# Internet Protocol version 4

Unit-III

# Session Objectives



- Discuss the IPv4 protocol
- Discuss ICMPv4 protocol

# Session Outcomes



At the end of this session, participants will be able to

- Describing the IPv4 datagram, fragmentation
- elaborate ICMPv4 purpose, its debugging functionality and checksum
  format

# Agenda

# Presentation Outline

# Internet Protocol version 4 (IPv4)



- Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer.
- The Internet Control Message Protocol version 4 (ICMPv4) helps IPv4 to handle some errors that may occur in the network-layer delivery.
- The Internet Group Management Protocol (IGMP) is used to help IPv4 in multicasting.
- The Address Resolution Protocol (ARP) is used to glue the network and data-link layers in mapping network-layer addresses to link-layer addresses.

# Position of IP and other network-layer protocols in TCP/IP protocol suite



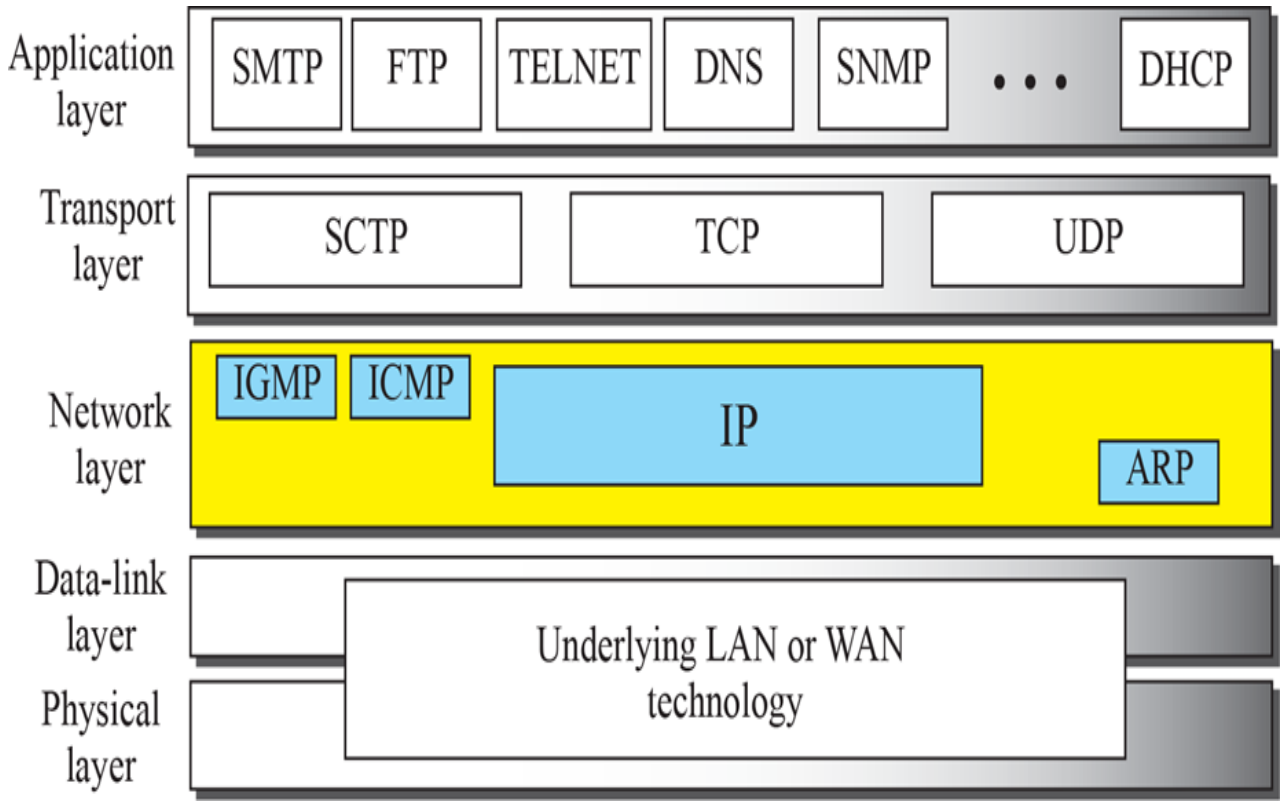
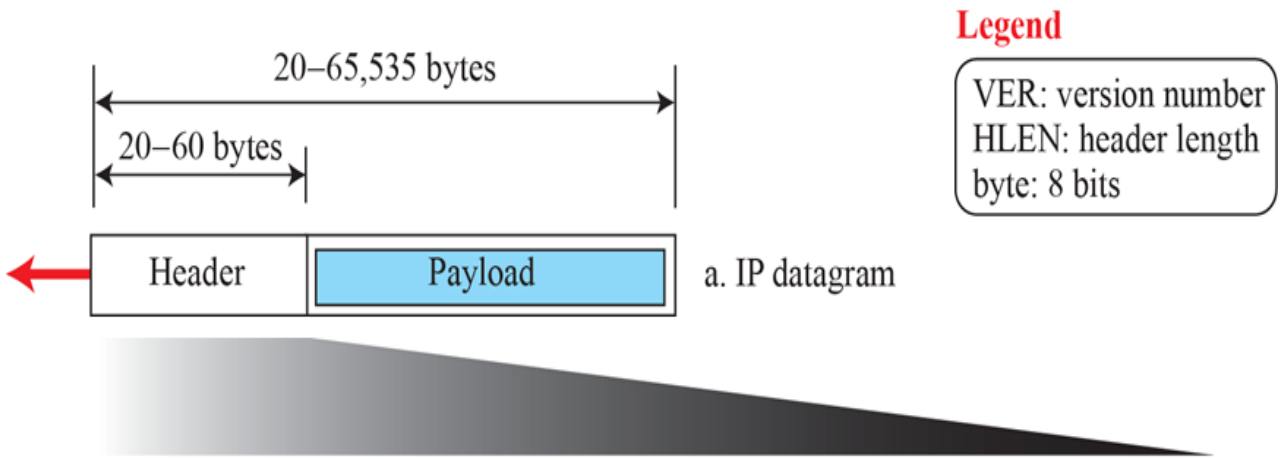


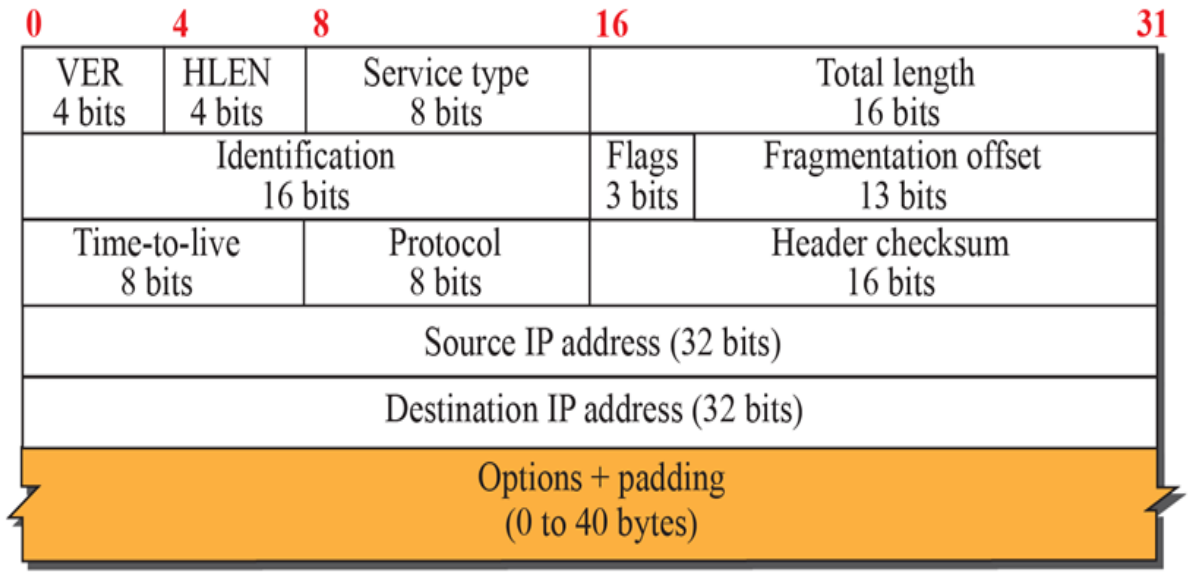

Figure: Forwarding process

# Presentation Outline

# IP datagram






b. Header format

# IPv4 Header fileds



- 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.
- When a device receives a datagram, it needs to know when the header stops and the data, which is encapsulated in the packet, starts.
- However, 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.

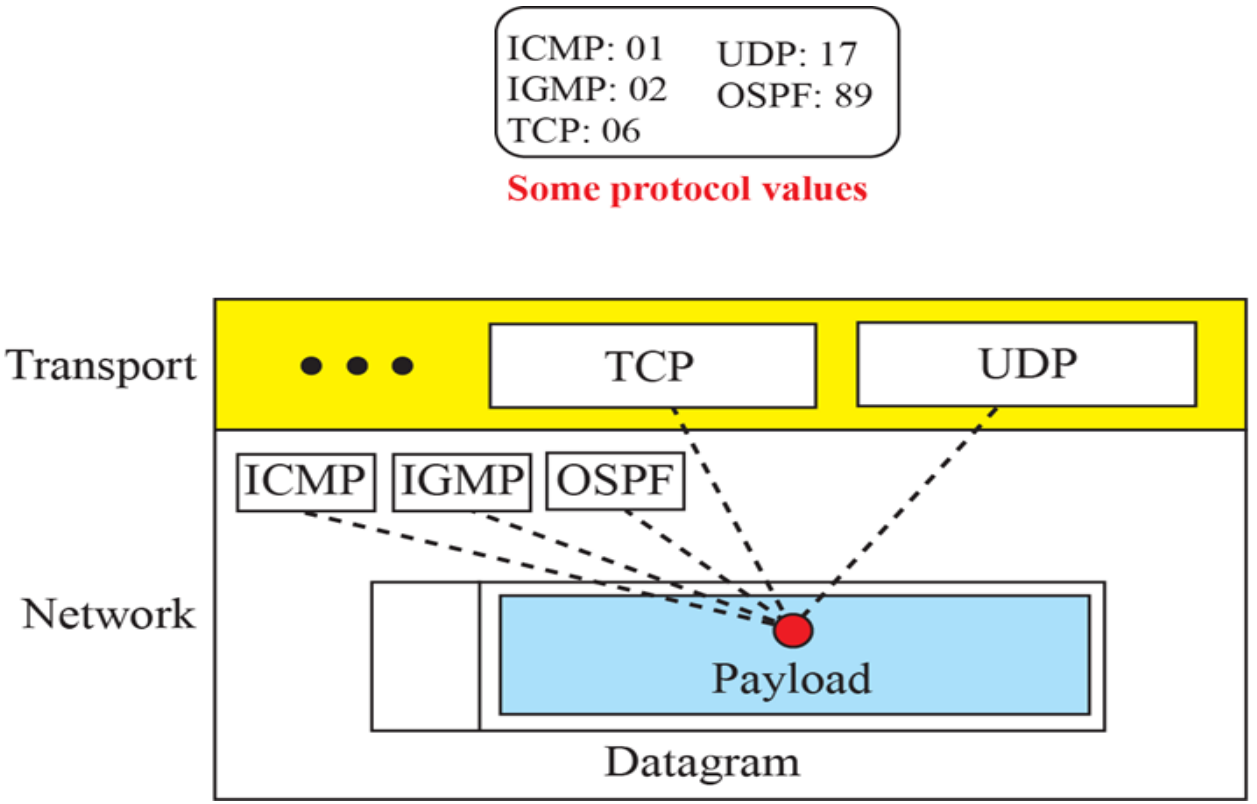
# IPv4 Header fileds



- **Total Length:** Length of data = total length - (HLEN) x 4
- The **time-to-live** (TTL) field is used to control the maximum number of hops (routers) visited by the datagram.
- When a source host sends the datagram, it stores a number in this field. 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.
- The Internet authority has given any protocol that uses the service of IP a unique 8-bit number which is inserted in the protocol field.

# Multiplexing and demultiplexing using the value of the protocol field





# IPv4 Header fileds



- Header checksum: If the protocol field is corrupted, the payload may be delivered to the wrong protocol.
- If the fields related to the fragmentation are corrupted, the datagram cannot be reassembled correctly at the destination, and so on.
- Hence IPv4 adds a header checksum field to check the header, but not the payload
- **Options:** Options can be used for network testing and debugging

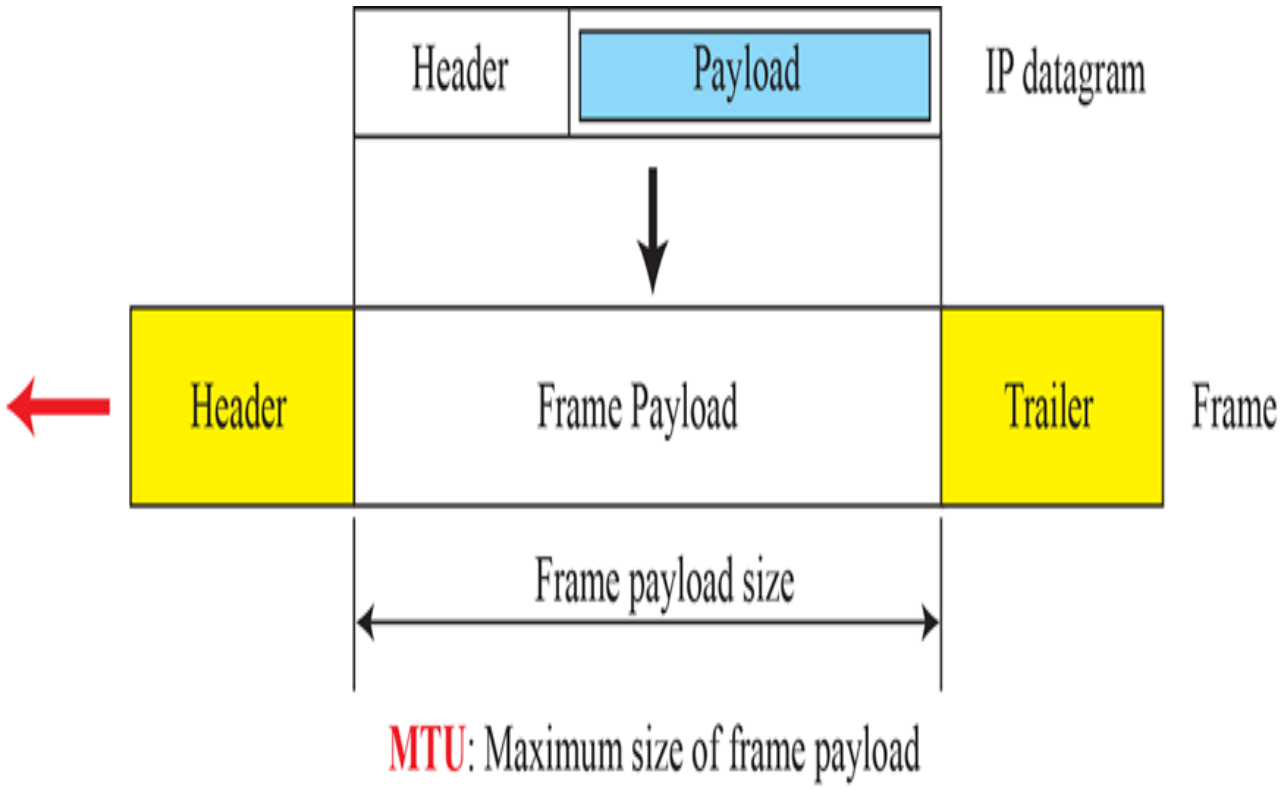
# Fragmentation



- Each router decapsulates the IP datagram from the frame it receives, processes it, and then encapsulates it in another frame
- **Maximum Transfer Unit (MTU):** when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size, which is defined by the restrictions imposed by the hardware and software used in the network
- The value of the MTU differs from one physical network protocol to another
- So divide the datagram to make it possible for it to pass through these networks.

# Maximum Transfer Unit






- When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but some have been changed
- Datagram may be fragmented several times before it reaches the final destination

# Fields Related to Fragmentation



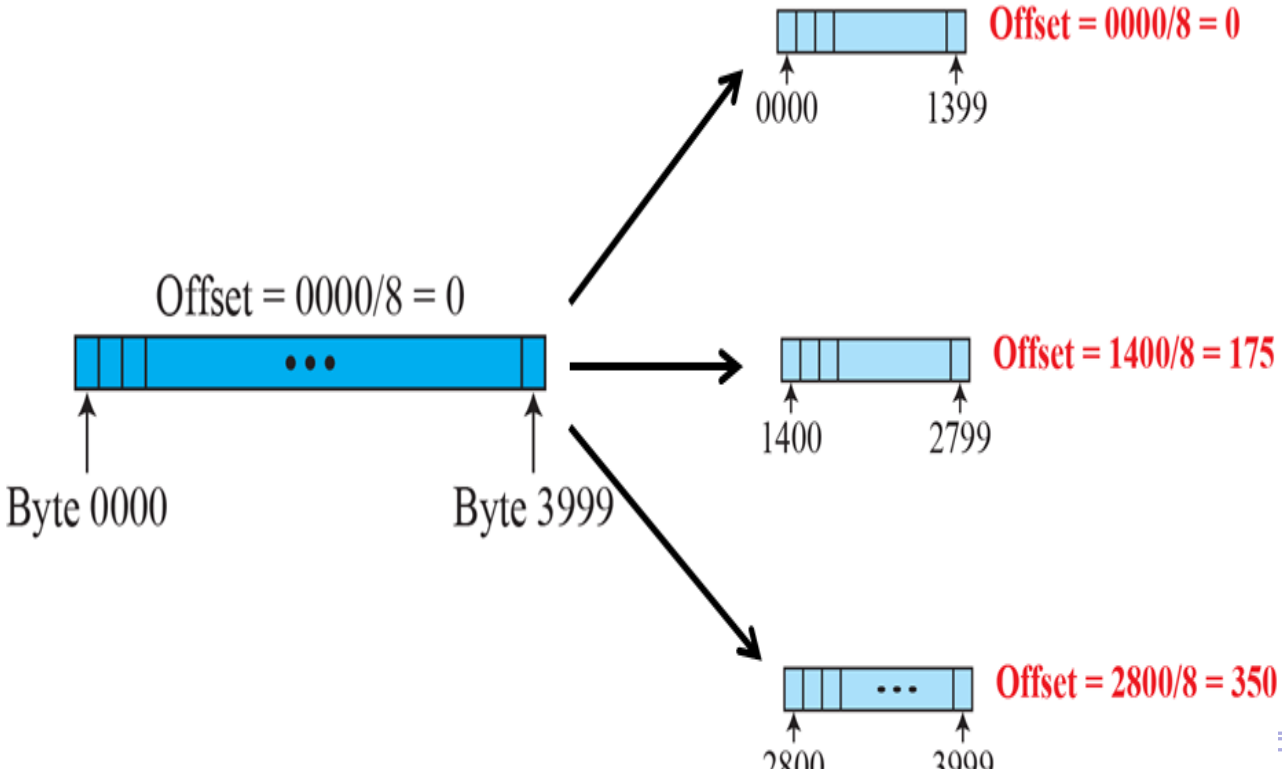
Identification, flags, and fragmentation offset

- **16-bit identification field:** All fragments have the same identification number, which is also the same as the original datagram. And hence all fragments having the same identification value should be assembled into one datagram.
- **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.
- 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**.

# Fragmentation

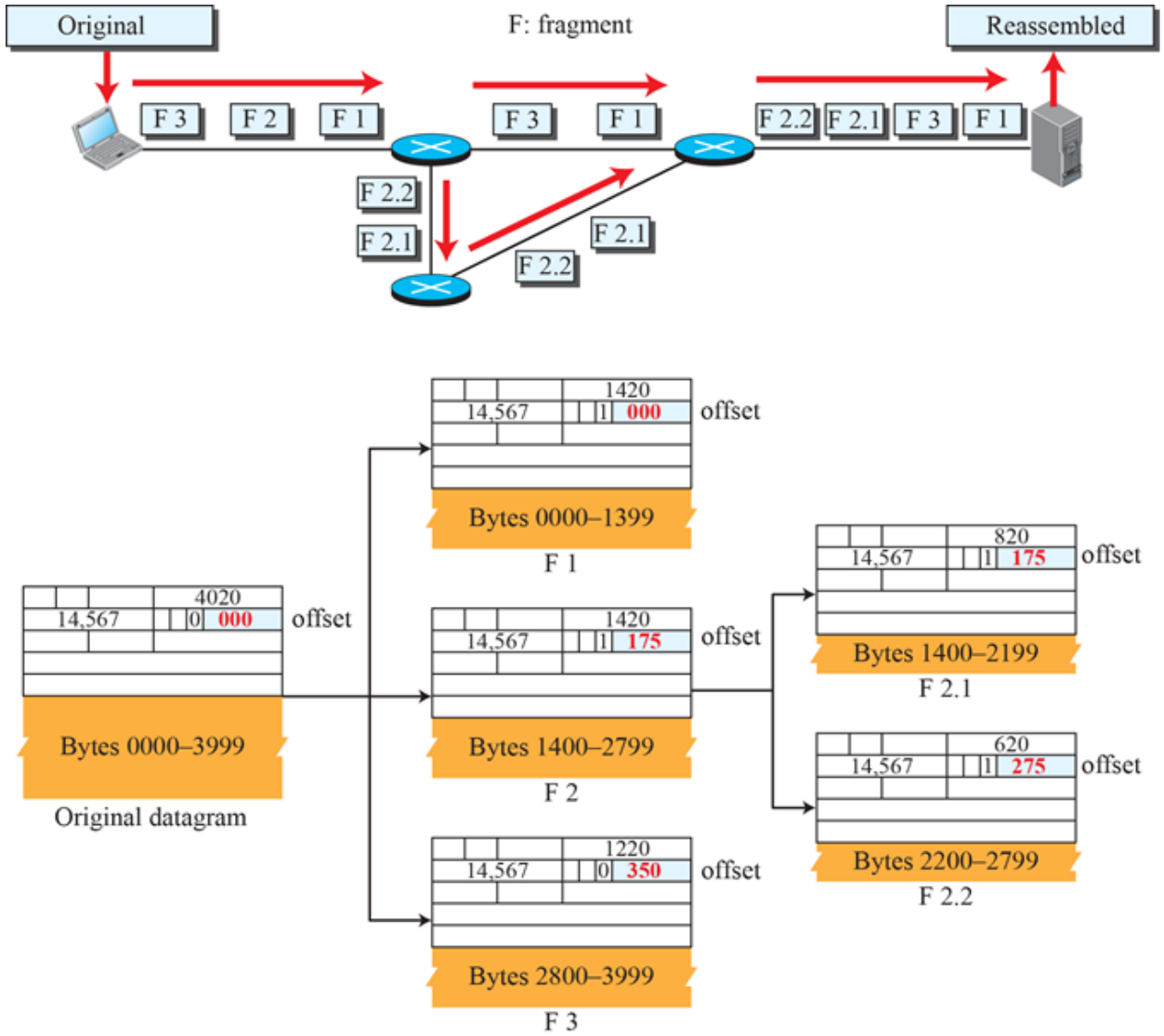


- **13-bit fragmentation offset field:** shows the relative position of this fragment with respect to the whole datagram.
- Hosts or routers that fragment datagrams to choose the size of each fragment so that the first byte number is divisible by 8.



# Detailed fragmentation example





# Options



- The **header** of the IPv4 datagram is made of two parts: **a fixed part and a variable part**.
- The fixed part is 20 bytes ; variable part comprises the options that can be a maximum of 40 bytes (in multiples of 4-bytes) to preserve the boundary of the header.
- Used for network testing and debugging.
- Options are divided into two broad categories: single-byte options and multiple-byte options

# Options



There are **two single-byte options**.

- **No Operation:** used as a filler between options.
- **End of Option:** An end-of-option option is a 1-byte option used for padding at the end of the option field.
- **Multliple-Byte Options : 4**
- **Record Route:** used to **record the Internet routers** that handle the datagram. It can list up to nine router addresses– used for **debugging and management** purposes.

# Options



- **Strict Source Route:** used by the source to predetermine a route for the datagram as it travels through the Internet
- The sender can choose a route with a **specific type of service**, such as minimum delay or maximum throughput
- **Loose Source Route:** 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:** used to record the time of datagram processing by a router. The time is expressed in milliseconds from midnight,

# Presentation Outline

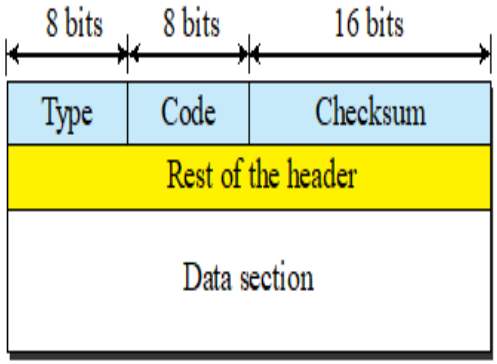
# ICMPv4



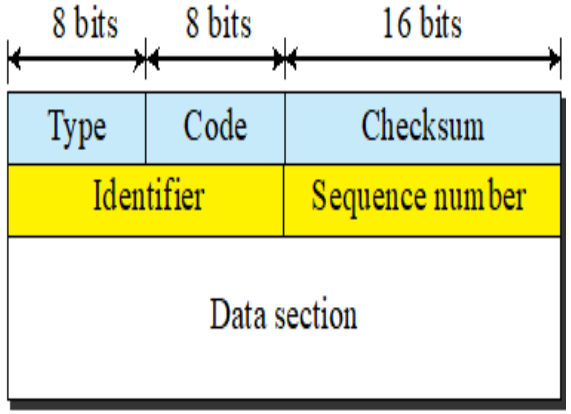
- A network-layer protocol; the messages are **encapsulated inside IP datagrams** before going to the lower layer.
- The value of the **protocol field** in the IP datagram is **set to 1**
- ICMP messages are divided into two broad categories: **error-reporting messages and query messages**
- ICMP message has an **8-byte header** and a **variable-size data** section. Although the general format of the header is different for each message type, **the first 4 bytes are common to all**

# Detailed fragmentation example






Error-reporting messages




Query messages

**Type and code values**

| Error-reporting messages | Query messages |
|---|---|
| 03: Destination unreachable (codes 0 to 15) | 08 and 00: Echo request and reply (only code 0) |
| 04: Source quench (only code 0) | 13 and 14: Timestamp request and reply (only code 0) |
| 05: Redirection (codes 0 to 3) | |
| 11: Time exceeded (codes 0 and 1) | |
| 12: Parameter problem (codes 0 and 1) | |

**Note:** See the book website for more explanation about the code values.

# ICMPv4



- The **data section** in error messages carries information for finding the original packet that had the error.
- In query messages, the data section carries extra information based on the type of query.
- Error messages are always sent to the original source

# ICMPv4

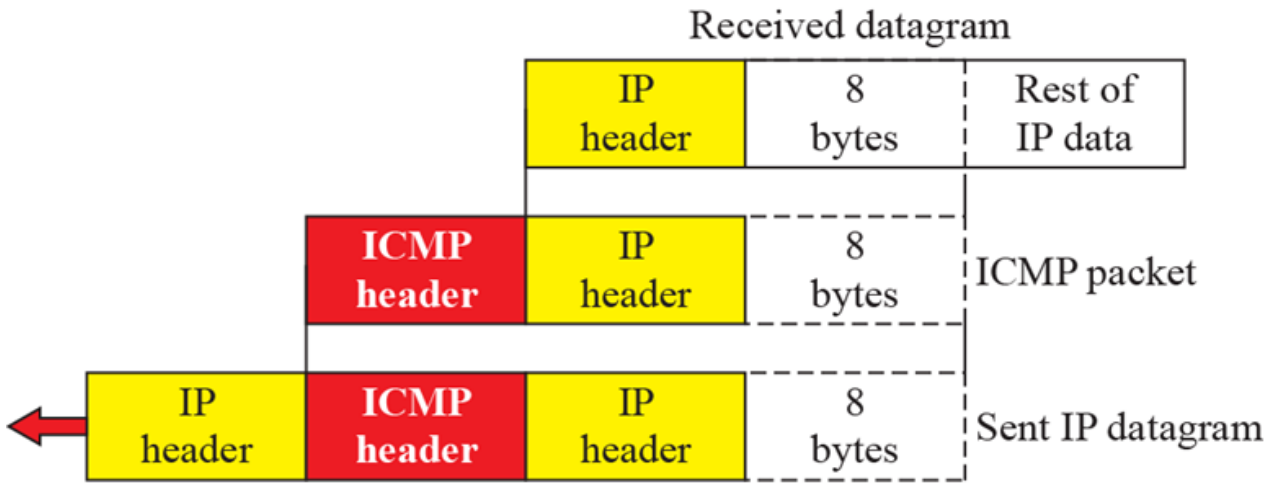


- No ICMP error message will be generated in response to a **datagram carrying an ICMP error message.**
- No ICMP error message will be generated for a fragmented datagram that is **not the first fragment**.
- No ICMP error message will be generated for a datagram **having a multicast** address.
- No ICMP error message will be generated for a datagram having a **special address** such as 127.0.0.0 or 0.0.0.0.
- The code field specifies the reason for the particular message type.
- The rest of the header is specific for each message type.

# ICMPv4



- All error messages contain a data section that includes the **IP header** of the original datagram plus the **first 8 bytes** of data
- the first 8 bytes provide information about the **port numbers (UDP and TCP) and sequence number** (TCP).



# ICMPv4



- **Destination Unreachable :** uses different codes (0 to 15) to define the type of error message and the reason why a datagram has not reached its final destination
- **Source Quench:** informs the sender that the network has encountered congestion and the datagram has been dropped
- **Redirection Message:** when the source uses a wrong router to send out its message.
- The router redirects the message to the appropriate router, but informs the source that it needs to change its default router in the future.

# ICMPv4



- **Parameter Problem:**when either there is a problem in the **header** of a datagram (code 0) or some **options are missing** or cannot be interpreted
- **Query Messages:** used to **probe or test the liveliness of hosts** or routers in the Internet, find the **one-way or the round-trip time** for an IP datagram between two devices, or even find out whether the **clocks** in two devices are **synchronized**
- Query messages come in pairs: request and reply.
-

# ICMPv4



- The **echo request (type 8) and the echo reply (type 0)** pair of messages are used by a host or a router to test the liveliness of another host or router
- **Timestamp request (type 13) and the timestamp reply (type 14)** pair of messages are used to find the round-trip time between two devices or to check whether the clocks in two devices are synchronized

# Debugging Tools: Ping



- **ping program** to find if a host is alive and responding.
- The source **host** sends ICMP **echo-request** messages; the **destination**, if alive, responds with ICMP **echo-reply** messages.
- The ping program sets the identifier field in the echo-request and echo-reply message and starts the sequence number from 0;
- This number is incremented by 1 each time
- Ping can calculate the round-trip time.

# Traceroute or Tracert



- The traceroute program in UNIX or tracert in Windows used to **trace the path** of a packet from a source to the destination
- Can **find the IP addresses of all the routers** that are visited along the path.
- The program is usually set to check for the maximum of 30 hops (routers) to be visited
- The traceroute application program is **encapsulated in a UDP** user datagram
- If there are n routers in the path, the traceroute program sends $(n + 1)$ messages. The first $n$ messages are discarded by the n routers, one by each router; the last message is discarded by the destination host.
- The traceroute client program uses the $(n + 1)$ ICMP error-reporting messages received to find the path between the routers.

# Summary



- IPv4 is an unreliable connectionless protocol responsible for source-to-destination delivery.
- Packets in the IP layer are called datagrams
- An IPv4 datagram can be fragmented; checksum for a datagram is calculated only for the header.
- Internet Control Message Protocol version 4 (ICMPv4) supports the unreliable and connectionless Internet Protocol (IP) – are encapsulated in IP datagrams.
- Two categories of ICMPv4 messages: error-reporting and query messages.

# Test your Understanding



- Can the value of the header length field in an IPv4 packet be less than 5?
- A host is sending 100 datagrams to another host. If the identification number of the first datagram is 1024, what is the identification number of the last?
- In an IPv4 datagram, the value of the header-length (HLEN) field is (6)16. How many bytes of options have been added to the packet?
- Which field(s) in the datagram is(are) responsible for gluing together all fragments belonging to an original datagram?