INTERNET PROTOCOL (IP)

SIDDAGANGA INSTITUTE OF TECHNOLOGY

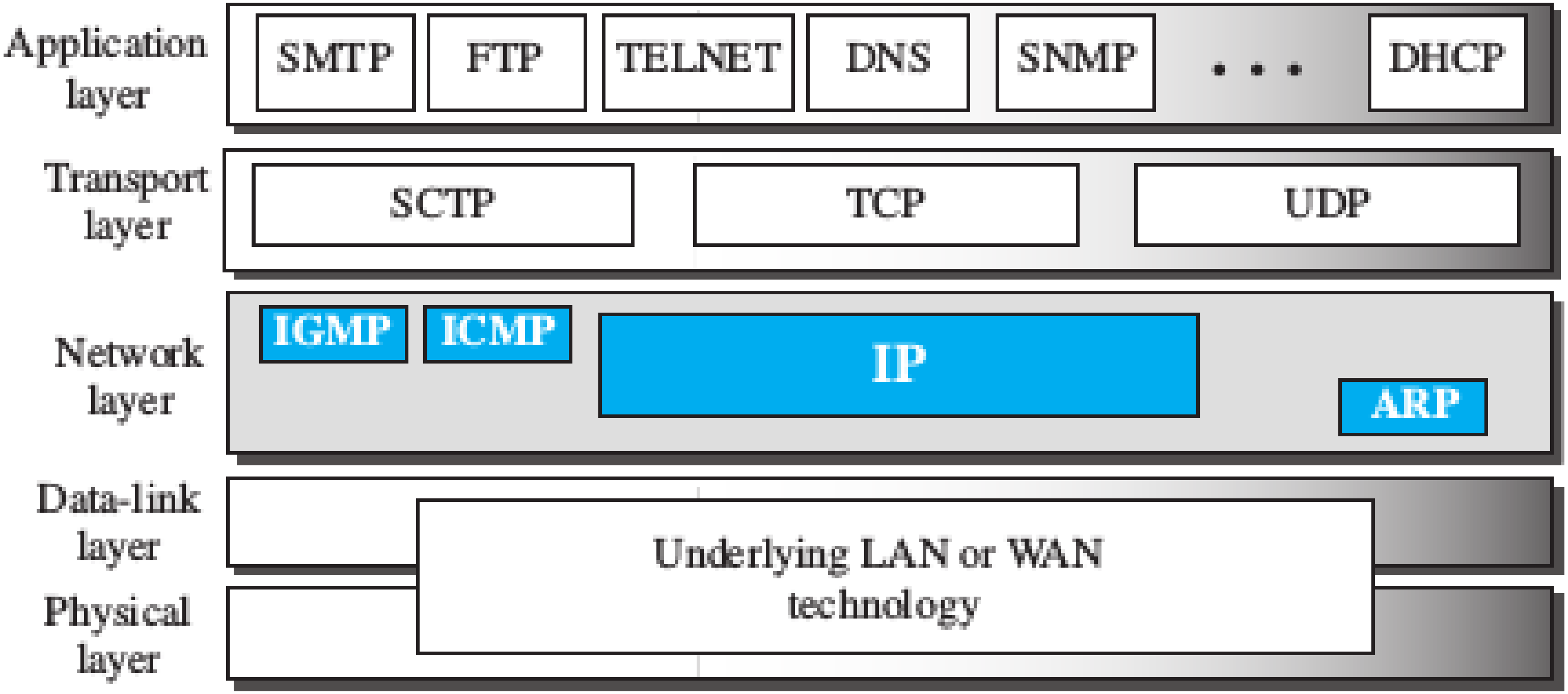
Department of CSE

Prabodh C P

Contents

- INTERNET PROTOCOL (IP)
  - Datagram Format
  - Fragmentation
  - Options
  - Security of IPv4 Datagrams

INTERNET PROTOCOL (IP)



INTERNET PROTOCOL (IP)

- The network layer in version 4 can be thought of as one main protocol and three auxiliary ones.
- The main protocol, 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.

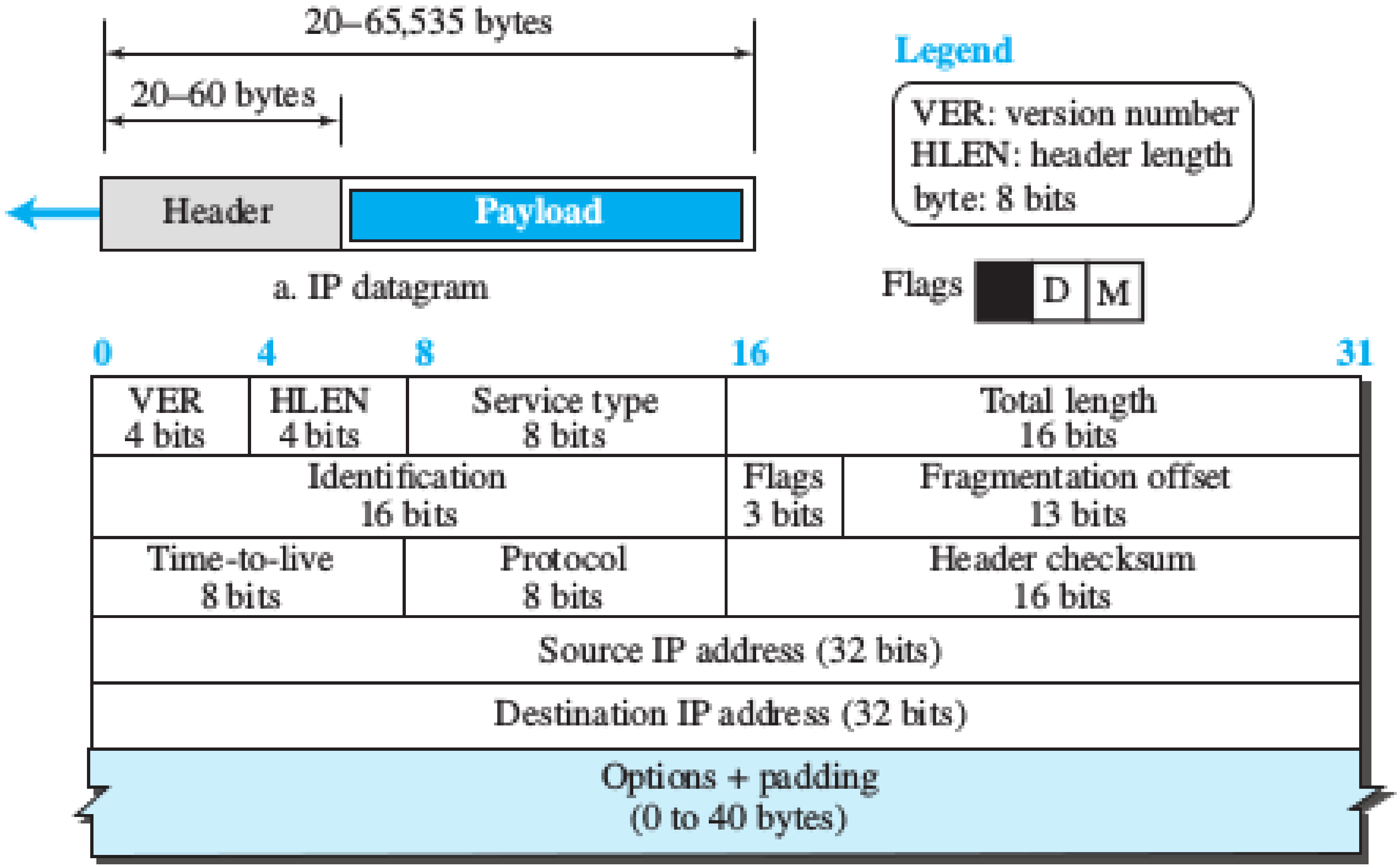
INTERNET PROTOCOL (IP)

- IPv4 is an unreliable datagram protocol—a best-effort delivery service.
- The term best-effort means that IPv4 packets can
  - be corrupted
  - be lost
  - arrive out of order
  - be delayed, and
  - may create congestion for the network.
- If reliability is important, IPv4 must be paired with a reliable transport-layer protocol such as TCP.
- Example Post Office

INTERNET PROTOCOL (IP)

- IPv4 is also a connectionless protocol that uses the datagram approach.
- This means that each datagram is handled independently, and each datagram can follow a different route to the destination.
- This implies that datagrams sent by the same source to the same destination could arrive out of order.

Datagram Format



a. IP datagram

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)				

b. Header

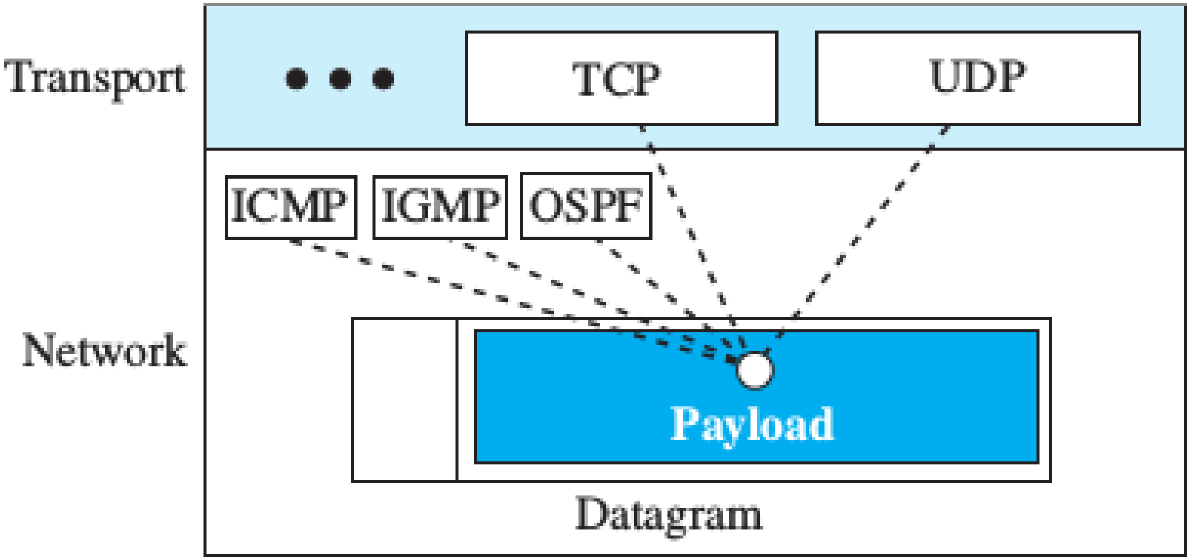
Datagram Format

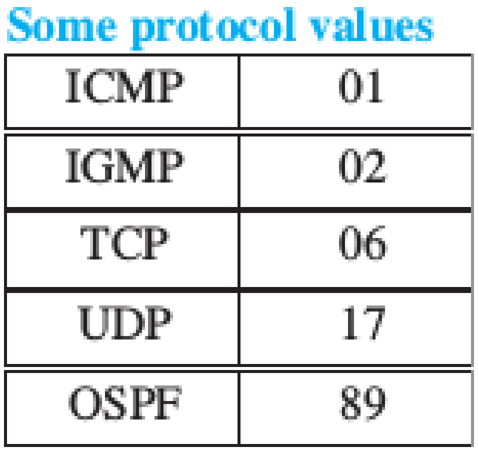
- Packets used by the IP are called datagrams.
- A datagram is a variable-length packet consisting of two parts: header and payload (data).
- The header is 20 to 60 bytes in length and contains information essential to routing and delivery.
- It is customary in TCP/IP to show the header in 4-byte sections.
- **Version Number**. The 4-bit version number (VER) field defines the version of the IPv4 protocol, which, obviously, 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. 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.

Datagram Format

- **Service Type** differentiated services (DiffServ).
- **Total Length.** This 16-bit field defines the total length (header plus data) of the IP datagram in bytes. (max value 65535)
  - Length of data = total length - (HLEN) × 4
  - padding
- **Identification, Flags, and Fragmentation Offset.**
- **Time-to-live** - maximum number of hops
- **Protocol.** Upper layer protocols
- **Header checksum. 16 bit internet checksum**
- **Source and Destination Addresses – 32 bit**
- **Options. - upto 40 bytes**
- **Payload.**

Multiplexing and demultiplexing using the value of the protocol field




Some protocol values

ICMP	01
IGMP	02
TCP	06
UDP	17
OSPF	89

Example

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

Solution

There is an error in this packet. The 4 leftmost bits $(0100)_2$ show the version, which is correct.

The next 4 bits $(0010)_2$ show an invalid header length $(2 \times 4 = 8)$. 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 $(1000)_2$. 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.

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?

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 $(0028)_{16}$ or 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. How many hops can this packet travel before being dropped? The data belong to what upper-layer protocol?

$(45000028000100000102\ ...\ )_{16}$

Solution

To find the time-to-live field, we skip 8 bytes (16 hex digits).

The time-to-live field is the ninth byte, which is $(01)_{16}$. This means the packet can travel only one hop.

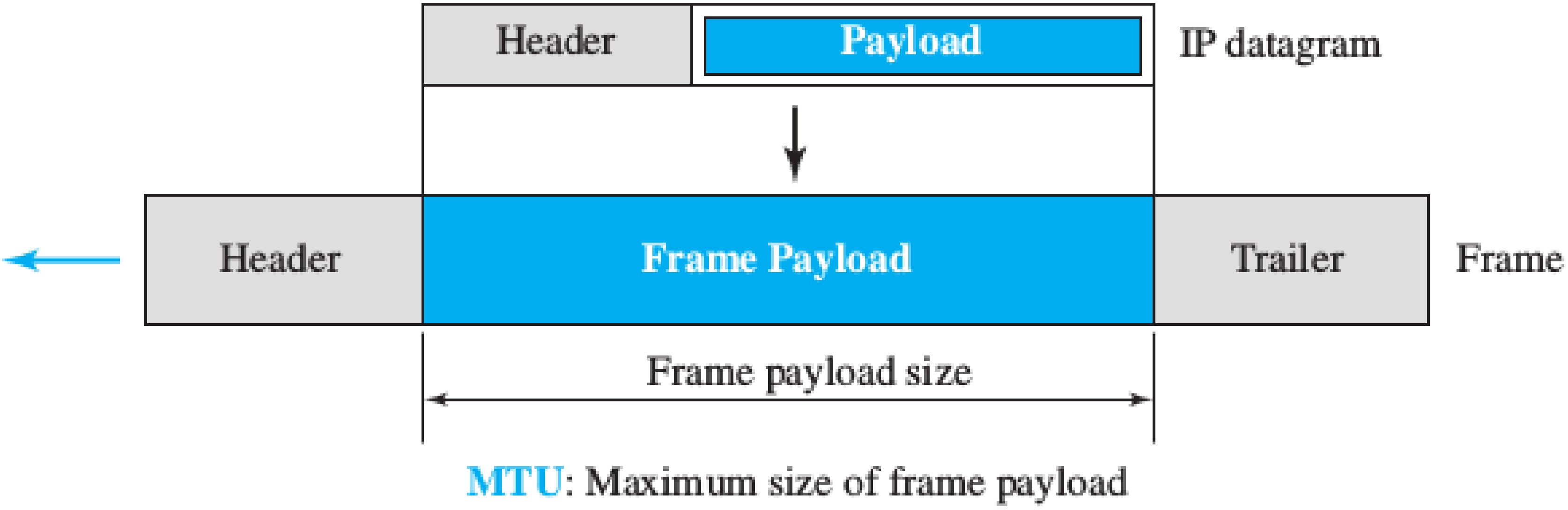
The protocol field is the next byte $(02)_{16}$, which means that the upper-layer protocol is IGMP.

Fragmentation

- A datagram can travel through different networks. Each router decapsulates the IP datagram from the frame it receives, processes it, and then encapsulates it in another frame.
- The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled.
- The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.
- 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)

- 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.



Fragmentation

- The value of the MTU differs from one physical network protocol to another.
- In order to make the IP protocol independent of the physical network, the designers decided to make the maximum length of the IP datagram equal to 65,535 bytes.
- For physical networks having a lesser MTU, we must divide the datagram to make it possible for it to pass through these networks. This is called fragmentation.
- When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but some have been changed.
- A fragmented datagram may itself be fragmented if it encounters a network with an even smaller MTU.
- In other words, a datagram may be fragmented several times before it reaches the final destination.

Fragmentation

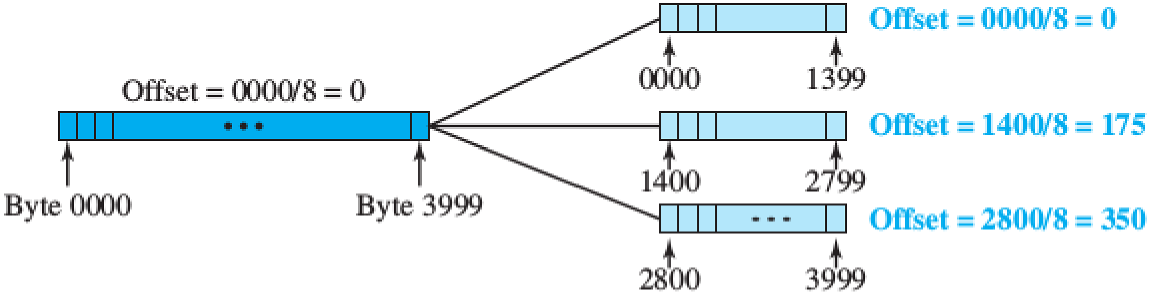
- A datagram can be fragmented by the source host or any router in the path.
- The reassembly of the datagram, however, is done only by the destination host
- When we talk about fragmentation, we mean that the payload of the IP datagram is fragmented.
- The host or router that fragments a datagram must change the values of three fields: flags, fragmentation offset, and total length.
- The rest of the fields must be copied.

Fragmentation Fields

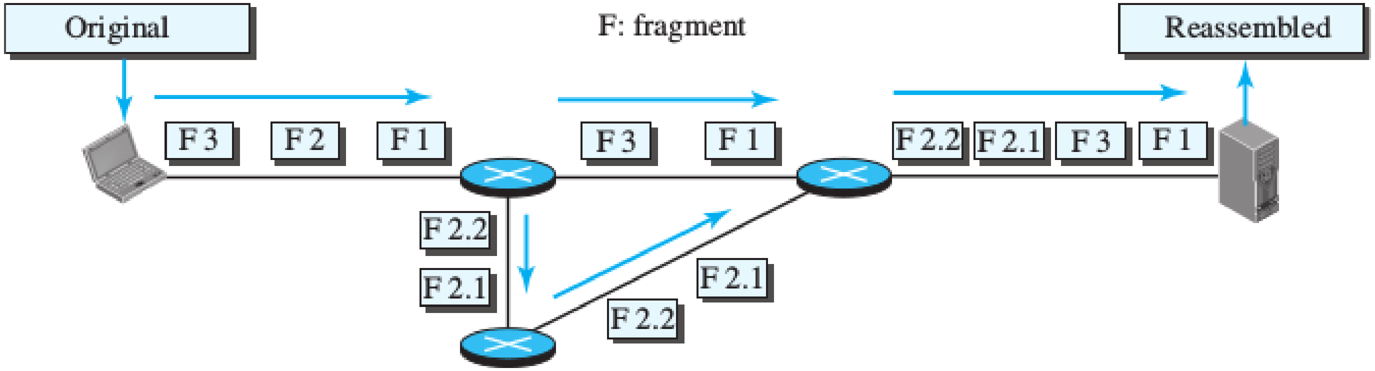
- three fields in an IP datagram are related to fragmentation:
  - identification, flags, and fragmentation offset
- The 16-bit identification field identifies a datagram originating from the source host. (Sequence Number)
- When a datagram is fragmented, the value in the identification field is copied into all fragments.
- The identification number helps the destination in reassembling the datagram.
- 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 it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source
- If its value is 0, the datagram can be fragmented if necessary.

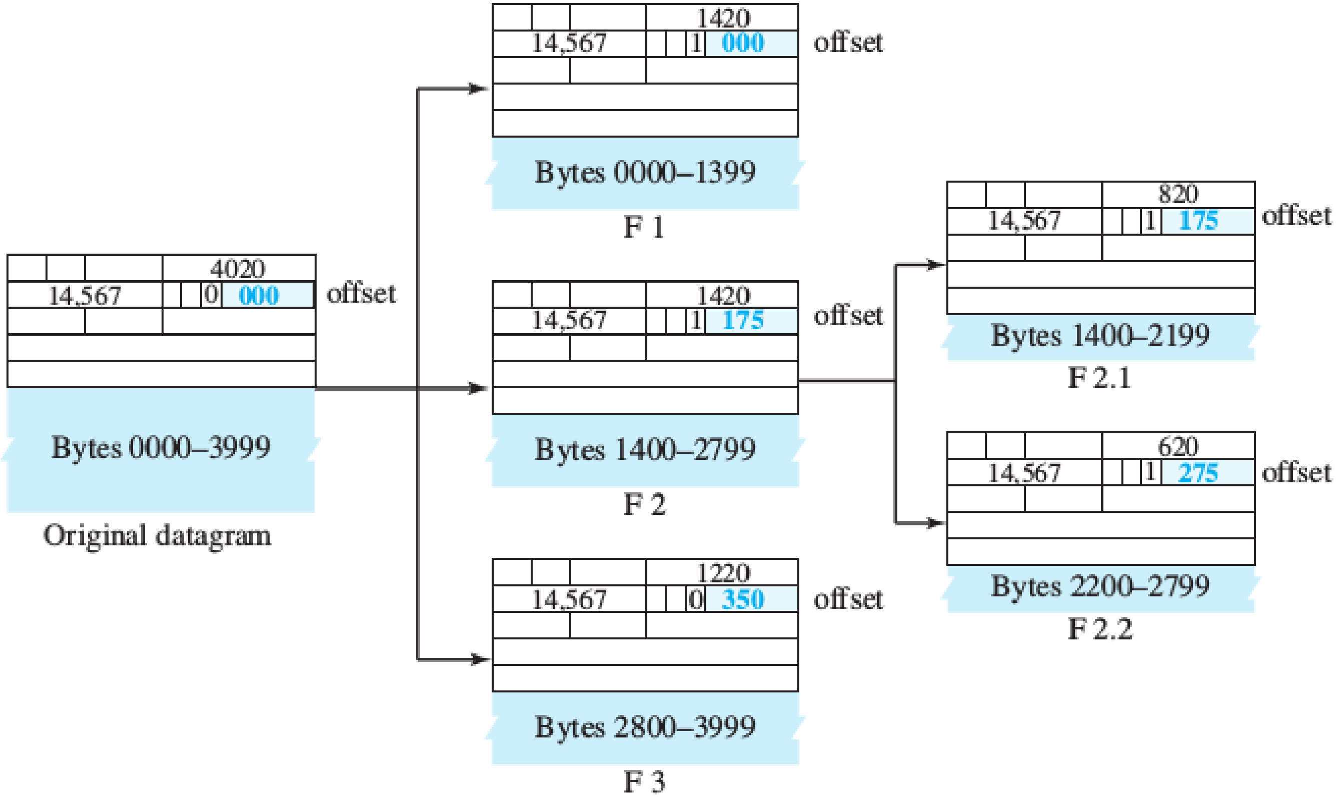
Fragmentation Fields

- 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.
- 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.



Detailed Fragmentation example





Fragmentation example

- what happens if a fragment itself is fragmented?
- In this case the value of the offset field is always relative to the original datagram.
- For example, in the figure, the second fragment is itself fragmented later into two fragments of 800 bytes and 600 bytes, but the offset shows the relative position of the fragments to the original data.

Fragment Re-assembly Strategy

a. The first fragment has an offset field value of zero.

b. Divide the length of the first fragment by 8. The second fragment has an offset value equal to that result.

c. Divide the total length of the first and second fragment by 8. The third fragment has an offset value equal to that result.

d. Continue the process. The last fragment has its M bit set to 0.

e. Continue the process. The last fragment has a more bit value of 0.

Exercises

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?

If 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 nonfragmented packet is considered the last fragment.

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?

If 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).

Exercises

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 fragent.

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?

Solution

To find the number of the first byte, we multiply the offset value by 8.

This means that the first byte number is 800. We cannot determine the number of the last byte unless we know the length of the data.

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?

Solution

The first byte number is 100 × 8 = 800. The total length is 100 bytes, and the header length is 20 bytes (5 × 4), which means that there are 80 bytes in this datagram. If the first byte numberis 800, the last byte number must be 879.

Options

Single-Byte Options

There are two single-byte options.

No Operation

A no-operation option is a 1-byte option 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. It, however, can only be used as the last option.

Options

Multiple-Byte Options

There are four multiple-byte options.

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.

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.

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.

Security of IPv4 Datagrams

- Packet Sniffing
- Packet Modification
- IP Spoofing
- IPSec
  - Algorithms and Keys
  - Packet Encryption
  - Data Integrity
  - Origin Authentication