Unit-1 Introduction

Date
Page

* Definition:

Data Communication:

Data communication refers to the transmission of digital data between two or more computers or systems.

Computer Network.

A computer network is a collection of interconnected computers and other devices that can communicate and share resources with each other through a transmission medium such as wire, cables, etc.

* Advantages:

Data Communication

- Safe and stable data exchange enviroment.
- Joint information protection system.
- Data transmission in compliance with Ip data transmission protocol.

- Quick network connection of new branches and partners.

- Access resources and services from anywhere at any time.

Date
Page

Computer Network

- It reduces the need for duplicate equipment and software license, leading to cost saving for organization.

- It enables connectivity across geographical boundaries and business expansion.

- It can easily accommodate growth by adding more devices or expanding infra-structure.

- It have security measures to keep your data safe from hackers and other threats.

- It can automate tasks like updates and monitoring making network management simpler.

* Disadvantages.

Data communication

- Data and information may be stolen by computer hackers if security of network is not reliable.

- If any computer in a network get affected by computer virus, there is a high chance of spreading computer viruses in the other computer.
- Computers on the network have to depend on the server computer for resources.
- This sharing of information may leak the privacy of other clients.

Computer Network

- Managing and maintaining a computer network can be complex, requiring specialized skills & resources.
- Setting up a computer network can be expensive, involving costs for hardware.
- Sharing data and resources over a network increases the risk of unauthorized access and privacy breaches.
- Running big network uses a lot of electricity, which can be bad for the environment.
- Things like storm or accident can damage computer network.

* Application :-

Data Communication

- Sending and recieving electronic messages over the internet.
- Making phone calls using cellular network or internet-based services.
- Using navigation app for direction and real-time traffic update
- Controlling smart devices like light and thermostats remotely.
- Accessing websites and searching for information online

Computer Network

- It allow users to share files and document with each other.
- It enable the exchange of electronic mail between users, providing a fast and efficient way.

Date
Page

- It support real-time audio and video communication between users in different location.
- It facilitate online transaction and electronic commerce
- It helps users to connect, communicate and share content with friends, family & colleagues.

1.2 Communication system:

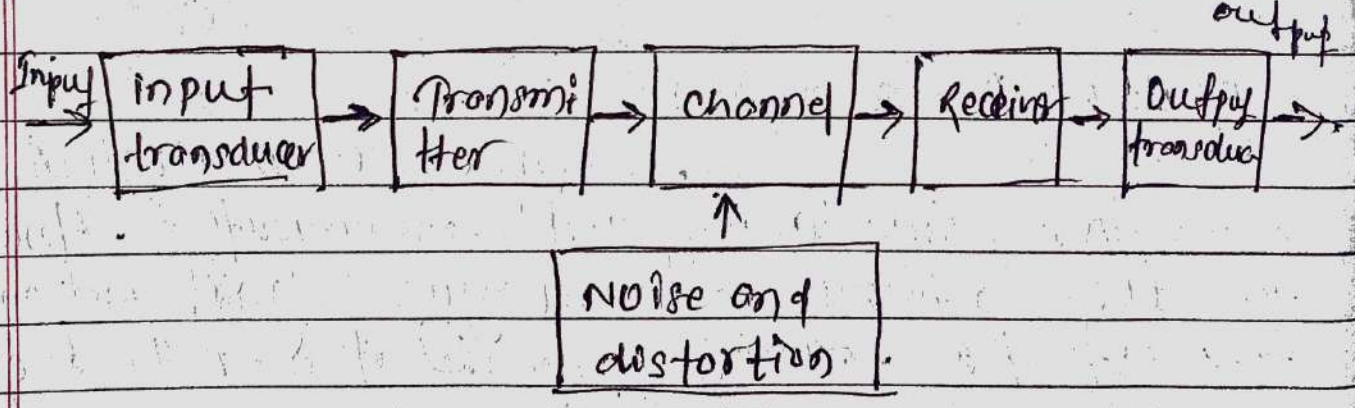
The fundamental purpose of communication system is the exchange of data between two parties. The process of transmission and reception of information is called communication. The major elements of communication are the transmitter of information, the channel or medium of communication and the receiver of information.

Analog Communication

Analog communication is made from two words 'analog' and 'communication'. Analog refers to the continous time-varying signal and communication refers to the exchanging information with the help of analog signal between two or more than two sources. Analog communication means communication with the help of analog signal. The analog communi-

on is communication from the sender to the receiver in the form of analog signal. The essential concept of the analog communication is modulation. It helps in removing the noise or external disturbances from the data, which may deteriorate the quality of the signal being transmitted. It combines elements that work together to establish a network between the sender and receiver. It consists of transducer, transmitter, channel, and receiver. The function of transducers is to convert one form of energy to the other. The channel acts as a medium to transmit electrical information from the transmitter to the receiver.

The block diagram of an analog communication system is given below:-



Date
Page

The block diagram of a communication system will have five blocks, including the information source (input transducer), transmitter, channel, receiver and destination block (output transducer).

* Information source

The objective of any communication system is to convey information from one point to the other. The information comes from the information source, which originates it.

Information is a very generic word signifying at the abstract level anything intended for communication, which may include some thoughts, news, feeling, visual scene and so on.

The information source converts the information into physical quantity.

The physical manifestation of the information is termed as message signal.

* Transmitter

- The objective of the transmitter block is to collect the incoming message signal and modify

it in a suitable fashion (if needed), such that it can be transmitted via the chosen channel to the receiving point.

The functionality of the transmitter block is mainly decided by the type or nature of the channel chosen for communication.

* Channel

Channel is the physical medium which connects the transmitter with that of the receiver.

The physical medium includes copper wire, coaxial cable, fibre optic cable, wave guide, and free space or atmosphere.

The choice of particular channel depends on the feasibility and also the purpose of the communication system.

* Receiver

The receiver block receives the incoming modified version of the message signal from the channel and processes it to recreate the original form of the message signal.

There are a great variety of receivers in communication systems, depending on the processing required to recreate the original message signal and also final presentation of the message to the destination.

* Destination (Output transducer)
The destination is the final block in the communication system which receives the message signal and processes it to comprehend the information present on it.

- Usually, human will be the destination block.

Data transmission:

Data or signal transmission occurs between transmitter and receiver over a transmission medium. The successful transmission of data depends on two factors ie. the quality of signal being transmitted and characteristic of transmission medium. Data is transformed in the form of electromagnetic signals across a transmission medium.

Date
Page

Analog Transmission:

Analog transmission is a transmission of analog data such as human voice using a continous signal which varies continously in amplitude, phase, or some other property of the variable.

During transmission of analog signal, the signal will become weaker after a certain distance. To achieve larger distance, the analog transmission system include amplifier that boosts the energy (strength) of the signal, Amplifier also amplifies the noise.

Digital Transmission:

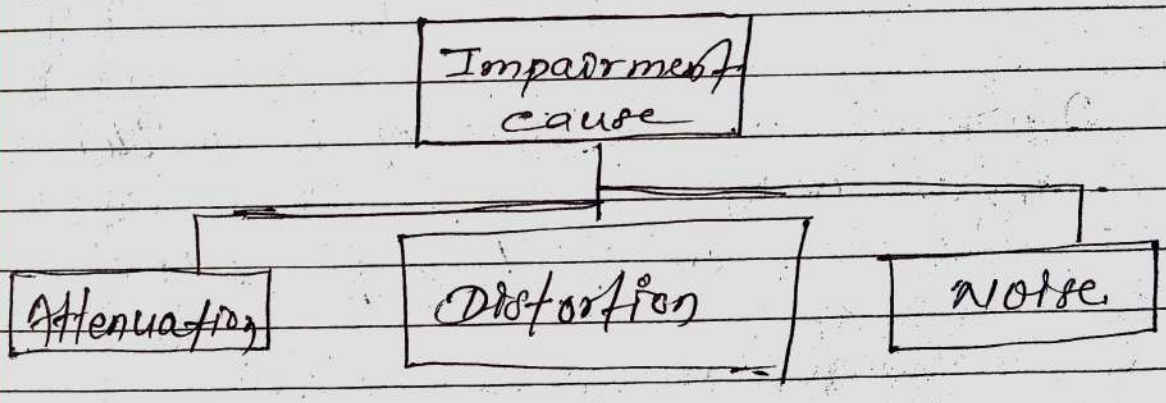
Digital Transmission is the transmission of signals that vary discretely with the time. Digital signals use discrete values for the transmission of binary information over a communication medium such as a network cable or a telecommunication link.

Unlike analog transmission, digital transmission uses repeaters to enhance the signal strength. A repeater recieves the digital signal, recovers the pattern

of 0's and 1's and retransmit the signal. Repeater regenerates the signal as a result noise gets eliminated.

1.5. Transmission impairments:

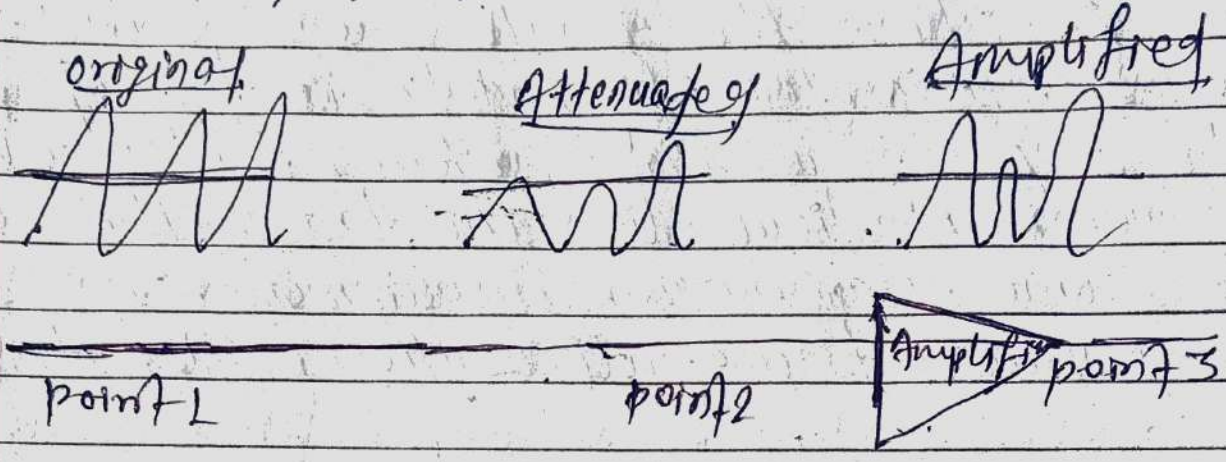
Transmission impairment is defined as a condition in which the signal's strength and quality gets deteriorated (degraded) as it get transmission. In any communication system, the received signal is never identical to the transmitted one due to some transmission impairment. Three causes of impairment are attenuation, distortion & noise



Attenuation:

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of the energy in overcoming the resistance

of the medium. That is why a wire carrying electric signals get warm, if not hot, after a while? Some of the eletrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal. Below figure show the effect of attenuation and amplification.



Attenuation may be expressed in decibles (dB) as under.

$$dB = 10 \log_{10} \frac{P_2}{P_1}$$ where

P_2 = power at receiving end.
P_1 = Power at sending end.

Date
Page

Distortion:

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and therefore, its own delay in arriving at the final destination. Differences in delay may create a different in phase if the delay is not exactly the same as the period duration. In other word, signal components at the receiver have phases different from what they had at the sender.

Noise:

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. Thermal noise is the random motion of electron in a wire which creates an extra signal not originally sent by the transmitter. Induced noise comes from source such as motor and appliances. These devices act as a sending antenna and the transmission medium acts as the receiving antenna. ~~One~~ Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna. Impulse noise is a spike that comes from power lines, lightning and so on

UNIT-2 Network Architecture and Hardware / Software

Date
Page

Network Architecture :

Network architecture refers to the design or layout of a computer network.

2.) Network topologies :

The arrangement of various element in a communication network is called network topology. There are two types of network topologies. They are :-

* (1) Physical Topology :

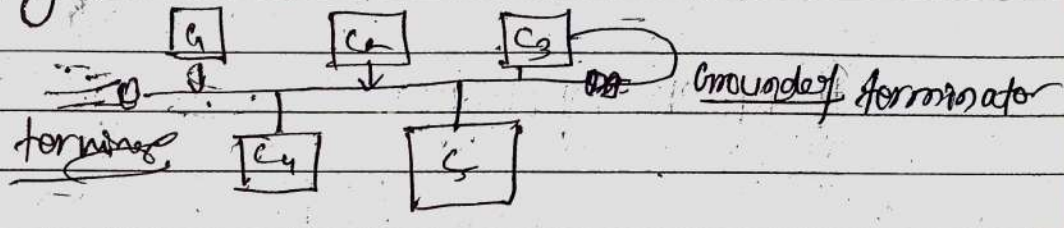
It describes the geometric arrangement of components that make up the LAN. It refers to the way computer are cabled together.

Physical topologies are bus topology, ring topology, star topology, mesh topology, tree topology, hybrid topology and Daisy chain topology.

Bus Topology :

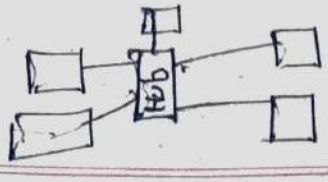
All nodes are connected to a single common cable known as the backbone. Both end of the backbone must be terminated with a terminating resister to prevent signal

bounce and complete the circuit. If the backbone cable fails, the entire network effectively becomes unusable. In this topology, Bus refers to the backbone which carries all network data. Bus network work best with a limited number of devices. When one computer sends a signal up the wire all the computers receive the information but only one with the address that matches accept the information, the rest disregard the message. Easy to implement. Failure of one station does not affect the others. Collision occurs when two node send message simultaneously. for eg.



Star Topology:

Most dominant topology type in contemporary LANs. Every node on the computer network is connected through a central device. Each computer on a star network communicates with a central device that resends the message either to each computer or only to the destination computer. A central device (hub) connects and nodes to the network. Each node connects its own dedicated port on the hub. Hubs broadcast transmitted

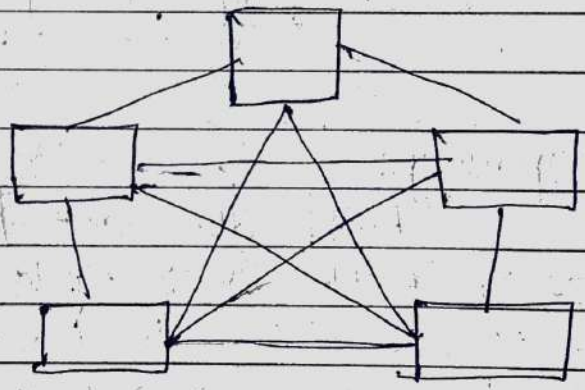


signals to all connected devices. We can connect multiple hubs to form a hierarchical star topology.

Less expensive because each device only need one I/O port and needs to be connected with hub with one link. Less amount of cables required because each device needs to be connected with the hub only. Robust if one link fails other links will work just fine.

- If hub goes down everything goes down, Hub requires more resources and regular maintenance because it is central system.

Mesh topology:



In mesh topology, each device is connected to every other device on the network through a dedicated it means that the link only carries data for the two connected devices only. Lets say we have n devices

in the network then each device must be connected with (n-1) devices of the network. Number of links in ~~mesh~~ mesh topology of n devices would be $\frac{n(n-1)}{2}$

Advantage

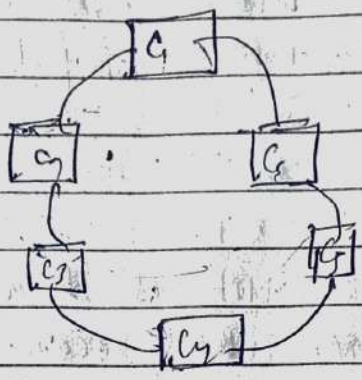
- No data traffic issues as there is a dedicated link between two devices which means the link is only for those two devices.
- It is reliable and robust as failure of one link doesn't affect other links and communication between two devices.
- It is secure because there is a point to point link.
- Fault can be easily detected.

Disadvantage

- Amount of wire required to connected each system is tedious and headache.
- Since each device needs to be connected with other devices, number of I/O ports required must be huge
- Scalability issues because a device can not be connected with large number of devices with a dedicated point to point link.

Date
Page

Ring Topology:



In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as ring topology. If a device want to send data to another devices then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other devices then repeater forwards this data until the intended device receives it.

Advantage

- Easy to install
- Managing is easier as to add or remove a device from the topology only two links are

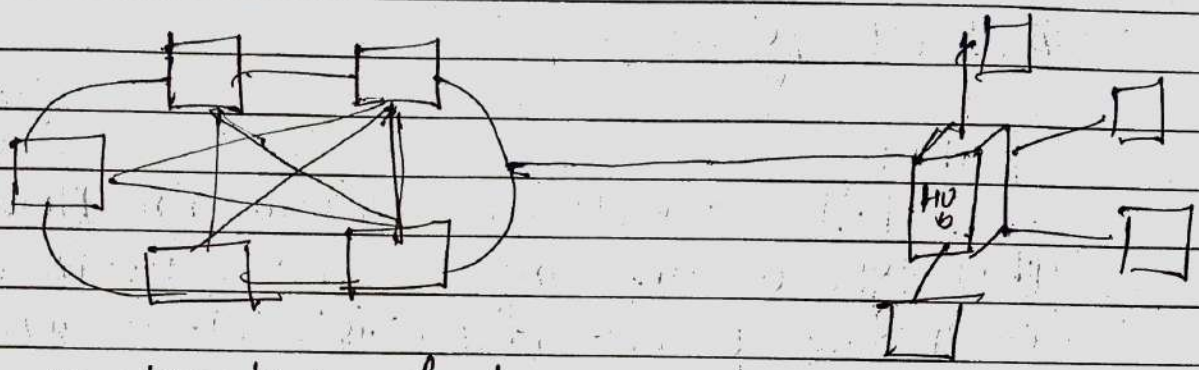
required to be changed.

Disadvantage

- A link failure can fail the entire network as the signal will not travel forward due to failure.

- Data traffic issues, since all the data is circulating in a ring.

Hybrid Topology:



A combination of two or more topology is known as hybrid topology. For example, a combination of star and mesh topology can be said as hybrid topology.

Advantage

- We can choose the topology based on the requirement.

- Scalable as we can further connect other computer networks with the existing networks with different topologies.

Disadvantage

- Fault detection is difficult.
- Installation is also difficult.
- Due to its complex design, maintenance charge is high.

2.2. Network types:

PAN:

PAN stands for Personal Area Network. This type of network is arranged within an individual person, typically within a range of 10 meters. It is used for connecting the computer devices of personal use. Is Personal computer devices that are used to develop the personal area network are the laptop, mobile phone, media player and play station.

Date
Page

LAN:

LAN stands for Local Area Network. LAN is a group of computers connected to each other in a small area such as building, office. It is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc. It is less costly as it is built with inexpensive hardware such as hubs, network adapters and Ethernet cables. It provides higher security.

MAN:

A MAN (metropolitan area network) is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network. Goverment agencies use this type of network to connect to the citizen and private industries. In MAN, various LANs are connected to each other through a telephone exchange line. It has a higher range than local area network. It is used in communication between the banks in a city, Airline reservation, and in the military.

WAN:

A wide Area Network is a network that extends over a large geographical area such as states or countries. A WAN network is quite bigger than MAN. It is not limited to a single location, but it

spans over a large geographical area through a telephone lone, fiber optic cable or satellite links

Intranet:

An intranet is a private network that can only be accessed by the authorized users. Its primary purpose is to help employees securely communicate with each other to store information and to help collaborate. This closed networks enables employees to access company resources such as documents, databases, and application, securely and efficiently. Intranet often feature tool like email, chat and forums to facilitate internal communication and collaboration across departments and geographic locations.

Internet:

Internet is a world wide publicly accessible computer network of interconnected computer network that transmitted data using the standard internet protocols. The largest internet network in the world is internet. The internet forms

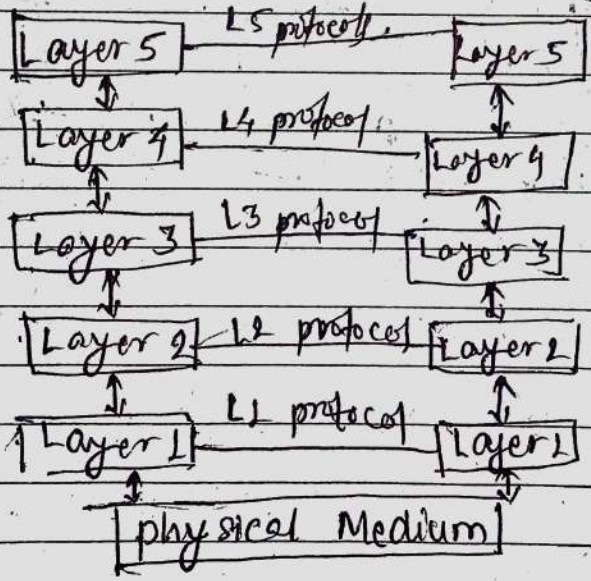
a well known component of the global information distributions network. It targets a wide range of e-commerce application such as video on demand, home shopping, email, information distribution network, video conferencing and many more. All the component of the I-way together provide a network information for the e-commerce activities.

Extranet:

An extranet is the private network that use the internet that allows people outside business. Internet protocols network connectivity and public communication system to security share part of a business. information or operation with supplier, vendors, partners, customers or other business. An extranet can be viewed as part of a company, internet that is extended to users outside a company. An extranet can be understand as a private internet over the internet creating a private network for sharing information and programs.

2.3 Layered network architecture, protocols, interfaces, services.

Every network consists of a specific number of functions, layers and tasks to perform. Layered architecture in a computer network is defined as a model where a whole network process is divided into various smaller sub-tasks. These divided sub-tasks are then assigned to a specific layer to perform only the dedicated tasks. A single layer performs only a specific type of task. To run the application and provide all types of services to clients a lower layer adds its services to the higher layer present above it. Therefor, layered architecture provides interaction between the sub system. If any type of modification is done in one layer it does not affect the next layer.



As shown in the above diagram, there are five different layers. Therefore, it is a five layered architecture. Each layer performs a dedicated task. The lower-level data for example from layer 1 data is transferred to layer 2. Below all the layers physical medium is present. The physical medium is responsible for the actual communication to take place. For the transfer of data and communication. Layered architecture provides with a clean cut interface.

Protocol:

Protocol is defined as a set rule used by the layer for exchanging and transmission of data with its peer entities. These rules can consists details regarding a type of content and their order passed from one layer to another.

Interfaces:

Interface is defined as a channel that allows to transmit the message from one layer to another.

Services:

Services is defined as a set of function and tasks being provided by a lower layer to a higher layer. Each layer performs a different

type of task. Therefore, action provided by each layer are different.

OSI reference model:

OSI stands for Open Systems Interconnection. OSI is a seven layered architecture. All these seven layer work collaboratively to transmit data from one layer to another. Each layer is responsible for specific tasks or data communication and exchange. Below are the layer of OSI model.

1. Physical layer:

Physical layer is the lowest layer of OSI model and is responsible for the physical connection between all the required devices. The information present in physical layer is in the form of bits. Physical layer performs various function such as bit rate control, bit synchronization, transmission mode etc.

2. Data Link Layer:

Data link layer provides with successful delivery of message from one node to the another. It checks whether the delivery of message is error free. Other function performed by data link layer are error control, framing, flow control, etc.

3. Network Layer:

Network layer is responsible for the transmission of data from one host to another host that is connected in different network. It performs other tasks such routing and local addressing.

4. Transport Layer:

Transport layer is defined as a layer that takes services from network layer and provides services to application layer. Other tasks performed by transport layer are service point addressing; segmentation and reassembling.

5. Session Layer:

Session layer is defined as a layer that is responsible for establishing a connection, maintenance of session and to provide with security. Other function of session

Layer are to establish session, termination and synchronization.

6. Presentation Layer:

The data from application layer is extracted at the presentation layer. This layer is also known as translation layer. The function of presentation layer are encryption, decryption, compression and translation.

7. Application Layer:

Application layer is the top most layer of OSI model. Application layer is also known as desktop layer. It provides with other function such as directory services, mail service, network virtual terminal etc.

TCP/IP Model

The TCP/IP model is also known as the Internet protocol suite, provides the foundation for modern networking. It is composed of four layers, each serving specific function on data transmission

Date
Page

and communication. At the top : the application layer facilitates interaction between user application and the network offering services like email, file transfer and web browsing. The transport layer ensures reliable data delivery with TCP managing connection-oriented communication and UDP handling connectionless transmission. The internet layer handles addressing and routing, allowing packets to traverse different networks to reach their destination. Finally, the link layer manages physical connection and data framing, enabling communication between devices on the same network. Together these layers enable the seamless exchange of data across the internet, supporting a wide range of applications and services that power modern communication and collaboration.

It consists of four layers, each responsible for specific task in data transmission and communication.

1. Application layer :

In application layer of TCP/IP model consists of OSI model's top three layers (Application, Presentation and Session) which provides network services directly to user application. This includes protocols such as HTTP for web browsing,

SMTP for email, FTP for file transfer and DNS (Domain Name Server) for translating domain names to IP addresses.

2. Transport layer:

Similar to the transport layer of the OSI model, this layer ensures reliable end-to-end communication between devices. It includes two main protocols.

- TCP (Transmission Control Protocol):

It provides reliable, connection oriented communication with features like error detection, flow control and congestion control

- User Datagram protocol: (UDP).

It offers connectionless unreliable transport for application that prioritize speed over reliability, such as real-time multimedia streaming and online gaming.

3. Internet Layer:

Equivalent to the network layer of the OS model, the internet layer handles logical addressing (IP addresses) and routing, allowing packets to traverse different network to reach their destination. The primary protocol

used at this layer is the internet protocols (IP).

4. Link Layer:

It is a combination of the OSI data link and physical layer. It handles physical connection and data framing with in a local network. It includes protocols like Ethernet, Wifi and PPP (Point-to-point protocol).

OSI model

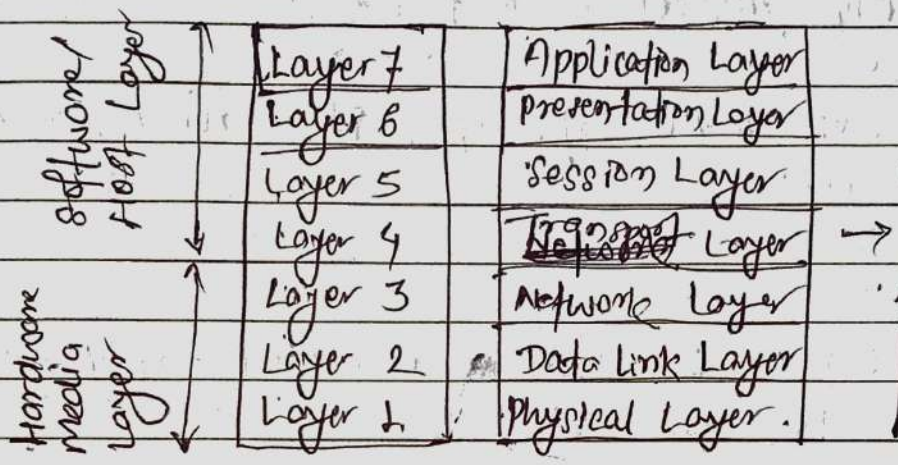


Figure: OSI model.

* Merits of TCP/IP
  - It operated independently.
  - It is scalable.
  - Client / server architecture.
  - Supports a number of routing protocols

Date
Page

- It can be used to establish a connection between two computers.

* Demerits of TCP/IP

- The transport layer does not guarantee delivery of packets.
- The model cannot be used in any other application.
- Replacing protocol is not easy.
- It has not clearly separated its service, interface and protocols.

* Comparison of OSI Reference Model and TCP/IP reference model

OSI model	TCP/IP model
(1) OSI provides layer functioning and also defines function of all the layers.	TCP/IP model is more based on protocols and protocols are not flexible with other layers.

Date
Page

OSI	TCP/IP
(i) The transport layer guarantees the delivery of packets.	In TCP/IP, the transport layer does not guarantees delivery of packets.
(ii) It has separated presentation layer.	It does not have a sperate presentation layer.
(iii) Network layer of OSI model provide both connection oriented and connectionless service.	In TCP/IP model, the network layer only provide connectionless service
(iv) Protocols are easily replaced as the technology changes.	In TCP/IP replacing protocols is too difficult.

TCP/IP Layers

Application
Transport Layer
Network Layer
Network interface Layer

TCP/IP protocols.

HTTP	FTP	Telnet	SMTP	DNS
TCP		UDP		
IP	ARP	ICMP	IGMP	
Ethernet	Token Ring	Other Link-layer protocol		

Date
Page

Q.6

Network workstation and ~~peer-to-peer~~ server | Hardware and software requirements.

↳ Network workstation, typically used by end-users, require hardware configuration optimized for task such as word processing, web browsing and multimedia consumption. Common hardware components include modern processor, sufficient RAM for multitasking, high-resolution displays, and adequate storage capacity for local data storage. Graphic cards may be necessary for graphic-intensive applications, while peripherals such as keyboards, mic and printers facilitate user interaction. On the software side, workstation typically run desktop operating system like windows, mac OS, or Linux, along with productivity software suites such as Microsoft Office or Google Workspace. Security software including antivirus programs and firewalls, helps protect workstation from malware and unauthorized access, while web browsers and email clients enable communication and Internet access.

Server, can be serve as the backbone of a network, providing centralized resources

and services to clients. Hardware requirement for server depends on their intended use, whether it be file storage, database management, web hosting or application serving. Common server hardware includes powerful multi-core processors, large amount of RAM for handling concurrent requests, redundant power supplies and storage for high availability and fast network interfaces for efficient data transfer. Server often operate without monitors or input devices and are managed remotely through a dedicated management interface or via command-line interfaces. Software requirements for servers include server operating system such as Windows server, Linux distribution like Ubuntu server or CentOS, and specialized server application like Apache for web hosting, MySQL for database management, or Microsoft Exchange for email service. Additionally, server software must include robust security features to protect against cyber threats and ensure data integrity and confidentially across the network.

2. Client-server and peer-to-peer model.

Date
Page

Client- Server Model.

A client- server network is designed for end-users, called clients, to access resources such as files, songs, video collection or some other service from a central computer called a server. A server's sole purpose is to do what its name implies - serve its clients.

The type of computing system in which one powerful workstation serves the requests of other system, is an example of client server technology.

Once the server has fulfilled the client's request, the connection is terminated. Your web browser is a client program that has requested a service from a server; in fact the service and resource the server provided by is the delivery of this web page.

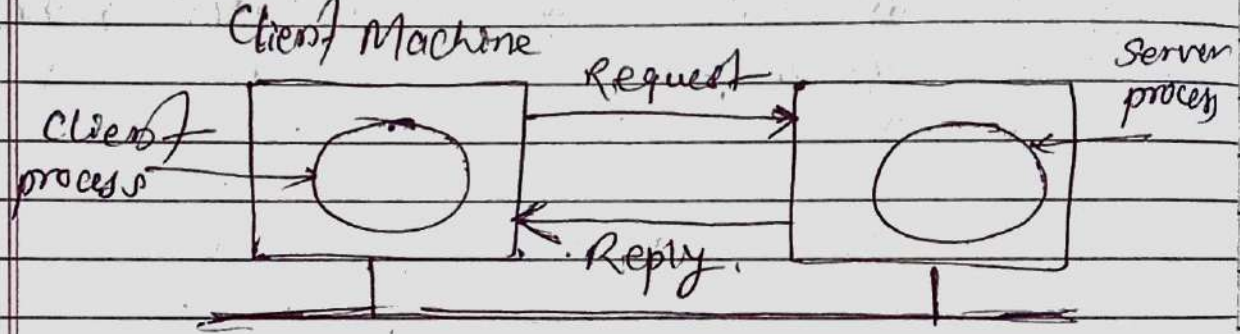


fig: Client Server Model.

- It is also known as centralized computing.
- In this type of system, multiple computers are joined to one powerful mainframe computer.
- The server or mainframe computer has huge storage and processing capabilities.
- The computers that are connected to the mainframe or servers are called clients or Nodes.
- These nodes are not connected to each other, they are only connected to server.

➤ Peer-to-peer Network Model

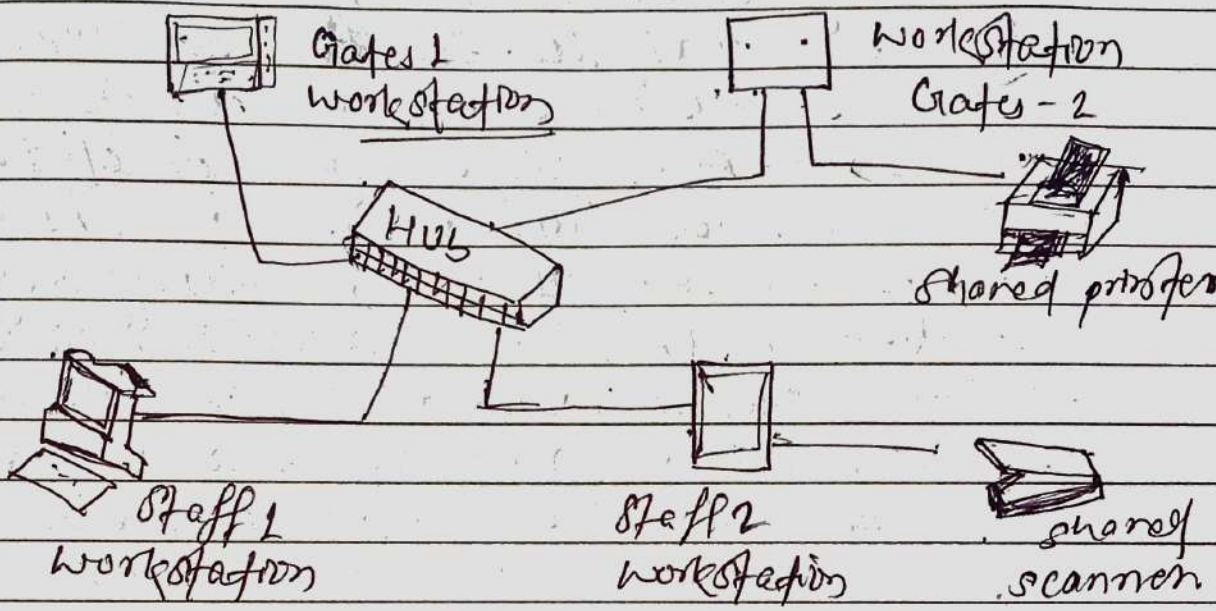


Fig: Peer-to-peer Model

Date
Page

In its simplest form, a peer-to-peer (P2P) network is created when two or more PCs are connected and share resources without going through a separate server computer. Peer to peer network are quite common on small offices that do not use a dedicated file server. All client versions of window, Mac and Linux can function as node in a p2p network and allow their files to be shared. It is easy to install and so is the configuration of computer on this network. P2P is more reliable as central dependency is eliminated. Failure of one peer does not affect the functioning of other peers. In case of client server, if server goes down whole network gets affected. The overall cost of building and maintaining this type of network is comparatively very less. Peer-to-peer (P2P) is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session. Unlike the client server model, in which the client makes a service request and the server fulfills the request, the P2P network model allows each node to function as both a client and server.

Date
Page

2.8. Network devices.

Network devices are the hardware or software components that enable communication and data exchange with in a computer network. Some are listed below:-

1. Repeater:

A repeater is a device similar to the Hub, but has additional features. It also works in the physical layer. The repeaters are used in places where amplification of input signal is necessary. But, the kind of amplification done by the repeater is different from the regular amplification by amplifier. The regular amplifies everything fed into it. That means, if the input signal has noise introduced into it, both the desired signal and noise signal are together amplified. But in the case of a repeater, it regenerates the input signal and amplifies only the desirable signal. Hence, the noise component of the signal is eliminated.

2. Hub

A Hub works in the physical layer of OSI model. It is basically a non-intelligent device and has no decision making capability. What

a Hub basically does is take the input data from one of the ports and broadcast the information to all the other ports connected to the network; so, there is a lack of security in Hub.

3. Bridge:

A bridge is also a device which works in the Data Link layer, but is more primitive when compared to a switch. Initial bridges were used to connect only 2 LAN's but the most recent ones perform similar operation as the switches. It also work on the principle of transfer of information using the MAC address of the ports. It can be noted is that the normal ADSL modem can be connected via bridging also. The only difference is that, when bridging is used each time the devices has to be connected to the internet. It has to dial to the internet and establish a connection. A bridge can not be used to connect to the internet because, the bridge work in the data link layer and had no knowledge of the IP addresses which are used on the internet.

Date
Page

4. Switch:

A switch is an intelligent device that works in the data link layer. The term intelligent refers to the decision making capacity of the switch. Since it works in the data link layer, it has knowledge of the Mac address of the ports in the network. It is also to be noted that a switch is a secure device, because, it sends information only to the desired destinations and also certain security features such as firewalls can be implemented in the switches.

5. Router:

A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect. A router may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithm to determine the best route for a given packet. Typically, a packet may travel through a number of networks points with routers before arriving at its destination.

Routing is a function associated with the Network layer (layer 3) in the standard model of network programming, the open systems interconnection (OSI) model.

6. Gateway:

A gateway is a device used to connects networks using different protocols. Gateways operate at the network layer of the OSI model. In order to communicate with a host on another network: an IP host must be configured with a route to the destination network. If a configuration route is not found, the host uses the gateways (default IP routes) to transmit the traffic to the destination host. The default gateway is where the IP sends packets that are destined for remote networks. A gateway is a network point that acts as an entrance to another network. Email gateways for example, a gateway that receives Simple Mail Transfer Protocol email, translates it into a standard X.400 format and forwards it to its destination.

NIC:

A Network Interface Card (NIC) is

a hardware component that enables devices to connect to a computer network. Installed internally in devices such as computer, server and routers. NICs provide the physical interface between the device and the network medium whether, it be on Ethernet cable, WIFI signal or other transmission medium. Operating at the data link layer of the OSI model, NICs facilitate the transmission and reception of data packets over the network. They contain built in circuitry and firmware that handle tasks such as data encapsulation, error detection and MAC addresses assignment. NIC play a critical role in enabling communication, resource sharing and access to network services and application.

Physical Layer

Date
Page

1. Channel bandwidth and throughput; Propagation time; transmission time

The physical layer is the first and lowest layer of the OSI model and TCP/IP model. It is responsible for the actual transmission of raw data bits over a physical medium such as copper wire, fibre optic cable or wireless signals. It manages aspects like encoding data into electrical signals, modulation for transmission and maintaining physical connection between devices. This layer ensures reliable data transmission by defining specification for signal timing, voltage level and error detection. It is also considered the domain of many hardware-related network design issues, such as LAN and WAN technology.

Channel bandwidth:

Channel bandwidth refers to the range of frequencies that communication channel can accommodate. It determines the maximum data transfer rate or capacity of the channel. A wider bandwidth allows for higher data transmission rates. This means that channel with greater bandwidth can transmit more data in a given amount of time

as compared to channel with narrower bandwidth. Bandwidth allocation is a critical consideration in network design and management. It involves allocating available bandwidth among different communication channel or users to ensure efficient and fair use of resource. It is measured in hertz (Hz) or its multiple such as kilohertz (kHz), megahertz (MHz), or gigahertz (GHz). In digital communication, it is often expressed in bits per second (bps) indicating the rate at which data can be transmitted through the channel.

Throughput:

Throughput refers to the actual rate of successful data transmission over a communication channel or network within a specific period. It represents the amount of data that can be transferred effectively from the sender to the reciever and is typically measured in bits per second (bps), kilo bits per second (kbps), Mbps or Gbps. The processing capabilities of devices at both ends of the communication channel can impact throughput. The nature of the application and its data transfer requirements influence the achievable throughput. Throughput is an essential metric for assessing (Bandwidth) the quality of service provided by network. Network administrator often monitor throughput to ensure that performance meets the requirement of user & application

Date
Page

Propagation time:

Propagation time is the time it takes for a signal to travel from the sender to the receiver and is influenced by distance, medium and the speed of light. While the speed of light is constant in a vaccum, it may vary slightly in different medium due to factors such as refraction and dispersion. These variation can affect the accuracy of timing in communication system. It is essential for maintaining signal integrity and synchronization in communication system, particularly in high-speed and time sensitive application. It also contributes to the overall latency or delay in a communication system.

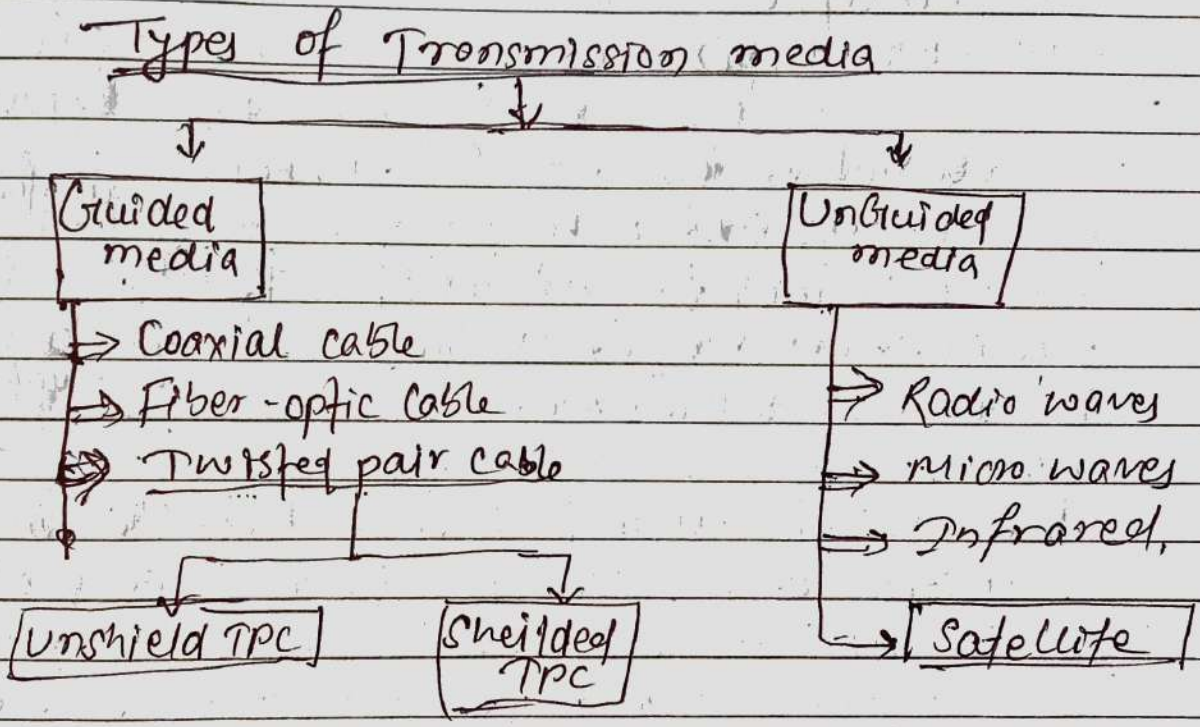
Transmission time:

Transmission time refers to the amount of time required to transfer a data packet from the sender to the reciever in a communication system. It encompasses the time needed to transmit the entire packet including the data payload as well as any additional overhead such as headers, trailers and error correction code. It is inversely proportional to the available bandwidth of the communication channel. Higher bandwidth allows for faster data transmission, reducing the transmission time for a given packet size. It may also

include the propagation delay, which is the time it takes for the signal to travel from sender to the reciever. However, in many cases, propagation delay is considered seperately from transmission time.

#2 Transmission media:

Transmission media is a communication channel that carries the information which is transmitted from the sender to the receiver. Data is transmitted through the electromagnetic signals. The main functionality of the transmission media is to carry the information in the form of bits through LAN.



Guided Media:

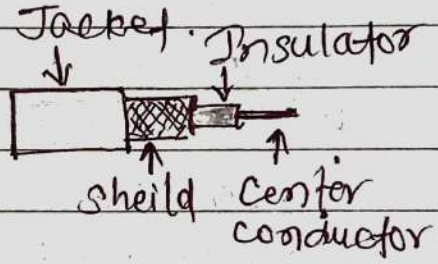
Guided media also known as bounded or wired media, refers to the physical media that provide a guided path for transmitting signals between devices in a communication network.

Features:

(i) Reliable in high speed transmission.
(ii) Greater Security.
(iii) Higher Bandwidth.

There are three types of guided media, they are,
(i) Coaxial
(ii) Fiber-optic
(iii) Twisted-pair.

(i) Coaxial Cable:



Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable. The name coaxial cable as it contains two conductor parallel to each other. The inner conductor of the coaxial cable is made up of copper and the outer conductor is made up of copper mesh. The middle core is made up of non

conductive cover that seperates the inner conductor from the outer conductor. The middle core is responsible for the data transferring whereas the copper mesh prevents from the EMI (Electromagnetic Interference)

Advantage

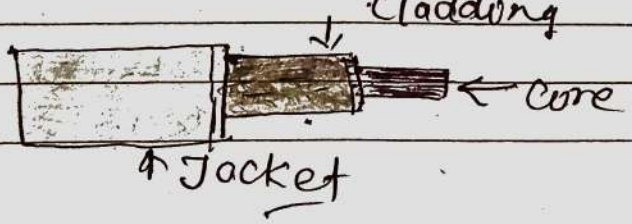
(i) The data can be transmitted at high speed.
(ii) It has better shielding as compared to twisted pair cable.
(iii) It provides higher bandwidth.

Disadvantage

(i) It is more expensive as compared to TPC.
(ii) If any fault occurs in the cable causes the failure in the entire network.

(2) Fiber-Optic Cable:

Fiber optic cable is a cable that uses optical signals for communication. The optical fibre coated in plastic that are used to send the data by pulses of light. The plastic coating protects the optical fibres from heat, cold, electromagnetic interference & from other types of wiring. It provide faster data transmission than copper wire.



Date
Page

Core:

The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fiber. The more the area of the core the more light will be transmitted into fiber.

Cladding:

The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fiber.

Jacket:

The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fiber strength, absorb shock.

Advantage

(i) Light weight
(ii) Higher data transmission
(iii) Resistance to corrosive elements.

Disadvantage

(i) Installation complexity
(ii) Highly expensive
(iii) Fragile. (नाजुक)

Date
Page

Twisted pair Cable:

It consists of 2 separately insulated conductor wires would each other. Generally, several such pairs are bundled together in a protective sheet. They are the most widely used transmission media. TPC is of two types:

(1) Unshielded Twisted Pair Cable: (UTP).

This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephone communication.

Advantage:

- Least expensive
- Easy to install
- High speed capacity.
- short distance transmission due to attenuation.

(2) Shielded Twisted pair (STP)

This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate. Ethernet and in voice and data channel of telephone lines. Better performance at a higher data rate in comparison to UTP. It is difficult to manufacture and install. Bulky.

Date
Page

3.3. Frame Relay:

Frame relay is the transmission mode, during which information is transferred through electric circuit layer, within the style of packets. It provides the information speed from 64 kbps to 45 Mbps. Frame Relay has variable packet size. It does not give error management & flow management, the responsibility of frame relay is a smaller amount.

➤ ATM, (Asynchronous Transmission Mode).

It is a telecommunication technology that uses fixed-size cells for efficient data transfer. It has mounted packet size. It provide the information speed of 155 Mbps or 622 Mbps. ATM provides error management and flow management. It is a versatile technology that offer connection-oriented communication and support for Quality of service (QoS).

➤ Integrated Services Digital Network (ISDN).

ISDN is a telecommunication technology that provide digital voice, data and video service for over traditional telephone networks. Before ISDN, the telephone system was seen

as a way to transmit voice, with some special services available for data. Here the interface of ISDN are given below:-

① Basic Rate Interface (BRI):

BRI is designed for small scale or residential use. It specifies a digital pipe consisting of two B-channel for data and one D-Channel for signaling, providing a total data rate of 144 Kbps (2x64 Kbps for B-channel + 16 Kbps for D-channel).

② Primary Rate Interface (PRI):

PRI is suitable for larger organization or businesses with higher communication needs. It offers multiple B channel and one or more D-channels. The total data rate for PRI depends on the number of B-channel and the region typically ranging from 1.544 Mbps to 2.048 Mbps.

③ BISDN

Broadband ISDN has been designed to operate over the current communication infrastructure which is heavily dependent on the copper cable However, BISDN release mainly on the evolution of fibre optic

➢ PSTN (Public Switched Telephone Network).

PSTN is an agglomeration (collection) of an inter-connected network of telephone lines owned by both government as well as commercial organization.

* Properties:

(i) It is also known as plain old Telephone service (POTS).

(ii) It has evolved from the invention of telephone by Alexander Graham Bell.

(iii) Its main objective is to transmit human voice in a recognizable form.

➢ X.25

X.25 is generally a protocol that was developed by telecommunication standardization sector of international telecommunication union. It usually allows various logical channel to make use of some physical line. It basically defines a services of document particularly issued by ITU. These document are also known as X.25 recommendation - X.25 also supports various conversation multiplexing packets and also with the help of virtual communication channel.

Unguided media

Date
Page

It is also referred to as wireless or unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Feature

(i) Signal is broadcasted through air.
(ii) Less secure
(iii) Used for longer distance

* Radio waves:

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range 3KHz - 1GHz. AM and FM radios and cordless phones use radiowaves for transmission.

Microwaves:

It is a line of sight transmission. ie the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency range 1GHz - to 300 GHz. These are mainly used for mobile phones communication and television distribution.

Date
Page

* Infrared:

Infrared waves are used for very short distance communication. They can not penetrate through obstacles. Thus prevent interference between systems. Frequency range 300 GHz – 400 THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

* Satellite:

Satellite are versatile tools used for communication, navigation, earth observation, scientific research and military purposes. They enable global connectivity, and supports a wide range of application that benefits society, and advance our understanding of the universe. Communication satellite are used to relay signals between different location on Earth. They facilitate various communication services, including television broadcasting, internet access, telephony, and data transmission.