Computer Networks

Computer Network :- It is a set of nodes connected by Communication links.

* A node can be a Computer, Printer or any other device Capable of Sending / receiving data generated by other nodes in the network.

* A Communication link Can be a wired link or wireless link.
The link Carries the information.

Intermediary devices :- They are those devices forward / deliver data. For example router, modem Switch etc.
End devices :- The devices Consumes the data. Example Computer, Phone, Server, Tablets etc.

Characteristics of Computer Network
→ Fault Tolerance
→ Scalability
→ Quality of Service (QoS)
→ Security

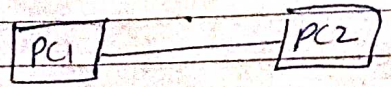
* Fault Tolerance
  ⁘ The ability to:
  → Continue working despite failures
  → Ensure no loss of Service.

* Scalability
  - The ability to:
    - Grow based on needs.
    - Have good Performance after growth.

* Quality of Service (QOS)
  - The ability to:
    - Set Priorities
    - Manage data traffic to reduce data loss, delay etc.

* Security
  - The ability to Prevent:
    - Unauthorized access
    - Misuse
    - Forgery.
  - The ability to Provide:
    - Confidentiality
    - Integrity
    - Availability

Data Communication :- Data Communications are the exchange of Data b/w two nodes via Some form of link [transmission medium] Such as a Cable.



Data Flow
- Simplex
- Half duplex
- Full duplex

→ Simplex :-) Communication is always in one direction.
-) one device can transmit & the other device will receive.
-) Example :- Keyboards, Traditional Monitors

→ Half Duplex :-) Communication is in both directions but not at the Same time.
-) If one device is Sending, the other can only receive, & vice versa.

Example :- Walkie-Talkies.

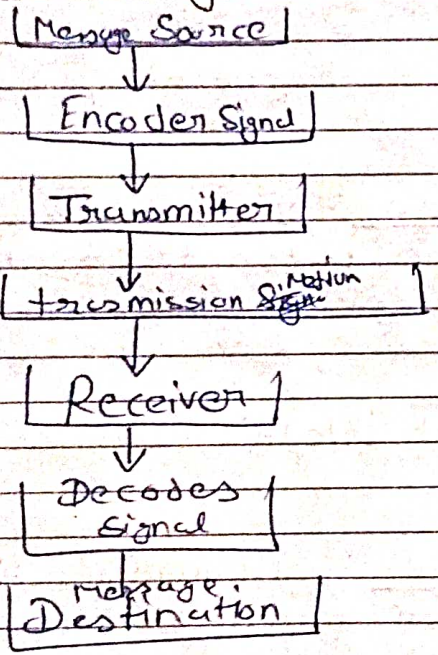
→ Full Duplex :-) Communication is in both direction Simultaneously.
-) Device Can Send & receive at the Same time.
-) Example :- Telephone line.

Protocols

All Communication Schemes will have the following things in Common:
-) Source or Sender) Destination or Receiver) Channel or Media
-) Rules or Protocols govern all methods of Communication.

Protocols used in NC also define:
* Message Encoding
* Message formatting and Encapsulation
* Message timing
* Message Size
* Message delivery options.

→ Message Encoding.



→ Message Formatting & Encapsulation
Agreed format
Encapsulate the information to identify the Sender & the receiver rightly.

→ Message Size
Humans break long Messages into Smaller Parts or Sentences.

Long messages must also be broken into Smaller Pieces to travel across a network

→ Message Timing
Flow Control:- [Sender is fast but receiver is slow so to maintain this]
Response Timeout:- [if Sender Sends data to the Receiver then Receiver has to acknowledge the data for the Confirmation.]

→ Message Delivery Options.
* Unicast:- [one Sender & one receiver]
* Multicast:- [one Sender & Set of receiver not all receiver]
* Broadcast:- [one Sender & multiple receiver]

Peer-To-Peer-Network

* No Centralized administration.
* All Peers are equal.
* Simple Sharing applications
* Not Scalable.

Client Server Network
* Centralized administration
* Request-Response model
* Scalable
* Server may be overloaded.

Media

Wired Medium [Guided Medium]
Wireless Medium [Unguided Medium]

Wired Media

Ethernet Straight-through cable
Ethernet Crossover cable
Fiber optic cable
Coaxial Cable
USB Cable.

Wireless Media

Infrared [short range communications]
Radio [Bluetooth, Wifi]
Microwaves [Cellular System]
Satellite [long range communication-GPS]

Services

e-mail	online game
Storage services	voice over IP
File sharing	video telephony
Instant messaging	world wide web.

Classification of Computer Networks

1. LAN
2. WAN
3. MAN

LAN {Local Area Network}

A LAN is a Computer Network that interconnects Computers within a limited area such as a residence, School, laboratory, university Campus etc.

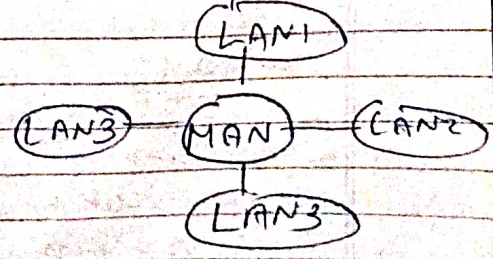
LAN Devices

* Wired LAN [Ethernet - Hub, Switch)
* Wireless LAN [Wi-Fi]

Note:- Ethernet Straight through Cable used to Connect different devices.

MAN [Metropolitan Area Network]

A MAN is a Computer network that interconnects users with Computer Resources in a geographic region of the size of a metropolitan area (City).



MAN Devices

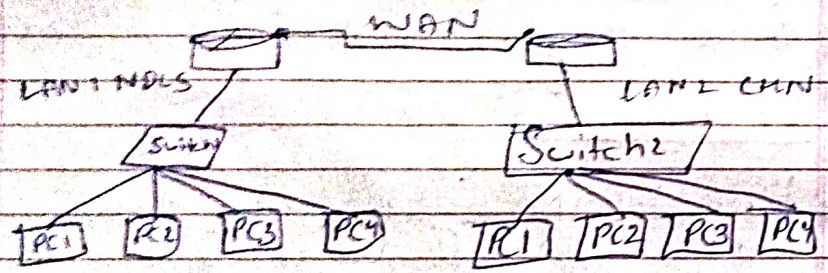
* Switches/Hub
* Routers/bridges

WAN [Wide Area Network]

A WAN is a telecommunications network that extends over a large geographical area for the primary purpose of computer networking.

WAN Devices

End devices & intermediary devices.



Storage Area Network (SAN)

Cloud Computing
It is the on-demand availability of Computer System resources, especially data Storage & Computing Power, Without direct active management by the user.

Topology

Connection of nodes or Arrangement of nodes of a Computer network.
Topology = layout

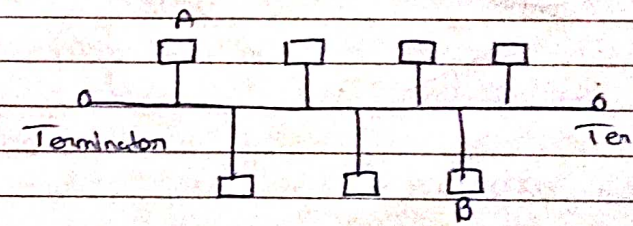
Physical Topology :- Placement of nodes.

Logical Topology :- Deals with the data flow in the network.

Network Topology

* All data transmitted between nodes in the network is transmitted over this common transmission medium & is able to be received by all nodes in the network simultaneously.

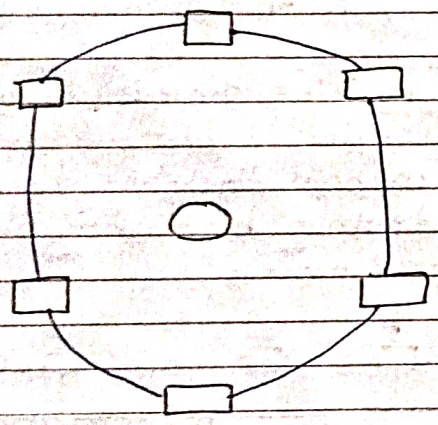
* A signal containing the address of the intended receiving machine travels from a source machine in both directions to all machines connected to the bus until it finds the intended recipient.



Advantages	Disadvantages
→ only one wire - less expensive	→ Not fault tolerant
→ Suited for temporary network.	→ Limited cable length
→ Node failures does not affect others.	→ No security

Ring Topology

* A ring topology is a bus topology in a closed loop.
* Peer to Peer LAN Topology.
* Two connections one to each of its nearest neighbors.
* Unidirectional.
* Sending & receiving data takes place with the help of a Token.

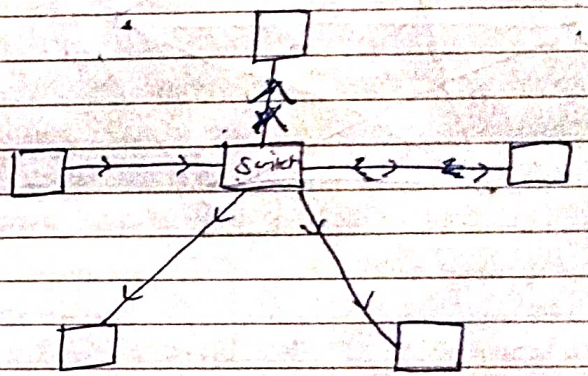


Ring Topology

Advantages	Disadvantages
* Performance better than Bus topology.	* Unidirectional Single Point of failure will affect the whole network.
* Can cause bottleneck due to weak links.	* ↑ In load → ↓ in Performance.
* All nodes with equal access.	* No security.

STAR Topology

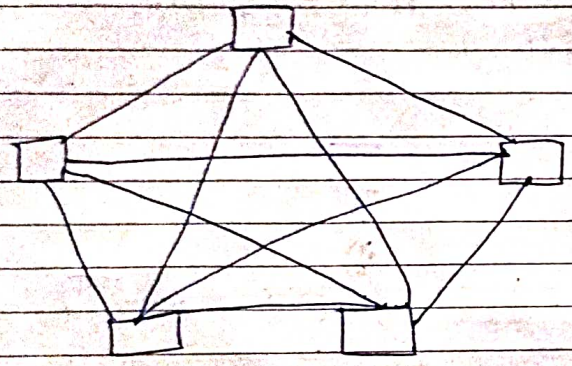
* Every node is connected to a Central node Called a hub or Switch.
* Centralized Management
* All traffic must pass through the hub or Switch.



Advantages	Disadvantages
* Easy to design & implement.	* Single Point of failure affects the whole network.
* Centralized administration	* Bottlenecks due to overbaded Switch/Hub.
* Scalable.	* Increased Cost due to Switch/Hub.

Mesh Topology

* Each node is directly Connected to every other nodes in the network.
* Fault tolerant & reliable.



Advantages
* Fault tolerant
* Reliable.

Disadvantages
* Issues with broadcasting messages.
* Expensive & impractical for large networks.

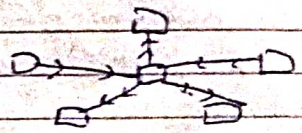
Hybrid Topology

Combination of Multiple Topology is Called Hybrid Topology.

Ring Topology

no. of nodes (N)	no. of cables (=N)	no. of Ports/device (NOP)	Total no. of Ports in the network (TNOP) = N×NOP
2	2	2	4
3	3	2	6
4	4	2	8
N	N	2	2×N

STAR TOPOLOGY



no. of nodes (N)	no. of cables (=N)	no of Ports/device (NOPD)	Total no. of Ports in the network (TNOP) = 2×N
2	2	1	4
3	3	1	6
4	4	1	8
N	N	1	2×N

Mesh Topology

no. of nodes N	no. of cables ((N-1)N)/2	no. of Ports/device (NOPD)	Total no. of Ports in the network (TNOP) = N×(N-1)
2	1	1	= 2
3	3	2	= 6
4	6	3	= 12
N	((N-1)N)/2	(N-1)	= N×(N-1)

IP Address

* I.P Stands for Internet Protocal.
* Every node in the Computer network is identified with the help of IP address.
* Logical address.

IP (IPV4)

* It can be change based on the location of the device.
* Assigned by Manually or dynamically
* Represented in decimal & it has 4 octets
* 0.0.0.0 to 255.255.255.255 (32 bits)

MAC Address

* MAC - Media Access Cotrol.
* Every node in the LAN is identified with the help of MAC address.
* IP address = location of a Person.
* MAC address = Name of the Person.

* IP - Router Friendly
* MAC - Switch Friendly

* Physical address or Hardware Address.
* Unique.
* Can't be changed.
* Assigned by the Manufacturer.
* Represented in hexadecimal.
* Ex:- 70-20-84-00-ED-FC [48 bits]
* Seperator :- hyphen (-), Period(.), and Colon(:)

IP Address	MAC address
* Needed for Communication	* Needed for Communication
* 32 bits	* 48 bits
* Represented in Decimal.	* Represented in hexadecimal
* Router needs ip address to forward data.	* Switch needs MAC address to forward data.
* Ex:- 10.10.23.5C	* Ex:- 70-20-84-00EDFC

Derivations From Analogy

Reaching our City = Reaching our network [IP Address]

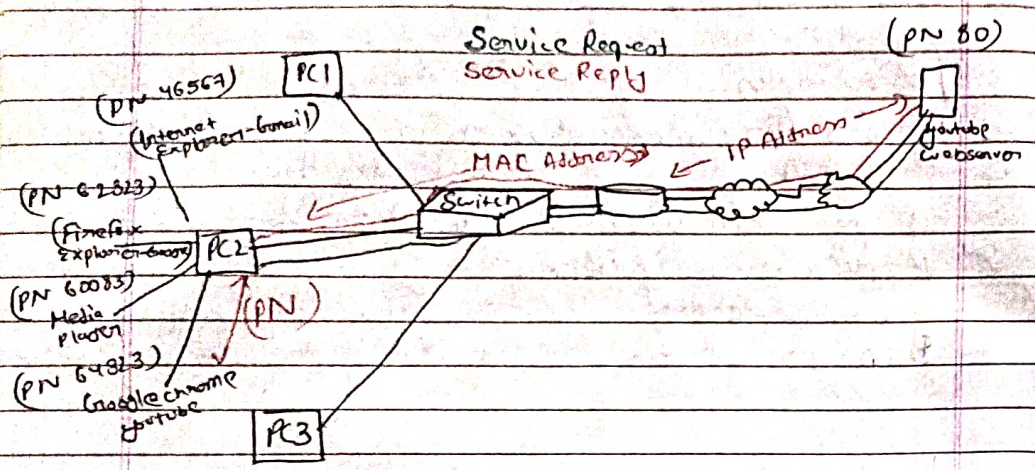
Reaching our Apartment = Reaching the host. [MAC Address]

Reaching the right Person = Reaching the right Process [Port Address]

Port Address or Port Number

* In a node, many Processes will be running.
* Data Send/Received must reach the right process.
* Every Process in a node is uniquely identified using port numbers.
* Port = Communication endpoint.
* Fixed port numbers & dynamic port numbers [0 - 65535]

Ex:- Fixed Port no. : 25, 80 etc.
OS assigned dynamic port numbers: 6249



Use "Resmon" to See PN

Circuit Switching

* A dedicated Path is established between the Sender & receiver.
* Before data trasfer, Connection will be established first.
* Ex. Telephone network.

3 Phases in Circuit Switching.
→ Connection establishment.
→ Data trasfer.
→ Connection Disconnection

Message Switching

→ Store & forward mechanism
→ Message is trasferred as a Complete unit & forwarded using Store & forward mechanism at the intermediary node.
→ Not Suited for Streaming media & real-time applications.

Packet Switching

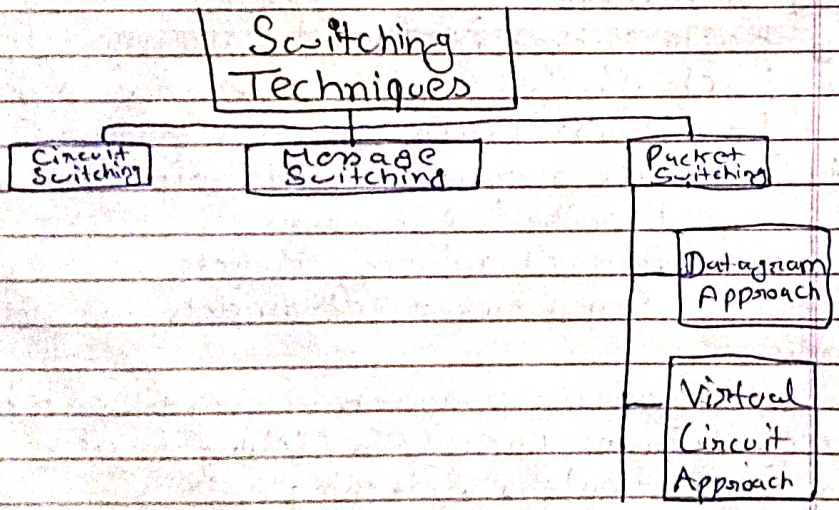
* The internet is a Packet Switched network.
* Message is broken into individual Chunks Called as Packets.
* Each Packet is Sent individually.
* Each Packet will have Source & destination IP address with Sequence number.
* Sequence numbers will help the receiver to
  - ·) Reorder the Packets
  - ·) Detect missing Packets
  - ·) Send acknowledgements

Datagram approach - Packet Switching

·) Datagram Packet Switching is also known as Connectionless Switching.
·) Each independent entity is Called as datagram.
·) Datagrams Contain destination information & the intermediary devices uses this information to forward datagrams to right destination.
·) In Datagram Packet Switching approach, the Path is not fixed.
·) Intermediate nodes take the routing decisions to forward the Packets.

Packet Switching - Virtual Circuit Approach.

* Virtual Circuit Switching is also known as Connection-oriented Switching.
* In the case of Virtual Circuit Switching, a preplanned route is established before the messages are sent.
* Call request & Call accept Packets are used to establish the Connection between Sender & receiver.
* In this approach, the Path is fixed for the duration of a logical Connection.



Layering

* It means decomposing the Problem of building a network into more manageable Components (Layers).
* More modular design & easy to troubleshoot.

The OSI Model

* The Purpose of the OSI model is to facilitate Communication between different systems without requiring changes to the logic of the underlying hardware & Software.

layers in the OSI REFERENCE MODEL

Shortcut

away
Pizza
Sausage
Throw
not
Do
Please

Application layer
Presentation layer
Session layer
Transport layer
Network layer
Data link layer
Physical layer

{Intermediate node access}

{Bottom up approach.}

Application Layer

It enables the user to access the network resources.

Services Provided by applications layer
* File Trasfer & access Management [FTAM]
* Mail Services
* Directory Services.

Presentation Layer

It is Concerned with the Syntax & Semantics of the information exchanged b/w two Systems.

Services Provided by P.L.
* Translation
* Encryption
* Compression

Session Layer

It establishes, main & Synchronizes the interaction among Communicating devices.

Services Provided By Sesion layer
* Dialog Control
* Synchronization

Transport layer

: It is responsible for Process to Process delivery of the entire message.

Services Provided By TL
* Port addressing
* Segmentation & Reassembly
* Connection Control
* End-to-End Flow Control
* Error Control

Network layer

It is responsible for delivery of data from the original Source to the destination network.

Services Provided By Data link layer
* Framing
* Physical Addresing
* Flow Control
* Error Control
* Accen Control

Physical Layer

It is responsible for transmitting bits over a medium. It also Provides electrical & mechanical Specifications.

Services Provided By Physical Layer
* Physical characteristics of the media.
* Representation of bits.
* Data rate.

* Synchronization of bits.
* Line Configuration
* Physical Topology.

Services offered by Each layer

Application layer
FTAM, Mail Services & Directory Services

Presentation layer
Translation, Encryption & Compression

Session Layer Dialog Control & Synchronization.

Transport layer Port addressing, Segmentation & Reassembly, Connection Control, Flow Control & Error Control.

Network layer Logical Addressing & Routing

Data link layer Framing Physical Addressing Flow Control, Error Control, & Access Control

Physical layer Physical Characteristics of the media, Representation of bits, Data rate, Synchronization of bits, Line Configuration, Physical Topology & Transmission mode.

OSI Reference Model Vs TCP/IP Model

OSI Reference Model		TCP/IP Model
Application layer	HTTP, DNS, DHCP, FTP	Application
Presentation layer		
Session layer		
Transport layer	TCP, UDP	Transport
Network layer	IPV4, IPV6, ICMPV4, ICMPV6	Internet
Datalink layer	PPP, Frame Relay, Ethernet	Network Access
Physical layer		

Application :- Represents data to the user, Plus encoding & dialog Control.

Transport :- Supports Communication b/w diverse devices across diverse networks.

Internet :- Determines the best Path through the network.

Network Access :- Controls the hardware devices & media that make up the network.

The TCP/IP Protocol Suite

Application Layer :-

Name System	Host	Email	File	Web
DNS	Config	SMTP	Transfer	HTTP
	BootP	POP	FTP	
	DHCP	IMAP	TFTP	

Transport layer
UDP TCP

Internet layer

IP	IP Support	Routing Protocols
NAT	ICMP	RIP/OSPF/EIGRP/BGP

Network Access layer
ARP PPP Ethernet Interface Drivers

PDU (Protocol Data units)
PDU are named according to the Protocols of the TCP/IP Suite : data, Segment, Packet, Frame, & bits.

Application layer - Data
Transport layer - Segment
Network layer - Packet
Data link layer - Frame
Physical layer - Bits.

Basic Commands of Networking

① IPCONFIG :- It will give you a IP address of a network.

② IPCONFIG/ALL :- It will give you a MAC address.

③ nslookup :- It also helps us to redirect to new computer.
ping :- allow us to to access the IP address

④ Tracert :- Server It shows the Several details about the Paths that a Packet takes from one Computer to another.

Cisco Packet Tracer

* Cisco :- The leaders in networking.
* An innovative & powerful networking Simulation tool used for Practice, discovery & troubleshooting
* Helps to understand networks Practically.

HUB

* A network Hub
* Hub works at the Physical layer of the OSI model.
* Used to Set up LAN
* Has multiple Ports.
* Star topology

* When a Packet arrives at one Port, it is Copied to the other Ports so that all Segments of the LAN Can See all Packets.
* It works in Half duplex mode.

Hub Pros & Cons

Pros

* Cheaper than Switches
* Works good for Smaller network

Cons

* Issues with broadcast
* No memory.
* normally runs in half duplex mode.

Router

* A router is a networking device that forwards data Packets between Computer networks.
* A router is Connected to at least two networks Commonly two LAN's ~~of~~ or WAN's or a LAN & its ISP's network
* It is a layer 3 (Network layer) device.
* Stores routing table.

Switch	Router
* A network Switch is a Computer networking device that is used to Connect many devices together as a Computer network.	* A router is a networking device that Connects a local network to other local networks
* Operates at Data link layer. [Layer 2 Device]	* Operates at a network layer. [Layer 3 Device]
* Has memory & Stores MAC address Table.	* Has memory & Stores Routing table.
* Decisions are taken based on MAC address.	* Decisions are taken based on IP address
* Half/Full duplex	* Full Duplex
* LAN	* WAN, LAN & MAN

Switch

* A Switch is a Networking hardware that Connects devices on a Computer network to establish a local area network.
* Unlike hub, Switch has memory.
* Stores MAC Address Table.
* layer 2 Device for Setting up LAN

Hub	Switch
* Layer 1 device	* Layer 2 device
* Works at Physical Layer	* Works at Data link Layer.
* Has no memory	* Has memory & Stores MAC Address Table.
* Not an intelligent device	* Intelligent device.
* Floods the network due to broadcasting.	* Can do unicasting, multicasting & broadcasting
* Security risks are high.	* Security risks are low.
* Less efficient	* More efficient
* Half-duplex	* Full Duplex.

Repeaters

* The data Signals generally become too weak or Corrupted if they tend travel a long distance.
* Repeater regenerates the Signal over the same network.
* It operates at the physical layer.
* They do not amplify the Signal.
* It is a 2-Port device.

Bridge

* Bridge = Repeater + functionality of reading MAC address
* It is a layer 2 device
* It is also used for interconnecting two LAN's on the same Protocol.
* It is also a two Port device.

Types of Bridges

* Transparent Bridges
* Source Routing Bridges

Transparent Bridge

* These are the bridge in which the Stations are Completely unaware of the bridge's existence.
* Reconfiguration of the Stations is unnecessary even if bridge is added or removed from network.

Source Routing Bridges

* In these bridges, routing operation is Performed by Source Station & the frame Specifies which route to follow.

List of Various Network Devices

* Repeater
* Hub
* Switch
* Bridge
* Router
* Multi-layer Switch [layer 3 Switch] (Switch + Router)
* Brouter (Bridge + Router)
* Modem [Modulator & demodulator]
* Firewall [Security Device]

Fundamental Principles of Physical Layer

* One of the major functions of the Physical layer is to move data in the form of electromagnetic signals across a transmission medium.
* The data usable to a Person or an application are not in a form that can be transmitted over a network.
* For example, an image must first be changed to a form that transmission media can accept.
* To be transmitted data must be transformed to electromagnetic signals.

Signal

It is a function that represents the variation of a Physical Quantity with respect to time.
Example:- Variation in temperature of a city in one day i.e 24 hours.
Analog Signal & Digital Signal

Analog Signal

It is the signal that can take any value in the defined range.
All real-life signals are analog in nature.

Digital Signal

It is the signal that can take on of the finite values at any given time.
In case of digital signals, we discretize both time & magnitude.

Comparison of Various Physical Media

Media	Physical Components	Signal
Copper Cable (Wired)	) UTP / STP ·) Coaxial ·) Connectors) NICs ·) Ports / Interface	Electromagnetic Signal
Fiber optic Cable (Wired)	·) Single-mode Fiber ·) Multimedia Fiber ·) Connectors ·) NICs & Interfaces ·) Lasers & LEDs	·) Light Pulse equals 1 ·) No light Pulse equals 0.
Wireless Media	·) Access Points) NICs ·) Radio) Antennae	·) Radio Wave

Wired Media

* Copper Cable [Ethernet Cable]
  -) Unshielded Twisted Pair (UTP)
  -) Shielded Twisted Pair (STP)
* Copper Coaxial cable
* Fiber optic Cable.

Crosstalk

* UTP Cable does not use shielding to Counter the effects of EMI & RFI.
* The negative effect of Crosstalk Can be limited by Varying the no. of twists Per wire Pair.

Fiber optic Media

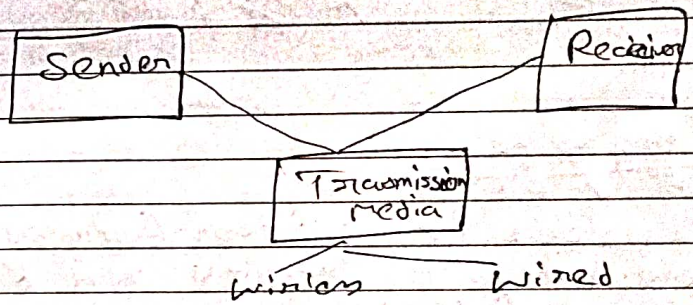
* Light waves
* High Speed Transmission.

Wireless Media [following ares of Concern]

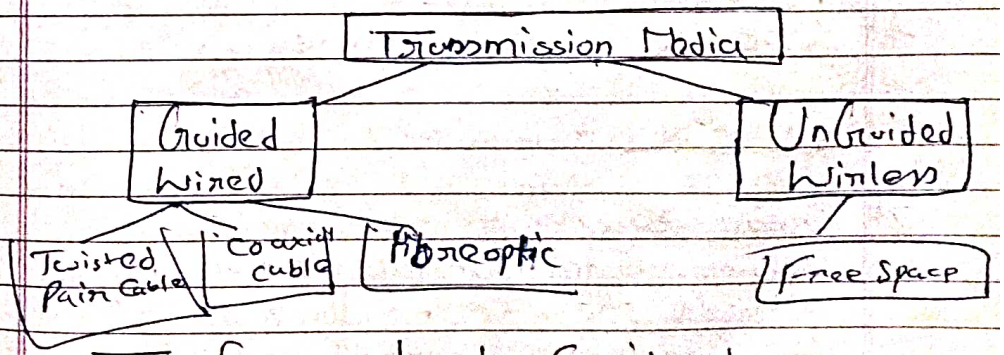
* Coverage crea
* Interference
* Security.

Transmission Media

* To send our data from one Place to another is Called TM
* The first layer [Physical layer] of Communication between OSI Seven layer model is dedicated to transmission media.
* It is a Physical Path between transmitter & Receiver.
* Repeater or amplifier may be used to Extend the length of medium.



Classes of Transmission Media



The factors to be Considered

1. Transmission rate
2. Cost & Ease of installation
3. Resistence
4. Distance.

Unguided Media

Radio Waves

* Frequency 3 KHz to 1 GHz
* Highly regulated, omni directional antennas [Spread out in all directions]
* Can Penetrate through walls.
* Multicast Communications such as Television and Telephone.

Microwaves

* It is used for unicast Communications.
* Telephone → Satellite n/w & wireless LAN's.
* Higher frequency ranges can't Penetrate walls.
* Uses directional antenna.

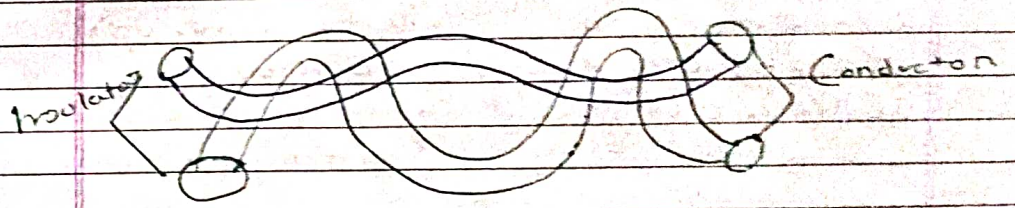
Infrared

* These signals can be used for Short range Communication in a closed area using line of sight Propagation.
* Eg. TV remote, Wireless Speakers etc.
* Due to Short range, it is considered to be one of the most Secured transmission media.

Guided Media

Twisted Pair Cable :-

* It Consists of two insulated Copper wires arranged in Spiral Pattern to minimize the electromagnetic interference b/w adjacent Pairs.
* Customer facilities & over distance & data Communications.
* Low frequency transmission medium.

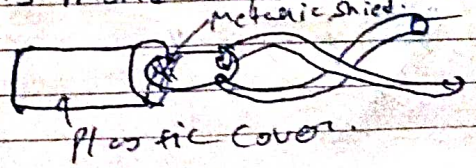


2 types of Twisted Pairs (T.P.)

1. STP [Shielded T.P.]
2. UTP [Unshielded T.P.]

→ STP

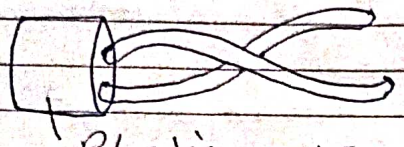
* The pair is wrapped with metallic foil to insulate the pair from Electromagnetic interface
* It is more expensive & harder to work.



(B)

→ UTP

Each wire is insulated with Plastic wrap but the Pair is encased in an outer covering.



Plastic sheathes

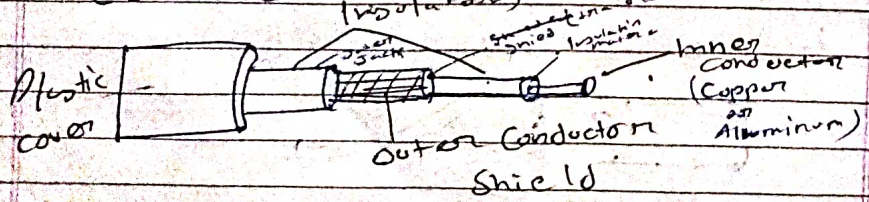
3 UTP	5 UTP
Data rates upto 16 mpps are achievable.	* Data rates upto 10 mbps. * More expensive * Better performance.

Coaxial Cable :-

Used for Cable Television, LAN's & telephone.

Has an inner Conductor Surrounded by braided mesh.

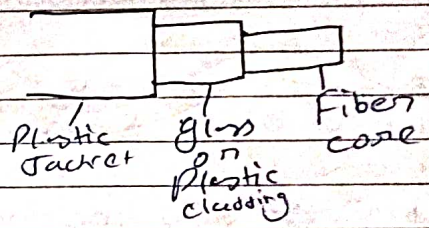
Both Conductors Share a Common Central axial, hence the term "Co-axial".



Fiber optic Cable

* New transmission Medium [For Telecom]
* long distance lines
* Used by Private Companies in implementing local data Communication ~~bto~~ networks.
* Requires a light Source with Injection laser Diode [ILD] Light emitting Diode [LED]

3 Concentric Sections Section



3 Types

① Multimode Step index fiber.
The reflective walls of the fiber moves the light Pulses to the Receiver.

② Multimode graded index fiber
Acts to refract the light towards the Center of the fiber by Variation in density.

③ Single Mode fiber
The light is guided down the center of an extremely narrow core.

Advantages

* Greater Capacity (2Gbps)
* Smaller size & lighter weight
* Lower attenuation
* Immunity to Environment.
* highly secure.

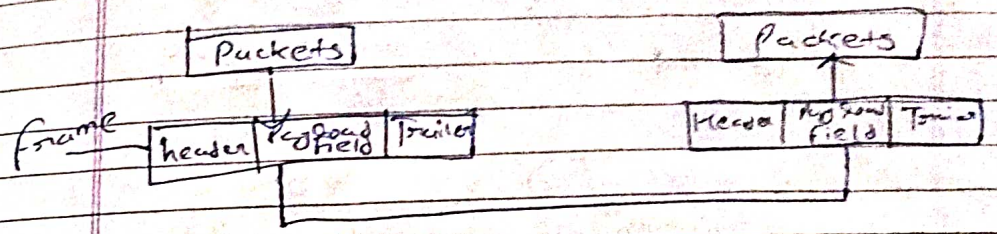
Disadvantage

* ~~Over~~ Expensive over short distance.
* Requires highly skilled installers.
* Adding additional nodes is difficult.

Data Link layer Design Issues

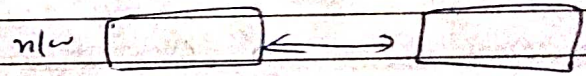
* Services Provided to N/w layer.
* Framing.
* Error Control
* Flow Control.

Functions of DLL



① Services Provided to Network layer
→ Unacknowledge Connectionless Service.
→ Acknowledge Connectionless Service.
→ Acknowledge Connection ~~less~~ oriented Service

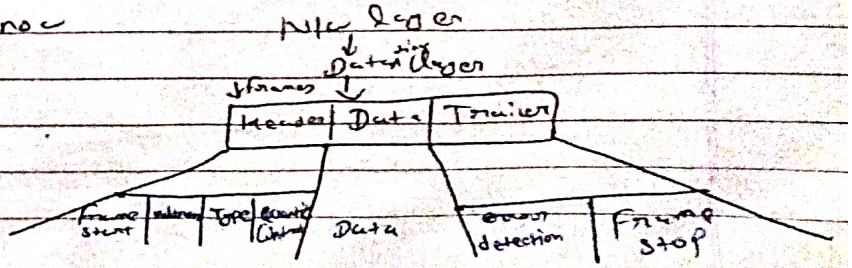
These are the Service Provided ~~by~~ to network layer by Data link layer.



Framing in DLL

Framing is a function in DLL that Provides a way to the Sender to transmit the set of bit that are meaningful to the receiver.

We know



Types of Frames

① Fixed length Frame
② Variable length Frame.

Eg. 200 bits of data to transmit

① Fixed length [how many frames?]

$20 \times 10 = 20$

10 frames

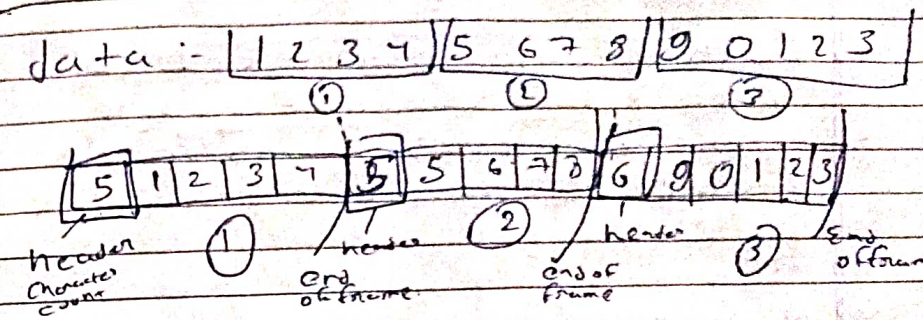
② Variabl length [how many frames?]

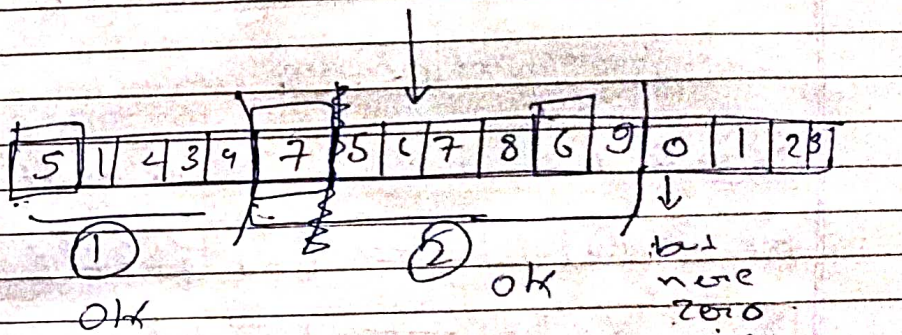
Only 1 frame 200 bits.

Four methods can be used to mark the start & end of each frame.

* Character Count
* byte Stuffing
* bit Stuffing
* Physical layer Coding Violations

Character Count





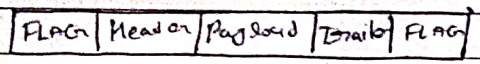
{means here data is not in Synchronized format}

Flag byte with byte Stuffing.

=) Each Frame Start & End with Special byte called Flag byte.

=) If the flag bytes occurs in the frame, Stuff an extra escape byte (ESC)

(a) A frame delimited by flag bytes

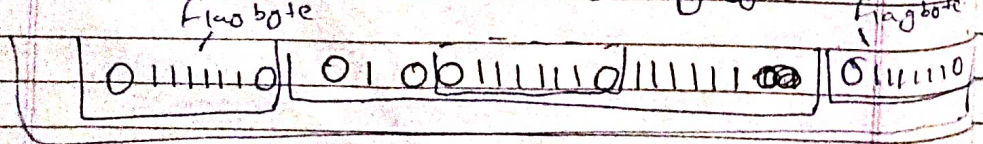


Signal Char			After Stuffing.			
A	FLAG	B	→	A	ESC	B
A	ESC	B	→	A	ESC	ESC	B
A	ESC	FLAG	B	→	A	ESC	ESC	ESC	B
A	ESC	ESC	B	→	A	ESC	ESC	ESC	ESC	B

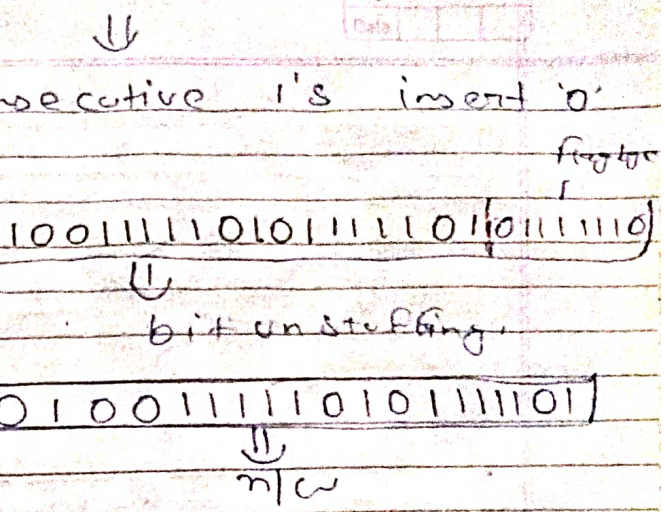
Bit Stuffing

The beginning & end of each frame. A Specific bit pattern

01111110 => flag byte



Data link layer



Physical layer Coding Violations.

* Encoding Violation is a method that is used only for n/w in which Encoding on physical medium include some sort of redundancy.

* LAN'S Encode: Each bit of data is represented by two Physical bit.

Eg. Manchesters Encoding => 1 => 10 {high-low}
0 => 01 {low-high}
low-low => 00 {not used for data}
high-high => 11 {may use for frame boundaries}

=) In order to operate a division b/w frames in DLL this approach Exploits the redundancy. So end Codes '00' & '11' Can be used as Escape b/w DL frame thus Violating Physical layer encoding

Switching

* Switching in Computer network helps in deciding the best route for data transmission if there are multiple Paths in a larger network.
* One-to-one Communication

Three types

- Circuit Switching
- Message Switching
- Packet Switching
  - Datagram approach
  - Virtual Circuit approach

Circuit Switching

* A dedicated Path is established between the Sender & Receiver.
* Before data transfer, Connection will be established first.
* Ex:- Telephone network.

3 Phases in Circuit Switching

1. Connection establishment
2. Data transfer
3. Connection Disconnection

Message Switching

* Store & forward mechanism
* Message is transferred as a Complete unit & forwarded using Store & Forward mechanism at the intermediary node.
* Not suited for Streaming media & real-time applications.

Packet Switching

* The internet is a Packet Switched network.
* Message is broken into individual Chunks called as Packets.
* Each Packet is sent individually.
* Each Packet will have Source & destination IP address with Sequence Sequence number.
* Sequence numbers will help the receiver to
  -) Reorder the Packets
  -) Detect missing Packets &
  -) Send acknowledgments.

Packet Switching - Datagram Approach

* Datagram Packet Switching is also known as Connectionless Switching.
* Each independent entity is called as datagram.
* Datagrams Contain destination information & the intermediary devices uses this information to forward datagrams to right destination.
* In Datagram Packet Switching approach, the

Path is not Fixed.

* Intermediate nodes take the routing decision to forward the Packets.

Virtual Circuit Approach

* Virtual Circuit Switching is also known as Connection-oriented Switching.
* In the case of Virtual Circuit Switching, a Preplanned route is established before the messages are sent
* Call request & Call accept Packets are used to establish the Connection b/w Sender & receiver.
* In this approach the Path is fixed for the duration of a logical Connection.

Error Detection & Correction

Note: (A) ——— 1 GBPS ——— (B)
(1 GBPS = Bandwidth)

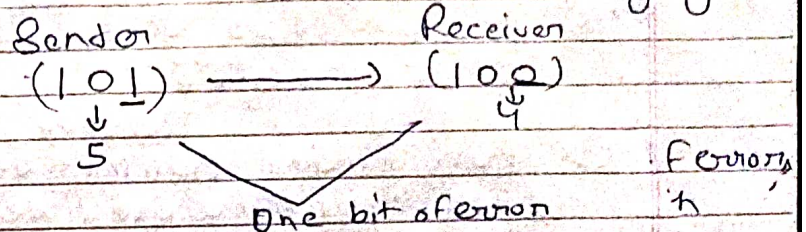
1 GPS → 10^9 bits in 1 sec

$$1 \text{ bit} = \frac{1}{10^9} \text{ sec} = 1 \text{ ns}$$

11011
11011

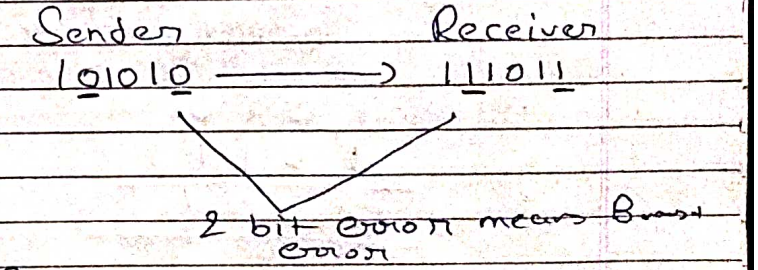
Error is of two types

① Single bit error
When there is 1 bit of error in a message then it is known as Single bit error.
like



② Burst error
When there is more than one bit of error in a message then it is known as Burst error. [most Common error]

Ex:-



Here length of the error is 5

Detection

① Single Parity [Even, ODD] ② 2D-Parity Check
③ Checksum ④ CRC [Cyclic Redundancy Check]
⑤ Hamming Codes

Single Parity

① Even Parity → no. of '1' even

② It Can detect all Single bit errors in Code word.

③ It Can also detect all odd no. of errors also.

④ For Finding Hamming distance we have to use XOR operation on a given bits.

like Ex: 1 0 1 0
0 1 1 0
1 1 0 0

hamming distance = 2

Ex: 1 0 1 0
1 0 1 1
0 0 0 1

d = Hamming distance = 1

Minimum no. of errors it Can detect are = d - 1

1 1 0 0

Cyclic Redundancy Check (CRC)

→ Based on binary division

→ total bits = (m + r) — m: no of bits in message, r: no of redundant bits

Polynomial $n^4 + n^3 + 1$

→ Polynomial should not be divisible by n

→ also not with n+1

→ It Can detect all odd numbers of errors, Single bit, burst errors of length equal to Polynomial degree.

Ex $n^4 + n^3 + 1$ — Division

Dividend = 1010101010

append 4 - 0s ~~as~~ Highest Power is 4

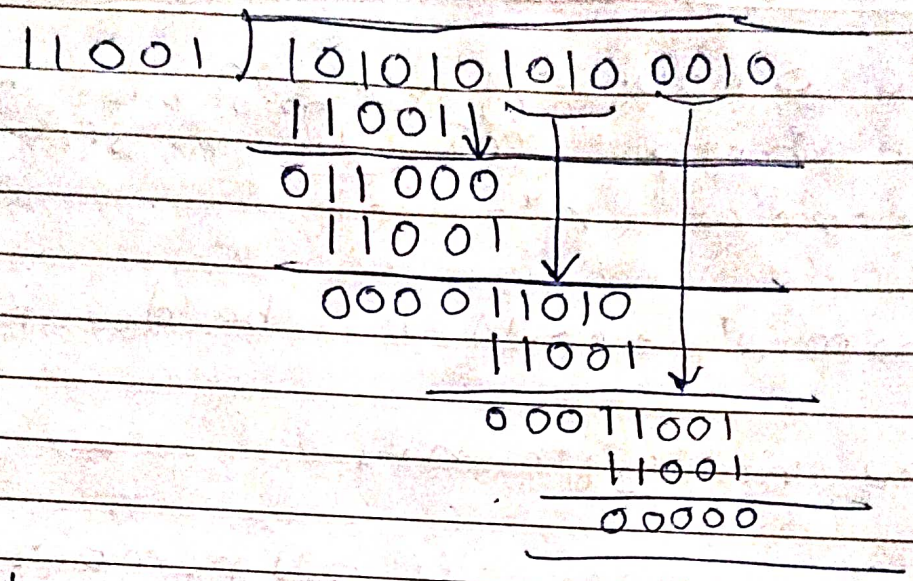
```
11001 | 1010101010 0000
        11001
        -----
        011000
         11001
        -------
        00001 1010
              11001
             -------
        00011000
            11001
           -------
        000010
```

0010 - Remainder

Having 4 ?

because we have have appended 4 redundant bits i.e LSB not MSB

Verification



Hence message has no error.

So Total bits = 10 + 4 = 14

$$\text{Efficiency} = \frac{\text{10 bits in message}}{\text{Total bits} = 14} \times 100$$

$$= \frac{10}{14} \times 100 = 71.42\%$$

Efficiency = 71.42%.