IP V4 / IP Header / IP datagram :-

VER	HLEN	DS	Total length
4 bits	4 bits	8 bits	16 bits
Identification		Flags	Fragmentation offset
16 bits		3 bits	13 bits
Time to Live	Protocol	Header checksum	
8 bits	8 bits	16 bits	
Source IP address			
Destination IP address			
Option			
Data			

1) VER (Version)
- It tells which version of IP is used.
- VER = 4 (IPV4)
- VER = 6 (IPV6)

4 bits = 2^4 = 16 (0-15)
[15 × 4 = 60]

2) HLEN
- It contains value which when multiplied by four give header length
for Eg. HLEN = 5
∴ Header length = 20 B (5×4) bytes

Minimum header length is of 20 bytes, In presence of options, It varies between 20B to 60B.

3) DS (Differentiated Services)
It tells whether any special type of service is requi to deliver the packet between sender & receiver.

D: Minimize delay R: Maximize reliability
T: Maximize throughput C: Minimize cost

X	X	X	D	T	R	C	X

Don't care (left) — Don't care (right)
Precedence — TOS Bits

Types of services

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

4) Total length
- It is responsible to give the total size of the packet.
Total length = Header length + Data length.

5) Fragmentation fields
① Identification
② Flags
③ Fragmentation offset
} Refer fragmentation.

6) Time to Live (TTL)
- This field limits unnecessary IP packet wandering ie the packet is routing in the network without reaching the destination.
- Router accepts the packet, checks the value of TTL, if TTL is zero, discards the packet else decrements TTL by one and pass it to the next router.

7) Protocol
It tells which protocol is responsible to handle this data.

Protocols

Value	Protocol	
1	ICMP	Internet Control Management Protocol
2	IGMP	
6	TCP	
17	UDP	
89	OSPF	Open shortest path first

8) Checksum
- It is used for error detection to find a error (noise) is added in the header.

9) Source IP and Destination IP
It is 32 bit IP address of sender and

V.V.Imp FRAGMENTATION :-

- The process of dividing the packets into packets known as fragments is known as fragmentation.

- MTU (Maximum Transfer Unit) tells whe the packet should be fragmented or not (At sending side).

- MTU knows the network carrying capacity and depending on the size of the packet the fragmentation decision is taken.

If packet size > network carrying capacit then do the fragmentation.

Tuesday
2/08/17

Fragmentation fields in IPV4 He

1. Identification :-
In network every packet is uniquely identified b identification number

and every fragment of the same packet would be assigned with same identification number which would help for reassembly at receiving side

Note : Order of sending the fragment & receiving the fragment is not same as all fragments may follow different paths to reach the destination

Flags:

X	DF	MF

DF : Do not fragment.
MF : More fragment.
X : Don't care

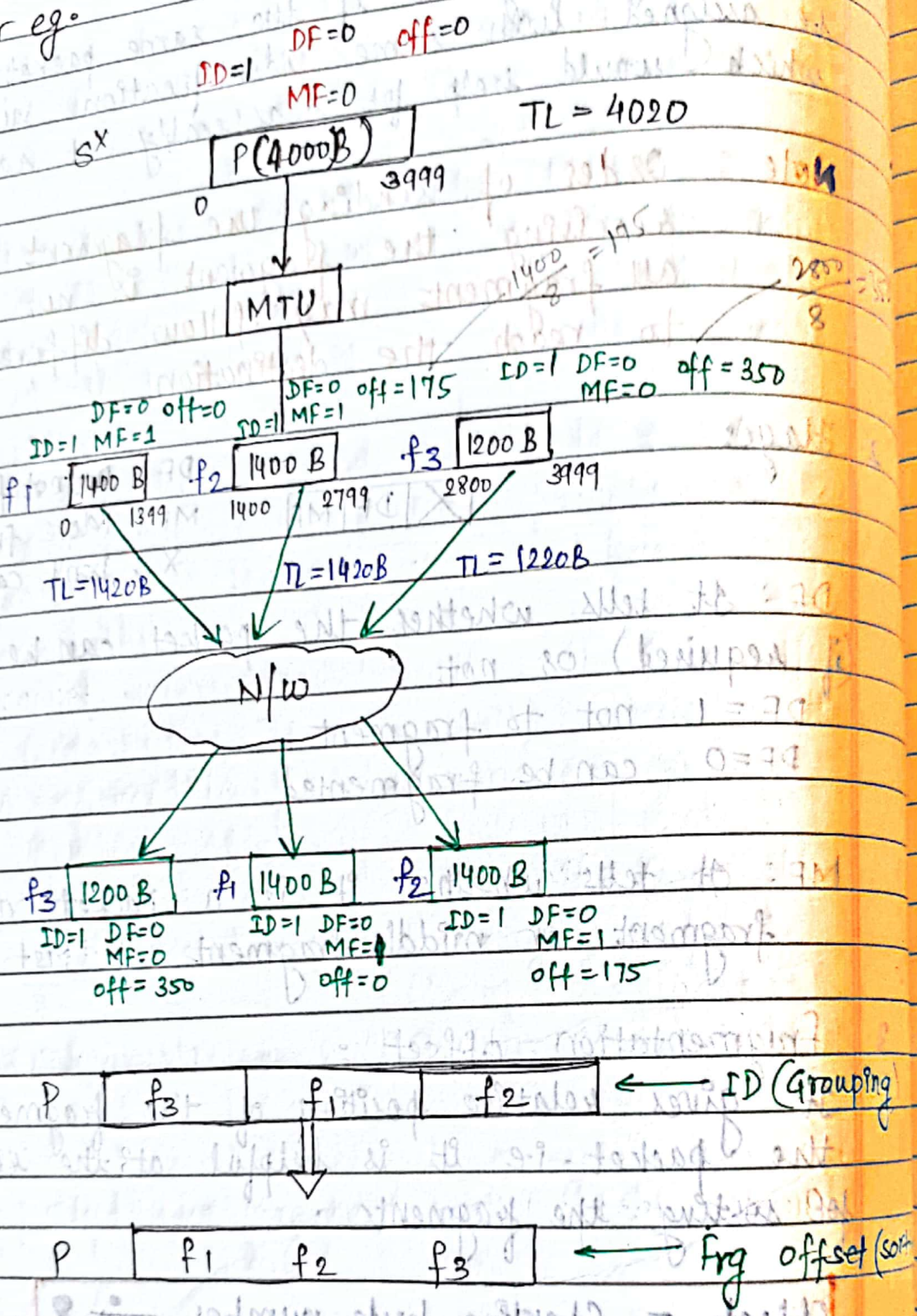
DF : It tells whether the packet can be fragmented (if required) or not.
DF = 1 not to fragment
DF = 0 can be fragmented

MF : It tells whether it is a packet or first fragment or middle fragment or last fragment

Fragmentation offset :
It gives relative position of the fragment in the packet. i.e it is helpful at the receiving for sorting the fragments.

Offset = Starting byte number ÷ 8.

For eg.

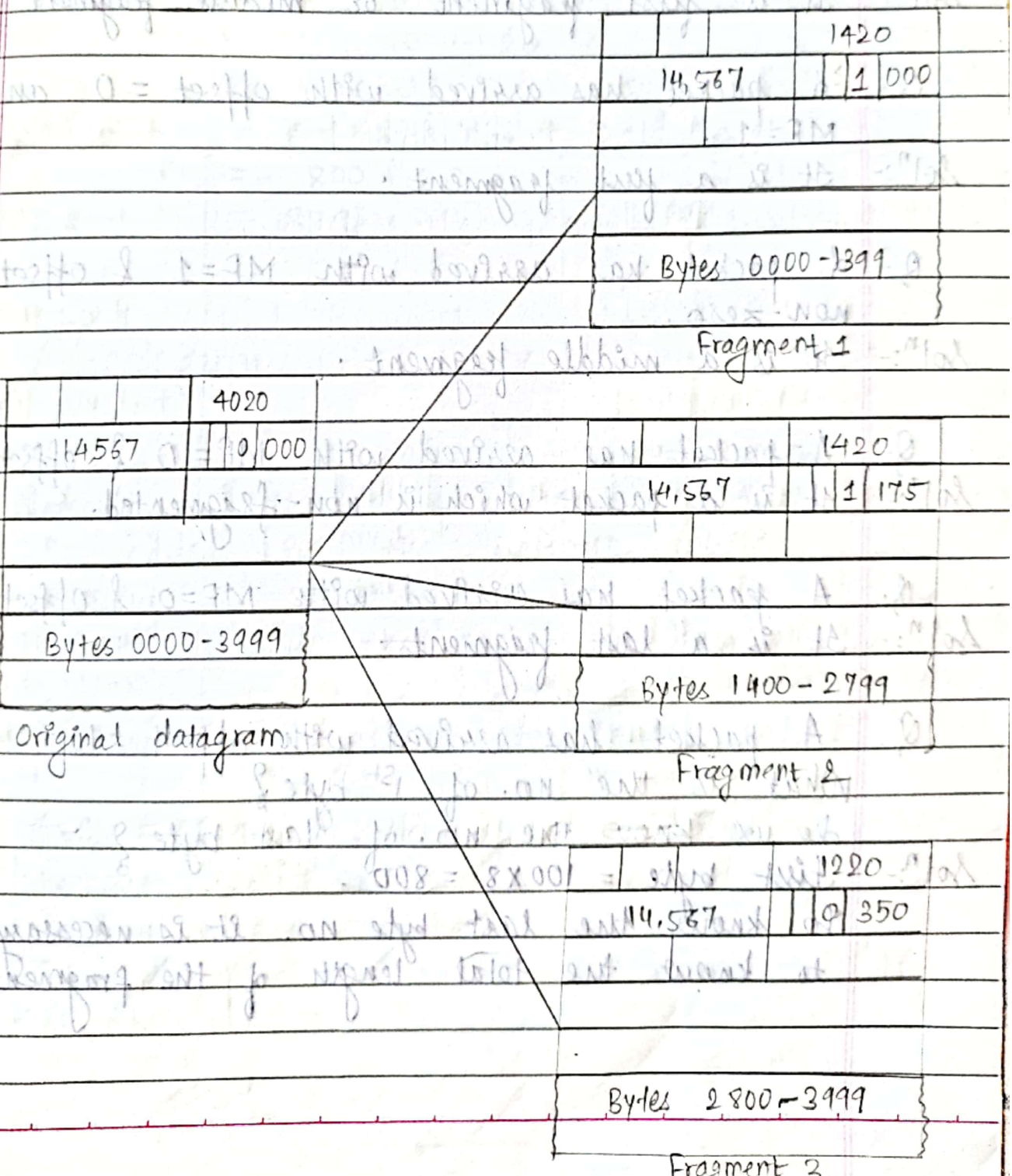


As shown in the diagram above, there is a packet of size 4000B which is divided into 3 fragments and the 3 fragments are sent sequentially but are received in any order.

Page No.
Date

At the receiving side, all the fragments are grouped into single packet with the help of identification no. & sorted w.r.t fragmentation offset.

For example: A detailed fragmentation with IP header.



Q. A packet has arrived with MF=0. Is it a packet or a fragment?

Soln: It is a packet or a last fragment.

Q. A packet has arrived with MF=1 Is it the first fragment, middle fragment or the last fragment?

Soln:- It is first fragment or middle fragment.

Q. A packet has arrived with offset = 0 and MF=1.

Soln:- It is a first fragment.

Q. A packet has arrived with MF=1 & offset is non-zero.

Soln:- It is a middle fragment.

Q. A packet has arrived with MF=0 & offset=0

Soln:- It is a packet which is non-fragmented.

Q. A packet has arrived with MF=0 & offset is non-zero

Soln:- It is a last fragment.

Q. A packet has arrived with offset = 100. What is the no. of 1st byte? Do we know the no. of last byte?

Soln:- First byte = 100 x 8 = 800.

To know the last byte no. it is necessary to know the total length of the fragment.

Q. A packet has arrived in which the offset value is 100, the value of HLEN is 5 and the value of the total

Soln:- Starting byte = 100 X 8 = 800
Header length = HLEN X 4 = 5 X 4 = 20
Total length = Data length + Header length
∴ Data length = Total length − Header length
= 100 − 20
= 80
∴ Last byte = first byte no. + Data length
= 800 + 80
= 879

V. Imp (10 Marks)

Checksum

- It is the most commonly used error detection method that checks is there any noise added in the network while traversing in the network.
- Receiver discards the packet in case of error.

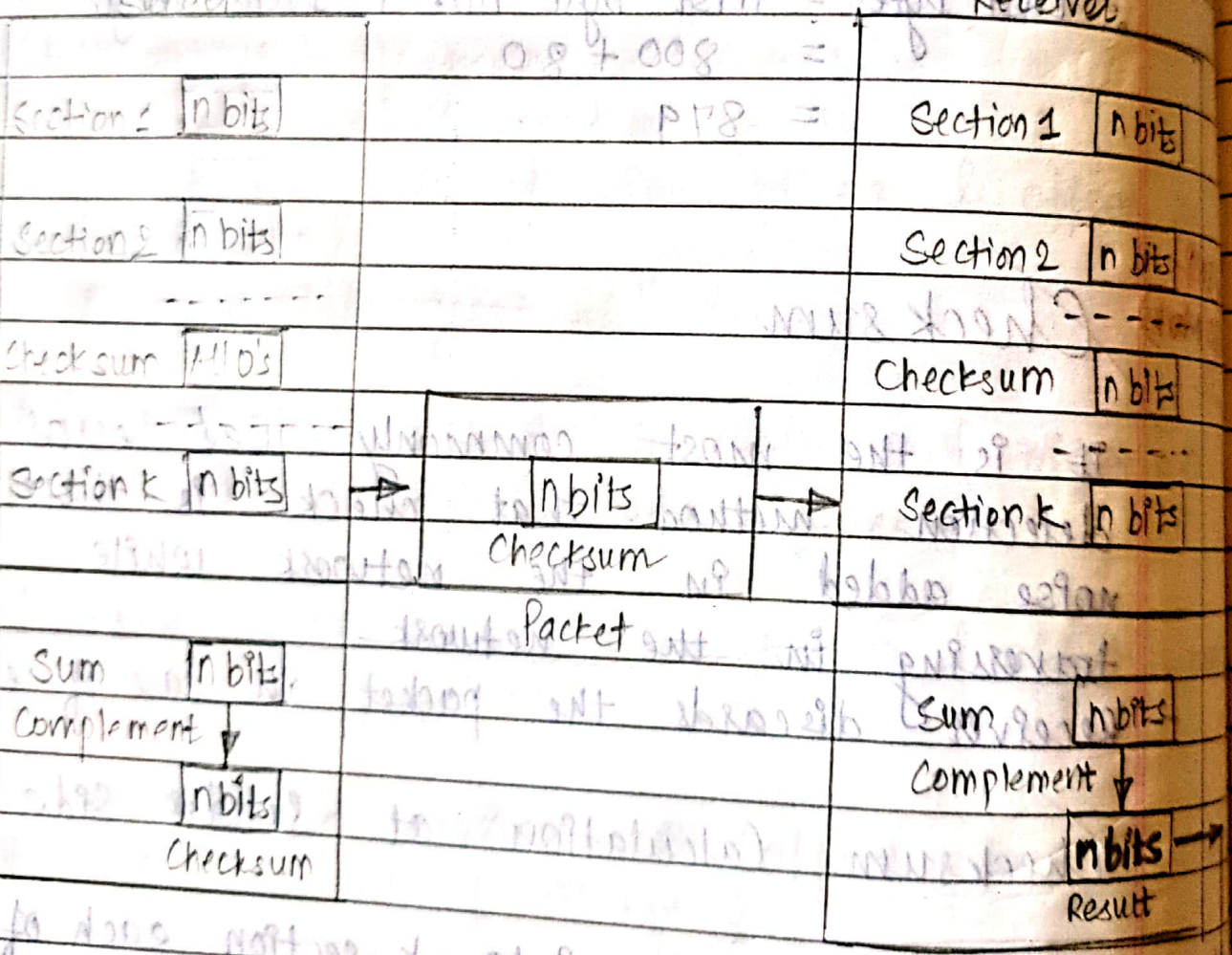
Checksum Calculation at Sender Side.

Step-1: Divide IP header into k section each of n bits
Step-2: set Checksum field to zero
Step-3: Perform binary addition
Step-4: Take 1's complement of the sum, this is the checksum.

Checksum Calculation at the Receiver side.

Step-1: Divide the IP header into k section each of n bits.
Step-2: Do not set checksum to zero.
Step-3: Perform binary addition.
Step-4: Take 1's complement of the sum, if the result is zero, accept it else discard it.

Block Diagram of Checksum :-



for example :

4	5	00	0028
0001		0	000
4	17	0000	
10.12.14.5			
12.6.7.9			

128 64 32 16 8 4 2 1

4, 5, and 0 →	01000101	00000000
0028 →	00000000	00011100
0001 →	00000000	00000001
0 and 000 →	00000000	00000000
4 and 17 →	00000100	00010001
0000 →	00000000	00000000
10.12 →	00001010	00001100
14.5 →	00001110	00000101
12.6 →	00001100	00000110
7.9 →	00000111	00001001
sum →	01110100	01001110
checksum →	10001011	10110001

* even no 1's then ans is zero.

* odd no 1's then ans is 1 & add carry.