) It is possible for a computer to have multiple IP addresses

(B) IP packets from the same source to the same destination can take different routes in the network

(C) IP ensures that a packet is discarded if it is unable to reach its destination within a given number of hops

(D) The packet source cannot set the route of an outgoing packets; the route is determined only by the routing tables in the routers on the way

Break

Additional protocols

- IP packets, however, need to be encapsulated in a frame, which needs physical addresses (node-to-node). We will see that a protocol called ARP, the Address Resolution Protocol.

- We sometimes need reverse mapping-mapping a physical address to a logical address. For example, when booting a diskless network or leasing an IP address to a host, RARP is used.

- Lack of flow and error control in the Internet Protocol has resulted in another protocol, ICMP, that provides alerts. It reports congestion and some types of errors in the network or destination host

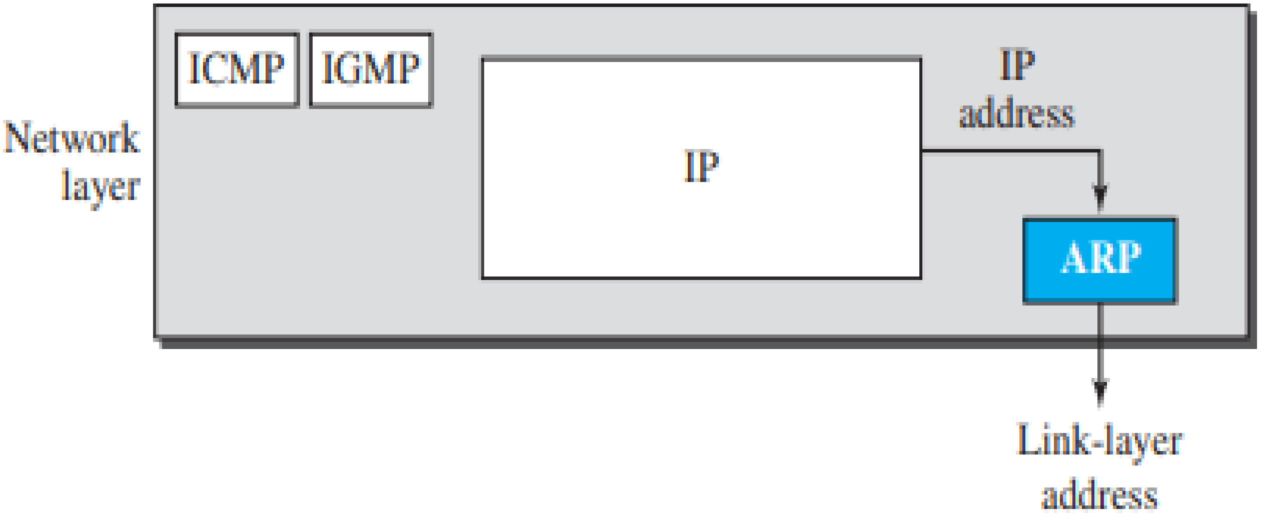
- IP was originally designed for unicast delivery, one source to one destination. As the Internet has evolved, the need for multicast delivery, one source to many destinations, has increased tremendously. IGMP gives IP a multicast capability.

Address Resolution Protocol (ARP)

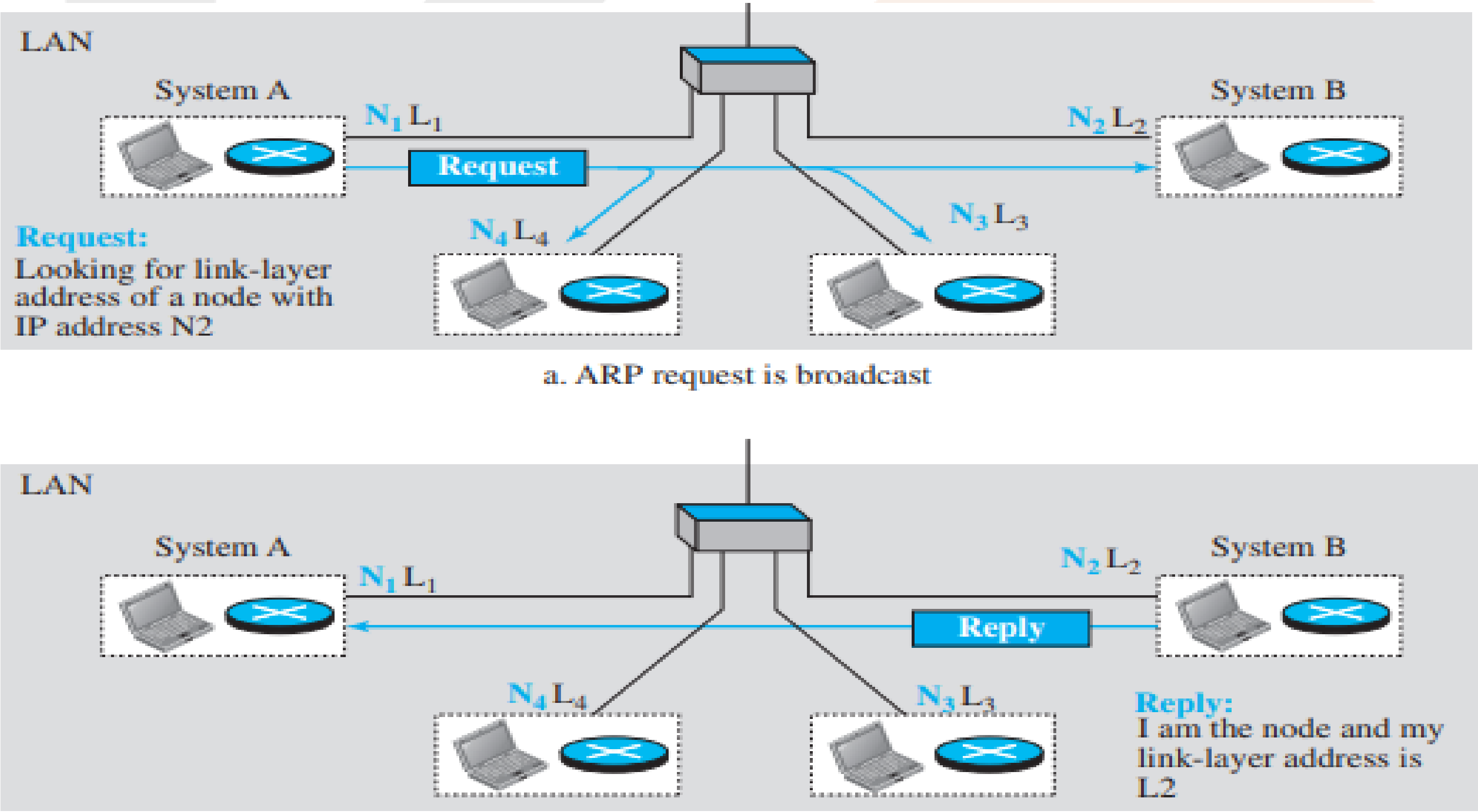
- The IP address of the next node alone is not helpful in moving a frame through a link; we need the link-layer address of the next node.

- ARP maps an IP address to a logical-link address. ARP accepts an IP address from the IP protocol, maps the address to the corresponding link-layer address, and passes it to the data-link layer.

- The ARP protocol is one of the auxiliary protocols defined in the **network layer.**



1. Anytime a host or a router needs to find the link-layer address of another host or router in its network, it sends an ARP request packet.
2. The packet includes the ***link-layer and IP addresses of the sender and the IP address of the receiver.***
3. Because the sender does not know the link-layer address of the receiver, the query is broadcast over the link.
4. Every host or router on the network receives and processes the ARP request packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.
5. The response packet contains the recipient's IP and link-layer addresses. ***The packet is unicast directly to the node that sent the request packet.***



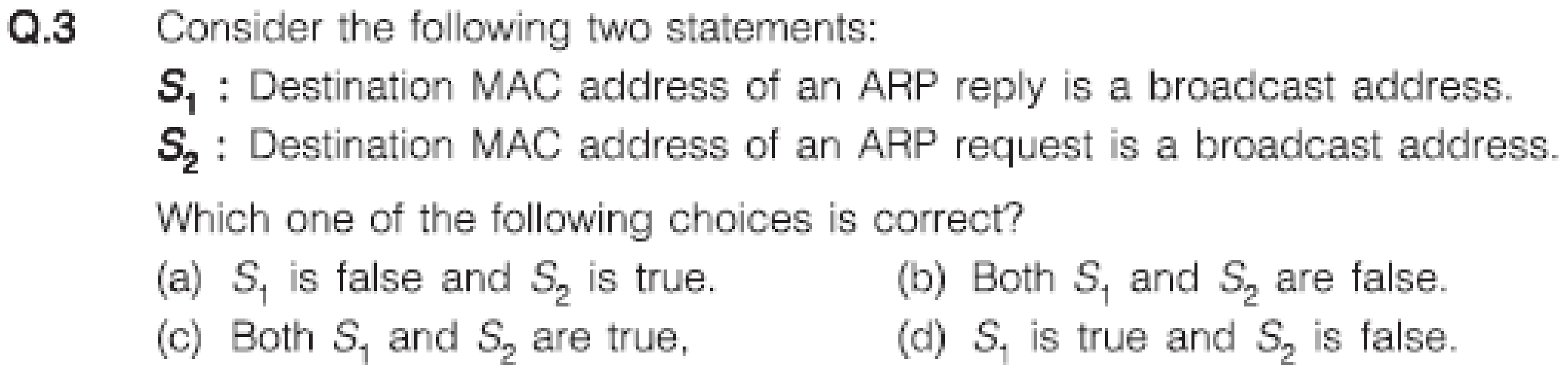
Request: Looking for link-layer address of a node with IP address N2

a. ARP request is broadcast

Reply: I am the node and my link-layer address is L2

b. ARP reply is unicast

(Gate-2021) (1 Marks)



Q.3 Consider the following two statements:

S_1 : Destination MAC address of an ARP reply is a broadcast address.

S_2 : Destination MAC address of an ARP request is a broadcast address.

Which one of the following choices is correct?

(a) S_1 is false and S_2 is true.

(b) Both S_1 and S_2 are false.

(c) Both S_1 and S_2 are true,

(d) S_1 is true and S_2 is false.

Break

RARP

- Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address.

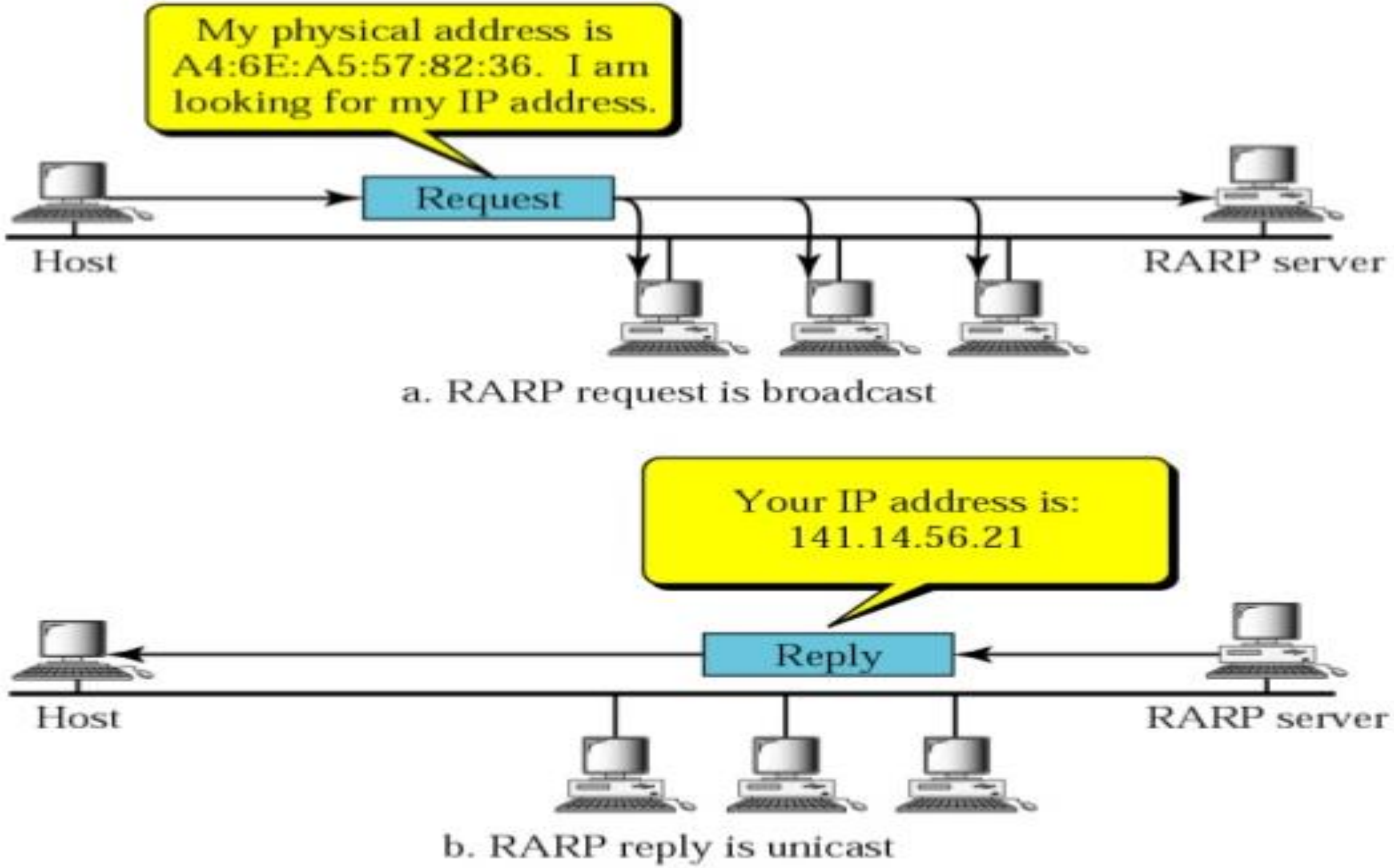
- Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine. To create an IP datagram, a host or a router needs to know its own IP address or addresses.

- The IP address of a machine is usually read from its configuration file stored on a disk file. However, a diskless machine is usually booted from ROM, which has minimum booting information. The ROM is installed by the manufacturer. It cannot include the IP address because the IP addresses on a network are assigned by the network administrator.

- The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol.

- A RARP request is created and broadcast on the local network. Another machine on the local network that knows all the IP addresses will respond with a RARP reply.

- The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program.


My physical address is A4:6E:A5:57:82:36. I am looking for my IP address.
Request
Host
RARP server
a. RARP request is broadcast
Your IP address is: 141.14.56.21
Reply
Host
RARP server
b. RARP reply is unicast

Break

ICMP

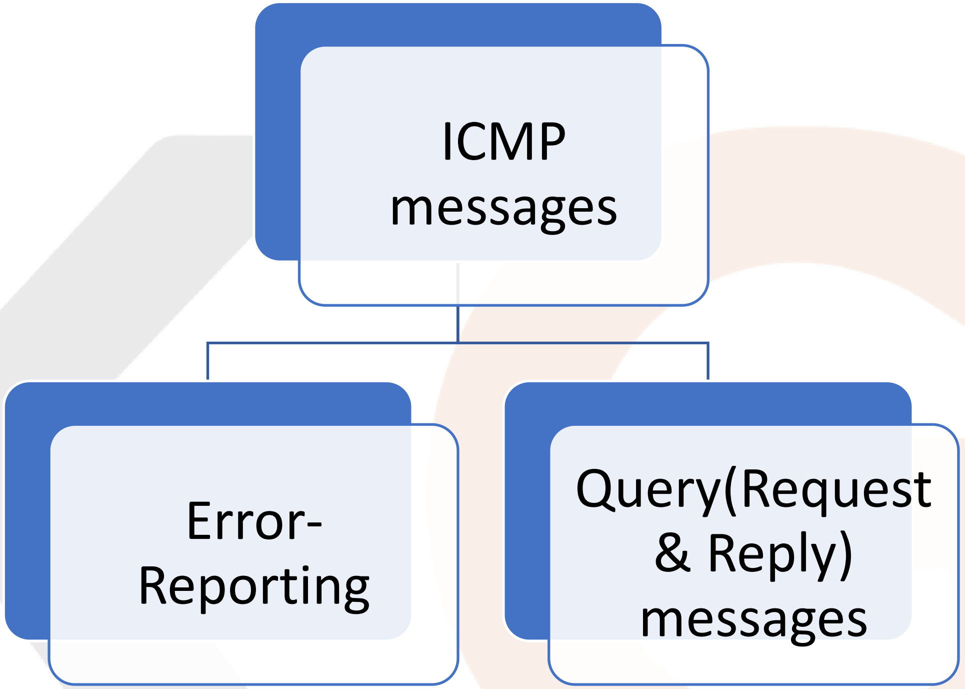
- IP has two deficiencies: lack of error control and lack of assistance mechanisms. The IP protocol has no error-reporting or error-correcting mechanism.
  - What happens if something goes wrong?
  - What happens if a router must discard a datagram because it cannot find a router to the final destination,
  - or because the time-to-live field has a zero value?
  - What happens if the final destination host must discard all fragments of a datagram because it has not received all fragments within a predetermined time limit?

- These are examples of situations where an error has occurred and the IP protocol has no built-in mechanism to notify the original host. The IP protocol also lacks a mechanism for host and management queries. A host sometimes needs to determine if a router or another host is alive. And sometimes a network administrator needs information from another host or router.

- The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol.

Types of Messages

- ICMP messages are divided into two broad categories: Error-Reporting messages and query(request & reply) messages.



The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.

The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.

Break

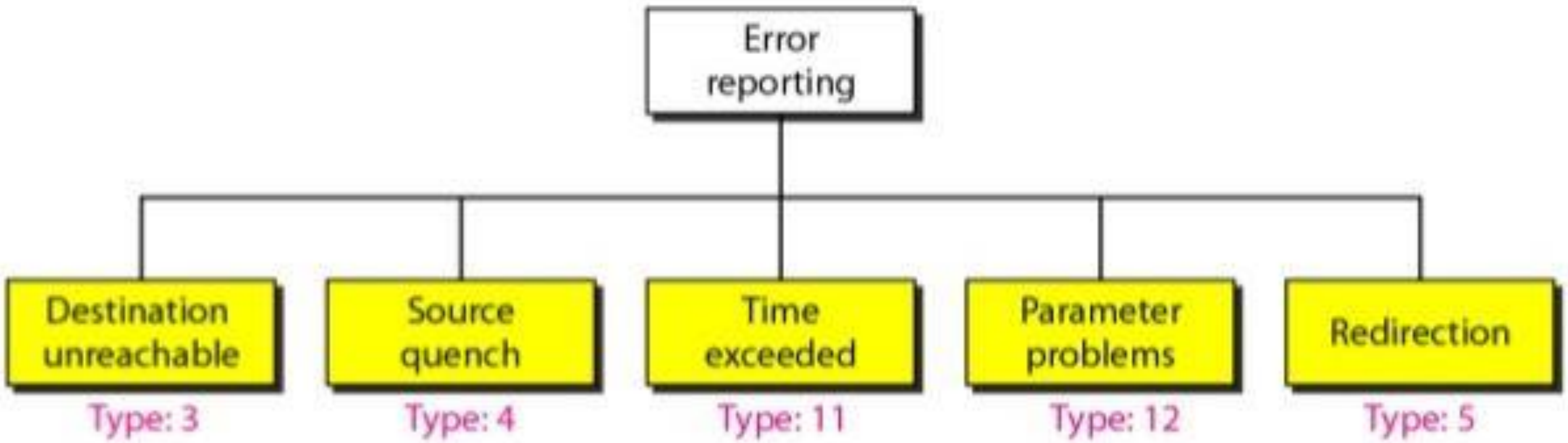
Error Reporting

- One of the main responsibilities of ICMP is to report errors.

- ICMP was designed, in part, to compensate for this shortcoming of IP. However, ICMP does not correct errors-it simply reports them.

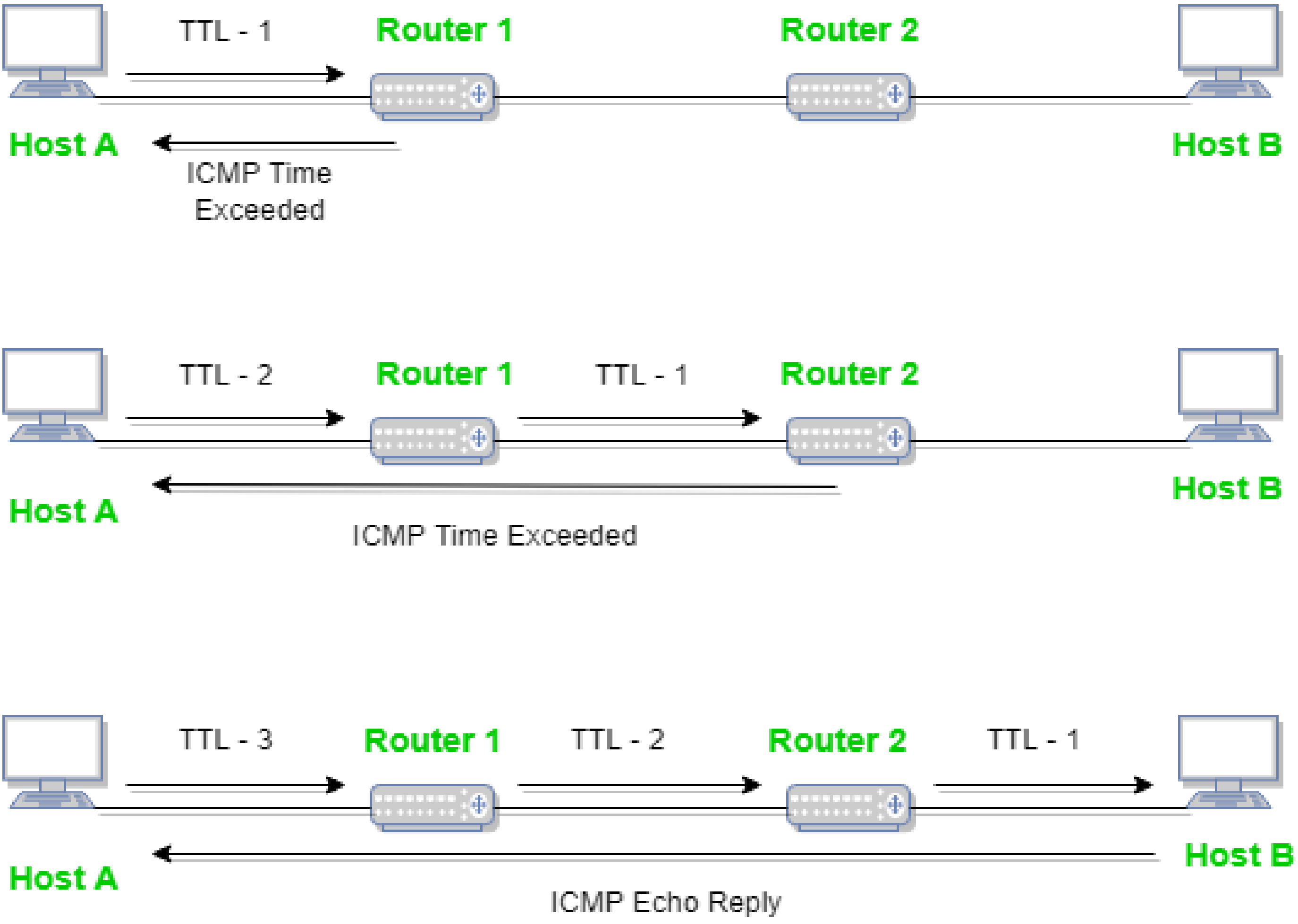
- Error correction is left to the higher-level protocols. Error messages are always sent to the original source because the only information available in the datagram about the route is the source and destination IP addresses.

- ICMP uses the source IP address to send the error message to the source (originator) of the datagram.



Time exceeded message

- ICMP will take source IP from discarded packet and informs to the source, of discarded datagram due to time to live field reaches to zero, by sending time exceeded message.

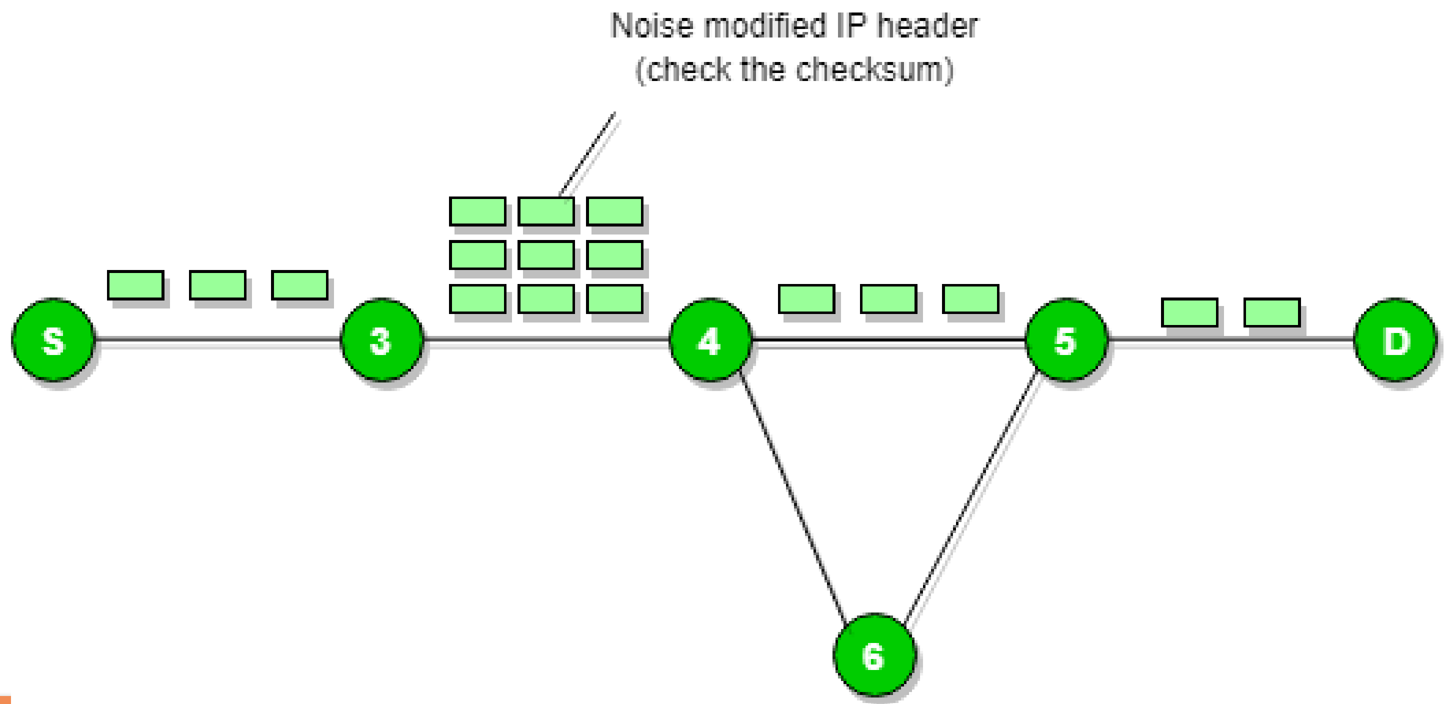


Parameter problem

- Whenever packets come to the router then calculated header checksum should be equal to received header checksum then only packet is accepted by the router.

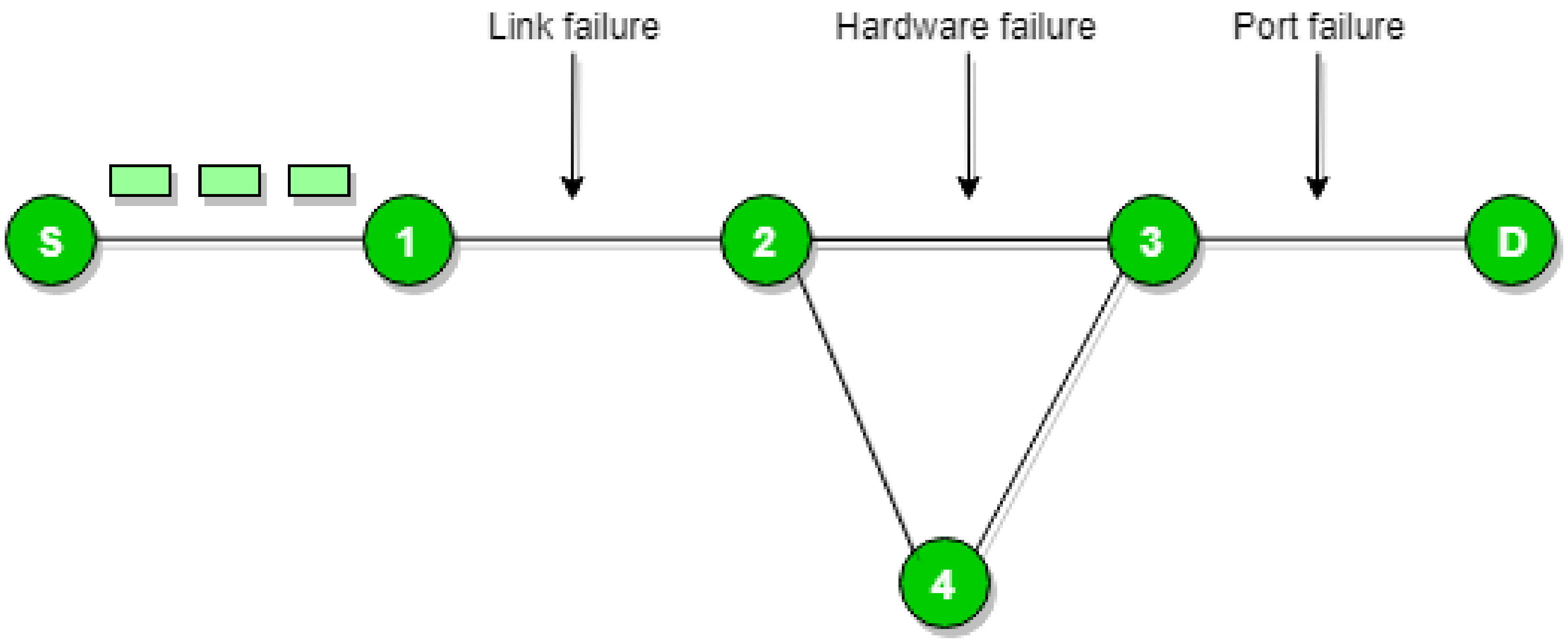
- If there is mismatch packet will be dropped by the router.

- ICMP will take the source IP from the discarded packet and informs to source by sending parameter problem message.



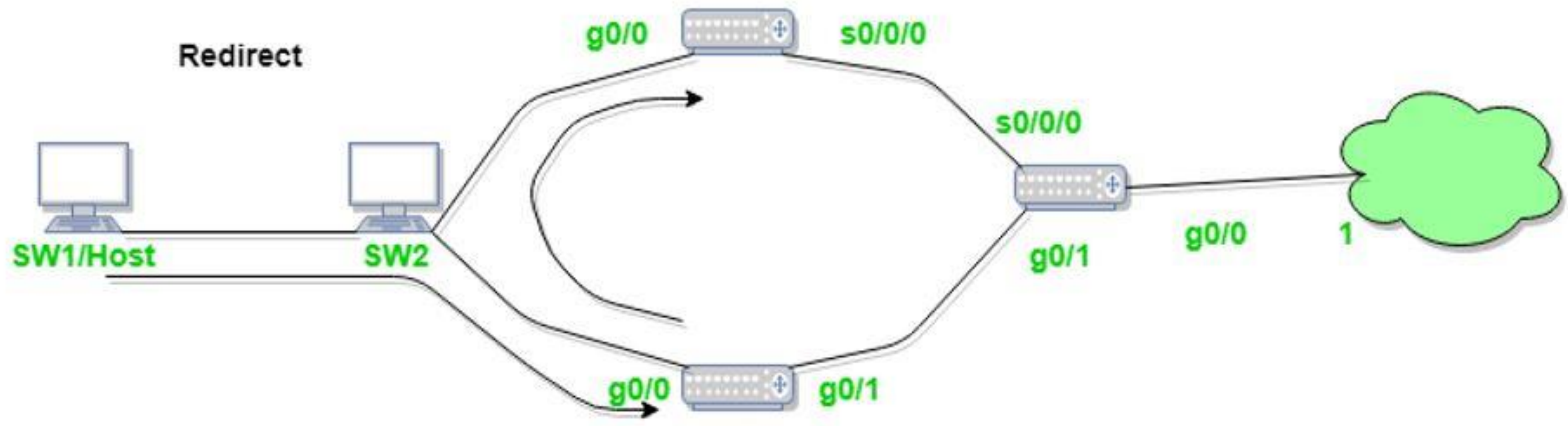
Destination Un-reachable

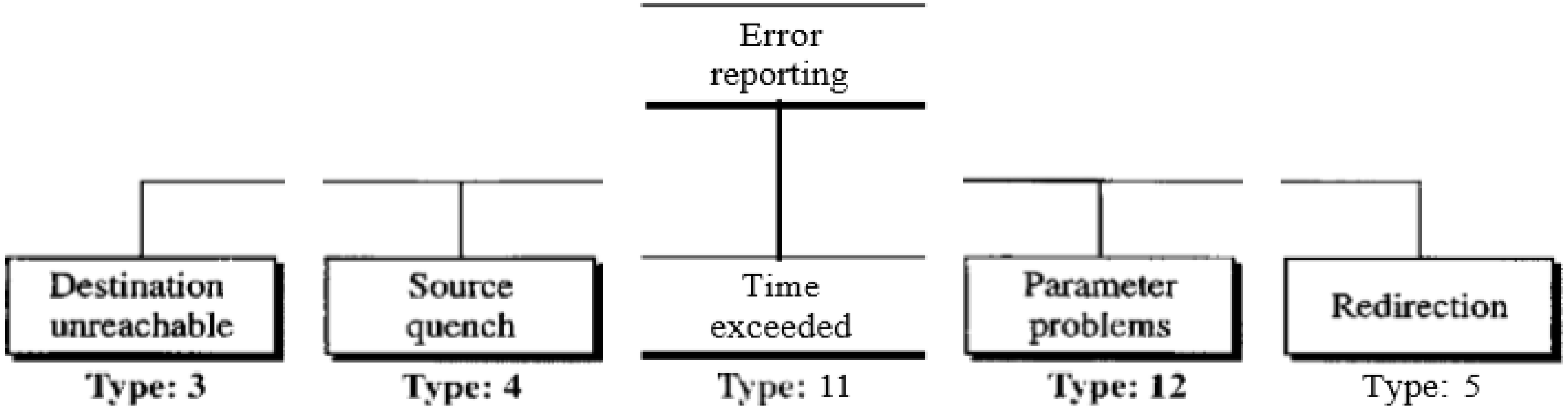
- Destination unreachable is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.
- There is no necessary condition that only router give the ICMP error message some time destination host send ICMP error message when any type of failure (link failure, hardware failure, port failure etc.) happen in the network.



Redirection message

- Redirect requests data packets be sent on an alternate route. The message informs to a host to update its routing information (to send packets on an alternate route).





Error reporting

Destination unreachable
Type: 3

Source quench
Type: 4

Time exceeded
Type: 11

Parameter problems
Type: 12

Redirection
Type: 5

The following are important points about ICMP error messages:

O No ICMP error message will be generated in response to a datagram carrying an ICMP error message.

D No ICMP error message will be generated for a fragmented datagram that is not the first fragment.

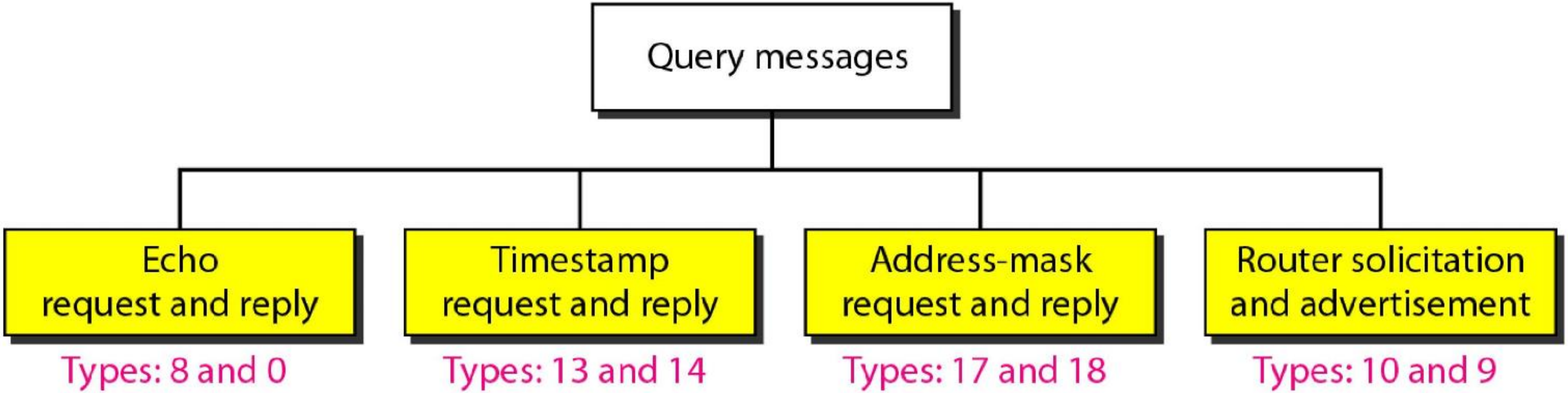
D No IeMP error message will be generated for a datagram having a multicast address.

D No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

Break

Query

- In addition to error reporting, ICMP can diagnose some network problems. This is accomplished through the query messages, a group of four different pairs of messages.
- In this type of ICMP message, a node sends a message that is answered in a specific format by the destination node. A query message is encapsulated in an IP packet, which in turn is encapsulated in a data link layer frame.



Echo Request and Reply

- The echo-request and echo-reply messages are designed for diagnostic purposes. Network managers and users utilize this pair of messages to identify network problems.

- The combination of echo-request and echo-reply messages determines whether two systems (hosts or routers) can communicate with each other.

- The echo-request and echo-reply messages can be used to determine if there is communication at the IP level. Because ICMP messages are encapsulated in IP datagrams, the receipt of an echo-reply message by the machine that sent the echo request is proof that the IP protocols in the sender and receiver are communicating with each other using the IP datagram.

- Also, it is proof that the intermediate routers are receiving, processing, and forwarding IP datagrams. Today, most systems provide a version of the ping command that can create a series (instead of just one) of echo-request and echo-reply messages, providing statistical information.

Router Solicitation and Advertisement

- As we discussed in the redirection message section, a host that wants to send data to a host on another network needs to know the address of routers connected to its own network.

- Also, the host must know if the routers are alive and functioning. The router-solicitation and router-advertisement messages can help in this situation.

- A host can broadcast (or multicast) a router-solicitation message. The router or routers that receive the solicitation message broadcast their routing information using the router-advertisement message.

- A router can also periodically send router-advertisement messages even if no host has solicited. Note that when a router sends out an advertisement, it announces not only its own presence but also the presence of all routers on the network of which it is aware.

Address-Mask Request and Reply

- A host may know its IP address, but it may not know the corresponding mask. For example, a host may know its IP address as 159.31.17.24, but it may not know that the corresponding mask is /24.

- To obtain its mask, a host sends an address-mask-request message to a router on the LAN. If the host knows the address of the router, it sends the request directly to the router. If it does not know, it broadcasts the message.

- The router receiving the address-mask-request message responds with an address-mask-reply message, providing the necessary mask for the host. This can be applied to its full IP address to get its subnet address.

Timestamp Request and Reply

- Two machines (hosts or routers) can use the timestamp request and timestamp reply messages to determine the round-trip time needed for an IP datagram to travel between them. It can also be used to synchronize the clocks in two machines.

Break

IGMP

- The IP protocol can be involved in two types of communication: unicasting and multicasting. Unicasting is the communication between one sender and one receiver. It is a one-to-one communication.

- However, some processes sometimes need to send the same message to a large number of receivers simultaneously. This is called multicasting, which is a one-to-many communication.

- Multicasting has many applications. For example, multiple stockbrokers can simultaneously be informed of changes in a stock price, or travel agents can be informed of a plane cancellation.

Note: For more details check out Wikipedia

Video-on-Demand

To acc

K HERE

Distance Learning