Date - 21.12.23

4.3. Ethernet

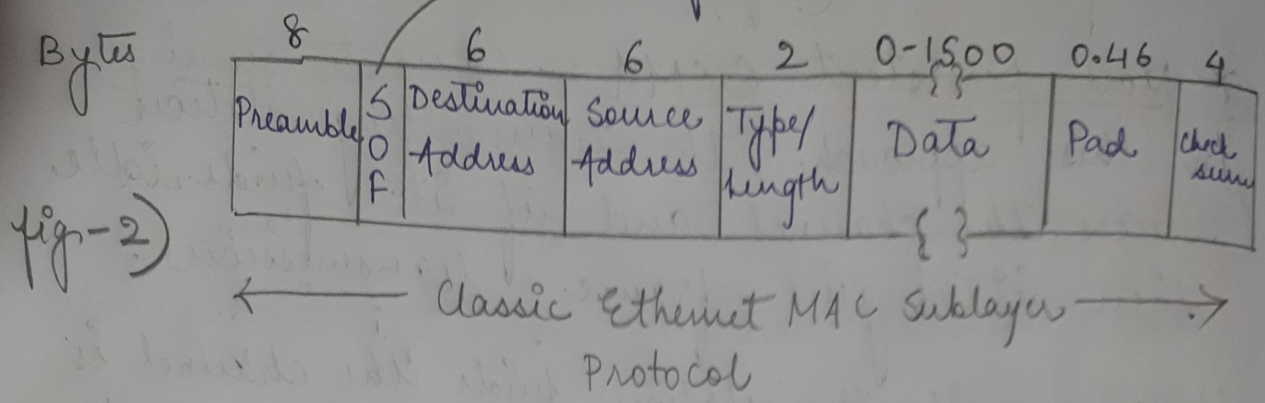


fig-2)

1) Ethernet is known as IEEE 802.3

2) Two types:
   * Classic Ethernet
   * Switched Ethernet (Switched LAN) → switch having ports where all the PC's are connected

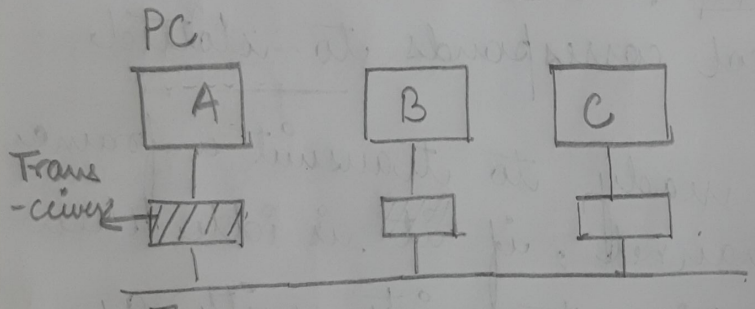


fig-1) Classic Ethernet

3) Difference between classic & switched Ethernet on the basis of speed.

Classic Ethernet :- 3Mbps - 10Mbps
Switched Ethernet :- 1 Gbps (Gigabit Ethernet)
100 Mbps (First Ethernet)
10 Gbps

* Classic Ethernet MAC Sublayer Protocol :-

1) Preamble :-

→ Each byte of preamble contains a bit pattern as 10101010, with an exception on the last byte where the last 2 bits are set to 1 and 1. (10101011)
   - 11 → works as frame delimiter
   - ↳ last byte in preamble.

→ The last byte of preamble is 10101011 and the last 2 consecutive 1's indicates the starting of a frame.

2) Destination Address and Source Address :-

• Dest^n addr^s -

→ Each address is of 6 bytes. (48 bits)

→ The first transmitted bit of "destination address" indicates :-

(i) '0' → indicates an ordinary address.
(ii) '1' → indicates a group address.

→ Sending dataframes to a group address is referred as Multicasting.

→ For special addresses, where all the bits are 1 is referred as Broadcasting.

• Src. addr^s -

→ These source addresses are globally unique and assigned by IEEE to ensure not to have station source address conflict.

→ To do this, the first 3 bytes of the address bits are assigned by IEEE and indicates a manufacturer.

→ Then manufacturers are assigned a block of addresses out of 2^{24} addresses.

→ The manufacturer assigns the last 3 bytes of the source address. These are programmed on the NIC, which stands for Network Interface Card.

3) Type/Length :-

→ 'Type' corresponds to the Classic Ethernet. However, the 'length' corresponds to the IEEE 802.3 standardization of the same field.

→ Range :- $0000_H - FFFF_H$

For values $\leq 0600_H$ → referred as 'Length' of the dataframe

For values $> 0600_H$ → corresponds to 'Type' of the dataframe.

4) Data :-

→ Range - (0 - 1500) bytes.

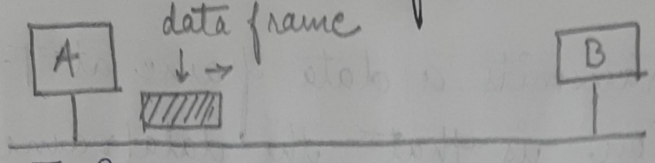
→ Increase in upperlimit of data would demand a higher RAM space and that would

increase the transceiver cost.

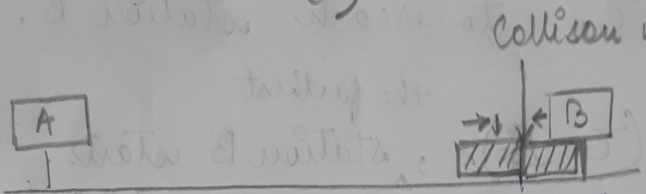
→ In addition to this maximum frame length, there is also a minimum frame length.

Date - 22.12.23

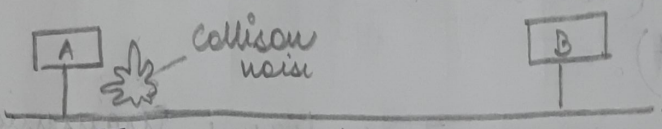
Q. What is the need of minimum frame length?



⊥(a)



⊥(b)



⊥(c)

'τ' → propn time from 'A' → 'B' } Assumption

fig - Diagram for Reason 2.

→ 6 + 6 + 2 + 0 + (0.46) + 4 = 64 bytes

DA — ↑ data$_{min}$ (0 → 1500) — ↓ pad field (46) — CS

Reason 1 }. Stations can distinguish between a valid frame and a garbage frame.

- Whenever a station detects a collison it truncates the current frame transmission which results in stray pieces of frame that appear on the ether/ link.

Reasons:

* In classic Ethernet, the minimum frame length has been computed to 64 bytes from destination address to checksum

Reason 2):

Fig 1(a) Station A transmits a data frame at T=0, and the assumption is that the dataframe takes time T=τ s to reach station B.

Fig 1(b) At time T=(τ-Δ)s, the farthest station B starts transmitting a dataframe. It gets collided with dataframe (which has been transmitted from station A).

So, station B immediately stops frame transmission and informs all other stations using Ethernet.

Fig 1(c) Station A will not be able to stop data frame transmission until and unless it gets the noise signal. (collison noise signal)

At about T= 2τ, the sender station A receives the collison noise and aborts the frame transmissio

* Thus, for stations transmitting very short dataframes, transmission would have been completed before the collison noise gets back to the sender station A and resulted a misinterpretation that the dataframe have been

transmitted successfully.

→ Thus, to prevent this situation, all dataframes must take greater than 2τ time ($> 2\tau$) for successfull frame transmission.

Q. For a 10 Mbps Classic Ethernet link with 2.5 km length having 4 no. of repeaters (used for amplification). The round trip delay time is 50 μs

10×10^6 bits → 1 s

1 bit → $\frac{1}{10^7}$ s = 10^{-7} s.

x bits → 50×10^{-6} s.

$x = \frac{50 \times 10^{-6}}{10^{-7}}$ bits

$x = 500$ bits

To make it in bytes = 500 + 12 (powers of 2) = 512 = $\frac{2^9}{8}$ bytes

$= 2^6$ bytes

$= 64$ bytes

5) Checksum :-

→ This field is of 4 bytes. It is a 32-bit CRC code to detect whether the received data frame is erroneous or not.

Date - 23.12.23

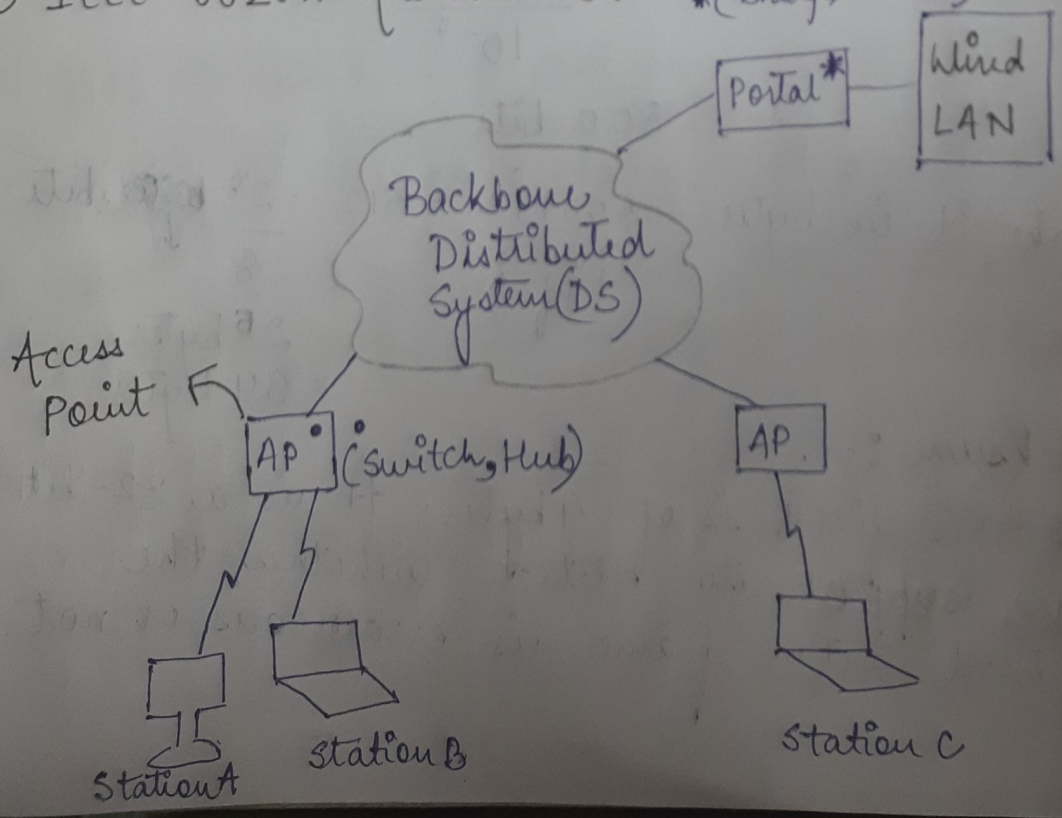
4.4. Wireless LAN :-

- Wireless LAN has standard as IEEE 802.11
- IEEE 802.11 Frame format @ MAC sublayer protocol :

Bytes	2	2	6	6	6 (Address$_3$)	2	0-2312	4
	Frame Control	Duration	Address$_1$ (recipant)	Address$_2$ (Transmitter)	Sequence control		Data	Check Sequence

Bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More fragment	Retry	Power Management	More Data	Protected	Order

⊙ IEEE 802.11 Architecture :- *(Bridge, Router)



1) → Frame Control field consists of 11 sub-fields.

→ Protocol version :- (2 bits)

• 00 → current version

→ Type :- (2 bits)

It indicates the type of frame. If it is 00 then it is management frame, if 01 then control frame, if 10 then data frame.

00 → Management frame
01 → Control frame
@10 → Data frame

→ Subtype :- (4 bits)

0000, 0001

In case of data frame,

10 0000 → indicates a normal data frame.
↓ ↓
Type Subtype

→ To DS :- (From station To DS)

This bit is set to 1, when a frame is transmitted to the distributed system (DS)

→ From DS :-

This bit is set to 1, when a frame leaves the distributed system (DS)

→ More Fragment :-

It is set to 1, when more data fragments are supposed to follow/receive.

→ Retry :-
It is set to 1, if there is a re-transmission for a previously sent frame happens

→ Power Mgmnt. :-
This bit is set to 1, if the transmitting station is in sleep mode.

→ More data :-
It indicates a station has some additional data to sent.

→ Protected :-
This is set to 1, then the frame body is encrypted/protected.

→ Order.
This is set to 1, which ensures that data transmission & reception is in ordered fashion/manner.

2) → Duration :-
This field indicates the time in microseconds that how long the channel has been used for transmission and receiving acknowledgements.

3) → Address$_1$:-
Recipient/Receiver Station Address

4) → Address$_2$:-
Transmitter Station Address.

5) → Address$_3$:-
Bridge/Router Address
(When station 1 tries to communicates with station C, but it is not in the vicinity of its endpoint, so it has to go through the DS first)

6) → Sequence Control :-
It is used for detection of duplicate frames.

7) → Data :-
It can contain (0-2312) bytes.

8) → Check Sequence :-
- It is of 4 bytes
- It is also a 32-bit CRC code.

Date - 03.01.24

Ch-6 (Transport Layer)

→ Accepts data from higher levels and splits it into smaller segments that can be sent to network layer

→ Transport layer takes the data from upper layer (i.e Application layer) and then breaks it into smaller size segments, numbers each byte and hands over to lower layer (Network layer) for delivery.

→ This layer is the first one which breaks the information data, supplied by Application layer in to smaller units called segments.

→ Puts segments in correct order (called sequencing) so they can be reassembled in correct order at destination.

→ May use a connection-oriented protocol such as TCP to ensure destination received segments.

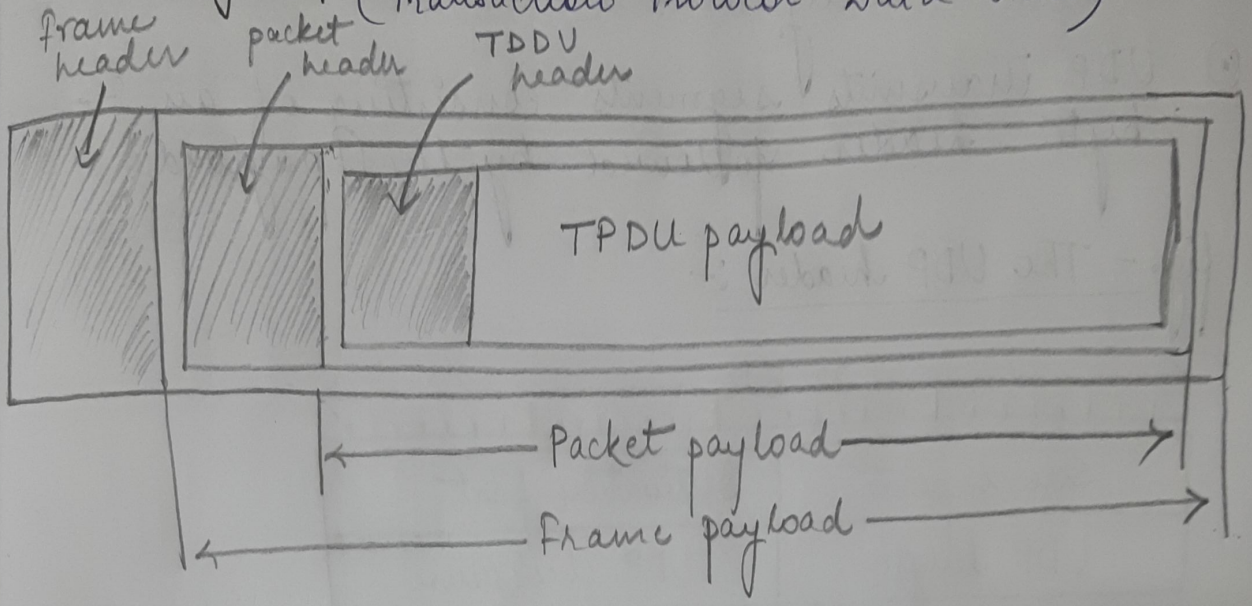
→ May use a connectionless protocol such as UDP to send segments without assurance of delivery.

* Transport Service Primitives :-

1) LISTEN
2) CONNECT
3) SEND
4) RECEIVE
5) DISCONNECT

* Transport Service Primitives :-

→ Nesting of TPDUs, packets and frames :- (Transaction Protocol Data Unit)



* The Internet Transport Protocols :-

- The Internet has two main protocols in the transport layer, a connectionless protocol and a connection-oriented one.

→ Connectionless - UDP
→ Connection-oriented - TCP

⊙ TCP → (Transmission Control Protocol) to ensure destination received segments.

⊙ UDP → (User Datagram Protocol) to send segments without assurance of delivery.

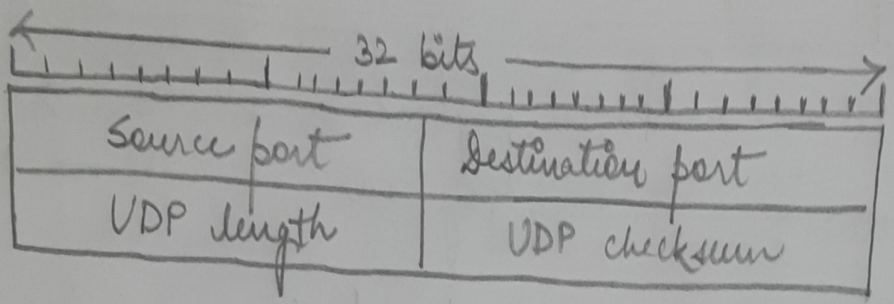
* Introduction to UDP :-

→ The Internet protocol suite supports a connectionless transport protocol, UPP (User Datagram Protocol)

⊙ UDP provides a way for applications to send encapsulated IP datagrams and send them without having to establish a connection.

⊙ UDP transmits segments consisting of an 8-byte header followed by the payload.

fig:- The UDP header :-



→ Some of the things that UDP does not do. It does not do flow control, error control, or re-transmission upon receipt of a bad segment

→ One area where UDP is especially useful is in client-server situations.

→ An application that uses a UDP this way is DNS (the Domain Name System)
- retransmission upon receipt of a bad segment.

→ No setup is needed in advance and no release is needed afterward. Just two messages go over the network.

⊙ The Internet Transport Protocols : TCP.

→ TCP (Transmission Control Protocol) was specifically designed to provide a reliable end-to-end byte stream over an unreliable internetwork.

→ TCP service is obtained by both the sender and receiver creating end points, called sockets.

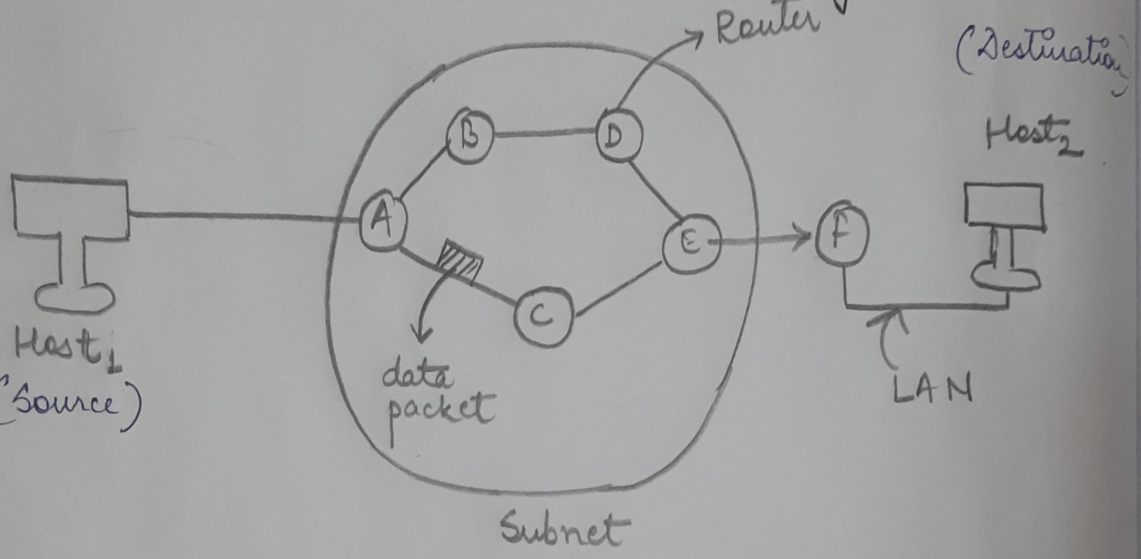
→ Each socket has a socket number (address) consisting of the IP address of the host and a 16-bit number local to the host, called a port.

Date - 04.01.23 Chapter - 5

Network layer

5.1 Network layer Design Issues :-

5.1.1 Store and forward Packet Switching :-



* Key points about Network layer :-

1) Network layer is responsible for packet forwarding and routing through intermediate routers.
   → forwading
   → routing

2) To do this, network layer must be aware of the topology of the subnet and choose the appropriate path.

#. Network Layer Design Issues :-

1) A host sends a packet to the nearest router.
2) The packet is stored until the checksum is

verified.

3) After that, the packet is forwarded to the nearest router along a best suitable route until it reaches the destination host.

. This mechanism is known as store and forward packet switching.

5.1.2 Services provided to the Transport layer :-

*) The network layer provides 3 services as follows :-

1) It is independent of router technology.
2) The transport layer should be shielded from the type, number, & topology of the router.
3) The network addresses provided to the transport layer must be uniform across LANs and WANs

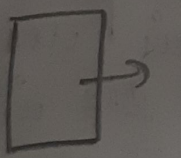
*) The services are classified into 2 groups :-
1) Connection Oriented Services 2) Connectionless Services

⊙ Connectionless Service Implementation :-

(1) In connectionless service, packets are injected into the subnet individually and routed independently to each other.

(2) No advance setup is necessary.

(3) The data packets often referred as datagrams and the subnet is referred as datagram subnet.

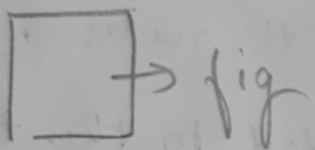


fig

⑥ Connection Oriented Service Implementation :-

1) In connection oriented service, a dedicated route from source router to destination router is established before any data packet transmission.

2) All data packets are routed through the same path which is often referred as Virtual Circuit. The subnet corresponding to it is known Virtual Circuit Subnet.



5.2 Routing Algorithm :-

1) The main objective of network layer is to perform the routing of the data packets from the source machine to destination machine.

2) Thus, routing involves hopping through multiple routers.

3) Routing Algorithm is that part of the network layer software which is responsible for deciding and injecting the incoming data

packets onto the subnet.

4) If the subnet uses datagram then the decision is made (at routing) for every arriving data packet (at routing).

5) However, if the subnet uses 'Virtual Circuits' then routing decisions are made only when a new virtual circuit is being set-up.
Thus, this latter case, is sometimes referred as 'Session Routing' because the route remain enforced for the entire user session.

6) A network device called as "Router" performs routing algorithms. It involves two major processes namely -
(1) Forwarding
(2) Responsible for Updating the Routing table.
↳ Here, comes the routing algorithm.

7) Certain properties of routing algorithms are desirable namely -
(i) Correctness
(ii) Simplicity
(iii) Robustness
(iv) Stability
(v) Fairness & Optimality

8) Routing algorithms can be classified into two groups -
(1) Non Adaptive Routing Algorithm
(2) Adaptive Routing Algorithm

⊙ Adaptive Routing Algorithm -

1) As the name says, the routing algorithms base their routing decisions on the measurements & estimates of the current data traffic and topology.

2) Adaptive algorithm can change their routing decision strategy to reflect any change in data traffic & topology.
Thus, sometimes it is referred as Dynamic Routing.

⊙ Non-Adaptive Routing Algorithm :-

1) Here, the routing decision is not based on any measurements and estimates of the current data traffic & topology.

2) Instead, the choice of route / data path has already been computed in advance prior to data packet transmission.
Thus, it is referred as Static Routing.

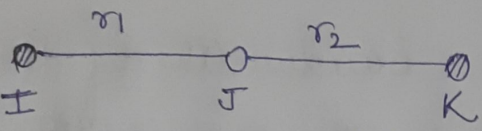
⊙ 5.2.1

* The Optimality Principle :-

Date - 05.01.24

5.2

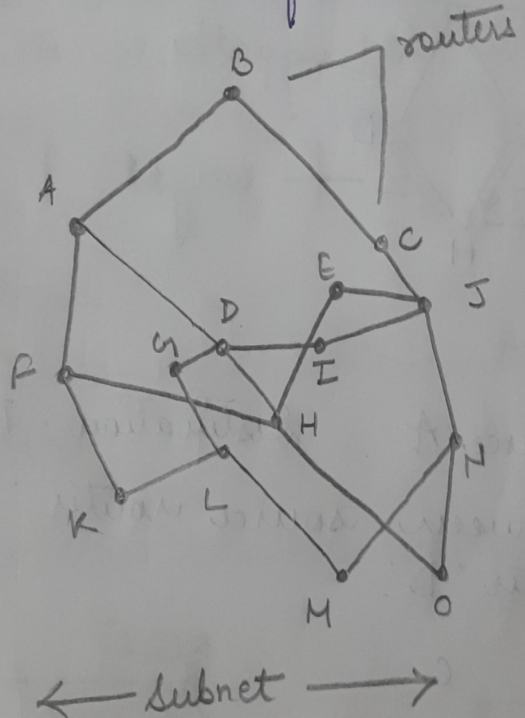
Def^n. It states that if a router J is on the optimal path in between router I and K, then the optimal path also falls on the same route/path.



r_1, r_2 → optimal path

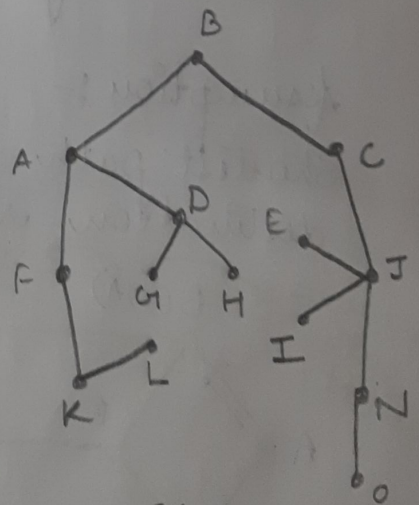
→ The direct consequence of the optimality principle is a set of optimal routes from all sources to a given destination will form a tree, that is rooted ~~on the~~ at the destination.

→ Such a tree is referred as "Sink Tree"



← Subnet →

by applying optimality principle



← Sink tree of destination router B →

→ Sink tree has no loops that means no. of hop count is minimum.

5.2.2. Shortest Path Routing Algorithm :-

→ One of the measure of shortest path algorithm is to minimize the no. of hop count. (apply principle of optimality)

→ { Geographical distance, bandwidth of the channel, average data traffic, communication cost, etc
↳ measure to consider while finding shortest path.

* Dikjstra Algorithm :-

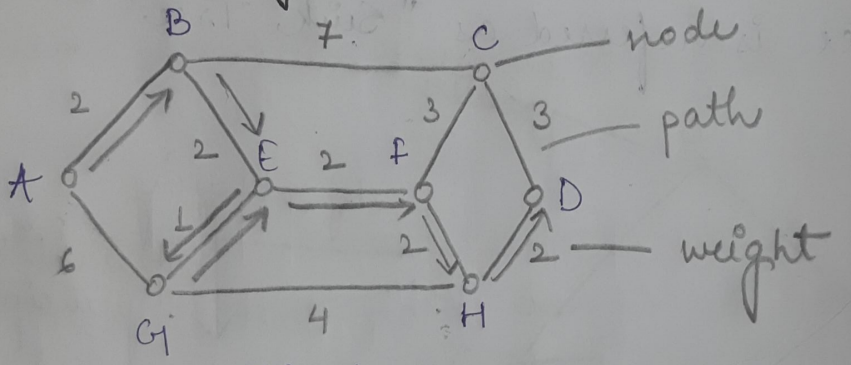


fig-1

Assumption :- Source-A Destination - D.
Shortest path between source router 'A' and destination router 'D'.

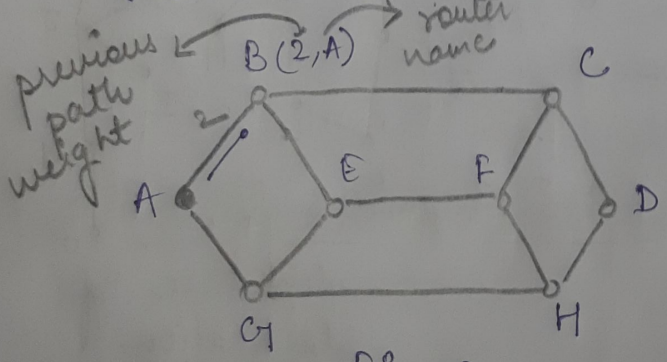


fig-2

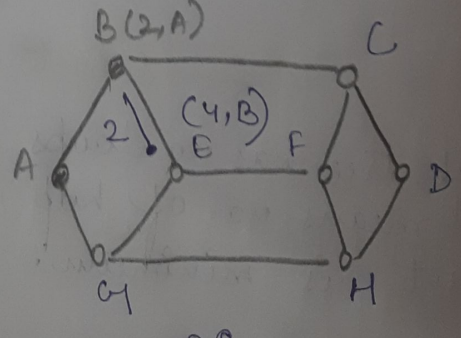


fig-3

5.2.3 Flooding :-

→ Flooding is a situation where static algorithm is implemented, where every incoming data packet is routed to every outgoing line except on which it has arrived.

→ The consequence is :-
The routers/nodes are full of duplicate data packets. Flooding generates a vast no. of duplicate data packets which may consequently jam the network. Congestion may happen.

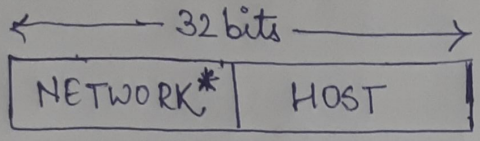
→ Advantages :-

→ Flooding can be implemented in military applications.

→ In wireless communication by broadcasting.

Date - 06.01.24

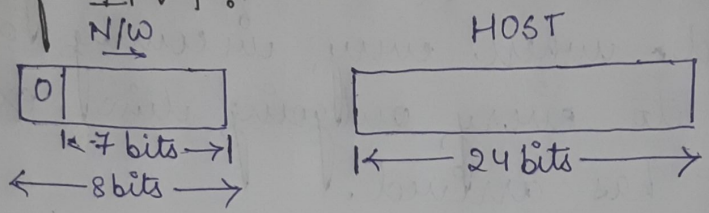
* IP - Address :-



* variable

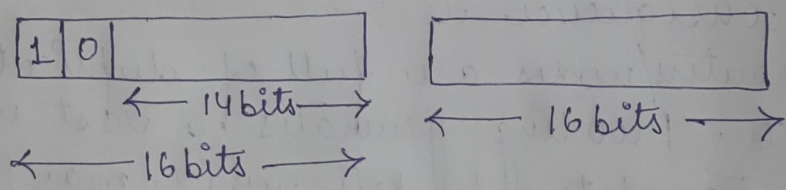
* Classes of IPv4 :-

Class A :



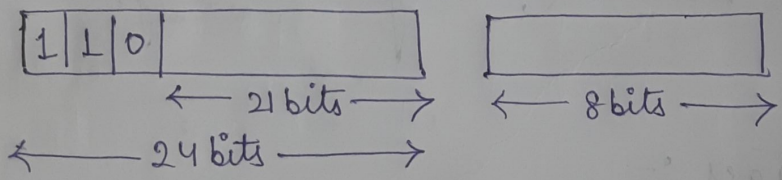
Range of IP Addr
1.0.0.0 to
127.255.255.255

Class B :



128.0.0.0 to
191.255.255.
255

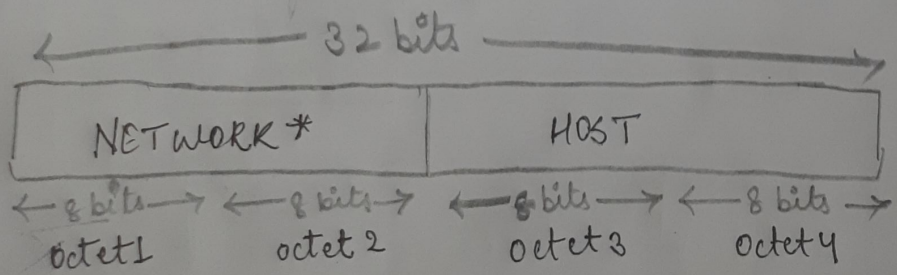
Class C :



192.0.0.0 to
223.255.255.255

Class D : Multicasting

Class E : Broadcasting



→ IPV4 is of 32 bits.

→ 32 bits IPV4 consists of a variable length NETWORK bit portion followed by HOST portion.

→ The IP Address is used as "source address" and "destination address", fields of IP packets.

→ IP Address always refers to a network interface rather than a particular host.

→ IP Address is specified in dotted decimal manner having 4 octets, each of which is of 8 bits.

→ for example :- IP-Address -
128.208.2.151

→ IP Address = Network interface, where Network means a collection of vast no. of hosts whose network address remains same. This is often referred as prefix.

* Prefix is same for all Hosts in one N/w.

→ Prefix -
128.208.2.0/24
- 128.208.2.0 : can vary from 0-255, total no. of hosts = 256.
- 24 : No. of bits in N/w field.
- / : Prefix length.

No. of Variations possible for N/w (Prefix size = 2^{24}
$= 2^4 \cdot 2^{20}$
= 16 Million).

→ However, prefix can't be inferred by looking at the IP Address entirely.

→ We need "Subnet MASK" ~~to infer~~ along with the IP Address to find out the prefix.

Q. What is Subnet MASK?

Subnet MASK corresponds to binary MASK of bit pattern 1's in the network portion of the IP Address followed by 0's in the host portion.

* SubnetMASK for $128.208.2.0/24$:-

1111 1111 1111 1111 1111 1111 0000 0000

Q. 128.208.2.151 → prefix ? } 255.255.255.0
Subnet Mask - 128.208.2.0 } $FF_H.FF_H.FF_H.00_H$

Step-1} Hexadecimal Octets

$0x80_H.0xD0_H.2_H.97_H$

$\Rightarrow 80_H.D0_H.2_H.97_H$

Step 2} In binary form :-

1000 0000. 1101 0000. 0000 0010. 1001 0111

Step 3} Perform logical AND operation b/w the IP Address in binary form with Subnet MASK in binary form.

10.

1000 0000 . 1101 0000 . 0000 0010 . 1001 0111
1111 1111 . 1111 1111 . 1111 1111 . 0000 0000

1000 0000 . 1101 0000 . 0000 0010 . 0000 0000

⇒ $80_H . D0_H . 02_H . 00_H .$

⇒ 128 . 208 . 2 . 0 .