31/1/24

CNIP [Unit 1]

* Computer network is a set of nodes connected by communication links.
  - Wired (cables)
  - Not Wired (air)

Layers	End Nodes devices	Intermediary Nodes
A. Presentation Session Transport N. D. Physical	Smart phone printer Tablet desktop Computer Web server	Cell Tower Switch Wireless router Router Internet Cloud Modem

OSI Model

* Basic Characteristics : Fault Tolerance Scalability Quality of Service (QoS) Security

Set of layers :

- Scalability → ability to grow based on needs, have good performance after growth.
- Fault Tolerance → ability to continue working despite Failures, ensure no loss of service.
- QoS → Set priorites and manage data traffic to reduce data loss, delay.
- Security → Unauthorized access prevention

13/2/24

CNIP (Layers)

(1) * **Application layer** is the top most layer in OSI reference model which enables the user to access the network resources.

→ The services provided by application layers are :-

1. FTAM (File Transfer Access management)
2. E-Mail Services
3. Directory Services

(2) * **Presentation layer** → It is concerned with the syntax and sematics of the information exchanged between the 2 systems.

→ The services provided by presentation layer are :-

1. Translation
2. Encryption
3. Compression

Page No.
Date

③ * Session layer establishes, maintains and synchronizes the interaction among communicating devices.
→ The services provided by the session link are:
① Dialouge control
② Synchronization.

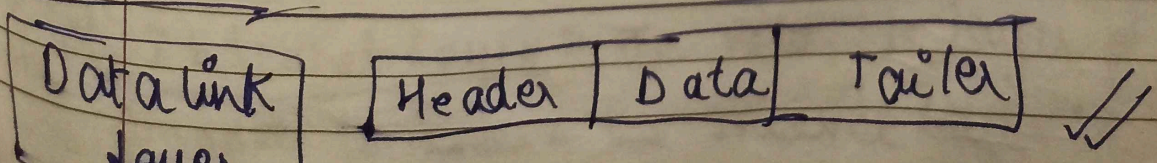
④ * Transport layer → For the exchange of information from sender to receiver it is ~~on~~ most imp. layer. In this Layer the port address of process is added. It also ensures about error control in the message or data into the computer network.

⑤ * Network layer → In this layer basically the logical addressing or ip addressing of the devices (sender and receiver) is added and it also ensure the routing path of the data

⑥ * Data link layer → In this layer the physical address or mac address is added into the data. In data link layer tailer is also used which is for finding errors in the signal or the data for the message routing in the computer network.

→ flow control
→ error control

⑦ * Physical layer → It is the lowest layer which deals with the 0 and 1 i.e in bits. It is also responsible for rate of data transfer, type of topology and synchronization with other devices.



* TCP/IP Model → 4 layered Architecture
→ Protocols.

Application layer	→ Combination of App./Presentation/session
Transport	
Internet	=> Same as Network layer
Network Access	=> Data link layer + Physical layer.

→ It is a 4 layer architecture with protocols. Transmission control protocol is widely used in communication i.e transmitting the signal from sender to receiver.

① Application layer of TCP/IP => It encomprates all the individual services provided by the layer. The widely used models are:-
HTTP, HTTPS, DNS & DHCP and FTP.

② Transport layer → It is same as OSI model with some protocols like TCP, UDP [User datagram Protocol]

③ Internet layer → The network layer of OSI model is known as Internet layer in TCP/IP.

It uses protocols like IPV4, IPV6, ICMPV4, ICMPV6.

IPV4	IPV6
(x.x.x.x)	(x.x.x.x)
32bit	128bit
0-255 (decimal)	More than 255 (Hexadecimal)

⊙ Network Access layer → It is the combination of data link layer and physical layer of OSI model with some protocols like PPP (point to point), Frame Relay, ethernet.

26/2/24

Unit 2 (CNIP)

Flow Control Protocols

- Noiseless Channel
  - Simple
  - Stop & wait
- Noisy Channel
  - Stop & wait ARQ
  - Go Back N ARQ
  - Selective request ARQ

ARQ → Automatic Repeat Request

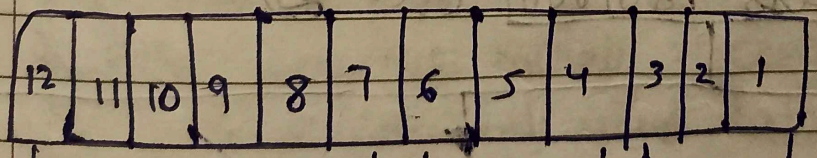
Sliding window protocol

* **Stop & Wait Protocol** → It is a data link layer protocol for transmission of frames over a noiseless channel.
→ It also provide unidirectional transmission by adding some facility without checking error control.
→ when sender sends signal or data, in ideal condition receiver should send ack. then after sender will send next packet.
→ If there is a data loss or acknowledgement signal loss in both the conditions sender & receiver will have to wait for infinite amount of time.
⇒ Suppose receiver sends the ack. signal to the sender with very delayed version which is almost act as a wrongly considered ack. of another data packet.

* Stop and Wait ARQ protocol provide certain timeframe for sending and receiving the signals. If there is delayed ack. received by receiver then there will be chances of data duplicacy which further leads in data garbeled.

* **Sliding Window Protocol** →

window of 3 size;



Yet to be sent

Data sent but Ack Not received

Ack received

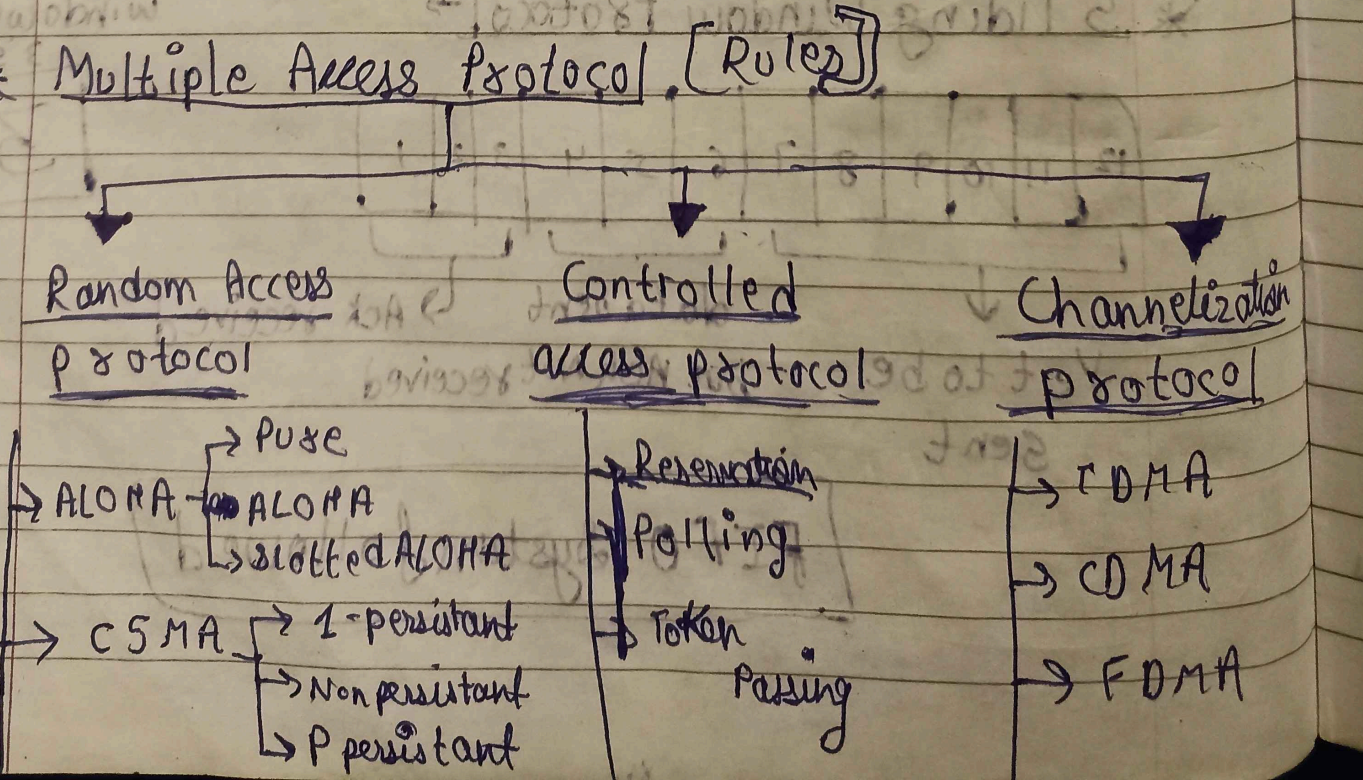
FIFO System followed

→ In this type of protocol we usually select window size, and acc. to that data packets are sent to receiver.
→ When sender receiver ack. for any data packet then only there will be a slide in the window which further results in sending another packet.
→ Packet string having 3 components :
① Ack Received
② Data Sent but waiting for Ack.
③ Yet to be sent

---

* Error Control Protocol → This is the essential service provided by datalink layer of OSI model. The main reason of error in data is a shared medium
→ The shared medium means no. of network devices are connected to same channel.
→ When channel is same there is probability of collision of data packet which further leads in garbeled of data..
→ To avoid such condition different types of protocols used known as multiple access protocol.

* Multiple Access Protocol [Rules]



[CSMA Types contd...]

Page No.
Date

→ CSMA/CD [Collision detection]
→ CSMA/CA [Collision Avoidance]

* TDMA → Time division multiple Access
* CDMA → Code division multiple Access
* FDMA → Frequency division multiple Access

(I) ALOHA → It is a random access protocol which is originally used for wireless network.
→ Aim is to avoid collision in shared channel while transmitting data packets from sender to receiver.
→ It is classified into 2 types :-

(a) Pure Aloha → In this the station can send the data packets at any instant time frame. Bcz of this random amount of time of sending data packets there may be chances of collision which further leads to garbeled in data.

(b) Slotted Aloha → In this we basically divide time frm into the slot to avoid collision of data packets. There are mainly 2 conditions :-

(i) Sender will send data packets in slot ...
(ii) Sender will send data packets at the beginning

→ Although multiple stations follow all collision there are ~~origin~~ collision of data packets which are less as compared to pure aloha.
→ If some station misses to send data packets then it will wait for next time slot to transmit.

(II)* CSMA [Carrier sense multiple Access] → The principle of CSMA is sense before sending in the shared channel.

→ Since all stations are connected with same channel, although all stations satisfying CSMA protocol still there will be a collission b/w data packet send by different airstations.

→ The main reason of collission is communication back and randomness of data packets send into the shared medium.

→ The collission is less than slotted & pure ALOHA because of sensing procedure.

TYPES OF CSMA :

① 1-Persistant CSMA → In this the station are continuously sensing the channel that is free or busy to send their packets.

→ The sensing of channel is depend on system req. (ms, microsec, nanosec).

→ The probability of transmitting the successful transmission is 1 in this case that's why it is known as 1-persistant CSMA.

→ Although prob. is 1 still there are chance of collission bcz if multiple station uses same protocol.

② Non Persistent CSMA → In this the station are sensing the carrier randomly to send the data. Bcz of this sensing of channel there will be poor utilization of channel & increase chances of collission further.

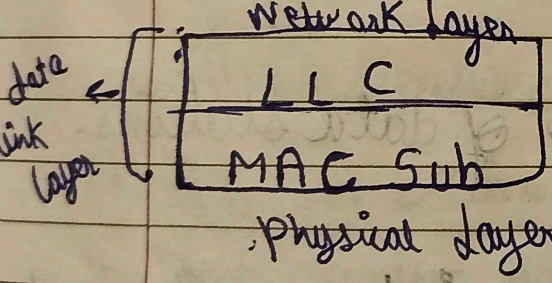
Page No.
Date

③ P-persistent → In this the time frame is divided into slots and stations are transmit or send data packets in the beginning of slot.

→ If some station sense the carrier which is free b/w the slot then it will wait for the next slot to transmit the data packet. While doing so there will be no proper utilisation of channel by the stations.

④ CSMA CD [Collision Detection] → In this protocol if 2 stations sense the channel to be ideal and begin transmitting data packets then there will be immediate chance of collission of data packets.

→ To avoid that collision CSMA CD is widely used with mac sub layer in LAN network.



[Consist of Congestionperiod or Contending period]

→ It is used in wired network (ethernet) standard IEEE 802.2 802.3

802.2 to 802.3

⑤ CSMA-CA → It is basically a collission avoidance protocol in which we try to avoid the collision by comparing the sender's and receiver data packets framed If there is a collision then there will be difference in frame width of sender and receiver data packets. and vice-versa.

→ It is used in a wireless computer network having a standard IEEE 802.11

Amess Protocol :

* Controlled ~~Sub layer~~ :

① Reservation - In this type of protocol, data station have to make the reservation of mini slots before sending the data packets..
In this protocol only reserved data stations are allowed to send the data packets into the channel & other stations stay connected.

→ Bcz of this process there will not be proper utilisation of channel which further leads to poor efficiency..

→ In some extent we can avoid the collision but there are multiple drawbacks of this protocol.

① Propagation delay
② Congestion Problem
③ Random amount of wait of data stations.

② Polling - In this protocol there will be a master node which having a responsibility to manage the data packets and send in the channel without collision. The efficiency of this protocol is better to reservation and at some extent collision are avoid. There are several drawbacks :-

① Propagation delay
② Congestion problem
③ Failing of masternode leads to collapse of data packet transmission.

③ Token Passing → In this all the data stations will send the data packets into the channel with same token that is called frame.

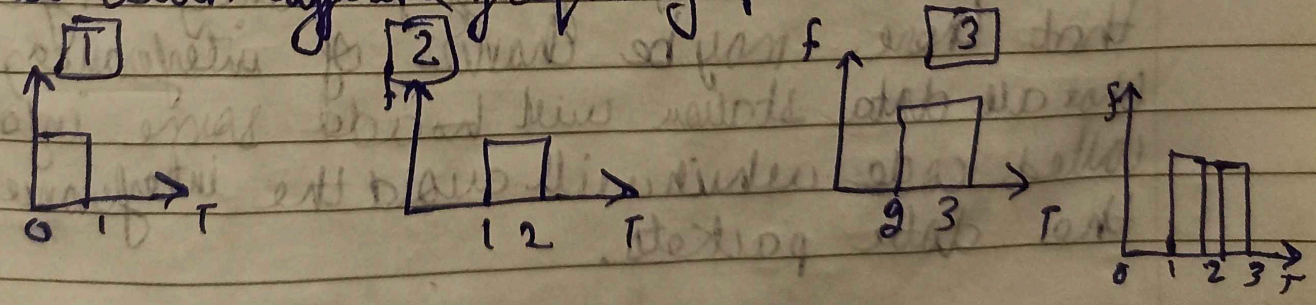
→ When data stations are finished with sending all data packets then only it will send token to the next node or data station.

- With this we are able to avoid the collision & congestion control problem.
- It having some drawbacks:
  ① Propagation delay
  ② If the station does not pass the token to the next one then communication or data packet may be interrupted.

---

* Channelization Protocol:

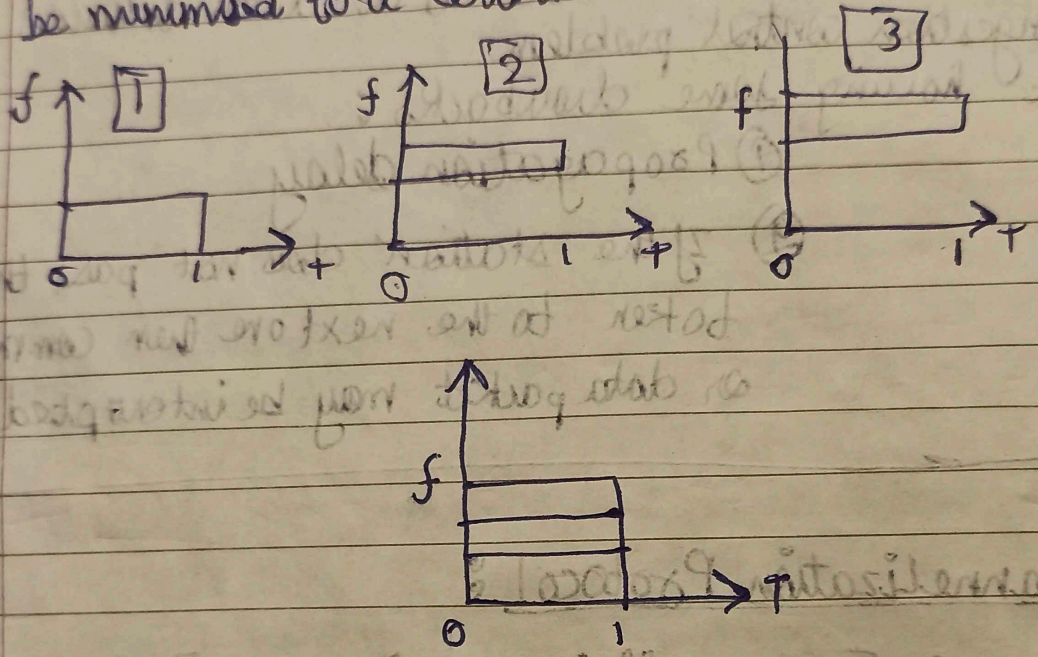
① TDMA [Time division Multiple Access] → It is used for wireless network. All the connected data stations can send the data into the channel in the given time slots with different frequency packets.



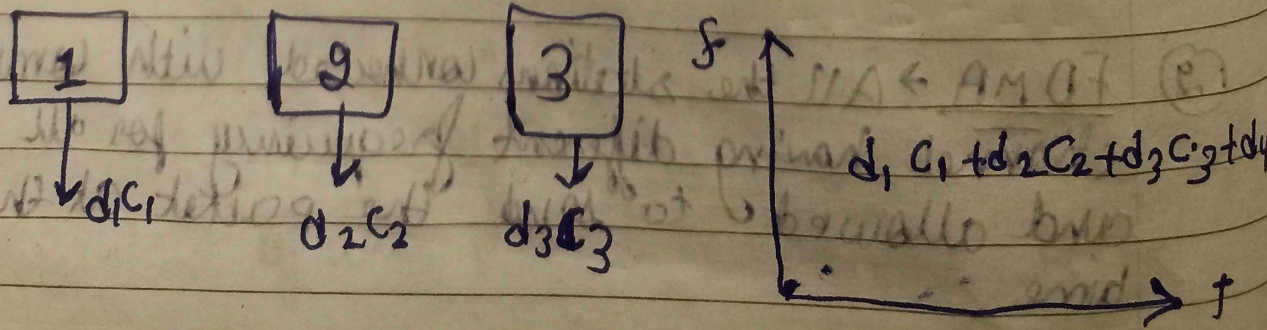
② FDMA → All the stations connected with common channel having different frequency for all packets and allowed to send the packet at the same time.

→ Since multiple stations have different frequencies there maybe chances of interference in data packet signals. To avoid this interference guard band are used to avoid this interference.

→ Guard band is the minimum time in which no station will send the data packet bcz of this interference can be minimised to a certain level.



(3) CDMA [Code Division multiple Access] → In this all channel can transmit data packet at any time and data packets having diff diff frequency range bcz of that there may be chances of interference to avoid that all data station will add some info that is called code which will avoid the interference b/w the data packets.



* FDDI [Fiber Distributed data interface]

→ Wired

→ Extended LAN → 200KM
WAN

→ IEEE -802.4

→ Token Passing

* It is an extented wired network upto 200KM is uses the IEEE-802.4 standard with token passing protocol. The working principle of FDDI is total internal reflection, that's why speed is fast as compared to other wired (ethernet) network.

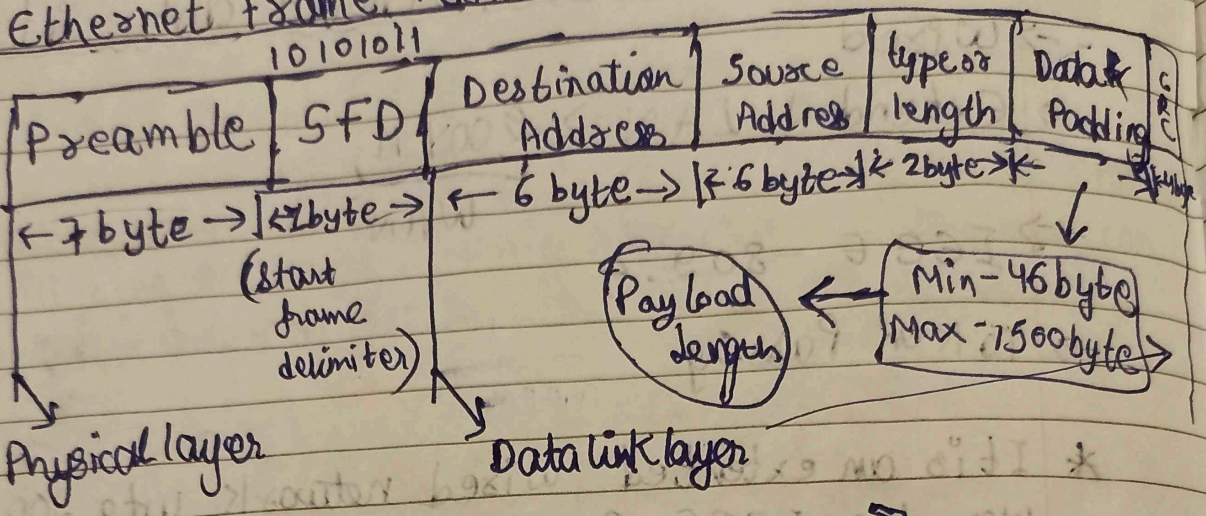
→ Physical layer and data link layer are directly involved in FDDI data transmission.

* Ethernet → Wired Network
→ LAN Network
→ ~~Token passing protocol~~ (Controlled Access)
→ IEEE 802.2 to 802.3

Ethernet Evolution

→ Standard Ethernet → 10Mbps
→ Fast ethernet → 100Mbps
→ Gigabit ethernet → 1Gbps
→ Ten gigabit ethernet → 10Gbps

* Ethernet Frame Format →



[Without data & Padding → 26 byte]

Max : 26 + 1500 = 1526 byte = 1518 byte

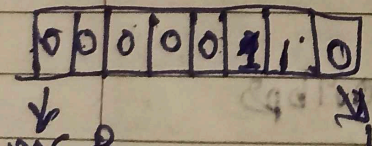
Min : 26 + 46 = 72 - 8 [excluding 8 byte]

= 64 bytes

→ Transmission of data = 512 bits = 12144 bits

→ Identify the following ethernet address about the cast.

06 : 9F : 9B : 01 : 1F : 2C → Unicast

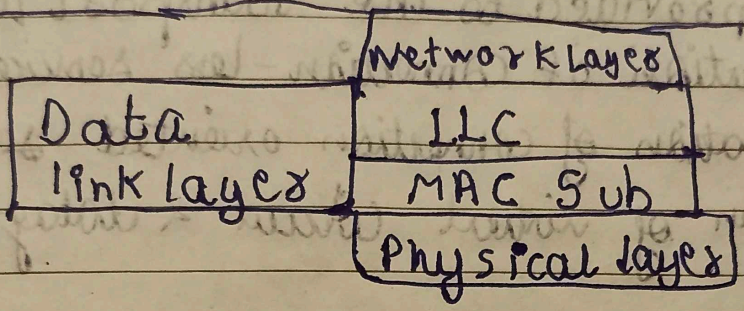


If LSB = 0 [Unicast]

If ~~MSB~~ LSB = 1 [Multicast]

For Broadcast, all the bits from MSB to LSB should be 1

-> WiFi is basically using IEEE 802.11 standard.
-> It is used for limited area or distance with CSMA/CA protocol.
-> If we want to use wifi with longer distance then multiple repeaters should be installed or used in the network.



* LLC [Logical link control] → It handles the comm. b/w upper and lower layers. It also takes the network protocol data and adds control info to help deliver the packet to the destination.

* MAC Sub layer → It is the lower sublayer of data link layer which is directly implemented by hardware. eg → NIC (Network Interface card)
There are 2 primary responsibility :-
① data encapsulation
② Media access control.