Traceroute, PMTDU, Routing and Flooding

Complete Course on Computer Networks - Part II

Ravindrababu Ravula • Lesson 17 • Mar 14, 2021

Computer Networks

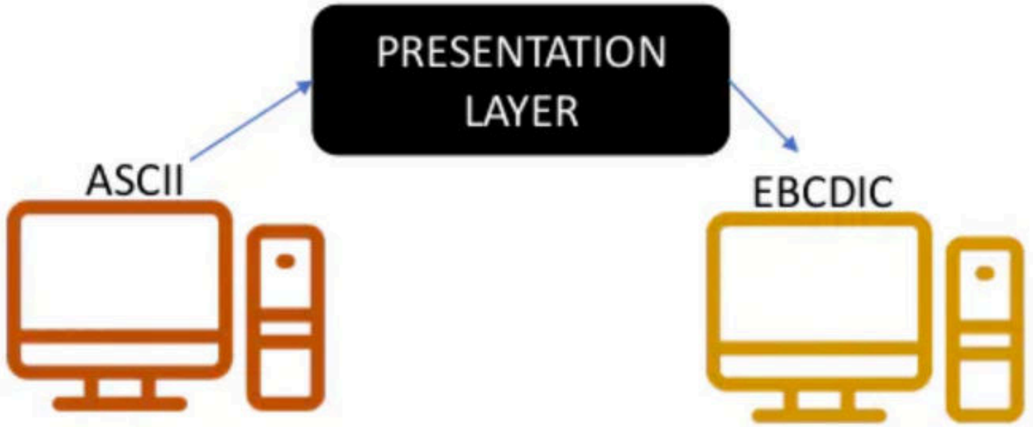
Presentation Layer and GATE 2014 question

Functions of Presentation Layer

- Data Translation
- Encryption and Decryption
- Data compression

Functions of Presentation Layer

- Data Translation
- Encryption and Decryption
- Data compression



Functions of Presentation Layer

- Data Translation
- Encryption and Decryption
- Data compression

Functions of Presentation Layer

- Data Translation
- Encryption and Decryption
- Data compression

GATE 2014

An IP machine Q has a path to another IP machine H via three IP routers R1, R2, and R3.

Q—R1—R2—R3—H

H acts as an HTTP server, and Q connects to H via HTTP and downloads a file. Session layer encryption is used, with DES as the shared key encryption protocol. Consider the following four pieces of information:

[I1] The URL of the file downloaded by Q

[I2] The TCP port numbers at Q and H

[I3] The IP addresses of Q and H

[I4] The link layer addresses of Q and H

Which of I1, I2, I3, and I4 can an intruder learn through sniffing at R2 alone?

A) Only I1 and I2

B) Only I1

C) Only I2 and I3

D) Only I3 and I4

GATE 2014

An IP machine Q has a path to another IP machine H via three IP routers R1, R2, and R3.

Q—R1—R2—R3—H

H acts as an HTTP server, and Q connects to H via HTTP and downloads a file. Session layer encryption is used, with DES as the shared key encryption protocol. Consider the following four pieces of information:

[I1] The URL of the file downloaded by Q

[I2] The TCP port numbers at Q and H

[I3] The IP addresses of Q and H

[I4] The link layer addresses of Q and H

Which of I1, I2, I3, and I4 can an intruder learn through sniffing at R2 alone?

A) Only I1 and I2

B) Only I1

C) Only I2 and I3

D) Only I3 and I4

Answer:

An Intruder can't learn [I1] through sniffing at R2 because URLs and Download are functioned at Application layer of OSI Model.

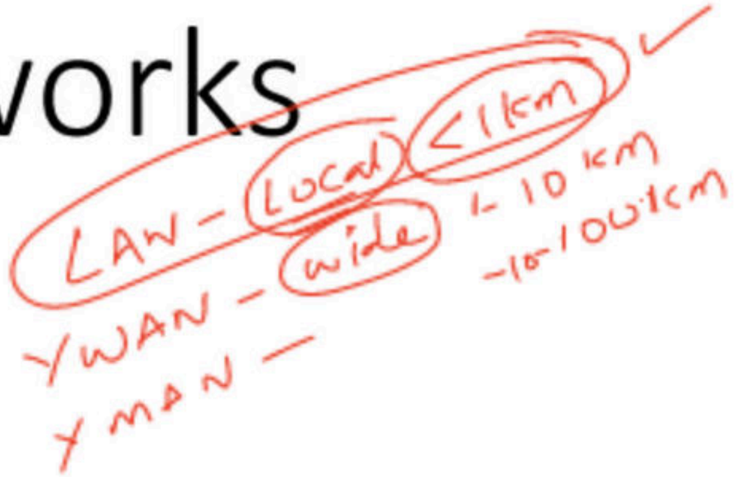
An Intruder can learn [I2] through sniffing at R2 because Port Numbers are encapsulated in the payload field of IP Datagram.

An Intruder can learn [I3] through sniffing at R2 because IP Addresses and Routers are functioned at network layer of OSI Model.

An Intruder can't learn [I4] through sniffing at R2 because it is related to Data Link Layer of OSI Model.

Computer Networks

Ethernet

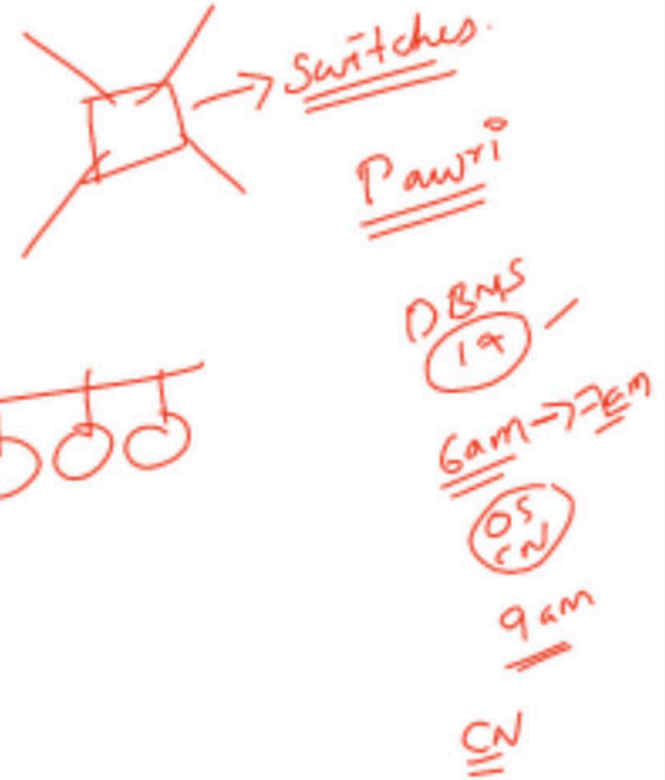


Ethernet is one of the standard LAN technologies used for building wired LANs.
It is defined under IEEE 802.3.

Ethernet uses bus topology.In bus topology, all the stations are connected to a single half duplex link.

Ethernet uses CSMA / CD as access control method to deal with the collisions.

Ethernet uses Manchester Encoding Technique for converting data bits into signals.

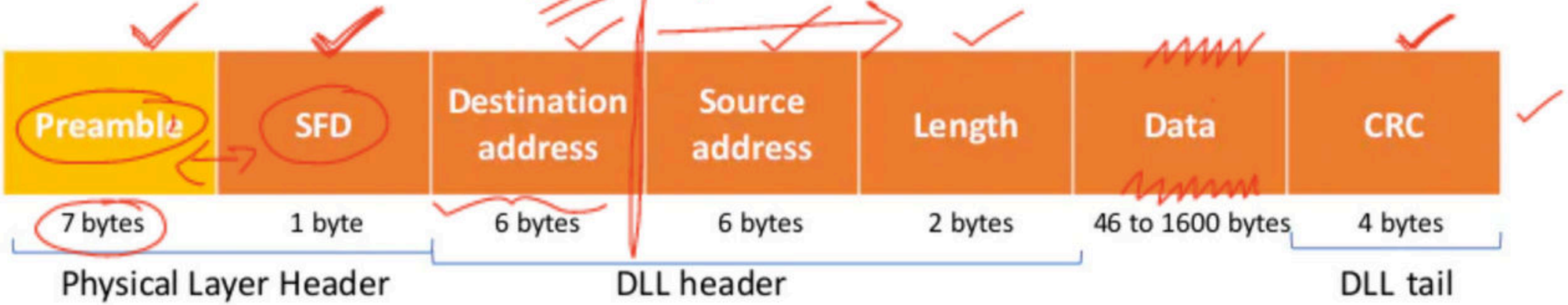


For Normal Ethernet, operational bandwidth is 10 Mbps.

For Fast Ethernet, operational bandwidth is 100 Mbps.

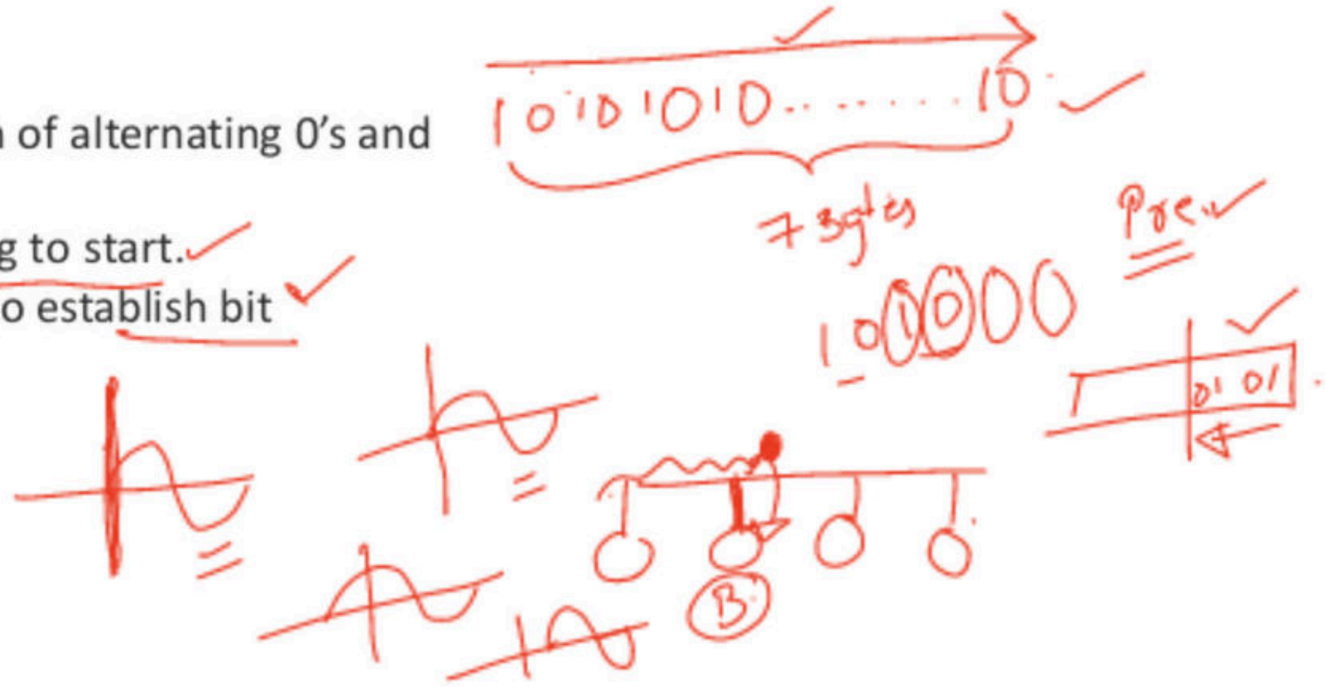
For Gigabit Ethernet, operational bandwidth is 1 Gbps.

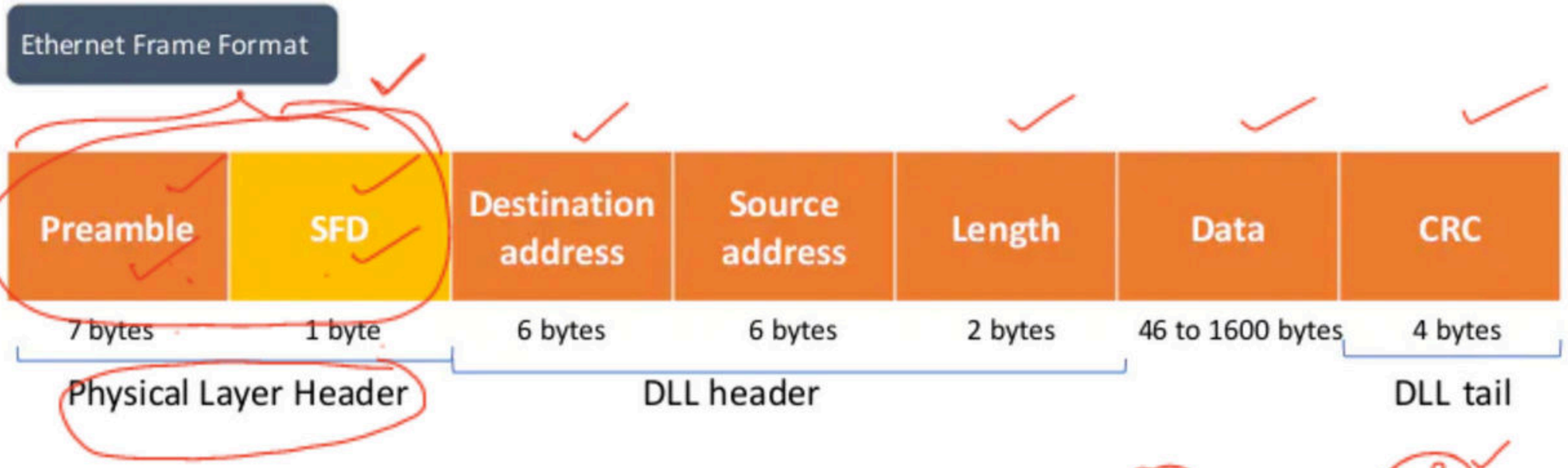
Ethernet Frame Format



1. Preamble-

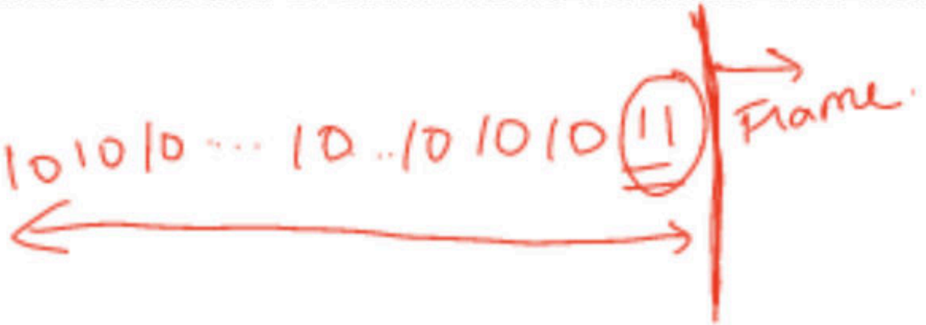
- It is a 7 byte field that contains a pattern of alternating 0's and 1's.
- It alerts the stations that a frame is going to start.
- It also enables the sender and receiver to establish bit synchronization.



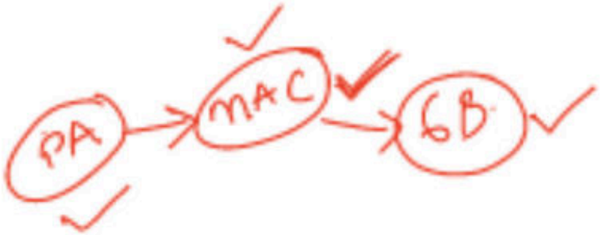


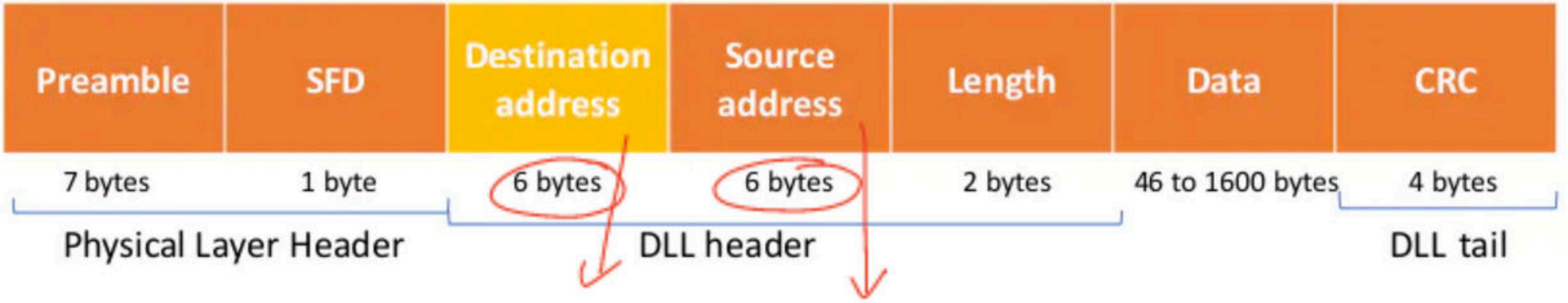
2. Start Frame Delimiter (SFD)-

- It is a 1 byte field which is always set to 10101011.
- The last two bits "11" indicate the end of Start Frame Delimiter and marks the beginning of the frame.



Ethernet Frame Format

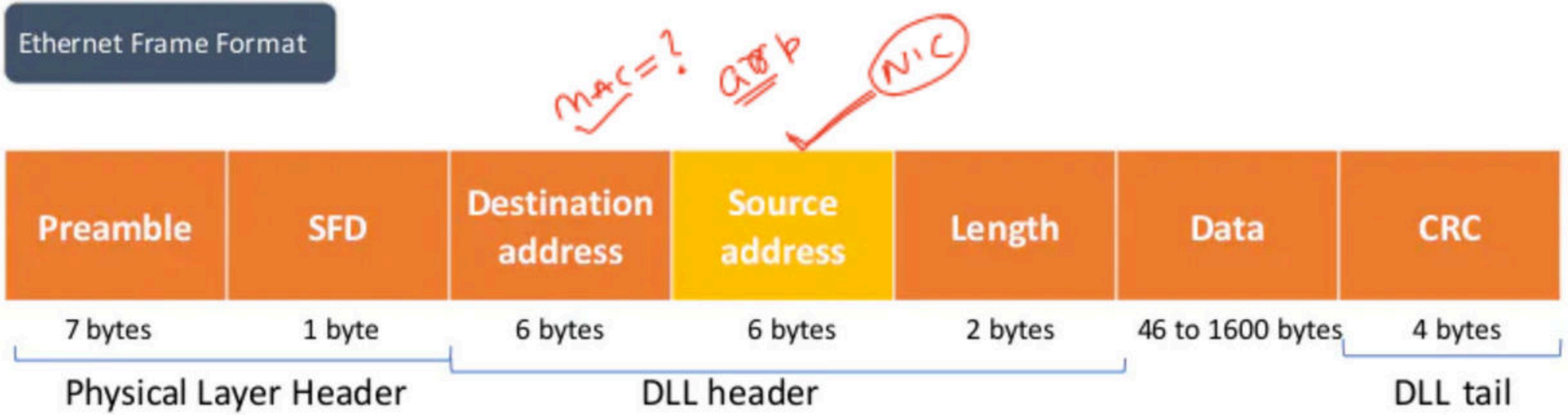




3. Destination Address-

•It is a 6 byte field that contains the MAC address of the destination for which the data is destined.

Ethernet Frame Format



4. Source Address-

•It is a 6 byte field that contains the MAC address of the source which is sending the data.

Types of MAC address :-
There are three types of MAC addresses, which are:

1. **Unicast MAC Address** ✓
2. **Multicast MAC address** ✓
3. **Broadcast MAC address** ✓

1.)Unicast MAC address:
The Unicast MAC address represents the specific NIC on the network.
A Unicast MAC address frame is only sent out to the interface which is assigned to a specific NIC and hence transmitted to the single destination device. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one destination NIC.

2.)Multicast MAC Address:
Multicast addresses enables the source device to transmit a data frame to multiple devices or NICs.
In Layer-2 (Ethernet) Multicast address, LSB (least significant bit) or first 3 bytes of the first octet of an address is set to one and reserved for the multicast addresses.

3.)Broadcast MAC address
It represents all devices within a Network. In broadcast MAC address, Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are known as a broadcast address.
All these bits are the reserved addresses for the broadcast. Frames that are destined with MAC address FF-FF-FF-FF-FF-FF will reach every computer belong to that LAN segment. Hence if a source device wants to send the data to all the devices within a network, that can use the broadcast address as the destination MAC address.

1. 2. 3. 4 → Hexa → Decimal

Dotted decimal Rep

10, 15, 16 7

A - 10
B - 11
C - 12
D - 13
E - 14
F - 15

If Config
Ip Config
} MAC

MAC: Hexa

1A : 2B : 3C : 4D : 5E : 6F → 6

00011010 : 00101011 : 0011 1100 : . . . . .

LSB

I byte

unicast add → 1-1

A1 : B2 : C3 : . . . . . .

1010 0001 ⇒ multicast add

LSB

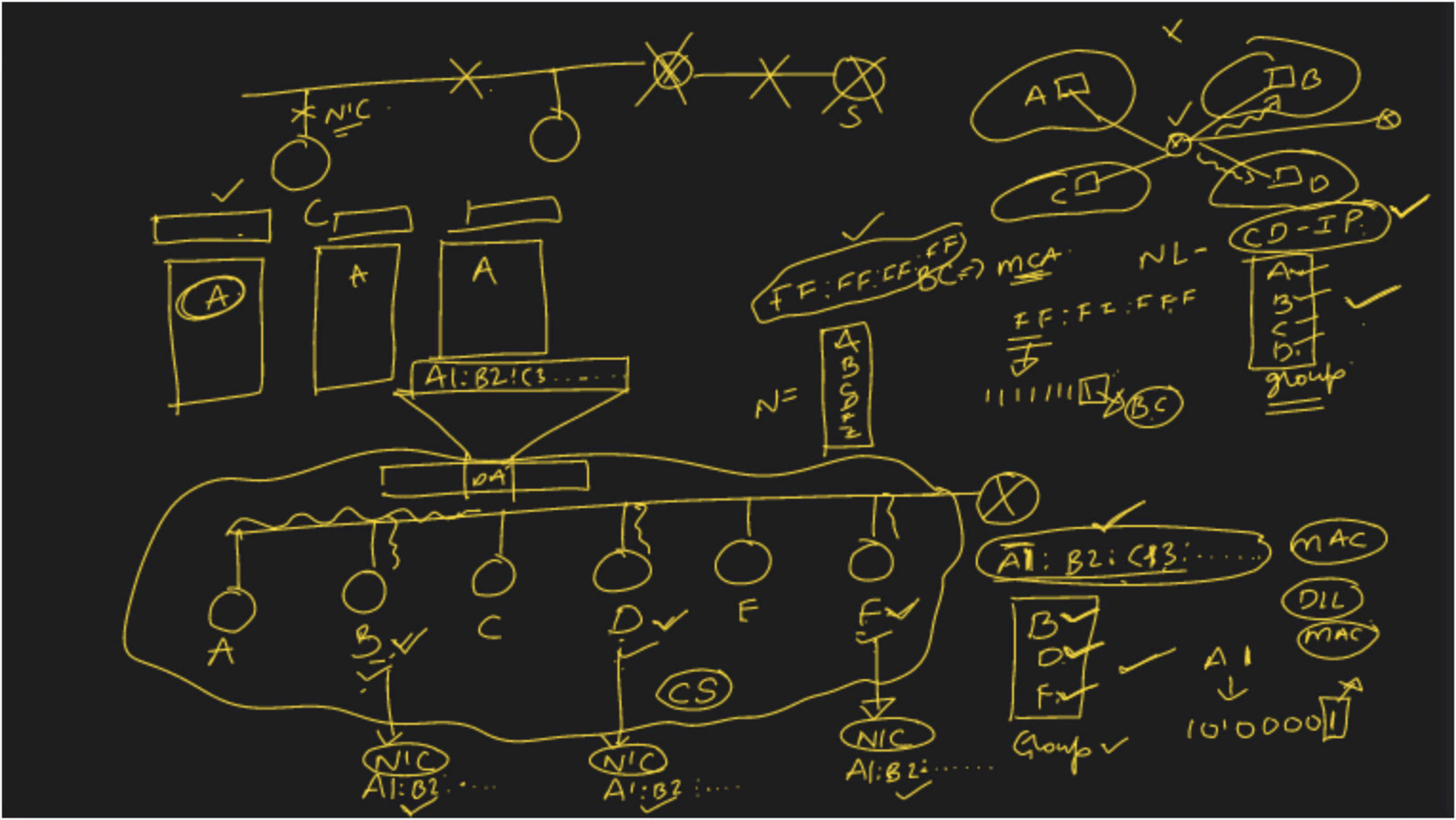
I Byte

FF:FF:FF:FF:FF:FF

BC address

Frame

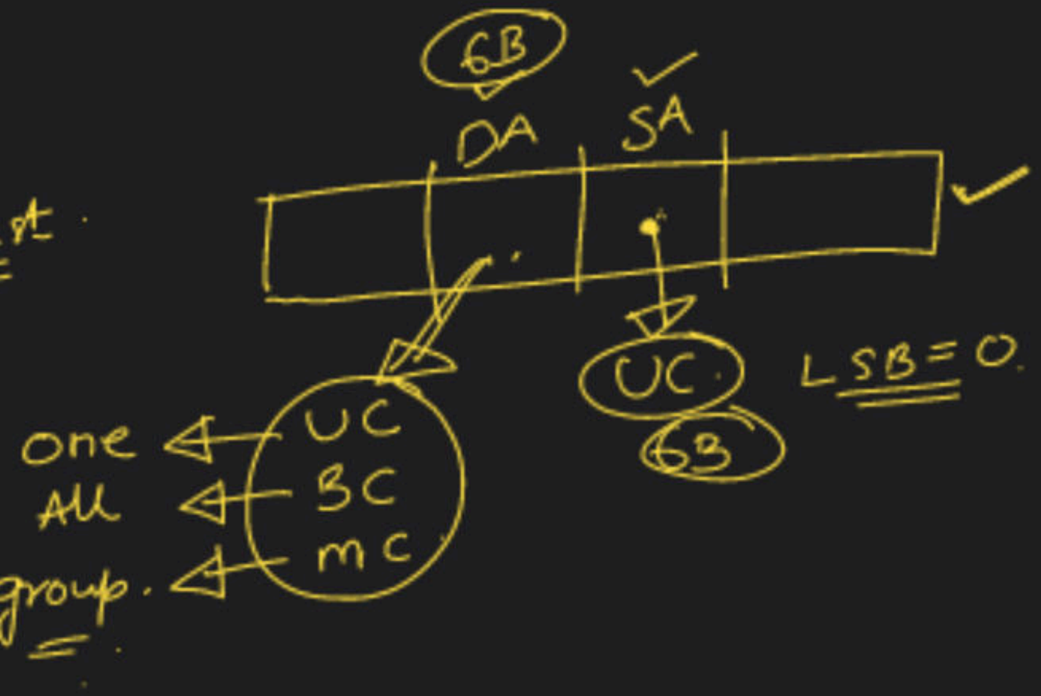
	FF:FFF	
	DA	


NIC
S
A
A
A
A1:B2:C3
DA
A
B
C
D
F
F
CS
NIC
A1:B2
NIC
A1:B2
NIC
A1:B2
FF:FF:FF:FF
N=
A
B
D
F
MCA
NL-
FF:FF:FF:FF
B.C
A
B
C
D
group
CD-IP
A1:B2:C3
Group
B
D
F
A1
10100001
MAC
DLL
MAC

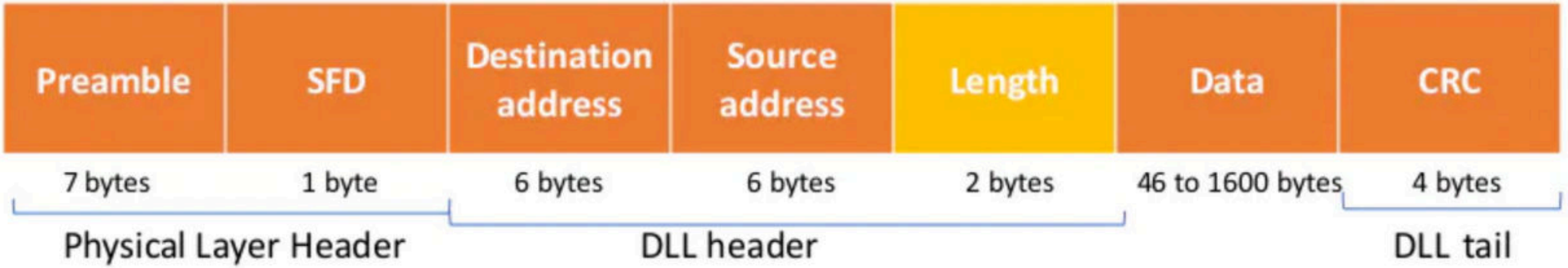
A) m1 ~
B) m2 ~
C) m3 ~
D) m4 ~

(C)

unicast.



Ethernet Frame Format

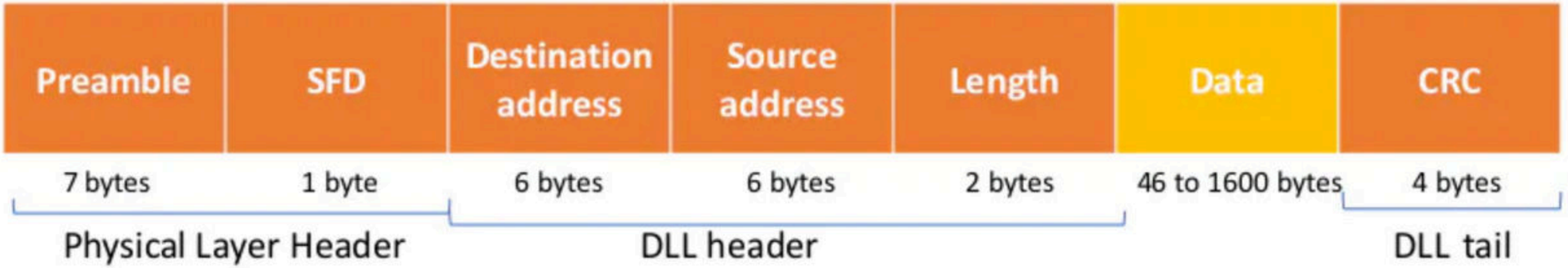


5. Length-

- It is a 2 byte field which specifies the length (number of bytes) of the data field.
- This field is required because Ethernet uses variable sized frames.

- The maximum value that can be accommodated in this field = $2^{16} - 1 = 65535$.
- But it does not mean maximum data that can be sent in one frame is 65535 bytes.
- The maximum amount of data that can be sent in a Ethernet frame is 1500 bytes.
- This is to avoid the monopoly of any single stati

Ethernet Frame Format



6. Data-

- It is a variable length field which contains the actual data.
- It is also called as a **payload field**.
- The length of this field lies in the range [46 bytes , 1500 bytes].
- Thus, in a Ethernet frame, minimum data has to be 46 bytes and maximum data can be 1500 bytes.

Minimum Length of Data Field

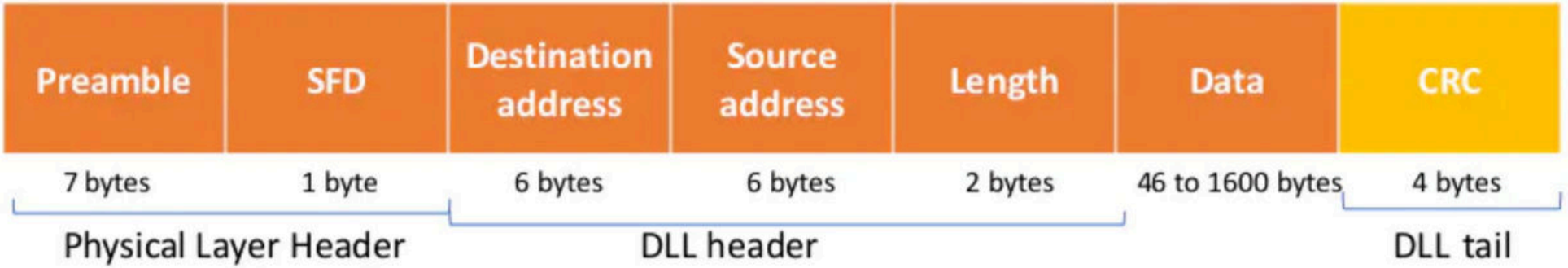
- Ethernet uses CSMA / CD as access control method to deal with collisions.
- For detecting the collisions, CSMA / CD requires-

  Minimum length of data packet = 2 x Propagation delay x Bandwidth
- Substituting the standard values of Ethernet, it is found that minimum length of the Ethernet frame has to be 64 bytes starting from the destination address field to the CRC field and 72 bytes including the Preamble and SFD fields.
- Therefore, minimum length of the data field has to be = 64 bytes – (6+6+2+4) bytes = 46 bytes

Maximum Length of Data Field

- The maximum amount of data that can be sent in a Ethernet frame is 1500 bytes.
- This is to avoid the monopoly of any single station.
- If Ethernet allows the frames of big sizes, then other stations may not get the fair chance to send their data.

Ethernet Frame Format



7. Frame Check Sequence (CRC)-

•It is a 4 byte field that contains the CRC code for error detection.

Advantages of Using Ethernet-

It is simple to understand and implement.

Its maintenance is easy.

It is cheap.

Limitations of Using Ethernet-

Point-01:

It can not be used for real time applications.

Real time applications require the delivery of data within some time limit.

Ethernet is not reliable because of high probability of collisions.

High number of collisions may cause a delay in delivering the data to its destination.

Point-02:

It can not be used for interactive applications.

Interactive applications like chatting requires the delivery of even very small amount of data.

Ethernet requires that minimum length of the data must be 46 bytes.

Point-03:

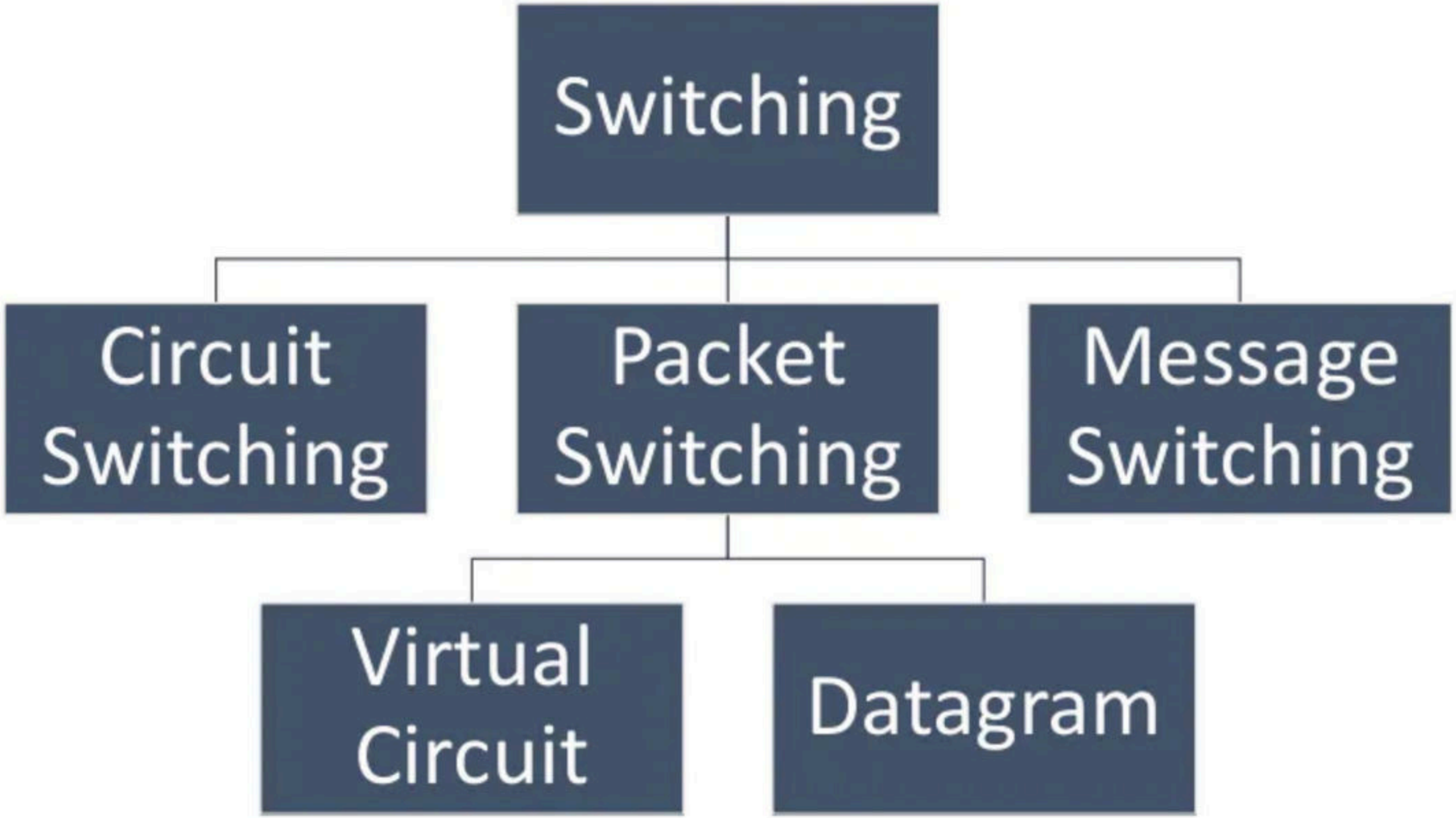
It can not be used for client server applications.

Client server applications require that server must be given higher priority than clients.

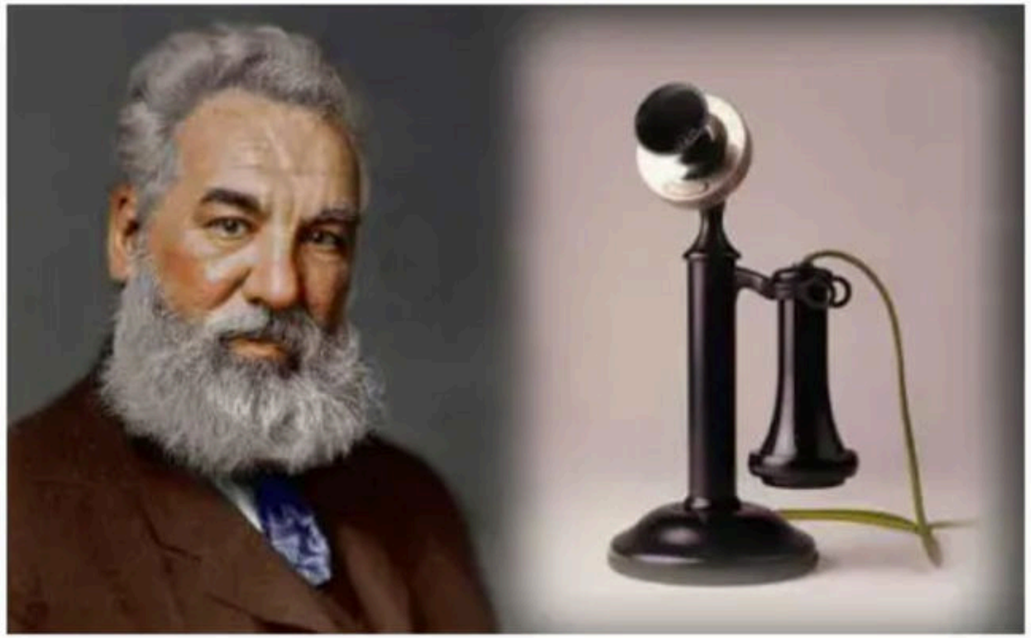
Ethernet has no facility to set priorities.

Computer Networks

Switching


Switching
Circuit Switching
Packet Switching
Message Switching
Virtual Circuit
Datagram

Before moving ahead, Let's see Alexander Graham Bell's Story and his invention.



Back in 1876, Alexander Graham Bell had just sent speech down a length of wire via a new device that came to be known as the telephone. As Bell and his co-investors sought to monetize their invention, they approached the then telecoms giant of the day, Western Union who had an industry monopoly with the telegraph system and offered to sell them the telephone patent for $100,000. Messers Hubbard and Bell want to install one of their “telephone devices” in every city.
Western Union thought the idea was ridiculous.

Graham bell then went out to sell his telephone licence to merchants, who purchased it and used it.
Western Union was doing quite well in their business that they didn't feel any threat from Graham bell's invention
Because the communication through telephone happened only within the cities (within short range).

Soon days passed and the range of the communication through telephone grew and connected cities, then states and then continents too. The telephone market grew a lot in 10 years and the merchants who ad purchased licence from Bell Started a new company AT&T and in few years AT&T bought western union.

TELEGRAPH

TELEPHONE

COMPUTER NETWORKS

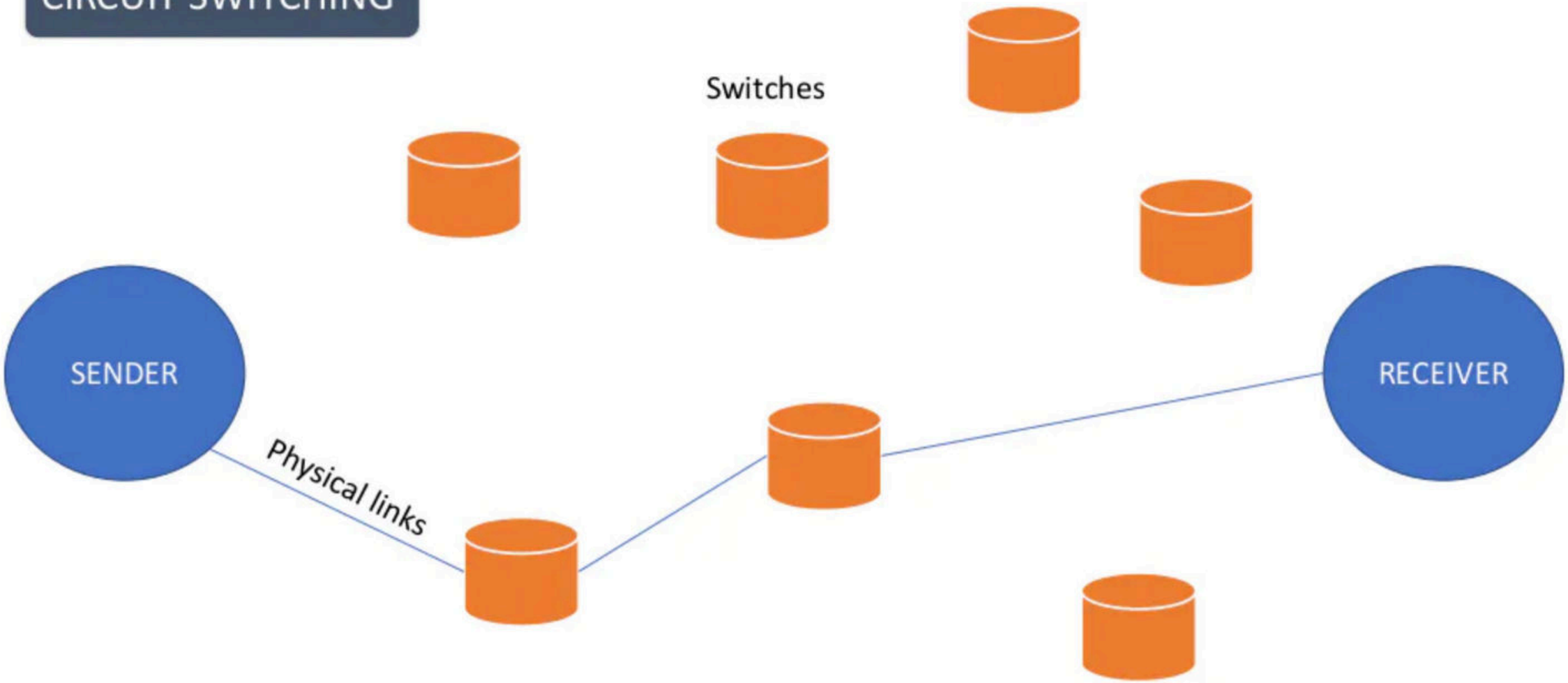
Basically when ever we have any problem in computer networks, we look back into telephone network and see how they solved it and come up with a solution.

Even in case of Classful addressing,
We looked back to Telephone Network and designed it in similar fashion.
A telephone system can be thought of as two parts: area code and local part.
the area code defines the area, the local part defines a particular telephone subscriber in that area.

Computer Networks

Circuit Switching

CIRCUIT SWITCHING



PHASES INVOLVED IN CIRCUIT SWITCHING

- Establishing a circuit
- Transferring the data
- Disconnecting the circuit

PHASES INVOLVED IN CIRCUIT SWITCHING

- Establishing a circuit
- Transferring the data
- Disconnecting the circuit

1. In this phase,
A circuit is established between the two ends.
Circuit provides a dedicated path for data to travel from one to the other end.
2. Resources are reserved at intermediate switches which are used during the transmission.
3. The intermediate switches are connected by the physical links.

PHASES INVOLVED IN CIRCUIT SWITCHING

- Establishing a circuit
- Transferring the data
- Disconnecting the circuit

After the circuit is established,
The entire data travels over the dedicated path from one end to the other end.

PHASES INVOLVED IN CIRCUIT SWITCHING

- Establishing a circuit
- Transferring the data
- Disconnecting the circuit

After the data transfer is completed,
The circuit is disconnected.

Total time taken to transmit a message in circuit switched network=

Connection set up time + Transmission delay + Propagation delay + Tear down time

where-
Transmission delay = Message size / Bandwidth
Propagation delay = (Number of hops on way x Distance between 2 hops) / Propagation speed

NOTE:
Circuit switching is implemented at physical layer.
Circuit switching is now outdated.

Advantages

- A well defined and dedicated path exists for the data to travel.
- There is no header overhead.
- There is no waiting time at any switch and the data is transmitted without any delay.
- Data always reaches the other end in order.
- No re ordering is required.

Disadvantages-

- It is inefficient in terms of utilization of system resources.
- The time required for establishing the circuit between the two ends is too long.
- Dedicated channels require more bandwidth.
- It is more expensive than other switching techniques.
- Routing decisions can not be changed once the circuit is established.

Computer Networks

Packet Switching

Packet Switching

- The entire message to be sent is divided into multiple smaller size packets.
- This process of dividing a single message into smaller size packets is called as **packetization**.
- These smaller packets are sent after the other.
- It gives the advantage of pipelining and reduces the total time taken to transmit the message.

If the packet size is not chosen wisely, then-

- It may result in adverse effects.
- It might increase the time taken to transmit the message.

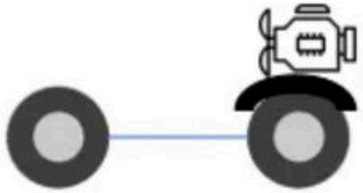
So, it is very important to choose the packet size wisely.

What is Pipelining?

Understanding with an example

PHASE 1

1 DAY



PHASE 2

1 DAY

PHASE 3

1 DAY

PHASE 4

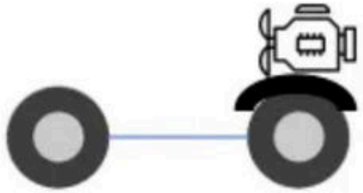
1 DAY

What is Pipelining?

Understanding with an example

PHASE 1

1 DAY



PHASE 2

1 DAY

PHASE 3

1 DAY

PHASE 4

1 DAY

Without Pipelining:
100 cars in 100 days
With Pipelining:
1 car in 4 days
Next 99 cars in 99 days

Example:
Consider there is a network having bandwidth of 1 Mbps. A message of size 1000 bytes has to be sent. Packet switching technique is used. Each packet contains a header of 100 bytes.

NOTE:
While calculating the total time, we often ignore the propagation delay.
The reason is in packet switching, transmission delay dominates over propagation delay.
This is because each packet is transmitted over the link at each hop.

Sending Message in 1 Packet-

In this case, the entire message is sent in a single packet.

Size Of Packet-

Packet size
= 1000 bytes of data + 100 bytes of header
= 1100 bytes

Transmission Delay-

Transmission delay
= Packet size / Bandwidth
= 1100 bytes / 1 MBps
= 1100×10^{-6} sec
= 1100 μsec
= 1.1 msec

Total Time Taken-

Total time taken to send the complete message from sender to receiver
= 3 x Transmission delay
= 3 x 1.1 msec
= 3.3 msec

Sending Message in 5 Packets-

In this case,
•The entire message is divided into total 5 packets.
•These packets are then sent one after the other.

Data Sent in One Packet-

Data sent in one packet
= Total data to be sent / Number of packets
= 1000 bytes / 5
= 200 bytes

Size Of One Packet-

Packet size
= 200 bytes of data + 100 bytes of header
= 300 bytes

Transmission Delay-

Transmission delay
= Packet size / Bandwidth
= 300 bytes / 1 MBps
= 300×10^{-6} sec
= 300 μsec
= 0.3 msec

Time Taken By First Packet-

Time taken by the first packet to reach from sender to receiver
= 3 x Transmission delay
= 3 x 0.3 msec
= 0.9 msec

Time Taken By Remaining Packets-

Time taken by the remaining packets to reach from sender to receiver
= Number of remaining packets x Transmission delay
= 4 x 0.3 msec
= 1.2 msec

Total Time Taken-

Total time taken to send the complete message from sender to receiver
= 0.9 msec + 1.2 msec
= 2.1 msec

Sending Data in 10 packets-

In this case,
•The entire message is divided into total 10 packets.
•These packets are then sent one after the other.

Data Sent in One Packet-

Data sent in one packet
= Total data to be sent / Number of packets
= 1000 bytes / 10
= 100 bytes

Size Of One Packet-

Packet size
= 100 bytes of data + 100 bytes of header
= 200 bytes

Transmission Delay-

Transmission delay
= Packet size / Bandwidth
= 200 bytes / 1 MBps
= 200×10^{-6} sec
= 200 µsec
= 0.2 msec

Time Taken By First Packet-

Time taken by the first packet to reach from sender to receiver
= 3 x Transmission delay
= 3 x 0.2 msec
= 0.6 msec

Time Taken By Remaining Packets-

Time taken by the remaining packets to reach from sender to receiver
= Number of remaining packets x Transmission delay
= 9 x 0.2 msec
= 1.8 msec

Total Time Taken-

Total time taken to send the complete message from sender to receiver
= 0.6 msec + 1.8 msec
= 2.4 msec

Sending Data in 20 Packets-

In this case,
•The entire message is divided into total 5 packets.
•These packets are then sent one after the other.

Data Sent in One Packet-

Data sent in one packet
= Total data to be sent / Number of packets
= 1000 bytes / 20
= 50 bytes

Size Of One Packet-

Packet size
= 50 bytes of data + 100 bytes of header
= 150 bytes

Transmission Delay-

Transmission delay
= Packet size / Bandwidth
= 150 bytes / 1 MBps
= 150×10^{-6} sec
= 150 μsec
= 0.15 msec

Time Taken By First Packet-

Time taken by the first packet to reach from sender to receiver
= 3 x Transmission delay
= 3 x 0.15 msec
= 0.45 msec

Time Taken By Remaining Packets-

Time taken by the remaining packets to reach from sender to receiver
= Number of remaining packets x Transmission delay
= 19 x 0.15 msec
= 2.85 msec

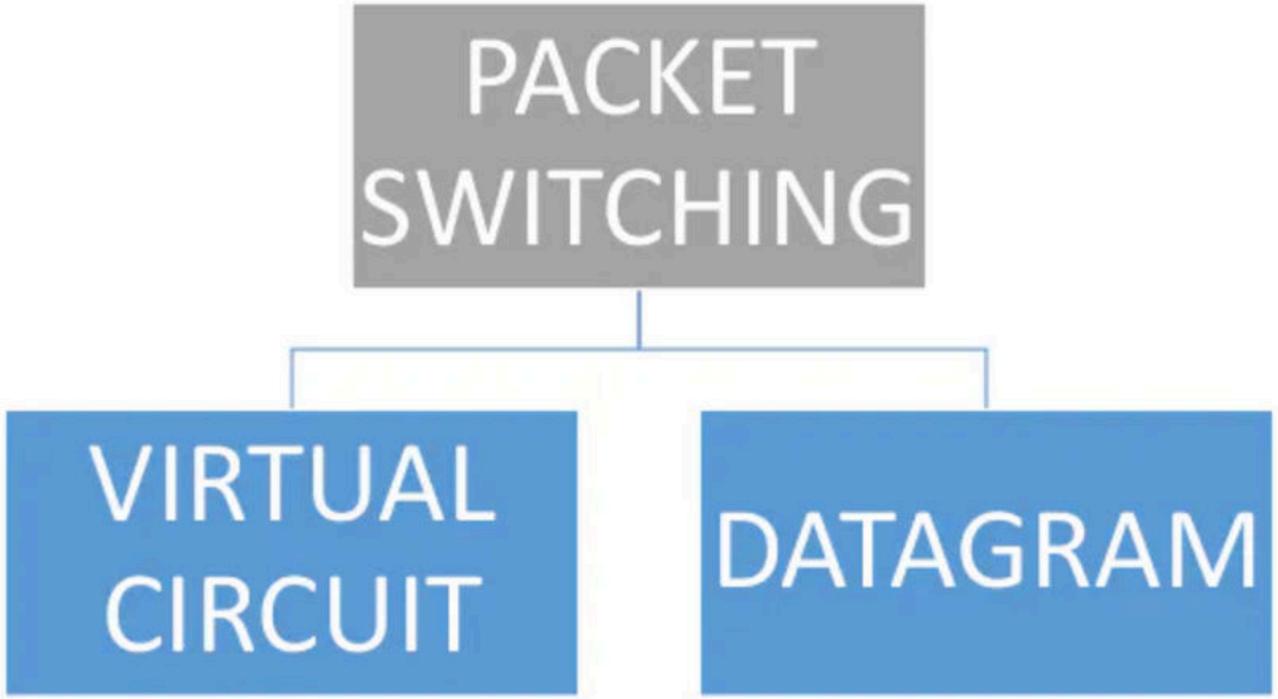
Total Time Taken-

Total time taken to send the complete message from sender to receiver
= 0.45 msec + 2.85 msec
= 3.3 msec

- When data is sent in 1 packet, total time taken = 3.3 msec
- When data is sent in 5 packets, total time taken = 2.1 msec
- When data is sent in 10 packets, total time taken = 2.4 msec
- When data is sent in 20 packets, total time taken = 3.3 msec

We conclude-
Total time decreases when packet size is reduced but only up to a certain limit.
If the packet size is reduced beyond a certain limit, then total time starts increasing.

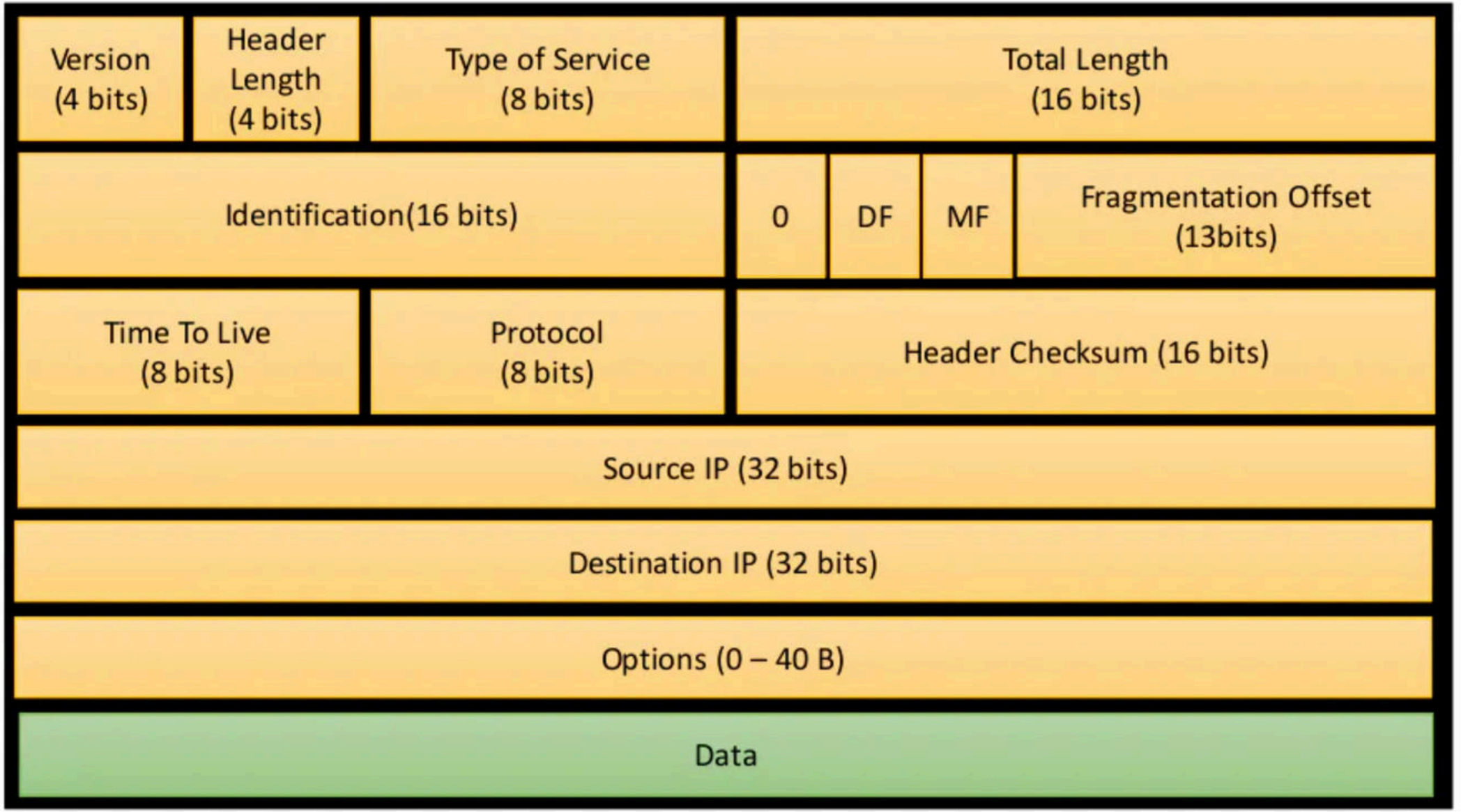
From the given choices,
Sending the message in 5 packets would be most efficient.
In other words, packet size = 300 bytes would be the best choice.


PACKET SWITCHING
VIRTUAL CIRCUIT
DATAGRAM

Virtual Circuit Switching	Datagram Switching
The first packet during its transmission- 1) Informs the intermediate switches that more packets are following. 2) Reserve resources (CPU, bandwidth and buffer) for the following packets at all the switches on the way.	The first packet does not perform any such task during its transmission.
The packets are never discarded at intermediate switches and immediately forwarded since resources are reserved for them.	The packets may be discarded at intermediate switches if sufficient resources are not available to process the packets.
It is a connection oriented service.	It is a connection less service.
All the packets follow the same dedicated path.	All the packets take path independently.
Data appears in order at the destination since all the packets take the same dedicated path.	Data may appear out of order at the destination since the packets take path independently.
It is highly reliable	It is not reliable since packets may be discarded.
It is costly.	It is cost effective.
Only first packet requires a global header which identifies the path from one end to other end. All the following packets require a local header which identifies the path from hop to hop.	All the packets require a global header which contains full information about the destination.
ATM (Asynchronous Transfer Mode) uses virtual circuit switching.	IP Networks use datagram switching.
Virtual circuit switching is normally implemented at data link layer.	Datagram switching is normally implemented at network layer.

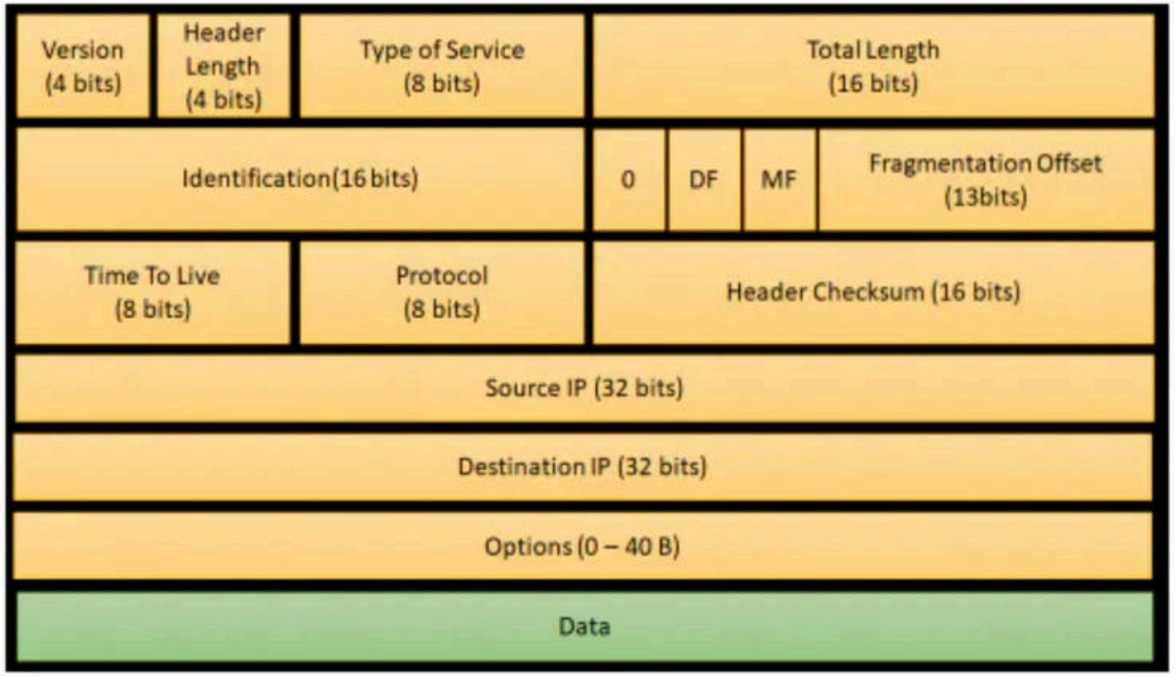
Computer Networks

IPV4


Version (4 bits)
Header Length (4 bits)
Type of Service (8 bits)
Total Length (16 bits)
Identification(16 bits)
0
DF
MF
Fragmentation Offset (13bits)
Time To Live (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)
Source IP (32 bits)
Destination IP (32 bits)
Options (0 – 40 B)
Data

Version

•Version is a 4 bit field that indicates the IP version used.
•The most popularly used IP versions are version-4 (IPv4) and version-6 (IPv6).
•Only IPv4 uses the above header.
•So, this field always contains the decimal value 4.



Header Length

•Header length is a 4 bit field that contains the length of the IP header.
•It helps in knowing from where the actual data begins.

Header length = Header length field value x 4 bytes

Ex. If header length field contains decimal value 5 (represented as 0101), then-

Header length = 5 x 4 = 20 bytes

Minimum And Maximum Header Length-

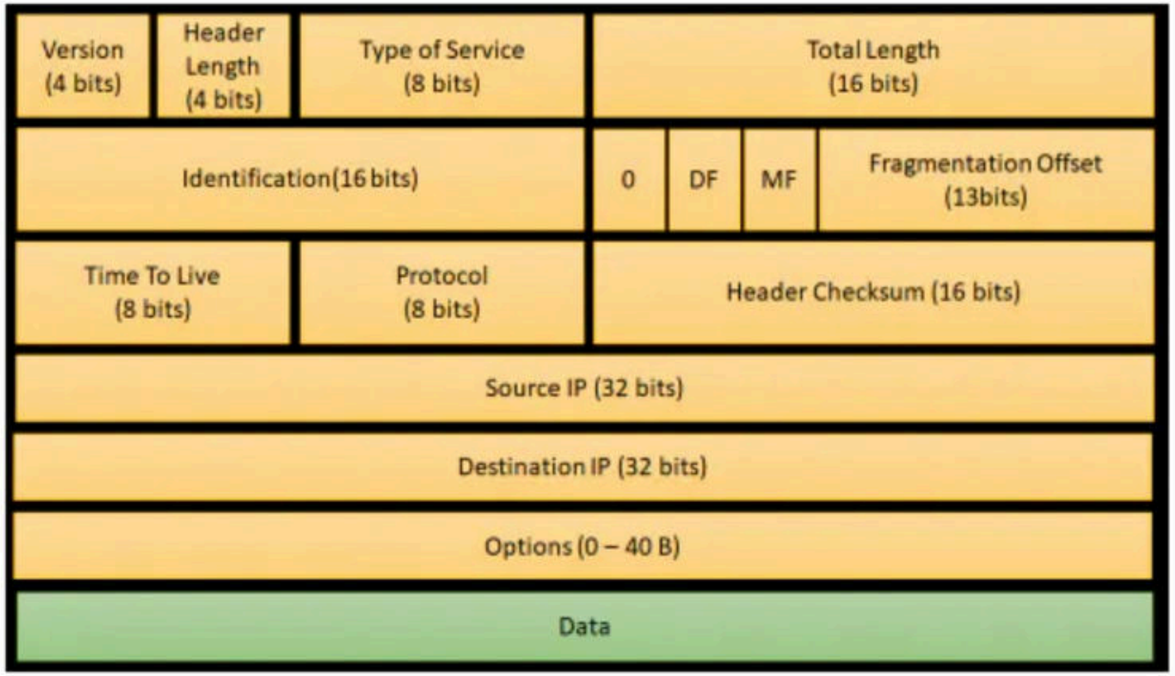
The length of IP header always lies in the range-

[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 the 6th row representing the Options field vary.
•The size of Options field can go up to 40 bytes.
•So, maximum length of IP header = 20 bytes + 40 bytes = 60 bytes.

Type Of Service

•Type of service is a 8 bit field that is used for Quality of Service (QoS).
•The datagram is marked for giving a certain treatment using this field.



Total Length

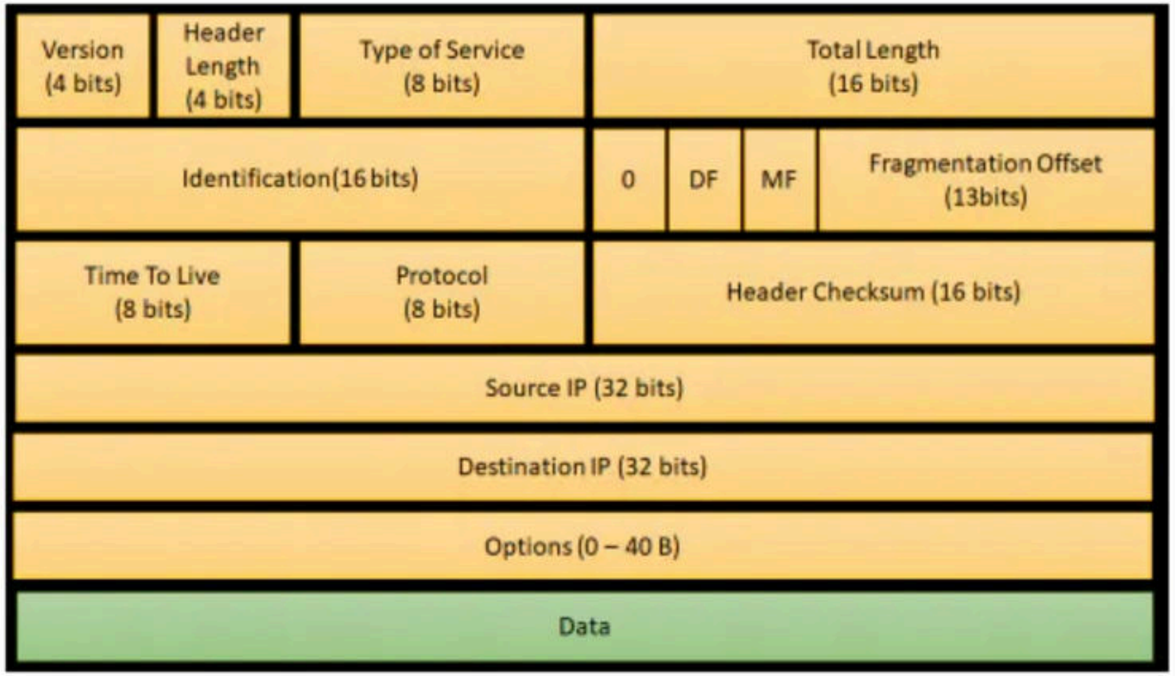
•Total length is a 16 bit field that contains the total length of the datagram (in bytes).

Total length = Header length + Payload length

•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

Identification

•Identification is a 16 bit field.
•It is used for the identification of the fragments of an original IP datagram.



DF Bit

•DF bit stands for Do Not Fragment bit.
•Its value may be 0 or 1.

When DF bit is set to 0,

•It grants the permission to the intermediate devices to fragment the datagram if required.

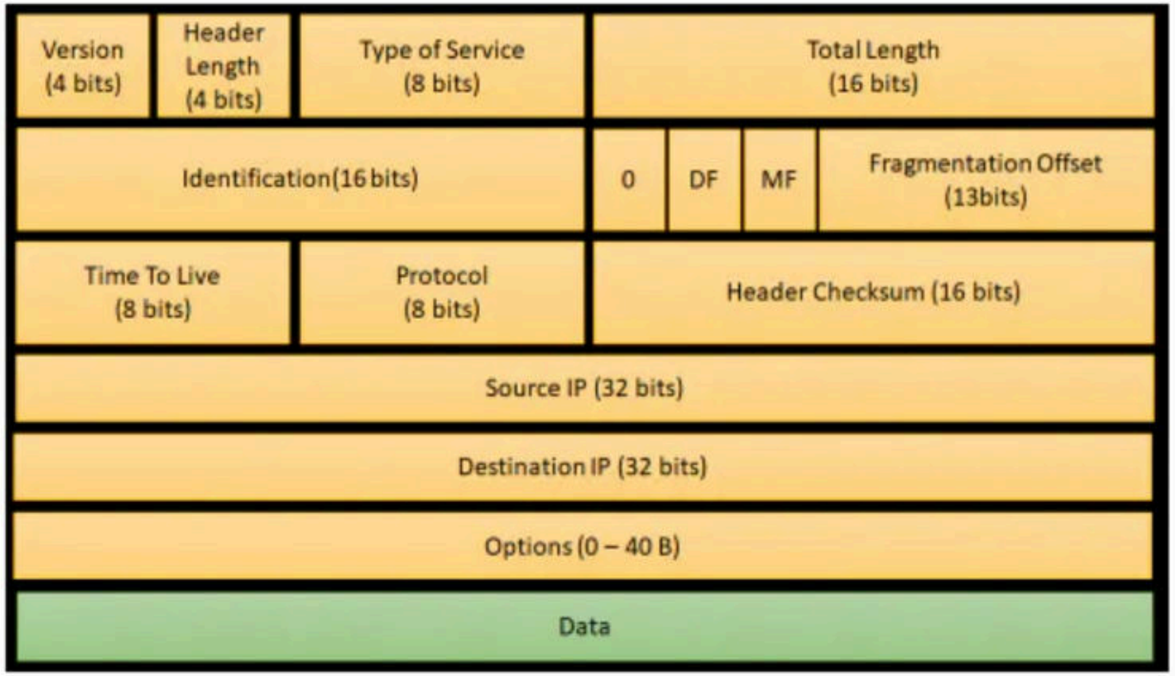
When DF bit is set to 1,
•It indicates the intermediate devices not to fragment the IP datagram at any cost.
•If network requires the datagram to be fragmented to travel further but settings does not allow its fragmentation, then it is discarded.
•An error message is sent to the sender saying that the datagram has been discarded due to its settings.

MF Bit

•MF bit stands for More Fragments bit.
•Its value may be 0 or 1.

When MF bit is set to 0,
•It indicates to the receiver that the current datagram is either the last fragment in the set or that it is the only fragment.

When MF bit is set to 1,
•It indicates to the receiver that the current datagram is a fragment of some larger datagram.
•More fragments are following.
•MF bit is set to 1 on all the fragments except the last one.



Fragment Offset

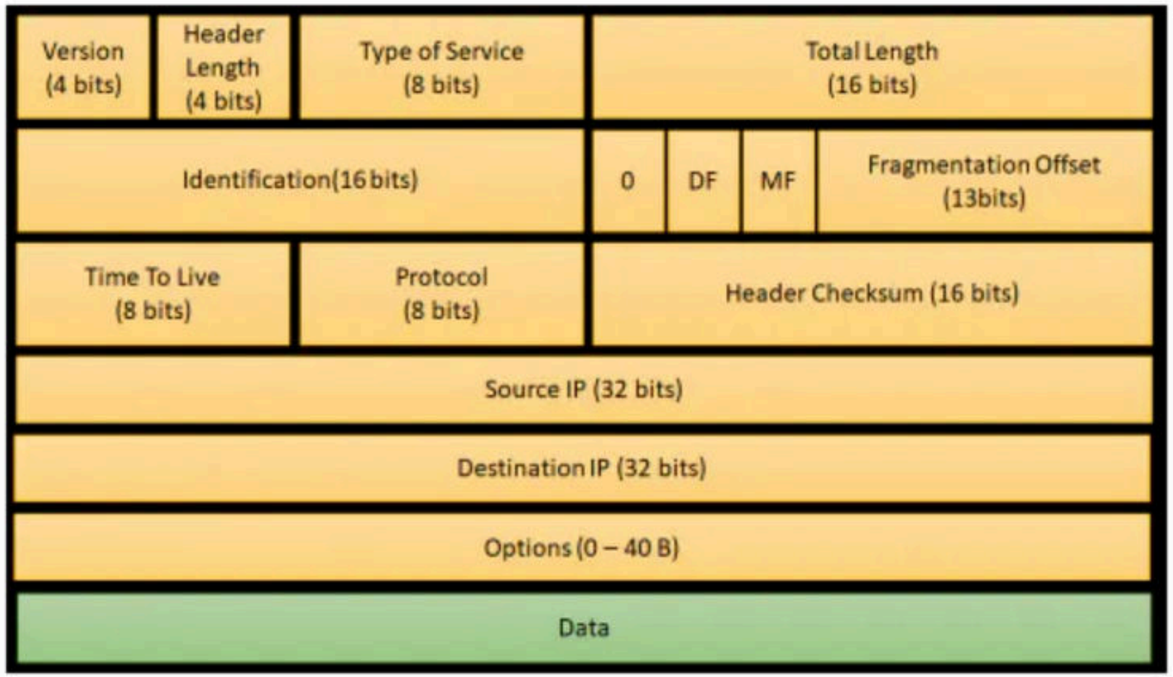
•Fragment Offset is a 13 bit field.
•It indicates the position of a fragmented datagram in the original unfragmented IP datagram.
•The first fragmented datagram has a fragment offset of zero.

Fragment offset for a given fragmented datagram
= Number of data bytes ahead of it in the original unfragmented datagram

Time To Live

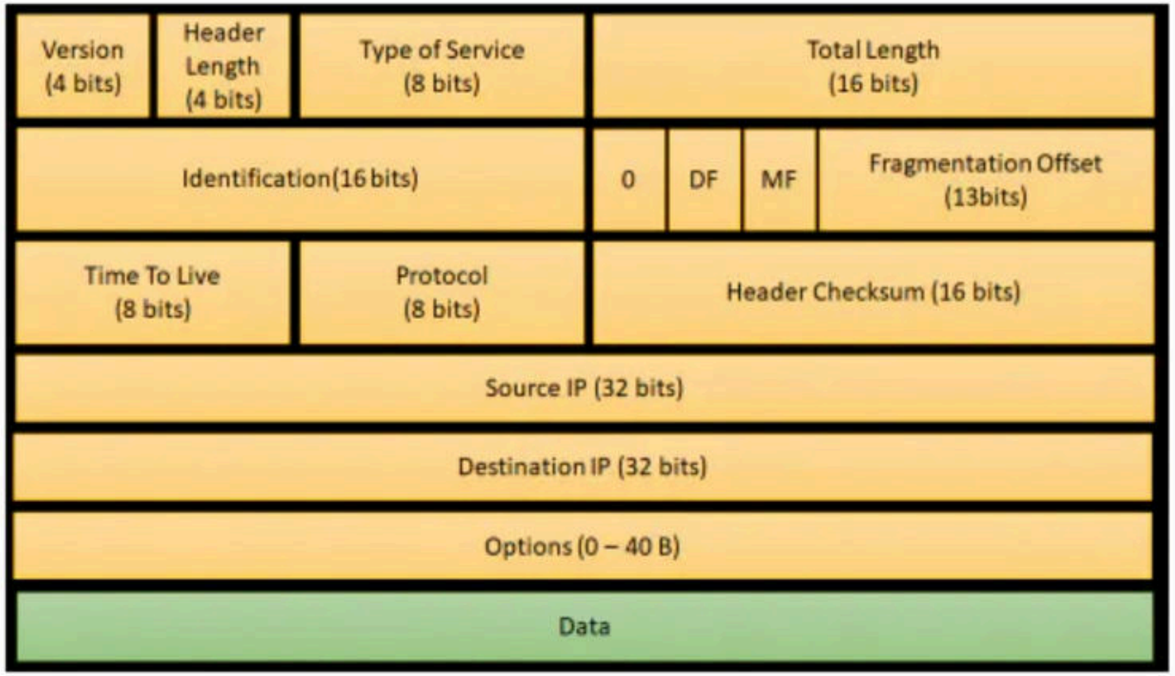
•Time to live (TTL) is a 8 bit field.
•It indicates the maximum number of hops a datagram can take to reach the destination.
•The main purpose of TTL is to prevent the IP datagrams from looping around forever in a routing loop.

The value of TTL is decremented by 1 when-
•Datagram takes a hop to any intermediate device having network layer.
•Datagram takes a hop to the destination.



Protocol

•Protocol is a 8 bit field.
•It tells the network layer at the destination host to which protocol the IP datagram belongs to.
•In other words, it tells the next level protocol to the network layer at the destination side.
•Protocol number of ICMP is 1, IGMP is 2, TCP is 6 and UDP is 17.



Why Protocol Number Is A Part Of IP Header?

Consider-
•An IP datagram is sent by the sender to the receiver.
•When datagram reaches at the router, it's buffer is already full.

In such a case,
•Router does not discard the datagram directly.
•Before discarding, router checks the next level protocol number mentioned in its IP header.
•If the datagram belongs to TCP, then it tries to make room for the datagram in its buffer.
•It creates a room by eliminating one of the datagrams having lower priority.
•This is because it knows that TCP is a reliable protocol and if it discards the datagram, then it will be sent again by the sender.
•The order in which router eliminate the datagrams from its buffer is-

ICMP > IGMP > UDP > TCP

If protocol number would have been inside the datagram, then-
•Router could not look into it.
•This is because router has only three layers- physical layer, data link layer and network layer.

That is why, protocol number is made a part of IP header.

Header Checksum

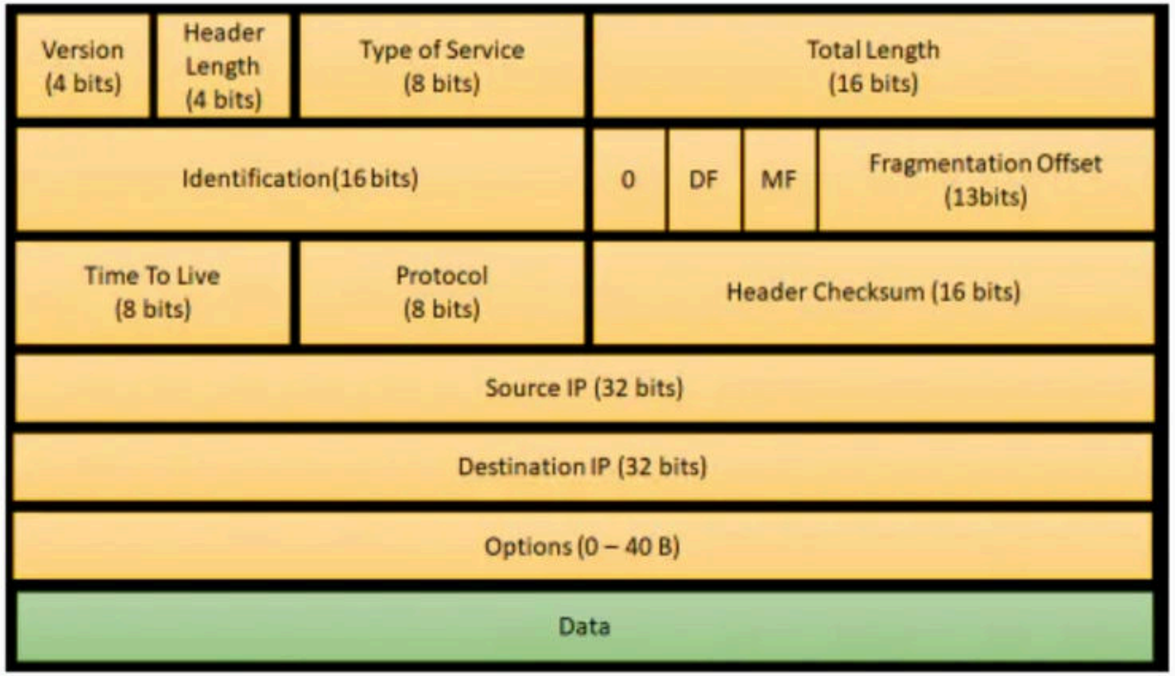
- Header checksum is a 16 bit field.
- It contains the checksum value of the entire header.
- The checksum value is used for error checking of the header.

At each hop,

- The header checksum is compared with the value contained in this field.
- If header checksum is found to be mismatched, then the datagram is discarded.
- Router updates the checksum field whenever it modifies the datagram header.

The fields that may be modified are-

1. TTL
2. Options
3. Datagram Length
4. Header Length
5. Fragment Offset



Source IP Address

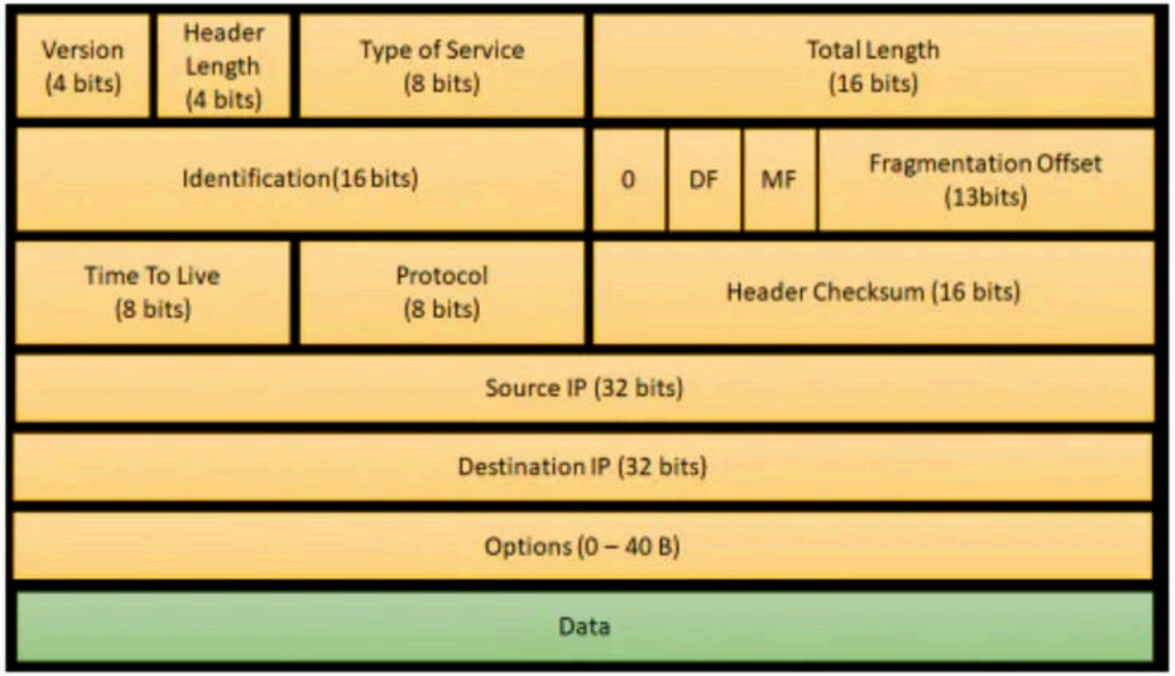
•Source IP Address is a 32 bit field.
•It contains the logical address of the sender of the datagram.

Destination IP Address

•Destination IP Address is a 32 bit field.
•It contains the logical address of the receiver of the datagram.

Options

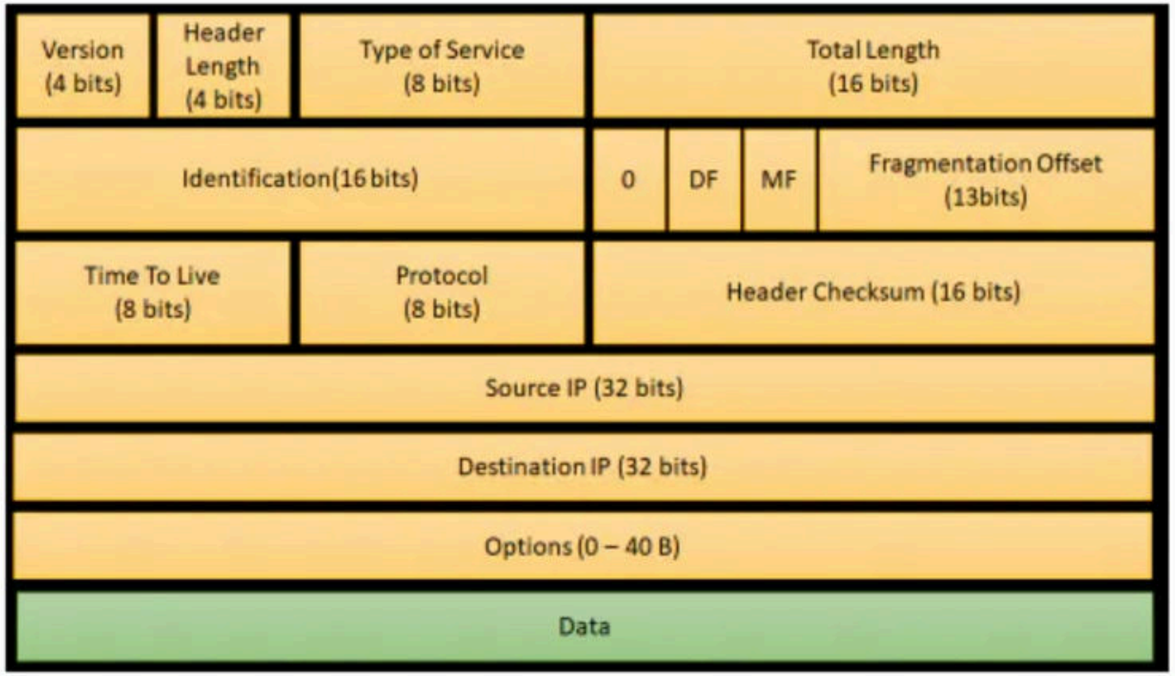
•Options is a field whose size vary from 0 bytes to 40 bytes.
•This field is used for several purposes such as-
1.Record route
2.Source routing
3.Padding



1. Record Route-

•A record route option is used to record the IP Address of the routers through which the datagram passes on its way.
•When record route option is set in the options field, IP Address of the router gets recorded in the Options field.

The maximum number of IPv4 router addresses that can be recorded in the Record Route option field of an IPv4 header is 9.



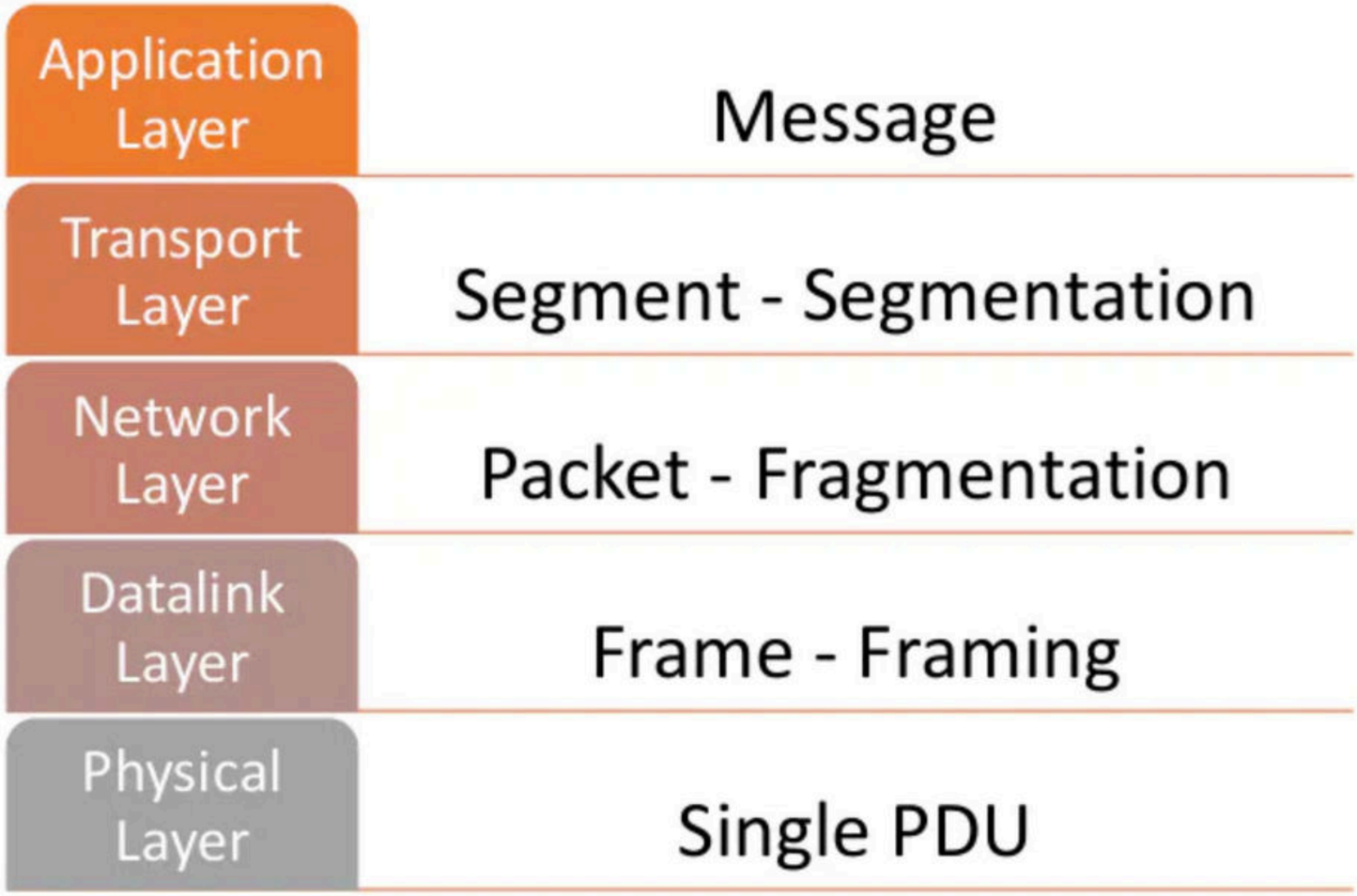
2. Source Routing-

•A source routing option is used to specify the route that the datagram must take to reach the destination.
•This option is generally used to check whether a certain path is working fine or not.
•Source routing may be loose or strict.

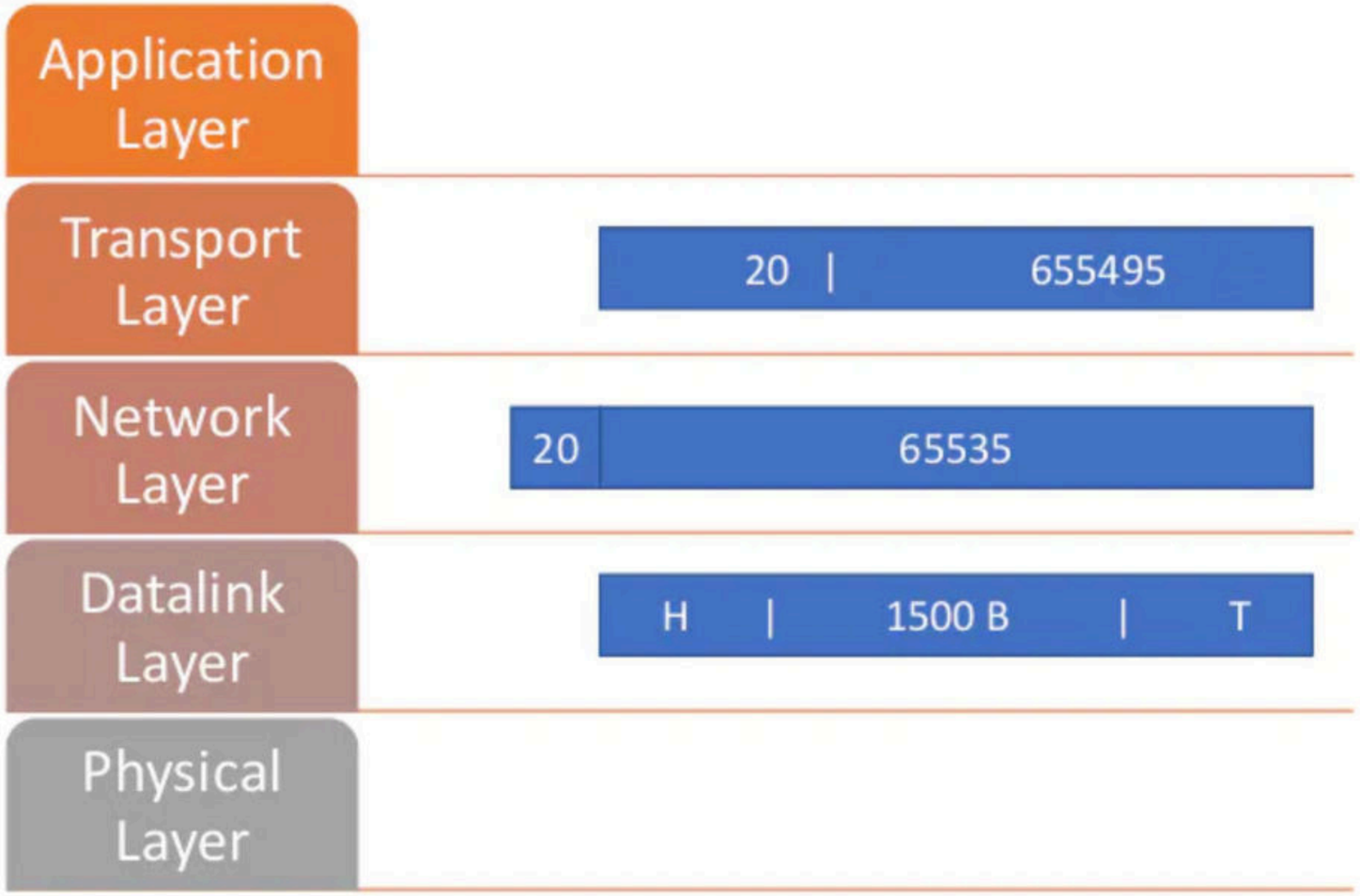
3. Padding-

•Addition of dummy data to fill up unused space in the transmission unit and make it conform to the standard size is called as padding.
•Options field is used for padding.

Computer Networks


Application Layer
Message
Transport Layer
Segment - Segmentation
Network Layer
Packet - Fragmentation
Datalink Layer
Frame - Framing
Physical Layer
Single PDU

Example: Segmentation and Fragmentation



SEGMENTATION AND FRAGMENTATION

This occurs during the original creation of the packets when a set of data doesn't fit within the "Maximum Segment Size (MSS)".
The data is then divided into multiple segments referred as "Protocol Data Unit". This process is known as **Segmentation.**

In order to avoid Fragmentation (which we will see further) , note that
(Number of bytes in the data segment + the header) < MTU

Fragmentation occurs during the original creation of frames where the network layer must send packets down to the Data Link Layer for transmission. Some Data Link Layer technologies have limits on the length of the data that can be sent. In short some links have smaller MTU (Maximum Transmission Unit).
If the packet that is to be sent is larger than the MTU then it is divided into pieces.
This process is known as fragmentation.
These pieces are reassembled once they arrive at the network layer of the destination.
As mentioned earlier Fragmentation can be avoided if,
(Number of bytes in the data segment + the header) < MTU

Computer Networks

Reassembly Algorithm

Reassembly Algorithm

Receiver applies the following steps for reassembly of all the fragments-

1.It identifies whether datagram is fragmented or not using MF bit and Fragment offset field.

2.It identifies all the fragments belonging to the same datagram using identification field.

3.It identifies the first fragment. Fragment with offset field value = 0 is the first fragment.

4.It identifies the subsequent fragments using total length, header length and fragment offset.

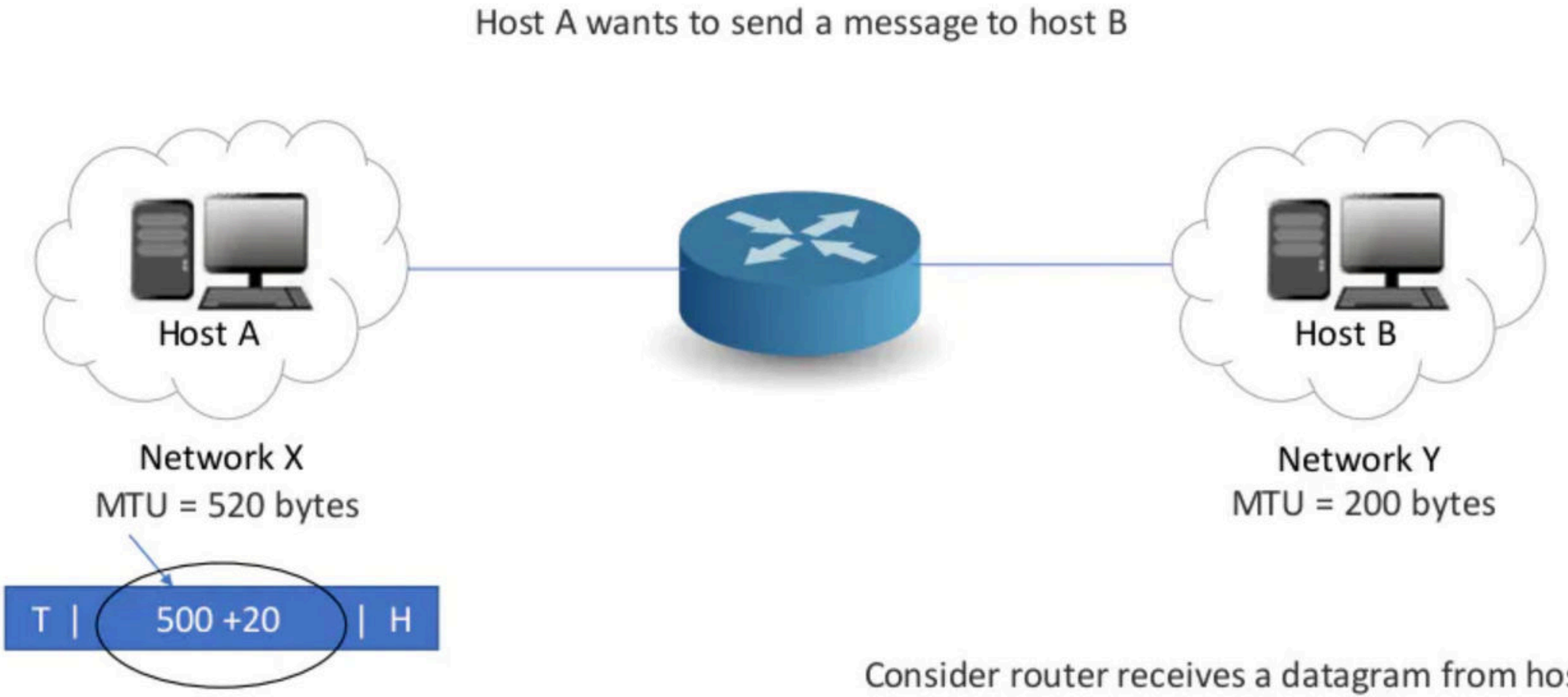
5.It repeats step-04 until MF bit = 0.

Computer Networks

Fragmentation

Lets us discuss some examples of IP fragmentation to understand how the fragmentation is actually carried out.

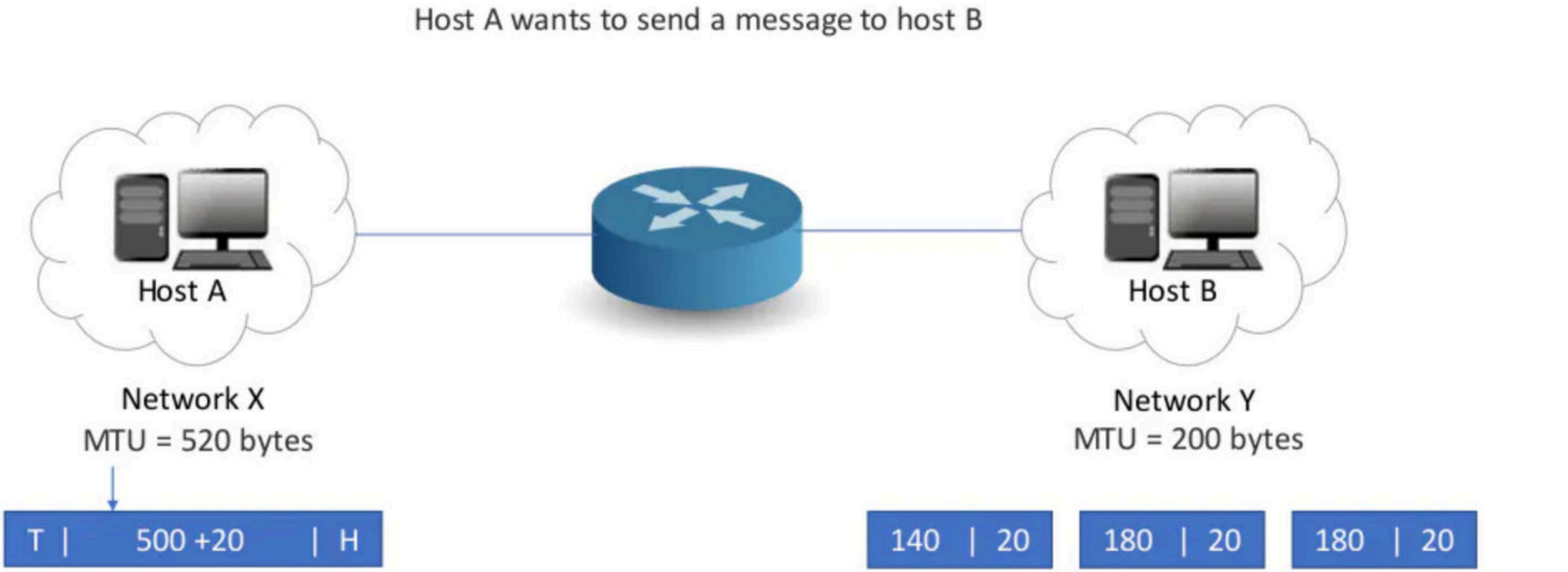
EXAMPLE 1



Consider router receives a datagram from host A having-
Header length = 20 bytes
Payload length = 500 bytes
Total length = 520 bytes

Lets us discuss some examples of IP fragmentation to understand how the fragmentation is actually carried out.

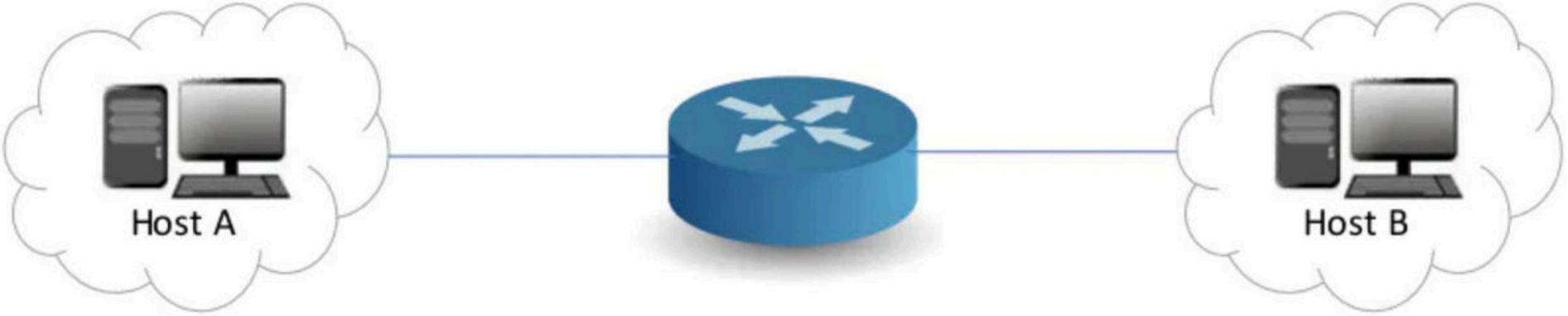
EXAMPLE 1



The amount of data sent in one fragment is chosen such that-
It is as large as possible but less than or equal to MTU.
It is a multiple of 8 so that pure decimal value can be obtained for the fragment offset field.

NOTE

- It is not compulsory for the last fragment to contain the amount of data that is a multiple of 8.
- This is because it does not have to decide the fragment offset value for any other fragment.



Network X
MTU = 520 bytes

500 +20

Network Y
MTU = 200 bytes

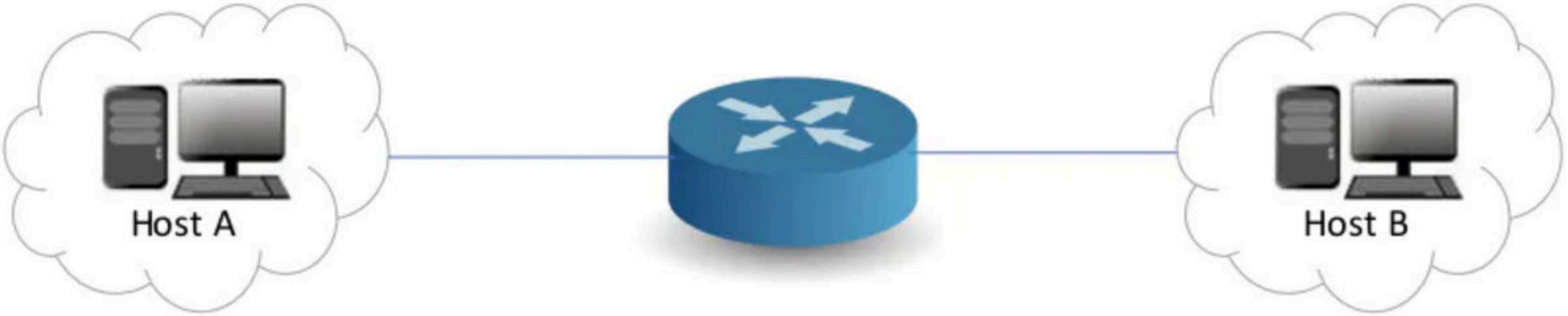
Following the above rule,
Router decides to send maximum 176 bytes of data in one fragment.
This is because it is the greatest value that is a multiple of 8 and less than MTU.

Router creates three fragments of the original datagram where-

First fragment contains the data = 176 bytes

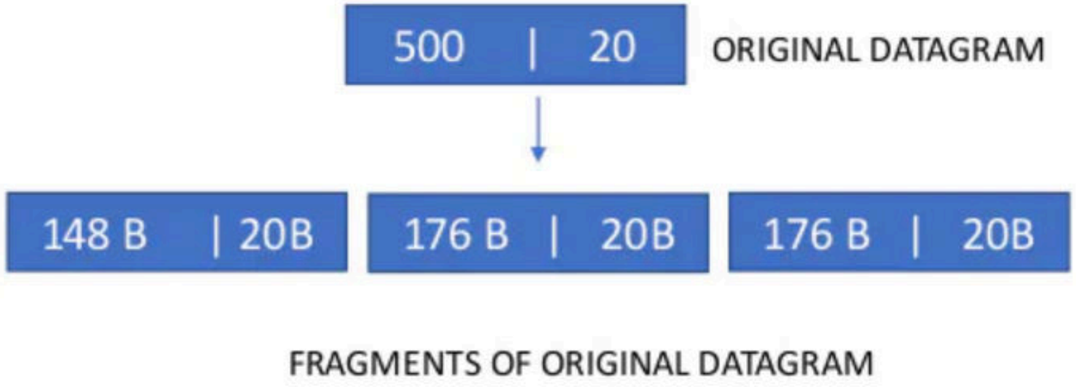
Second fragment contains the data = 176 byes

Third fragment contains the data = 148 bytes



Network X
MTU = 520 bytes

Network Y
MTU = 200 bytes



The information contained in the IP header of each fragment is-

Header Information Of 1st Fragment-

- Header length field value = 20 / 4 = 5
- Total length field value = 176 + 20 = 196
- MF bit = 1
- Fragment offset field value = 0
- Header checksum is recalculated.
- Identification number is same as that of original datagram.

Header Information Of 2nd Fragment-

- Header length field value = 20 / 4 = 5
- Total length field value = 176 + 20 = 196
- MF bit = 1
- Fragment offset field value = 176 / 8 = 22
- Header checksum is recalculated.
- Identification number is same as that of original datagram.

Header Information Of 3rd Fragment-

- Header length field value = 20 / 4 = 5
- Total length field value = 148 + 20 = 168
- MF bit = 0
- Fragment offset field value = (176 + 176) / 8 = 44
- Header checksum is recalculated.
- Identification number is same as that of original datagram.

Router transmits all the fragments.

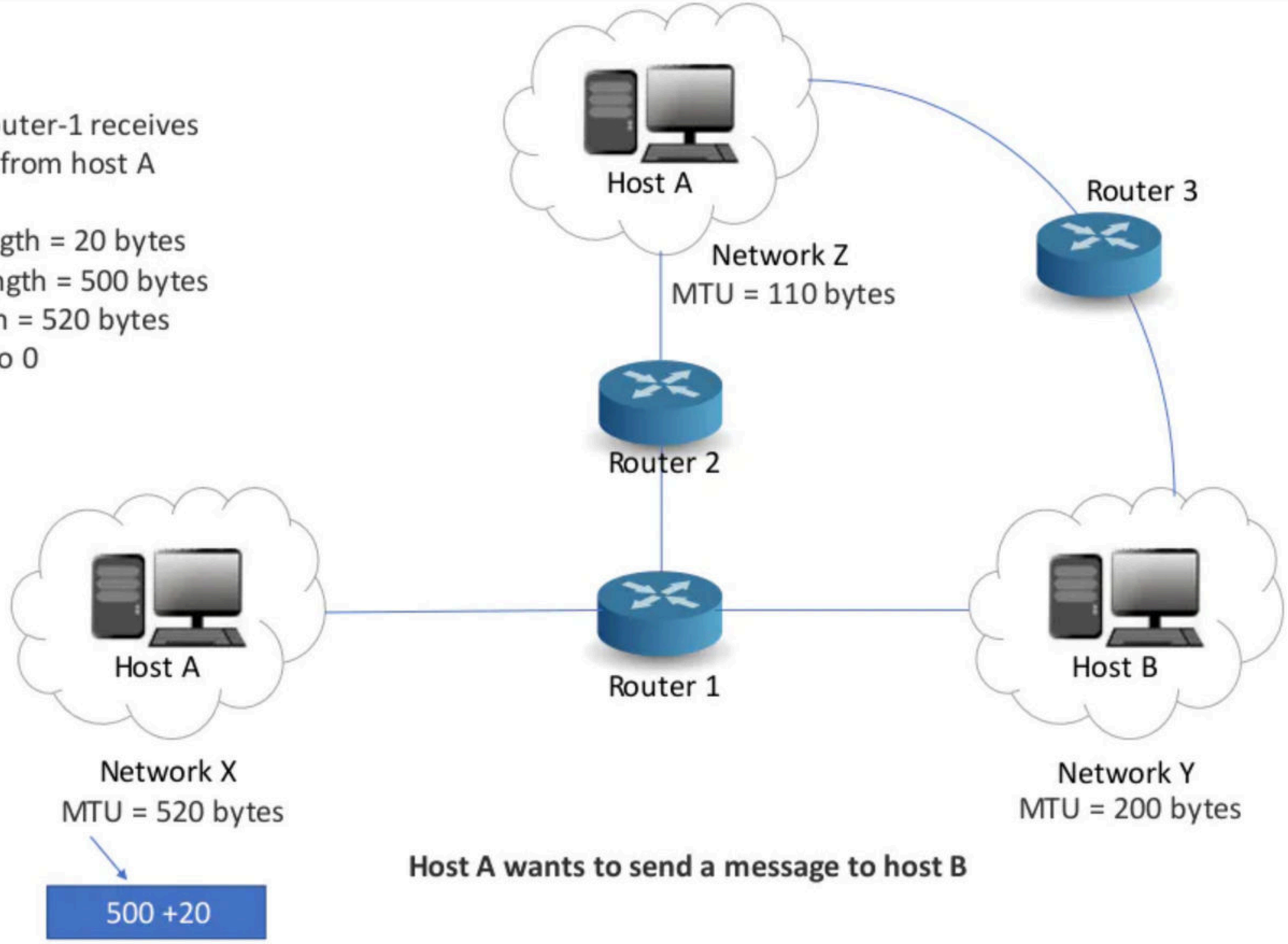
At destination side,

- Receiver receives 3 fragments of the datagram.
- Reassembly algorithm is applied to combine all the fragments to obtain the original datagram.

EXAMPLE 2

Consider Router-1 receives a datagram from host A having-

- Header length = 20 bytes
- Payload length = 500 bytes
- Total length = 520 bytes
- DF bit set to 0

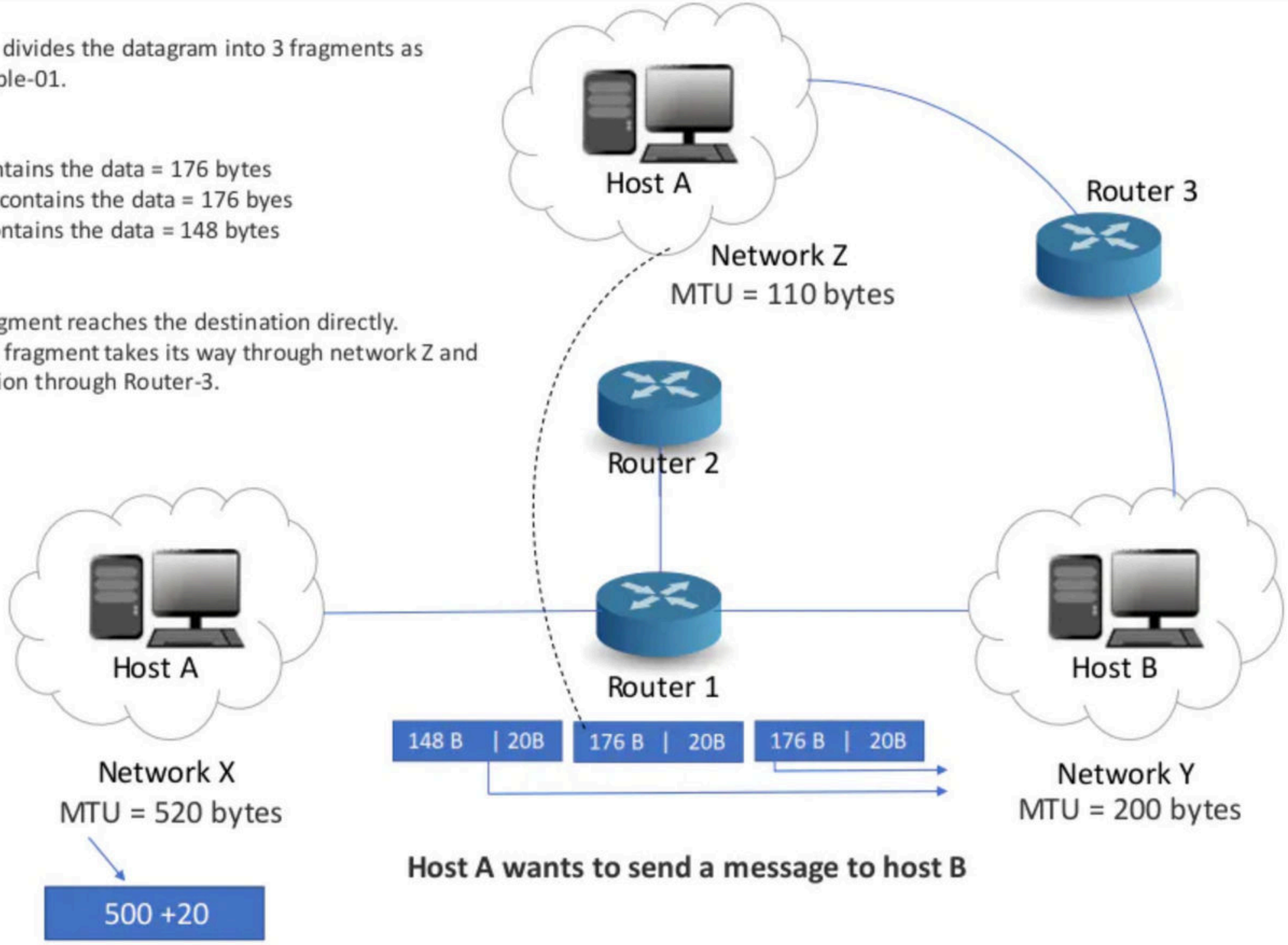


Host A wants to send a message to host B

Consider Router-1 divides the datagram into 3 fragments as discussed in Example-01.

Then,
- First fragment contains the data = 176 bytes
- Second fragment contains the data = 176 byes
- Third fragment contains the data = 148 bytes

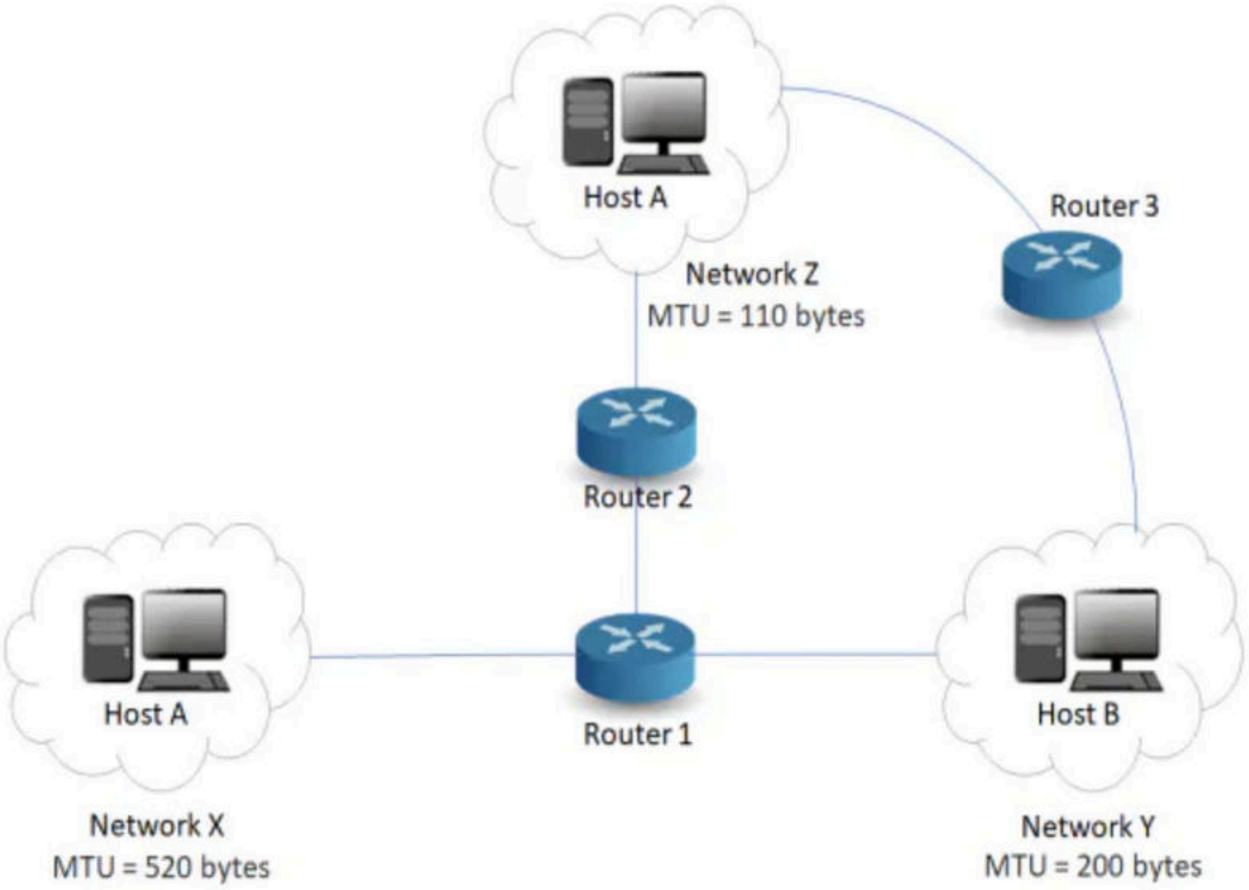
Now, consider-
- First and third fragment reaches the destination directly.
- However, second fragment takes its way through network Z and reach the destination through Router-3.



Now, let us discuss the journey of fragment-2 and how it finally reaches the destination.

Router-2 receives a datagram (second fragment of original datagram) where-

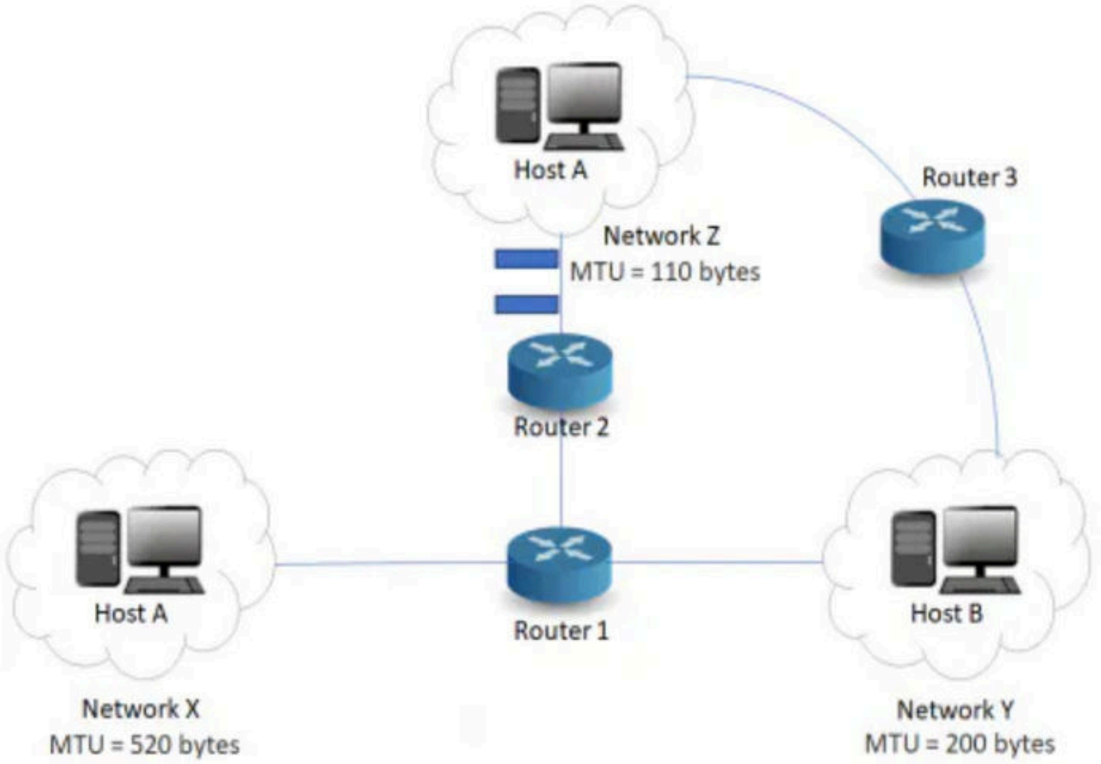
- Header length = 20 bytes
- Payload length = 176 bytes
- Total length = 196 bytes
- DF bit set to 0



Step-01:

Router-2 examines the datagram and finds-
•Size of the datagram = 196 bytes
•Destination is network Z having MTU = 110 bytes
•DF bit is set to 0

Router-2 concludes-
•Size of the datagram is greater than MTU.
•So, it will have to divide the datagram into fragments.
•DF bit is set to 0.
•So, it is allowed to create fragments of the datagram.



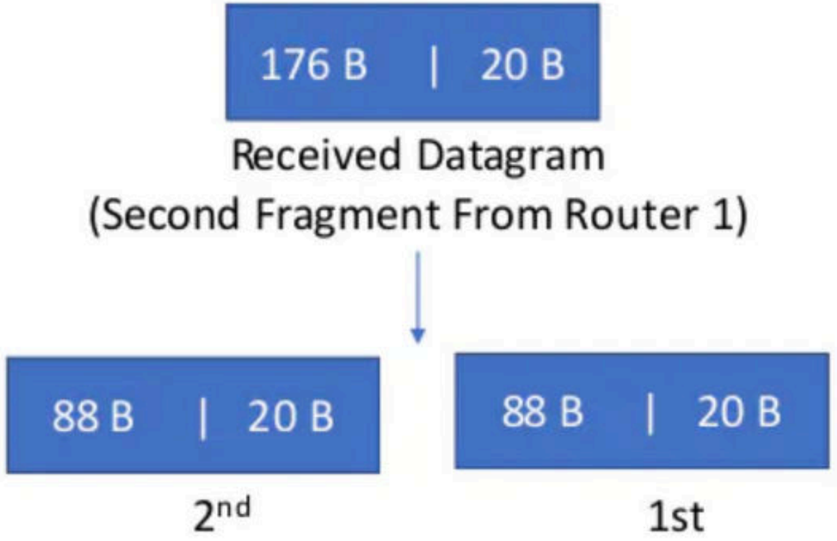
Step-02:

Router-2 decides the amount of data that it should transmit in each fragment.

Router-2 knows-
•MTU of the destination network = 110 bytes.
•So, maximum total length of any fragment can be only 110 bytes.
•Out of 110 bytes, 20 bytes will be taken by the header.
•So, maximum amount of data that can be sent in any fragment = 90 bytes.

Following the rule,
•Router-2 decides to send maximum 88 bytes of data in one fragment.
•This is because it is the greatest value that is a multiple of 8 and less than MTU.

Router-2 creates two fragments of the received datagram where-



The information contained in the IP header of each fragment is-

Header Information Of 1st Fragment-

- Header length field value = 20 / 4 = 5
- Total length field value = 88 + 20 = 108
- MF bit = 1
- Fragment offset field value = 176 / 8 = 22
- Header checksum is recalculated.
- Identification number is same as that of original datagram.

NOTE-

- This fragment is **NOT** the first fragment of the original datagram.
- It is the first fragment of the datagram received by Router-2.
- The datagram received by Router-2 is the second fragment of the original datagram.
- This datagram will serve as the second fragment of the original datagram.
- Therefore, fragment offset field is set according to the first fragment of the original datagram.

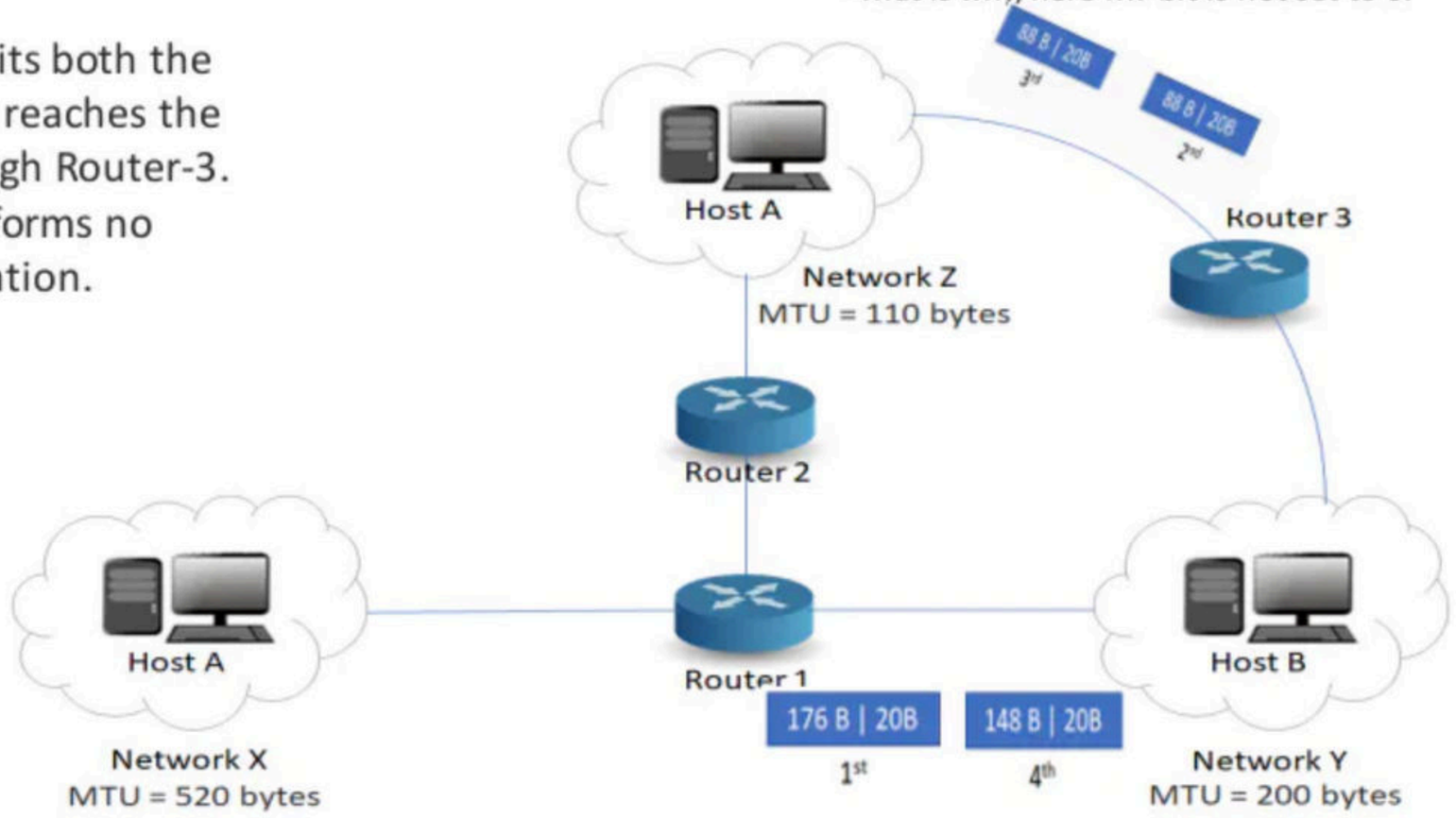
Header Information Of 2nd Fragment-

- Header length field value = 20 / 4 = 5
- Total length field value = 88 + 20 = 108
- MF bit = 1
- Fragment offset field value = (176 + 88) / 8 = 33
- Header checksum is recalculated.
- Identification number is same as that of original datagram.

Router-2 transmits both the fragments which reaches the destination through Router-3. Router-3 performs no fragmentation.

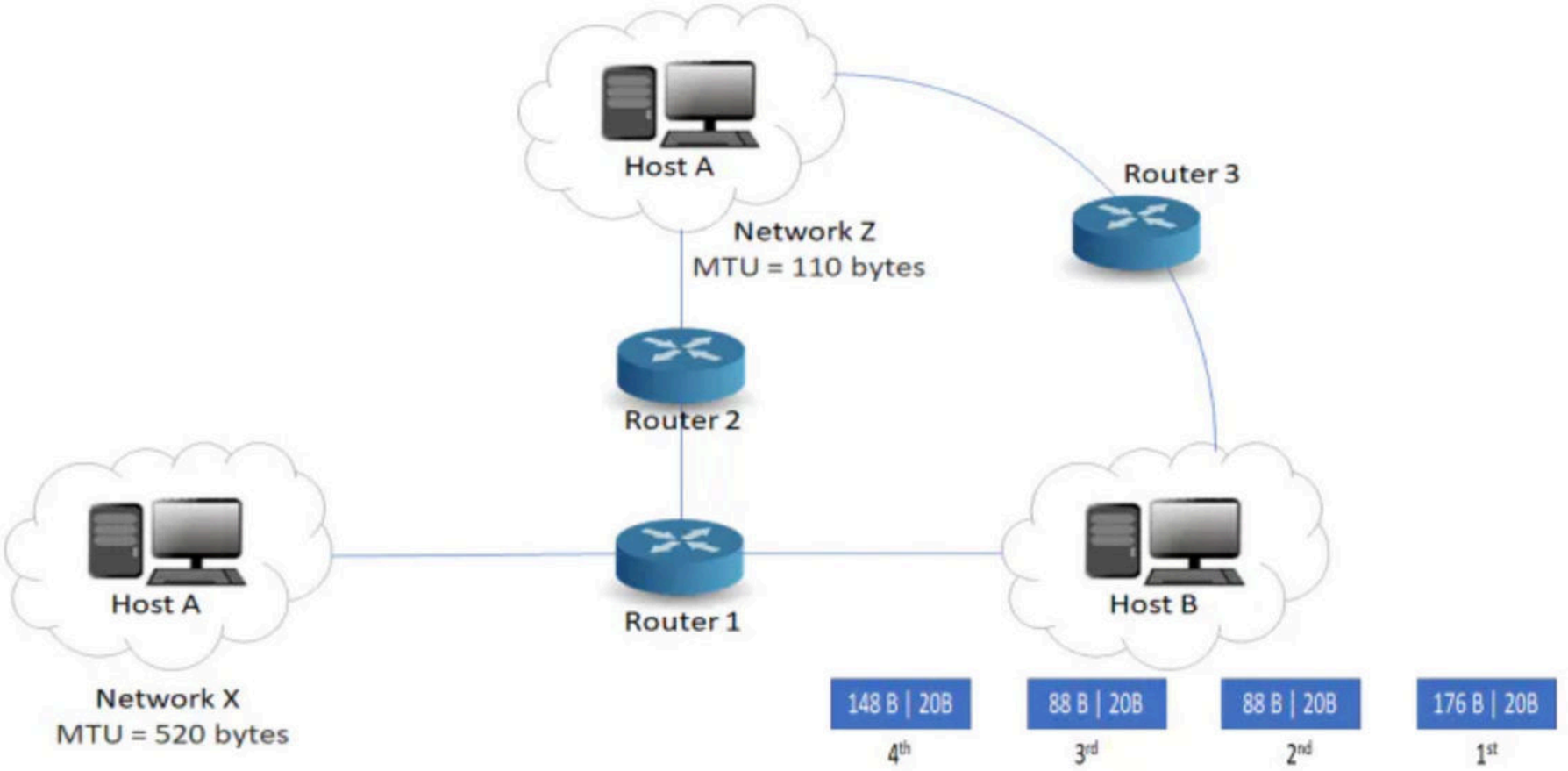
NOTE-

- This fragment is **NOT** the last fragment of the original datagram.
- It is the last fragment of the datagram received by Router-2.
- The datagram received by Router-2 is the second fragment of the original datagram.
- This datagram will serve as the third fragment of the original datagram.
- There is another fragment of the original datagram that follows it.
- That is why, here MF bit is not set to 0.



At destination side,

- Receiver receives 4 fragments of the datagram.
- Reassembly algorithm is applied to combine all the fragments to obtain the original datagram.



Fragment Offset field value for the next subsequent fragment
= (Payload length of the current fragment / 8) + Offset field value of the current fragment
= (Total length – Header length / 8) + Offset field value of the current fragment

Fragmentation Overhead

- Fragmentation of datagram increases the overhead.
- This is because after fragmentation, IP header has to be attached with each fragment.

Total Overhead
= (Total number of fragmented datagrams – 1) x size of IP header

Efficiency = Useful bytes transferred / Total bytes transferred
OR
Efficiency = Data without header / Data with header

Bandwidth Utilization or Throughput = Efficiency x Bandwidth

NOTE:

MF bit	Offset value	Represents
1	0	1st Fragment
1	!=0	Intermediate Fragment
0	!=0	Last Fragment
0	0	No Fragmentation

Reassembly is not done at the routers because-

All the fragments may not meet at the router.

Fragmented datagrams may reach the destination through independent paths.

There may be a need for further fragmentation.