Network Protocols and Security 23EC2210A

Co-1 :-
Introduction to Computer Networks and Data.

Link layer :-
Introduction to Computer networks :- Use of Computer Networks, Network Hardware, Network Software. Reference models :- OSI and TCP/IP, Ex :- Networks Physical layer :- Theoretical basis for Data Communication, Guided and Unguided Transmission Media, switching, Modems, ADSI, Trunks and Multiplexing.

Data link layer :- DLL design issues. Error Detection and Correction, Elementary data link protocols, sliding window protocols. Medium Access Control Sub layer. channel allocation problem, multiple access protocols, Ethernet.

Network Protocols And Security (NPS)

Computer Network is Required to establish the Secure Connections b/w the devices.

* Based on the range we established the different types of Networks.
* Different types of Networks can be design based on the different types of architecture and the architecture consists of different types of devices based on the mode of operation, protocols - ~~giv~~ and some topologies.

Protocols - giving guidlines.

Types - LAN, WAN, MAN

Architecture - P-P, cls, OSI, TCP/IP

Devices - Router, bridge, Repeater, Switch, gateways, modem (modulation & demodulation)

Mode - Wired and Wireless.

Topologies - Bus, star, Ring, Mesh (Some Random Connections). Hybrid (Combination of all the above).

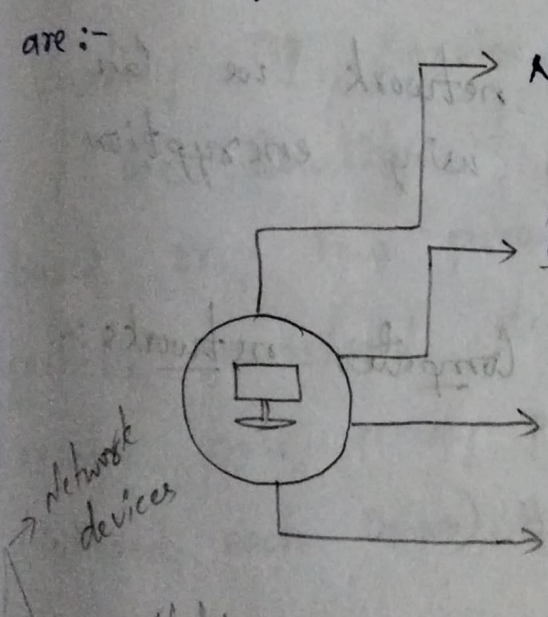
Protocol - UDP, TCP.

Computer Network :-

It is defined as it consists of different nodes [end devices], intermeditory devices] which are linked with either wire Communication or wireless Communication to exchange information from one device to another device.

One of the key resource of Computer network is resource ~~shell~~ sharing.

The key Components of Computer networks are :-



End devices :- The devices which are able to transmitt and receive data.

Eg :- PC, Mobile, Web Server.

Intermeditory devices :- The devices which are able to exchange of data cycle.

Eg :- Switch.

* Devices are also known as Nodes.

- links is of two types :-

  i) Wired link.

  ii) Wireless link

* We can link the devices with wireless link or wired link.

* Protocols :- set of rules.
  each network is followed by some set of rules.

Network Defense :-

After Completion of network we can protect the network by using encryption and decryption methods.

Basic characterstics of Computer networks :-

→ Fault Tolerance
→ Scalability
→ Quality of Service
→ Security

Scalability :- sharing the resource to small and large amount of devices.

To the existing device we can add the devices at that time we can able to access the internet.

Fault Tolerance :- In a Network if any System interrupted or damaged its services the other systems which are in that networks must be able to transmitt the data or receive the data. Therefore loss of packets will not be happen even the system failed.

Scalability :-

In a particular network a new system and device added the resource sharing must be done equally to the added device.

Quality Of Service :-

The Quality of Service is identified based on few parameters. Such as how many packets transfered successfully, acknowledgement receive how many packets Colision happend (Collided each other). Based on loss rate.

Security :-

To provide Confidentiality the User will add Cipher text to the original data.

Msg = Cipher text + data

Types of Networks :-

→ Division Based on Area Covered. Geographical Area

→ Based on types of Communication. Simplex, half duplex, full duplex

→ Based on type of Architecture. P-P, c/s, OSI, TCP/IP

→ Division Based on the Communication medium. Wired & Wireless

→ Based on protocols UDP, TCP

→ Network Topology Star, Ring, Bus, mesh, hybrid

→ Networking Devices

Division Based on Area Covered :-

Based on Geographical Area Covered the network classified into different Categeries they are :-

→ Local Area Network (LAN) End devices, Switch

→ Metropolitan Area Network (MAN)

→ Wide Area Network (WAN)

→ Personal Area Network (PAN)

→ Wireless Local Area Network. (WLAN)

9/1/25

LAN :- Eg:- Switch/Hub

Transferring the data b/w the person in that particular region.

* The Systems or devices which are Connected together in a Small Geographical Area that Network is Considered as local Area Network.

* In Local Area Network the IP address of all the devices will be same the Variation Can be experienced only in the class Id.

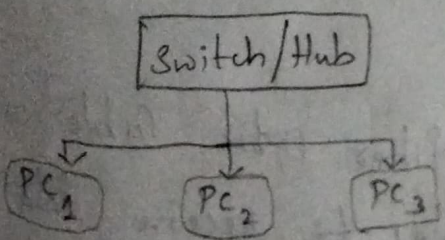
Eg:- 192.255.255.14 → class id

* In LAN the hardware devices include NIC. (National Interface Card) (Ethernet is Connected Switch/Hub)

* LAN Network is less Costly when Compared to Other Network (MAN, WAN, WWAN).

* It provides high Security.

Disadvantage :- Lack of Privacy.



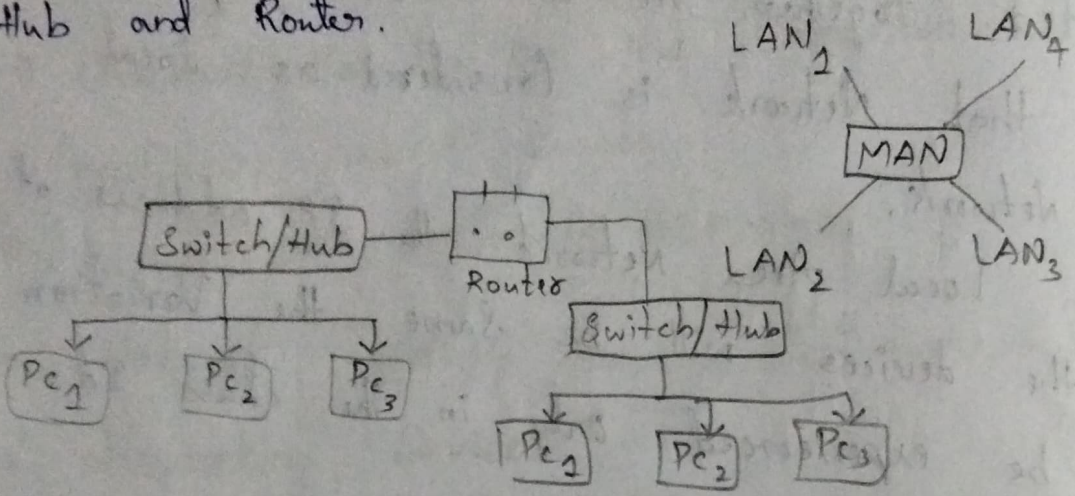
It is Consider as LAN Network 1.

Uses of LAN :-

* Easy to manage data store.
* Sharing of one Copy by all Users.

MAN :-

* In this Network large Geographical Area is Covered When Compared to the LAN.
* The Hardware devices includes NIC, Switch, Hub and Router.



Uses of MAN :-

* It Can be used an Airline Reservation.
* It Can be used an College within a city.
* MAN is used to Communication b/w the banks in a City.

WAN :-

* It Covers more Geographical Area when Compared to LAN & MAN.
* It uses telephone line, fiber Optic Cable or Satelite links to transfer or to receive data from one place to another place.

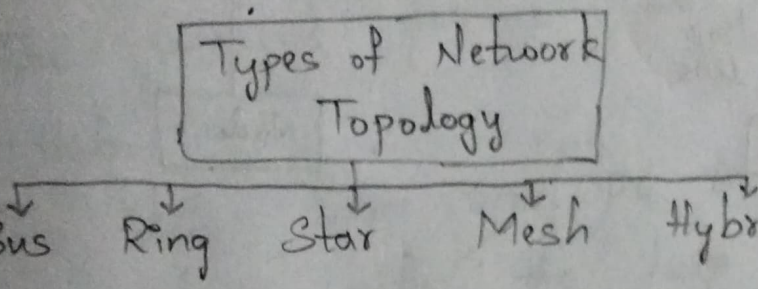
Note :- In MAN & WAN Servers are included

Therefore the Architecture is known as client server Architecture.

Network Topologies :-

* The arrangement of end devices and intermeditary devices (any) to establish a Network is known as Topology.

Topology = Arrangement of devices.

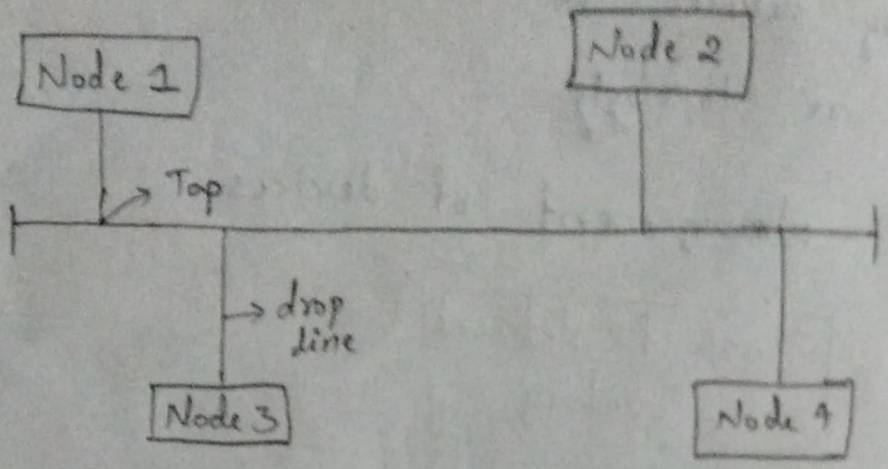


* The Arrangement of devices is Categorized as follows :-
  * Bus
  * Ring
  * star
  * Mesh
  * Hybrid

Bus :- (No privacy everyone will receive the data)

* In Bus Topology all the devices in the network will be Connected by the Coaxial Cable or twisted pair Cable which is considered as back bone.

* If any device in that network failed to transmitt the data the Other devices will not be able to resoive the data (the entire System is Crashed

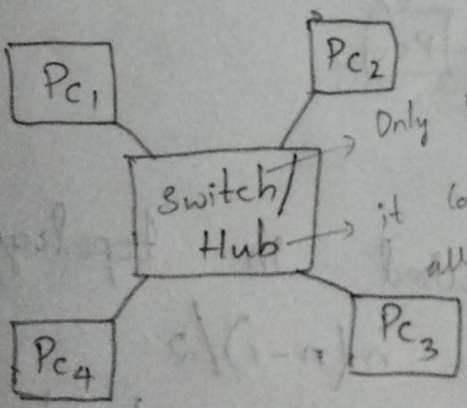


Ring :-

* The devices which are Connected in this network are arranged in ring (or) Circle.
* This Topology is Older topology it Can be designed with low Cost (less expensive) the data Can be transferred in Unidirectional way.
* The device which wants to transmitt must have token.
* If a Single Cable Connection is disc lost/damage the data Can not be transfered to from one device to another device.

Note :-
The Bus topology and Ring topology are considered as peer to peer Architecture.

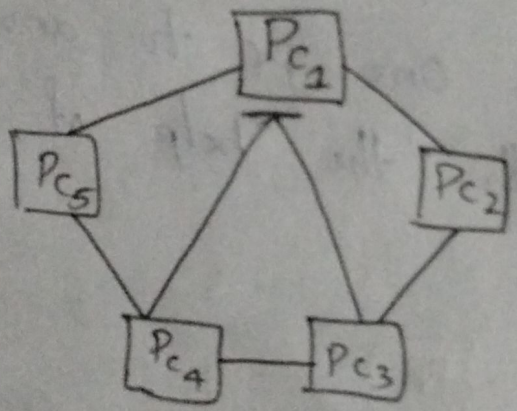
Star :-
* In star topology all the devices which are in the network will be connected to a central device.
* The central device can be switch or Hub.
* The data from one pc to another pc will be done with the help of central device.



Advantage :- If any ~~one~~ device is failed other systems can communicate its own way.
* In star topology if any device is damaged or failed to transmit or receive the data the entire device won't be crashed and other devices will work.

Mesh :-

* The devices which are in the network can be connected one to many either full mesh topology or partial mesh topology.
* In Mesh topology also if any of the device is down (Not working) the other devices will not effect the Communication b/w connected devices.



Note :-

* No. of Cables required in topology can be Calculated by $n(n-1)/2$
* No. of ports required in topology can be Calculated by $n(n-1)$.

Open System interConnection (OSI) layers

* OSI is Considered as a reference model which specify how the Communication is taken place from Sender to Receiver (or) Transmitter to Receiver.
* OSI Model was developed by International Organization for Standardization (ISO) in 1984, which involves both hardware and Software elements.
* OSI Model Consists of 7 layers where each layer divides the given or ~~hold the~~ whole data into the required format. [as per the layer operation].
* The 7 layers are as shown below.
* 3 layers are Considered as Software layers
3 layers are Considered as Hardware layers and the middle layer of the OSI is Considered as heart of OSI layers.
* Application layer:- HTTP, HTTPS, FTP, TELL NET, RDS these are Protocols we need in application layer.

Function of OSI layers

Application → It acts as user interference layer
→ The user can interact with outside use with the help of protocols.

Software layer

Presentation → Translation, Encryption & Compression.

Session → Dialog Control and Synchronization.

Transport → Port addressing, Segmentation & Reassembly, Connection Control, flow Control & Error Control
→ It acts as bridge from Upper to Lower layers.
(acts as BASE)

Network → Logical addressing and Routing.

Hardware layer

Data Link → Framing, physical addressing, flow Control, error Control and Access Control.

Physical → Physical characteristics of the media, Representation of bits, data rate, Synchronization of bits, line Configuration, physical topology and Transmission Mode.

* SKP is used for Skype (video calls).
* FTP is used for Transmit the files.
* PTAM, Mail services and Directory Services.

Presentation layer:-

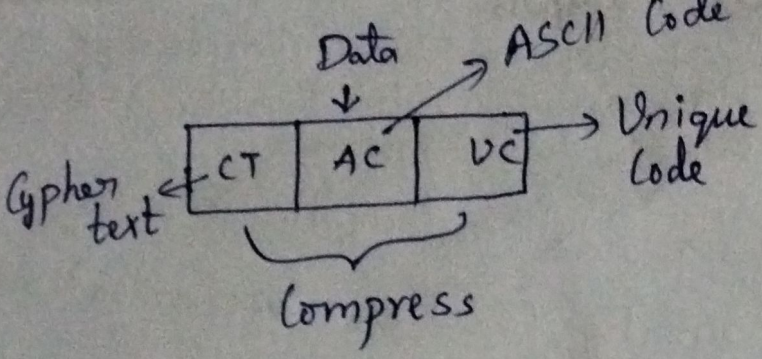
* Translation, Encryption and Compression

Encryption:- Adding Cypher text which gives securing to the data.

Translation :- Two types of translations we have:-

* Unicode translation
* ASCII translation.

* Along the data it will perform the encryption, translation and Compressing the data.



* According to the User we Can Convert the data from one form to ASCII Code/Unique Code.

Conversions of data in each layer :-

Data (Application, Presentation, Session layer)
↓
Segment (Transport layer)
↓
Packets (Network layer)
↓
frames (Data link layer)
↓
Bits (physical layer).

Application layer :-

From the Sender side the application layer is the first layer to interact with the network.

* In this layer the user Can use following protocols :- for browsing data - HTTP, HTTPS.
To transfer file through internet - FTPS (file transfers Protocol)
To Send or receive mail - SMTP Protocol (Simple mail Transfer protocol).

for remote desk applications - TELNET.

* In this layer the User can visualize the data in the return or developed format.

Presentation layer :-

* It is mainly used for three different operations. They are :-

1. Translation :- It converts data from one ~~from~~ form to ASCII code format / Unicode format / Binary format.

2. Compression :- It not only translates the data but also compress the file size.

Eg :- Converts 6GB file to 3GB / 2GB.

* All the single files can be compressed to zipfile. which are related to the same domain.

3. Encryption / Decryption :- To provide the security or to protect the data from external person's access the converted data needs to encrypted with cipher text or password at the or sender side / end.

Eg :- NAN : 1101011

* In presentation layer we use Secure Socket layer protocol.

Session layer :- Session layer used to manage session (Session establishment, data transfer and session termination) authentication and authorization.

* In session management Connectivity + Data transfer + termination.

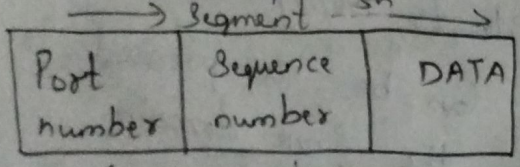
* Authentication :- If the User wants to establish Connectivity the User needs to enter username and password to enter into the particular network.

Eg:- ERP, LMS.

* Authorization :- In authorization permission needs to be given by a person to view the documents or to see the design of the network.

Eg:- Hiding stories from some people in instagram.

Transport layer :- In this layer the data is divided into segments and each segment is assigned with sequence number & port number.



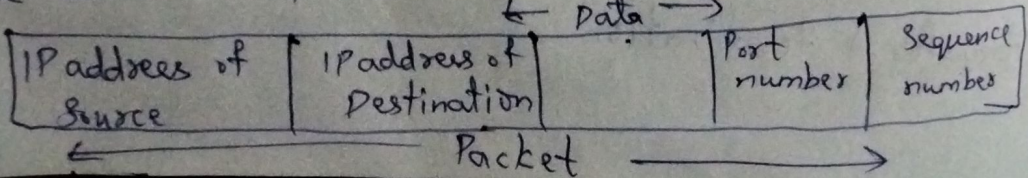
In each segment it consists of port number (http - 80, https - 443 --), Sequence number as 1, 2, ... n.

* In each segment the sequence number is varied port number is same and data is different.
* Transport layer is Heart of OSI.

Network layer :- In this layer the segment is divided into chunks known as packets.

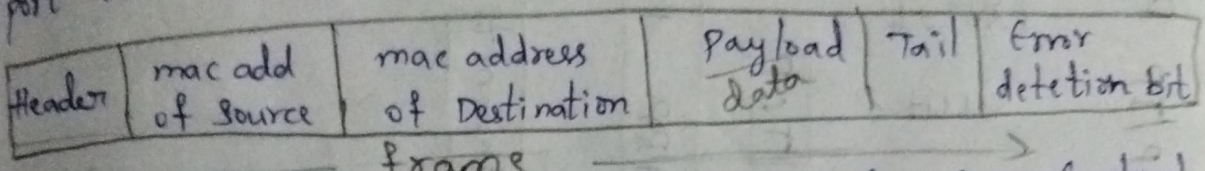
* It deals with logical Address./IP address.
* In this layer we use Routers as intermediatery nodes.

The format of packet is as shown. below,



Data link layer :-

* This layer deals with physical address which is of 12-digit -alpha- numeric Value [1234:5678:9ABC]
* It is also known as mac address / physical address
* The data in data link layer reffered as frames. Each frame consists of Header, tail, Error detection bits, mac address of Source and destination & payload.
* Payload Consists of IP address of Source & destination, port number & Sequence number along with data.



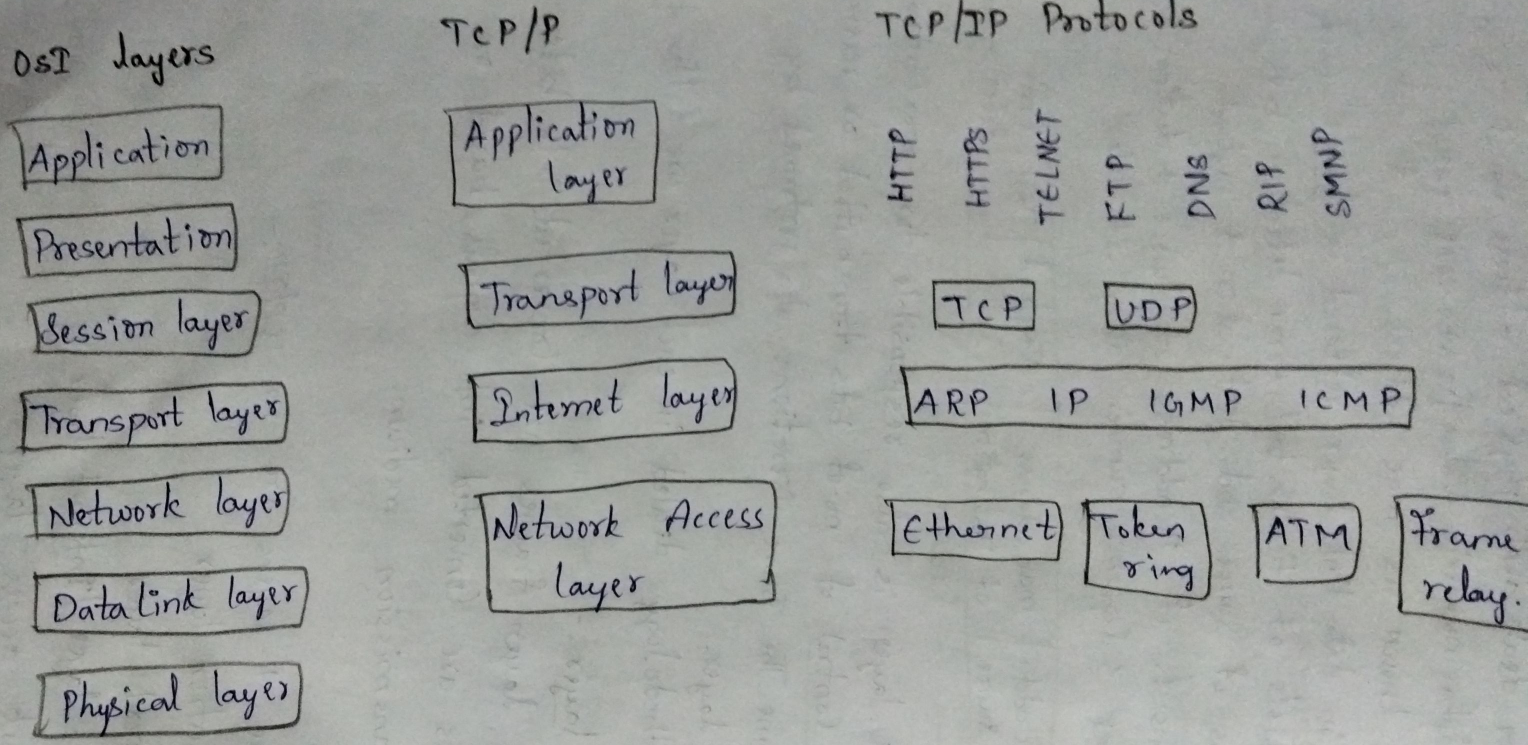
* Data link layer is also responsible for Error Control and flow Control of no.of bits transmitted or received at one time. The same operations also performed by Transport layer.
* The methodology dealed in each layer are different.

Physical layer :-

* In this layer frames are converted into bits.
* The bits are Converted into Signals based on the transmission medium.

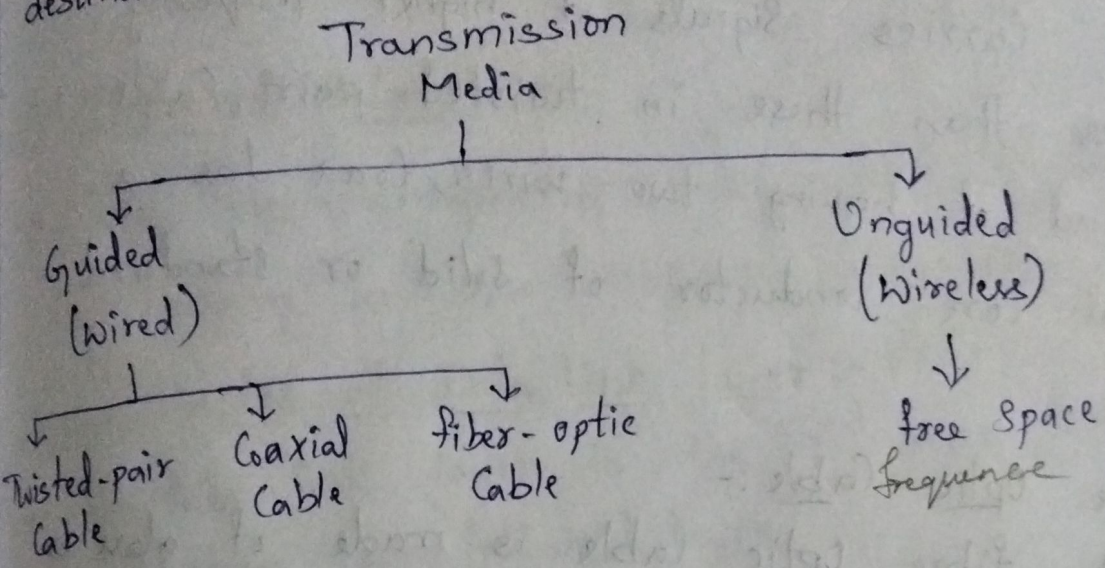
TCP/IP :-

* There are 4-layers are in TCP/IP :-
  (i) application layer
  (ii) Transport layer
  (iii) Network layer / Internet layer
  (iv) Network access layer.


OSI layers
Application
Presentation
Session layer
Transport layer
Network layer
Data link layer
Physical layer
TCP/IP
Application layer
Transport layer
Internet layer
Network Access layer
TCP/IP Protocols
HTTP
HTTPS
TELNET
FTP
DNS
RIP
SMNP
TCP
UDP
ARP
IP
IGMP
ICMP
Ethernet
Token ring
ATM
Frame relay.

Transmission Media :-

It can be broadly defined as anything that can carry information from a source to a destination.



Guided Media :-

Guided media are those that provide a conduct from one device to another.

i) Twisted pair Cable
ii) Coaxial Cable
iii) Fiber-Optic Cable

Twisted Pair Cable :-

* It consists of two conductors, each with its own plastic insulation, twisted together.
* One of the wire is used to carry the signals to the receiver and the other is used only as a ground reference.

Two types of twisted pairs we have.
i) sheilded ii) Unsheilded

Coaxial Cable :-
It Carries Signals of higher frequency ranges than those in twisted-pair Cable. Instead of having two wires, Coax has a Central Core Conductor of solid or standard wire.

Fibre Optic Cable :-
A fibre Optic Cable is made of glass or plastic and transmitts Signals in the form of light.

Unguided Media :-
* It transport electromagnetic waves without using a physical Conductor. This type of Communication is known as Wireless Communicati
In this we have.

1) Micro waves :-
* Electro magnetic waves having frequencies b/w 1 and 300GHz are Called microwaves.
* Microwaves are Undirection.

ii) Radio-waves :-

* The electro-magnetic waves which are ranging their freq's from 3kHz to 1GHz.
* Radio waves are Omnidirectional.

iii) Infrared Waves :-

* The Electro magnetic waves whose frequency is ranging in b/w 300GHz to 400THz.

Design issues of Data link layer :-

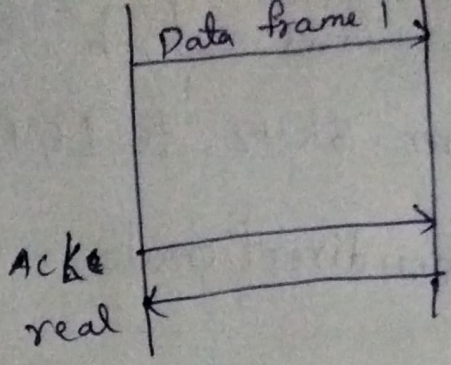
* The data link layer is the 2nd layer from the bottom layer (physical layer).
* This layer mainly Concentrate on four aspects.

They are :-

1. It acts as a bridge or intermediatery layer b/w network layer to physical layer (Sender part) or physical layer to network layer (Receiver part).
2. It helps in transmitting the data or receiving the data from one device to another and it helps in flow control of the bits.

By Receiving an acknowledgment Signal from the receiver.

If the acknowledgment Signal is not received the Sender will retransmitt the data.



Ack = acknowledgement Sign

3. In data link layer along with frame the extra bits are added to identify an error in the transmitted or received data. This process is known as Error detection and Error Correction.

Error Detection :-

Error is defined as misplacement of one bit or more bits in the given data. There are two types of errors:-

i) Single-bit error (Misplacement of 1bit)

ii) Burst Error (Misplacement of more than 1 bits)

The different types of Error detection techniques are:-

- Parity check Method :- It can be done in two ways. They are :-

  (i) 1-Dimensional Parity check.

  (ii) 2-Dimensional Parity check.

* Adding of parity bits can be done either by adding '0' (or) '1'. Parity bits can be added based on even no. of bits in the data (or) odd no. of bits in the given data.

i) 1- Dimensional Parity check :- (VRC) Vertical Redendency check.

* Based on the given data split the data into n-parts (or) segments. Each segment must have k-bits. The k-bits will be decided based on the no. of bits available in the original data.
* Usually, the User can consider 'k' as 4, (8), 16... best
* Consider an original message as "Network".

Network
↓
ASCII Code
↓
Binary formal
↓
Perform's Parity check method.

ASCII Values

A to Z a to z

65 to 90 99 to 122.

		8 4 2 1 8 4 2 1
N -	78 -	01111000
E -	69 -	01101001
T -	84 -	10000100
W -	87 -	10000111
O -	79 -	01111001
R -	82 -	10000010
K -	85 -	01110110

NETWORK :-

01111000|01101001|10000100|10000111|01111001|10000010|01110110

Note :- If there are sufficient bits for dividing into 8 parts. We can add '0' at the end of the data.

We are going to perform the even parity.

if no.of '1's = even = add '0'

if no.of '1's = odd = add '1'.

01111000[0] | 01101001[0] | 10000100[0] | 10000111[0] |
01111001[1] | 10000010[0] | 01110101[1].

* Parity check is only used for 1-bit detection.

Sender Message :-

S.M = 01111000[0] | 01101001[0] | 10000100[0] | 10000111[0] |
01111101[1] | 10000010[0] | 01110101[1].

R.M = 01111000[0] | 01101001[0] | 10000100[0] | 10000111[0] |
01111101[1] | 10000110[1] | 01110101[1].
replaced.

an error is occured.

* If any error is not occured, then the data received Correctly.

Problems :-

Consider the Original message as :

10101111111101011010101010110

Sol :- S: 10101111|1111010|1010101|10000000

R:- 10101111[1] 1111010[1] 1010101[1] 10000000[1]

Consider odd parity.

2-Dimensional Parity Check :-

In 2-Dimensional parity check the given is splitted into 'n' segments and each segment will have k-bits. For ex, Consider data has "Nani".

	8	4	2	1	8	4	2	1
N - 78 -	0	1	1	1	1	0	0	0
A - 65 -	0	1	1	0	0	1	0	1
N - 78 -	0	1	1	1	1	0	0	0
I - 73 -	0	1	1	1	0	0	1	1

01111000 01100101 01111000 01110011

Even Parity :-

01111000	0
01100101	0
01111000	0
01110011	1
00010110	1

Odd Parity :-

01111000	1
01100101	1
01111000	1
01110011	0
11101001	0

Check Sum :-

Check Sum is the most Common metho which will be followed by both Sender and receiver in transmitting the data.

→ To identify checksum the following procedure is used.

1) At the Sender Side the data is divided into Segments each Segments have k-bits.

2) The User will perform binary addition operation to get the Sum Value. If the Carry bits are available at the MSB bit the bit will be added to the Sum. The obtained final Sum Value will be Complemented by using is Complement. The Complemented Value is known as checksum Value.

3) At the receiver Side along with the original data checkSum bits are also

If we Consider the data NET.

At Sender Side :-

N - 01111000

E - 01101001

T - 10000100

(1) 01100101

→ 1

01100110 → By Complementing this we get, 10011001 → checkSum for SenderSide.

At Receiver Side :-

We have to add the checksum which we get in Sender Side to Original data and Complement it

```
  0 1 1 1 1 0 0 0
  0 1 1 0 1 0 0 1
  1 0 0 0 0 1 0 0
  1 0 0 1 1 0 0 1
-------------------
1 1 1 1 1 1 1 1 0
  ↳ 1
-------------------
  1 1 1 1 1 1 1 1
```

→ By Complementing this we get = 00000000.

* At the Receiver End if we get all '0's then the data transmitted Successfully and Correctly.
* In Case if the result is Combination of '0's and '1's then the received data has errors.

Consider the Network Data ?

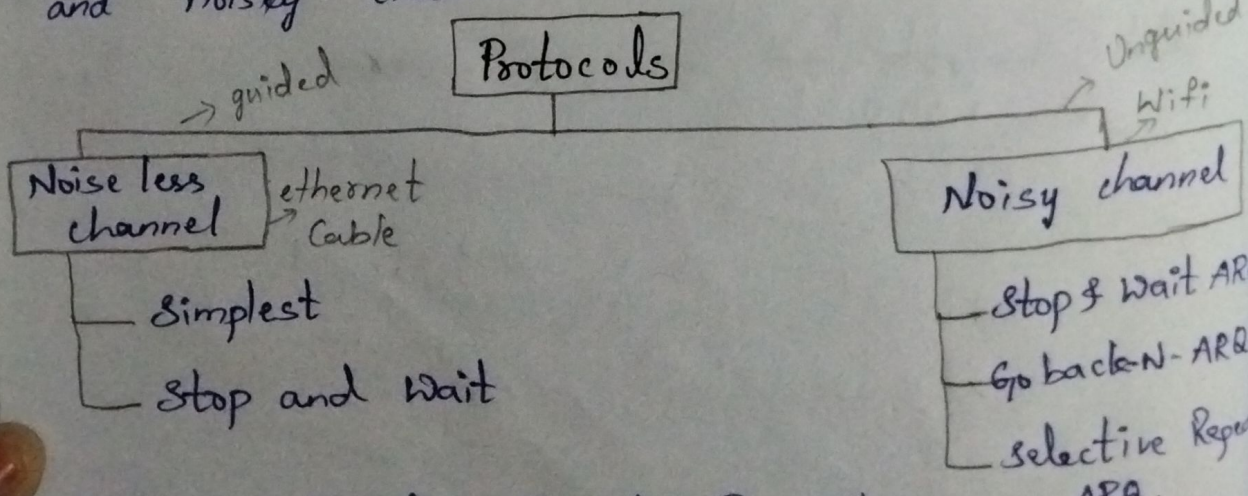
```
  0 1 1 1 1 0 0 0
  0 1 1 0 1 0 0 1
  1 0 0 0 0 1 0 0
  1 0 0 0 0 1 1 1
  0 1 1 1 1 0 0 1
  1 0 0 0 0 0 1 0
  0 1 1 1 0 1 0 1
-------------------
1 1 0 1 0 1 1 1 0 0
      1 1 -> added
-------------------
  0 1 0 1 1 1 1 1  -> By complement
  1 0 1 0 0 0 0 0  } add
-------------------
  1 1 1 1 1 1 1 1  -> Complement
```

This we get : 0 0 0 0 0 0 0 0

8 4 2 1
1 0 0
1 0
1 0 1
1 1

6/2/25

* Data link layer is divided into sublayers they are :-
  - → logical link Control (LLC)
  - → Medium Access Control (MAC)
* LLC is also known as data link Contro
* LLC is used for linking Upper and lower laye (Network layer to physical layer).
* MAC will take care about physical address of the devices.
* Both layers Combinely take care about framin flow Control and Error Control.
* In Flow Control the techinques will be Valid base on channel (transmission Medium).
* The channels are named as noise less channel and noisey channel.



ARQ - Automative Repeat Request

* Noise less channel is an ideal channel in which no frames are lost, duplicated or corrected.

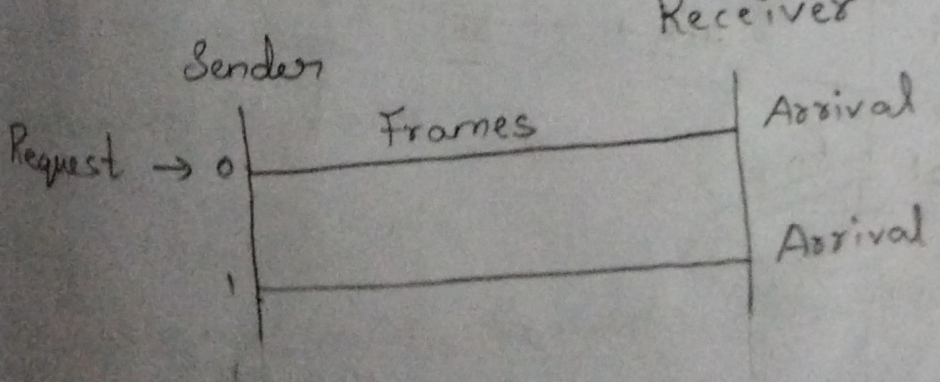
Noise less channel :-

1. Simplest Protocol :-

* This Protocol is based on two factors.
  a) Request
  b) Arrival
* It is Unidirectional.
* The Sender will Send the frames to the receiver simultaneously without receiving any acknowledgement.
* The User don't know that wheather the receiver receiving the frame Successfully or Not.
* The Sender will Send the frames one-by-one.

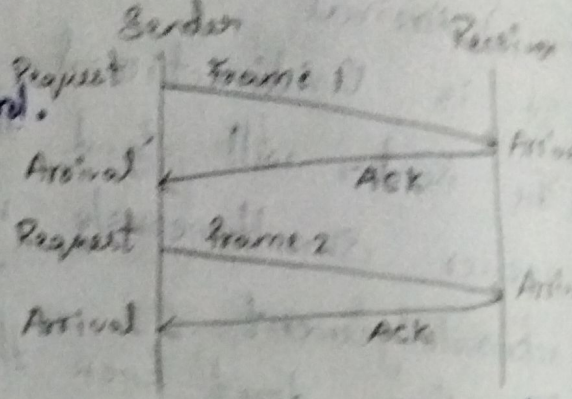
Drawbacks :-

* No acknowledgement.
* Infinite time / Amp of time.
* The Sender doesn't know that is receiver or not.



2. Stop and Wait :-

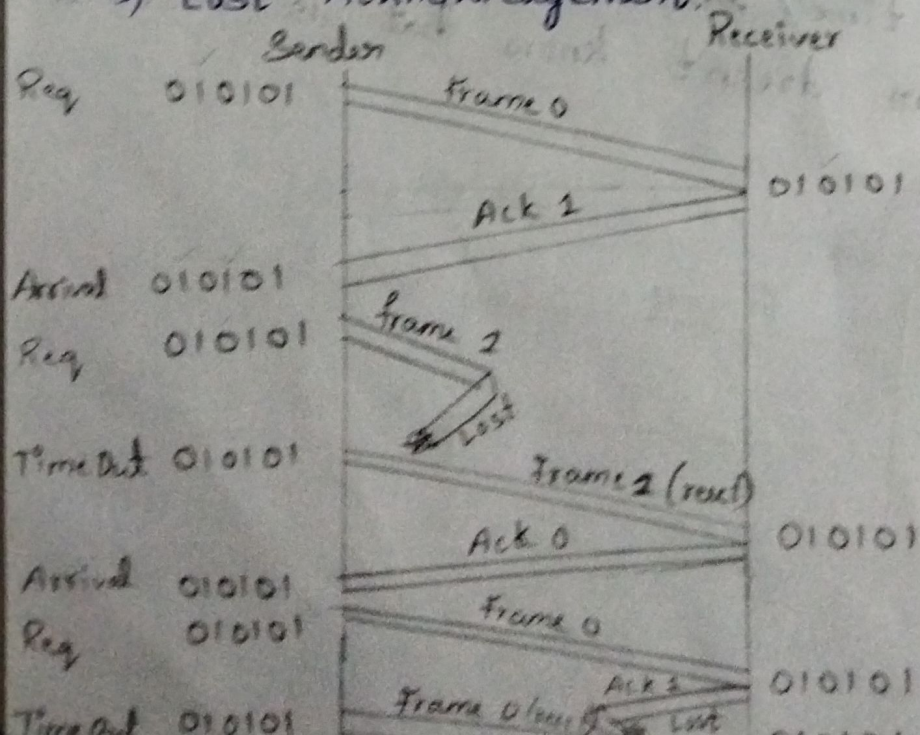
* In this protocol the sender will send the frame to the receiver and the sender will wait for the acknowledgement from the receiver.
* This will reduce the drawbacks of Simple protocol.
* Protocol with flow control.



* Noisy channel :-

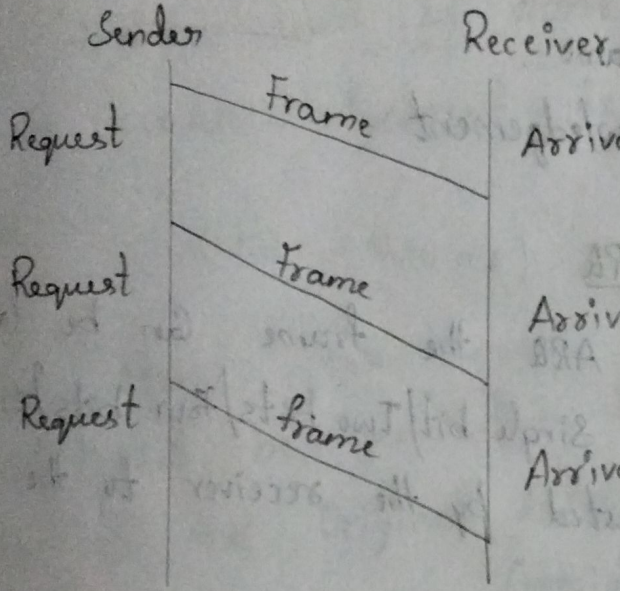
Stop and wait with ARQ

* In this protocol we are retransmitting the frames because of some conditions.
  1) Lost Frame
  2) Damaged Frame
  3) Lost Acknowledgement.



1. Simplest Protocol :-

* In Simplest protocol the Sender Sends Sequence of frames without knowing whether the receiver receive the frames or Not.
* In Simplest Protocol the Receiver will request the Sender to Send the frame. Once the frame is received the receiver will Consider the frame is arrived. (arrival Request)



2. Stop and Wait :-

* Protocol with Flow Control.
* The Sender will not transmitt the next frame until it receives the acknowledgement of the last transmitted frame.

Noisy Channel:-

* In Noisy channel the data link layer uses stop and wait ARQ and sliding window protocol.
* The wireless Communication is Considered as noisy channel. As a sliding window protocol.

we Can Use Go-Back-N-ARQ, selective Repeat ARQ

* ARQ stands for Automatic Repeat Request.
* In sliding window protocol the Sender as well as receiver has to maintain same window size.
* Based on three parameters the retransmission of the bytes Can be happen. they are :-
  a) Lost frame
  b) Damaged frame
  c) Lost Acknowledgement

Stop and Wait ARQ (1 nibble = 4 bits)

* In Stop & Wait ARQ the frame Can be Consid which Can be of Single bit/Two bits/Four bits/Eight which Can be requested by the receiver to the Sender.
* During transmission if any bit from the fram is lost that is Considered as lost frame. the retransmission of the frame will Carried based on. lost frame Condition.
* If the acknowledgement is not received from the receiver the retransmission of frame will be done.
* In Single bit error (or) Bus error occured in the frame that is Considered as Damaged frame. then also retransmission is

Sliding Window Protocol depending upon the frame size the data is moved

* slide window protocol is used to avoid error during transmission.
* A single Acknowledgement is received for the no. bits transmitted from the Sender side. If Acknowledgement is not receive after the frame transmission the resend of the frames will be done only for the bits whose acknowledgement is missing.

7/2/25

CRC :-

* CRC stands for Cyclic Redundence Code which will be generated by adding redundent bits to the Original data. Initially the redundent bits are considered as 0. Based on the no. of ~~devicer~~ divisor bits.
* for Example divisor is of k-bits the redundent bit can be k-1.
* The XOR Operation is perform to Calculate redundent bits.

XOR Truth Table

A	B	Output
0	0	0
0	1	1
1	0	1
1	1	0

* The CRC Method is applied at both Sender and Receiver at receiver side the remainder must be 0's then we can state that the transmission of data is Successful.
* The Divisor can be identified in a binary format or polynomial format.
* The Divisor can be same at both Sender as well as Receiver.

* Consider Original Data as 11011010 and the divisor has 1100. Calculate redundent bits and identify transmissi of data is Successful or Not.

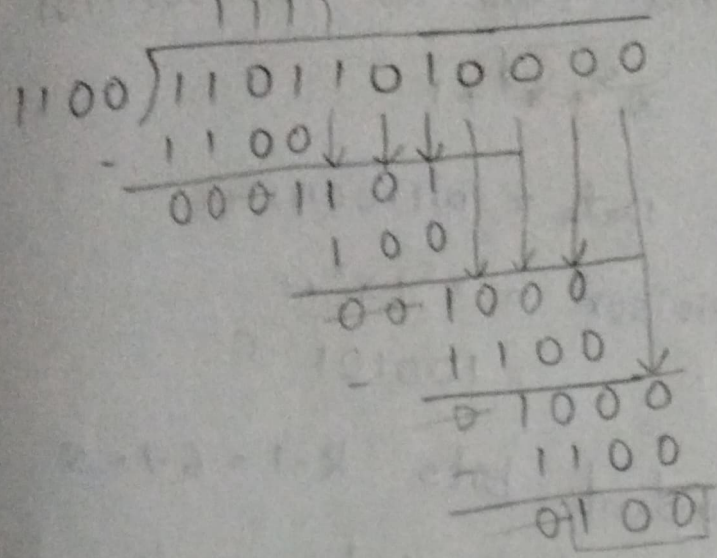
Sol:- The given divisor = 1100

No. of redundent bits = N-1 = 4-1 = 3

The Original data = 11011010

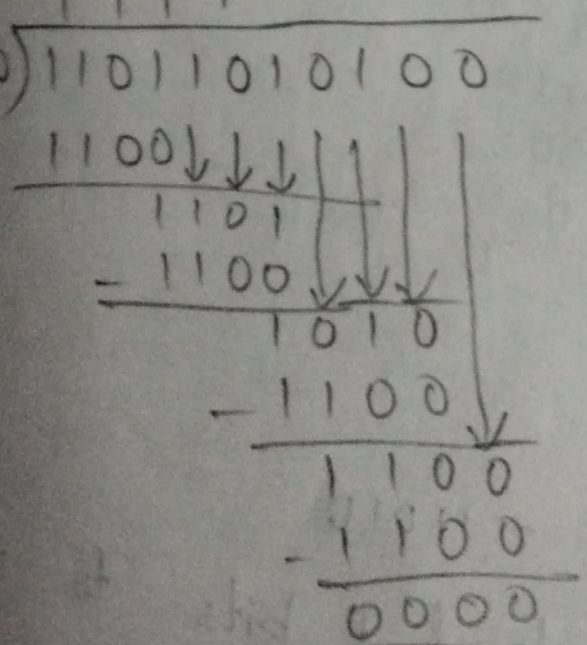
apperd the 3 redundent bits as 0's to the Original data.

= 11011010



The 3 redundent are 100.

Consider Original Data as 10111001111101 with divisor as $x^5+x^2+x^1+1$ now add the redundent bits to the Original data and perform XOR Operation.



* Consider Original Data as 10111001111101 with divisor as x^5+x^2+1

The Original Data = 10111001111101

Given Divisor = x^5+x^2+1

= 100101

The no. of redundent bits $k-1 = 6-1 = 5$

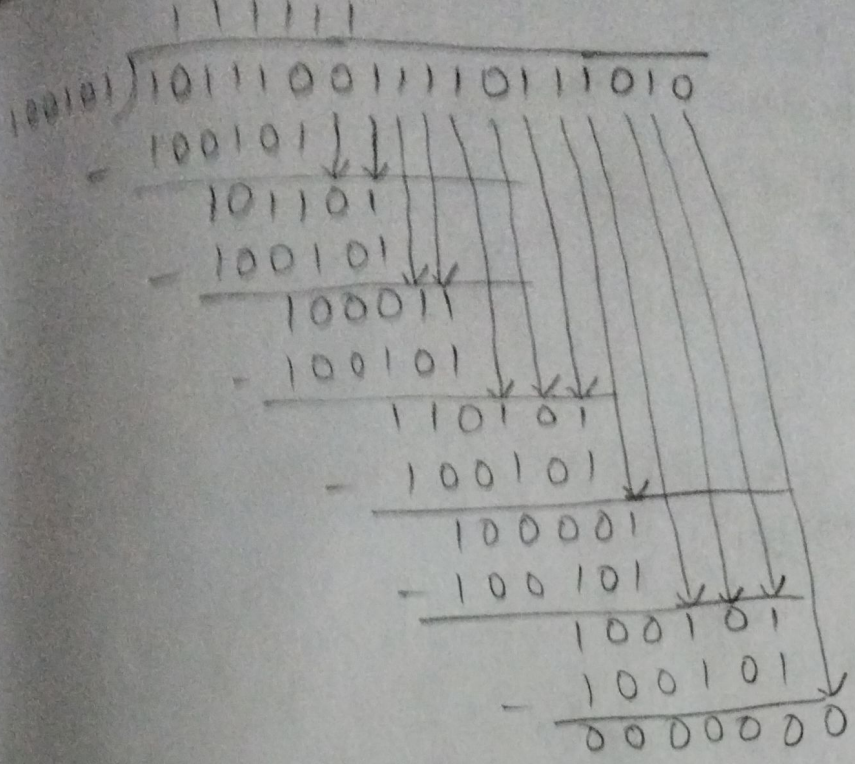
Appending the redundent bits as '0's to the original data. = 10111001111101 00000

```
                1 1 1 1 1 1
100101 ) 10111001111101 00000
         - 100101
           101101
         - 100101
           100011
         - 100101
           110101
         - 100101
           100000
         - 100101
           101000
         - 100101
           110100 → redundent bit
```

The Redundent bit = 11010

Now append the redundent bits to the Original data. = 10111001111101

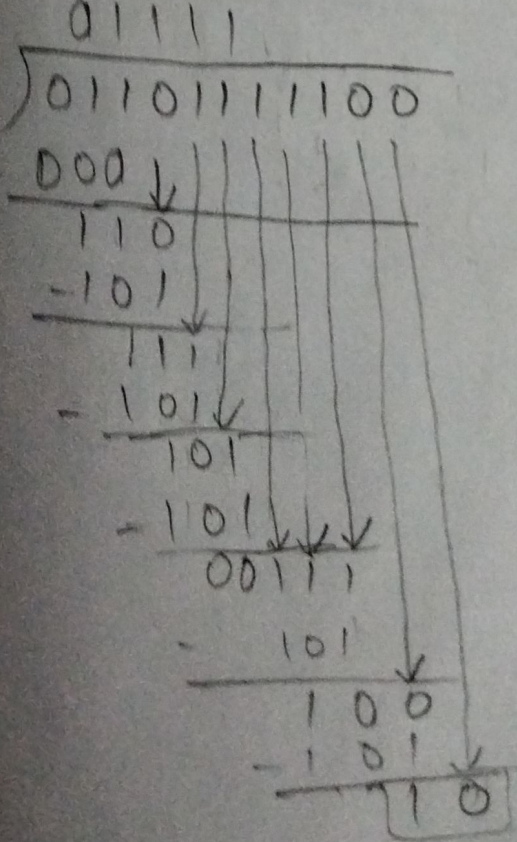
= 10111001111101 11010

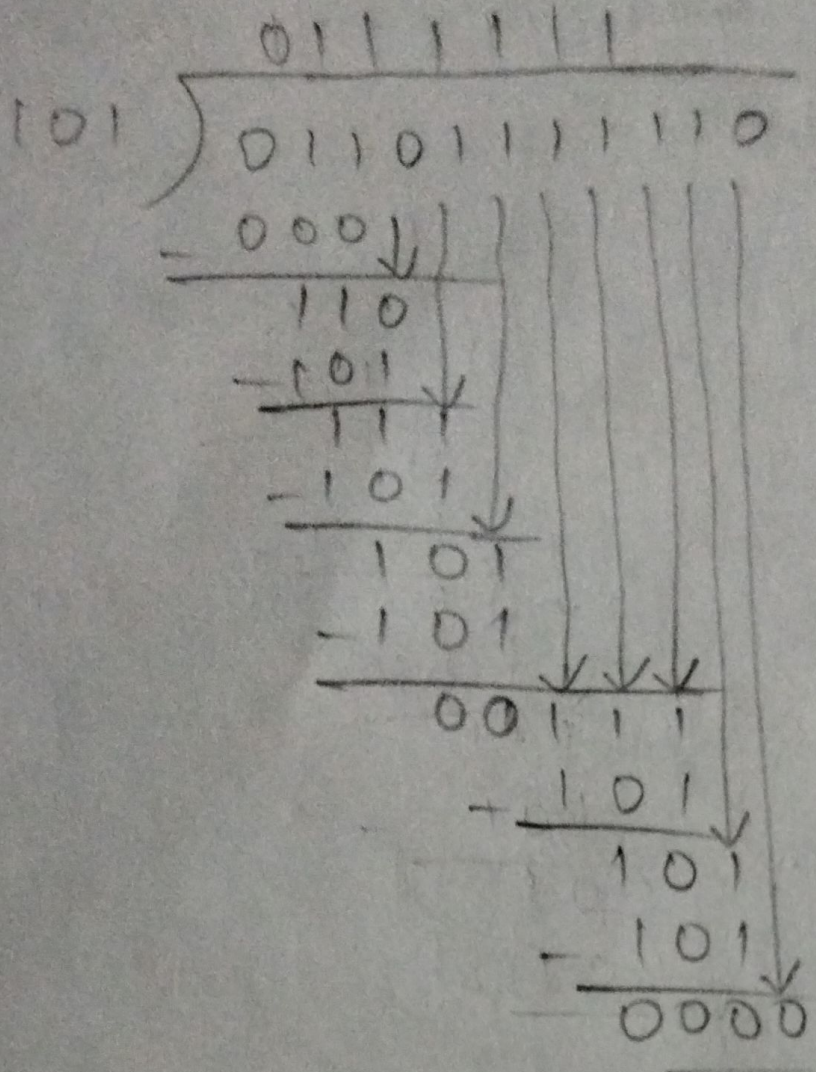


Remainder = 0000000

Hence the data transmitted successfully.

Consider the data 011011111 with divisor as 101.





Hence, the data transmitted successfully.

Co-2

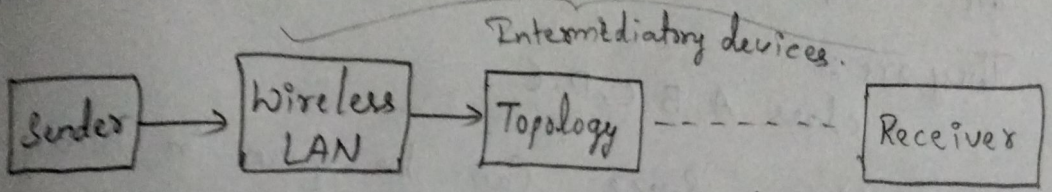
Contents:-

→ Medium Access Control Sublayer

Design Issues of Network layer :-

* The Network layer is the 3rd layer from the bottom. In this layer the frame is converted to a packet and in each packet both physical address as well as logical static address of both Source and destination must be placed along with frame of bits.
* Network layer deals with logical address which is known as IP address.
* The IP addresses can be divided into small groups or small groups can be integrated together this concept is known as Subnetting (small network) and Supernetting. (large network)
* Routing protocols are introduced in the network layer to find the best part while transfering or receiving the data.
* Routing Protocols will be taken care by Router. Each Router has Routing table which consists of IP address and MAC address of a particular devices.
* Network layer will also taken care about fragmentation of the bytes which are in

* Consider a device in Hyderabad wants to transmit data to the device which is available in Aziznagar.
* During exchange of information the Sender will come across different networks which consists of many intermediatory devices.
* Based up on the Capacity of the networks the fragmentation of the bits (division of bits) will be done by the Network layer.



MAC address & IP address is different for all the devices.

IP Addresses

* An IP address is a numeric identifier assigned to each machine on an Ip network
* It was designed to allow host devices on one network can communicate with different host device of a different network.
* ISP = Internet Service Provider.
* IP addresses are of 2 versions. They are:-
  - → IPv_4
  - → IPv_6
* IPv_4 :- The address size is 2^{32} (4294967296)
* The IPv_6 address space is 40,282,366,920,938,463,463,374,607,431,768,211,456.

* The IPv4 can be represented in Binary notation, dotted decimal notation, hexa decimal notation. (IPv6)
* In IPv4 we will see the Binary notation and dotted decimal notation.

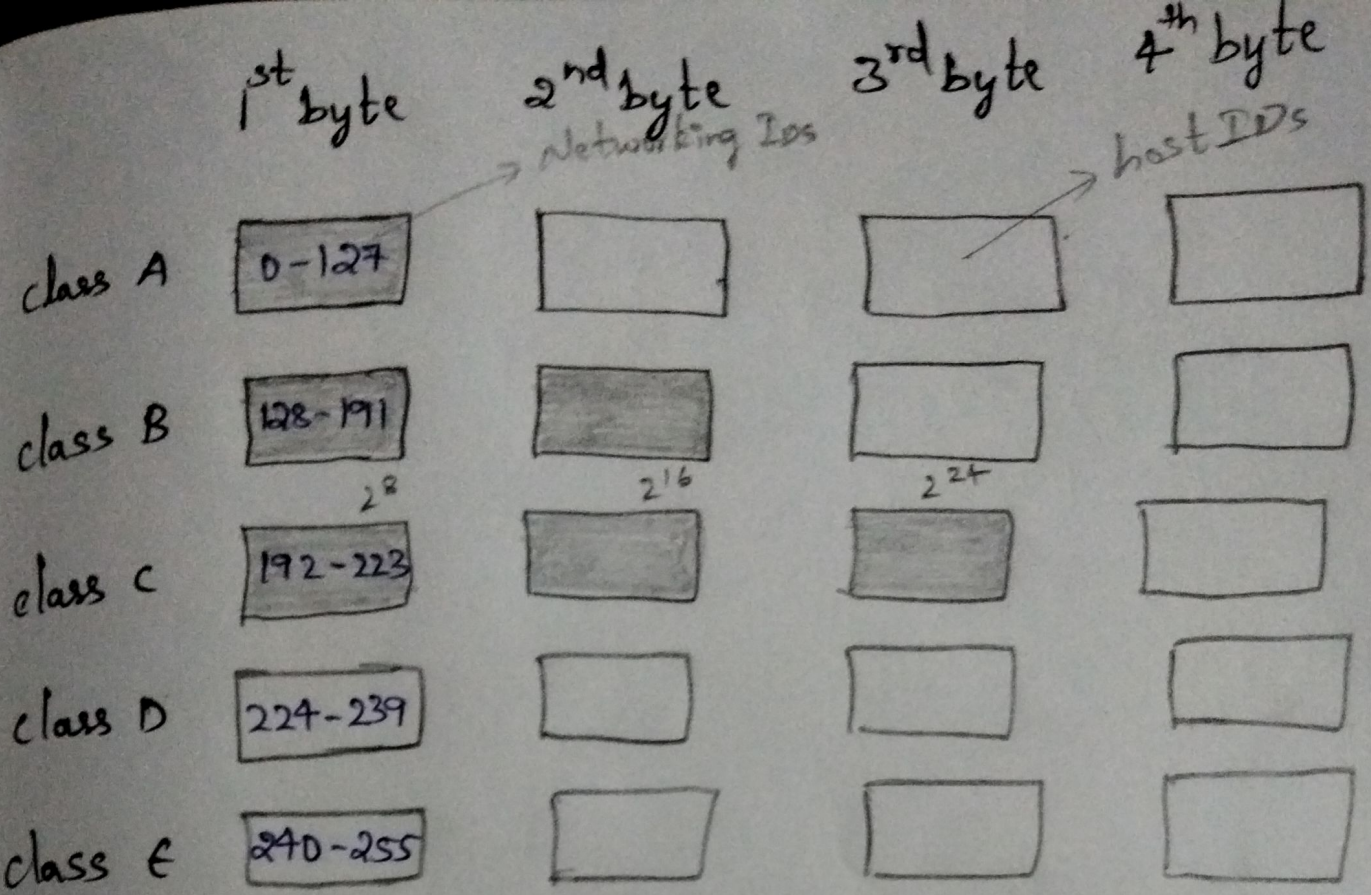
Classfull IP-Addresses :-

* The IPv4 address space is divided into 5 classes.

They are :-

* class A, B, C, D, E (D & E are not used)

* The address space can be given in Binary notation or dotted decimal notation.
* If the address is given in binary notation the first few bits tells us class of the address.
* If the Address is in dotted decimal notation the first byte define the class.
* For every IP address of a class have a by default Subnet mask. (i.e, 255.255.255.255)
* class D is reserved for multicasting applications and class E is reserved for researching applications.



Let us Consider the IP address as

133.10.90.20

By seeing the starting bits we can say that ip address belongs to class B. So in class B we have two network id's and two host id's. So we can write network IP address as.

Network IP address : 133.10.0.0

BroadCast IP address : 133.10.255.255