CORE THEORY PAPER – 7

DATA COMMUNICATION & NETWORKS

Course: BSc. Computer Science Subject Code: BCS53

Objective: To equip students to basics of Data Communication and prepare them for better computer networking

UNIT I

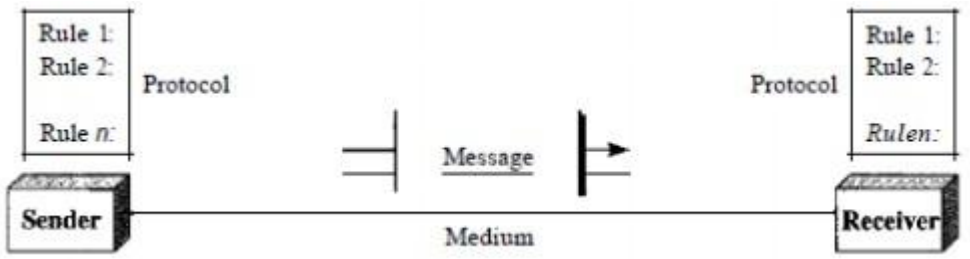
Introductory Concepts - Network hardware - Network software – Network Architecture - Physical layer Guided transmission media - Cable television.

UNIT I - INTRODUCTORY CONCEPTS

1.1 Introduction:

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance.

Components: A data communications system has five components.

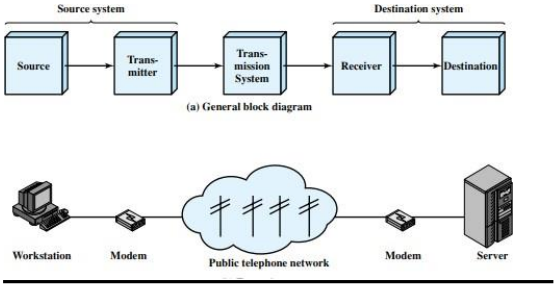


1. **Message.** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. **Sender.** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver**. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium**. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

1.1.1 Communication Model

- The fundamental purpose of a communications system is the exchange of data between two parties.
- Figure 1.2b presents one particular example, which is communication between a workstation and a server over a public telephone network.
- Another example is the exchange of voice signals between two telephones over the same network.
- The key elements of the model are as follows

  Source. This device generates the data to be transmitted; examples are telephones and personal computers.



Source: A source is an origin of message/data that is to be communicated between the sender and receiver .the message may be of text, In general, the natural information source is analog.

Transmitter: It is capable of transmitting information from source to destination via a communication channel. It can be a computer, telephone, mobile etc.

1.1.2 Transmission media: this is the path or communication link through which data travels. It may be

- ✓ Wired /guided media Example: twisted pair, co-axial cable, optical fiber.
- ✓ Wireless /Unguided media Example: RF waves, AM, FM, RADAR, etc
- ✓ While transmission through the channel, channel impairments are introduced that cause error in the data.
- ✓ Channel impairments may be noise, delay distortion, attenuation etc

Receiver: it is capable of receiving information that is delivered from a transmitter. The task of a receiver is to demote the modulated signal and send to the destination.

· **Protocols:** Protocols is the set of standard or rules that govern *data communication* system.

It is an agreement between sender and receiver. Data communication system model should undergo different protocols for reliable and effective communication.

1.1.3 Networks

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

1.1.4 Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are **performance, reliability, and security.**

Performance: Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response.

The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Reliability: Network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

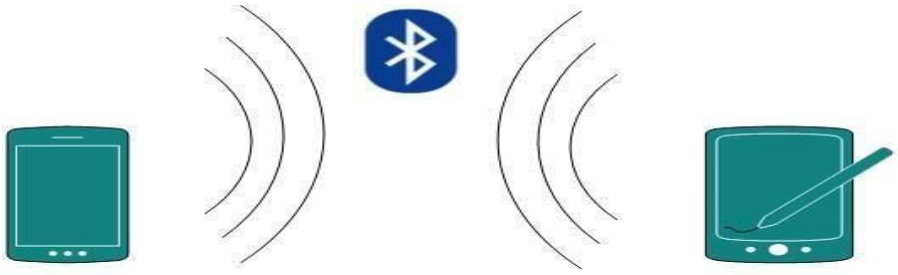
Security: Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

1.2 Network hardware:

Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the internet itself, covering the whole geographical world.

1.2.1 Personal Area Network

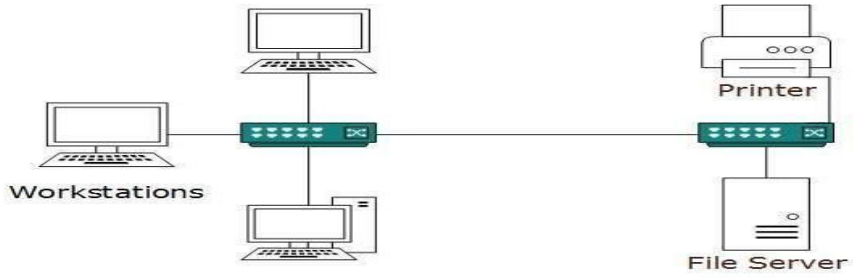
- ✓ A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices.
- ✓ PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes.



- ✓ For example, Piconet is Bluetooth-enabled Personal Area Network which may contain up to 8 devices connected together in a master-slave fashion.

1.2.2 Local Area Network

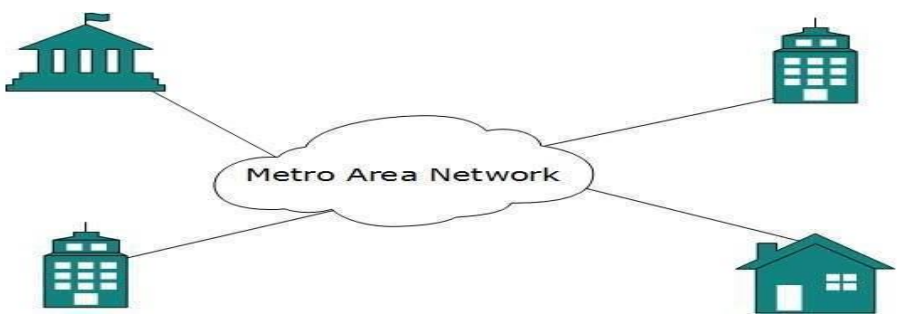
- ✓ A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually, LAN covers an organization' offices, schools, colleges or universities. Number of systems connected in LAN may vary from as least as two to as much as 16 million.
- ✓ LAN provides a useful way of sharing the resources between end users. The resources such as printers, file servers, scanners, and internet are easily sharable among computers.



- ✓ LANs are composed of inexpensive networking and routing equipment. It may contain local servers serving file storage and other locally shared applications.
- ✓ It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally.
- ✓ LAN uses either Ethernet or Token-ring technology.
- ✓ Ethernet is most widely employed LAN technology and uses Star topology, while Token-ring is rarely seen.
- ✓ LAN can be wired, wireless, or in both forms at once.

1.2.3 Metropolitan Area Network

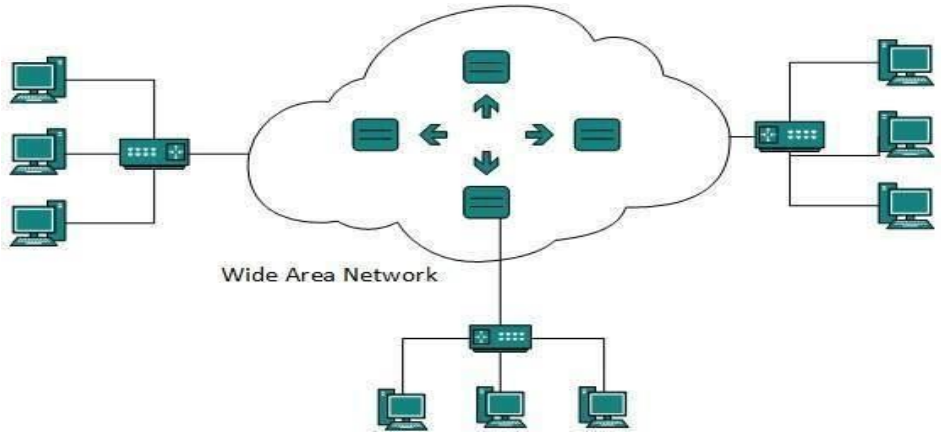
- The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).
- Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.
-



- Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet.

1.2.4 Wide Area Network

- As the name suggests, the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network.
- These networks provide connectivity to MANs and LANs. Since they are equipped with high speed backbone, WANs use very expensive network equipment.



- WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET). WAN may be managed by multiple administrations.

1.2.5 Internetwork

- A network of networks is called an internetwork, or simply the internet. It is the largest network in existence on this planet.
- The internet hugely connects all WANs and it can have connection to LANs and Home networks. Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6.
- Internet enables its users to share and access enormous amount of information worldwide. It uses WWW, FTP, email services, audio and video streaming etc. At huge level, internet works on Client-Server model.
- Internet uses high speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

- Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by client software known as Web Browsers.
- When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page.

    - The communication delay is very low. Internet is serving many proposes and is involved in many aspects of life.

Some of them are:

- Web sites
- E-mail
- Instant Messaging
- Blogging
- Social Media
- Marketing
- Networking
- Resource Sharing
- Audio and Video Streaming

1.3Network Software

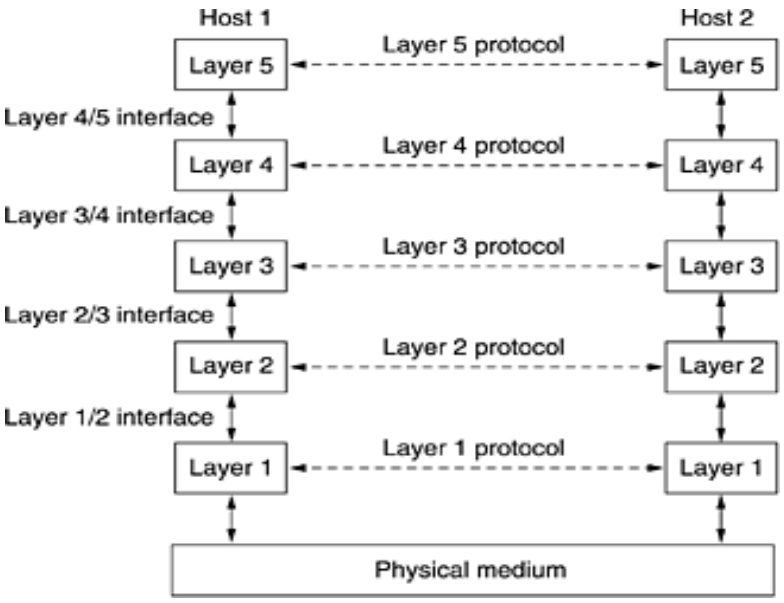
1.3.1Protocol Hierarchies

- To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
- The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented. In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.
- Layer n on one machine carries on a conversation with layer n on another machine.
- The rules and conventions used in this conversation are collectively known as the layer n protocol. Basically, a protocol is an agreement between the communicating parties on how communication is to proceed.

- A five-layer network is illustrated in Fig. 1-13. The entities comprising the corresponding layers on different machines are called peers.

- The peers may be processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol.

Figure 1-13. Layers, protocols, and interfaces



- In reality, no data are directly transferred from layer n on one machine to layer n on another machine. Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which actual communication occurs. In Fig. 1-13, virtual communication is shown by dotted lines and physical communication by solid lines.
- Between each pair of adjacent layers is an interface. The interface defines which primitive operations and services the lower layer makes available to the upper one.

1.3.2Design Issues for the Layers

- Number of design issues exists for the layer to layer approach of computer networks. Some of the main design issues are as follows:

Reliability:

- Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

Scalability:

- Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues.
- Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

Addressing

- At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

Error Control

- Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

Flow Control

- If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

Resource Allocation

- Computer networks provide services in the form of network resources to the end users.
- The main design issue is to allocate and deallocate resources to processes.

- The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

Routing

- There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time.
- There are several routing algorithms that are used in network systems.

Security

- A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages.
- So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

1.3.3 Connection-Oriented and Connectionless Services

These are the two services given by the layers to layers above them. These services are:

1. Connection Oriented Service
2. Connectionless Services

Connection Oriented Services

There is a sequence of operation to be followed by the users of connection oriented service. These are:

1. Connection is established.
2. Information is sent.
3. Connection is released.

- In the connection oriented service we have to establish a connection before starting the communication.
- When connection is established, we send the message or the information and then we release the connection.
- Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

Connection less Services

- It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination.
- The order of message sent can be different from the order received.
- In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message.
- Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

Difference: Connection oriented and Connectionless service

1. In connection oriented service authentication is needed, while connectionless service does not need any authentication.
2. Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs, while connectionless service protocol does not guarantees a message delivery.
3. Connection oriented service is more reliable than connectionless service.
4. Connection oriented service interface is stream based and connectionless is message based.

1.3.4 Service Primitives

- A service is formally specified by a set of primitives (operations) available to a user process to access the service.
- These primitives tell the service to perform some action or report on an action taken by a peer entity. If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls.
- These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets.
- The set of primitives available depends on the nature of the service being provided. The primitives for connection-oriented service are different from those of connection-less service.
  There are five types of service primitives

1. **LISTEN:** When a server is ready to accept an incoming connection it executes the LISTEN primitive. It blocks waiting for an incoming connection.
2. **CONNECT:** It connects the server by establishing a connection. Response is awaited.
3. **RECIEVE:** Then the RECIEVE call blocks the server.

4. **SEND:** Then the client executes SEND primitive to transmit its request followed by the execution of RECIEVE to get the reply. Send the message.
5. **DISCONNECT:** This primitive is used for terminating the connection. After this primitive one can't send any message. When the client sends DISCONNECT packet then the server also sends the DISCONNECT packet to acknowledge the client. When the server package is received by client then the process is terminated.

Connection Oriented Service Primitives

There are 5 types of primitives for Connection Oriented Service:

LISTEN	Block waiting for an incoming connection
CONNECTION	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Sending a message to the peer
DISCONNECT	Terminate a connection

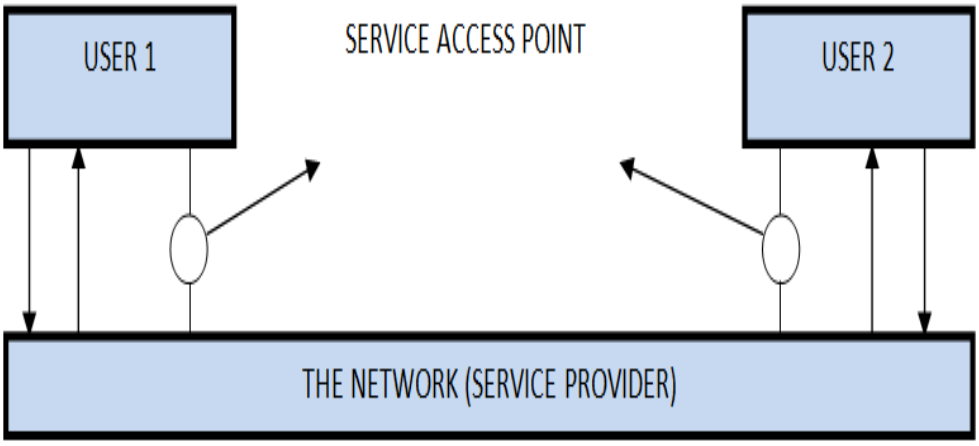
Connectionless Service Primitives

There are 4 types of primitives for Connectionless Oriented Service:

UNIDATA	This primitive sends a packet of data
FACILITY, REPORT	Primitive for enquiring about the performance of the network, like delivery statistics.

1.3.5 The Relationship of Services to Protocols

- A service is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented.
- A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.



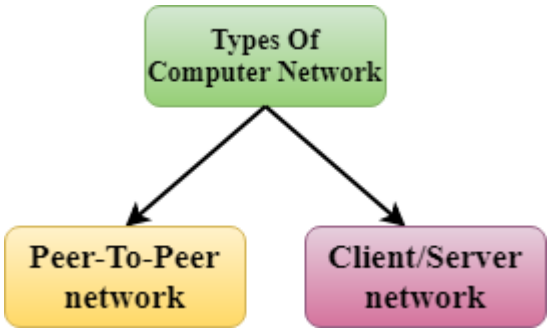
- A protocol is a set of rules that govern the format and meaning of frames, messages or packets that are exchanged between the server and client.

1.4 Network Architecture

- Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.
- Simply we can say that how computers are organized and how tasks are allocated to the computer.

The two types of network architectures are used:

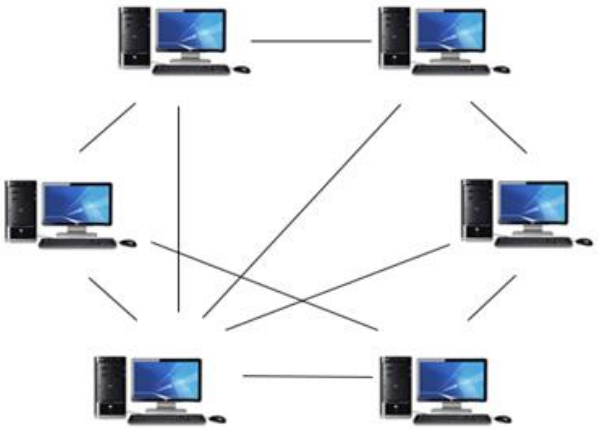
- Peer-To-Peer network
- Client/Server network



1.4.1 Peer-To-Peer network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.

- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages of Peer-To-Peer Network:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

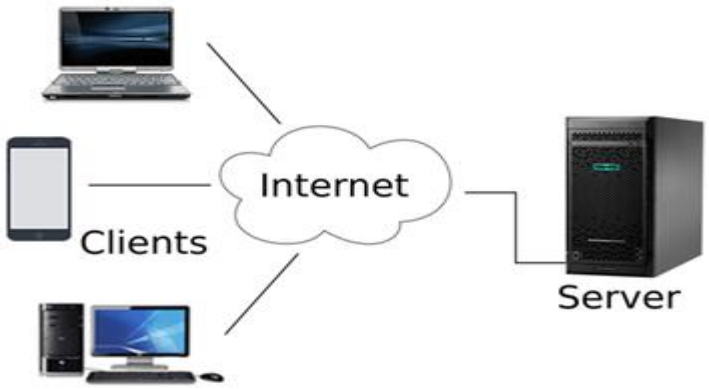
Disadvantages of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

1.4.2 Client/Server Network:

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.

- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages of Client/Server network:

- A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages of Client/Server network:

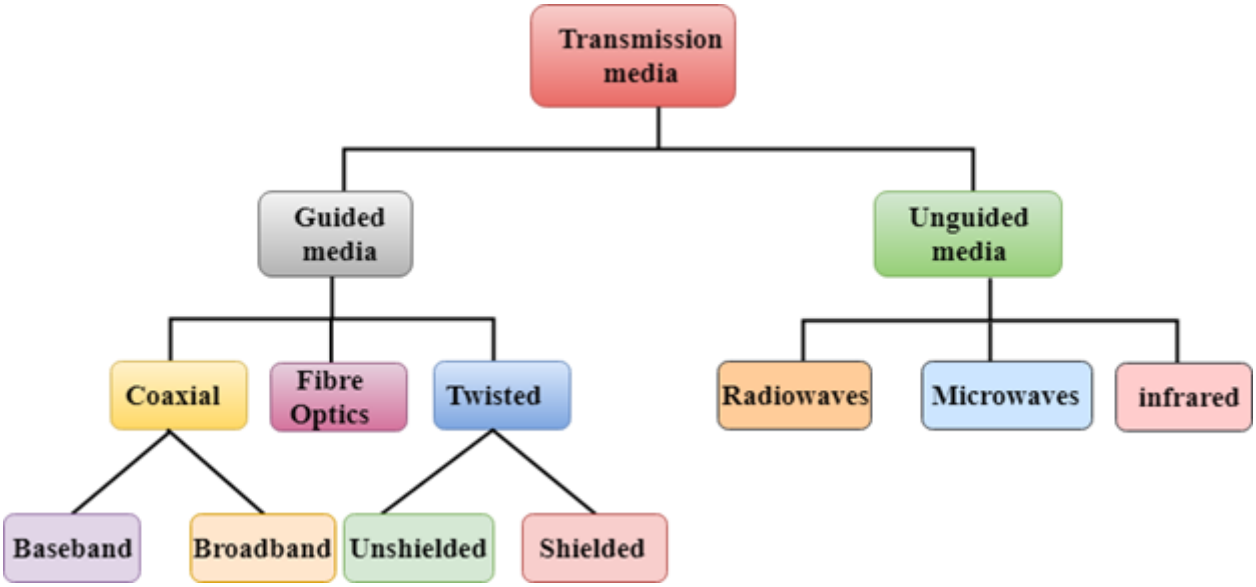
- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

1.5 Transmission media

- Data is represented by computers and other telecommunication devices using signals. Signals are transmitted in the form of electromagnetic energy from one device to another.
- Electromagnetic signals travel through vacuum, air or other transmission mediums to move from one point to another (from sender to receiver).
- Electromagnetic energy (includes electrical and magnetic fields) consists of power, voice, visible light, radio waves, ultraviolet light, gamma rays etc.

- Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of Communication Networks OSI Seven layer model is dedicated to the transmission media.

  Classification of Transmission Media



1.5.1 Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

Types of Guided media:

1.5.2Twisted pair:

- Twisted pair is a physical media made up of a pair of cables twisted with each other.
- A twisted pair cable is cheap as compared to other transmission media.
- Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from **0 to 3.5 KHz.**
- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
- One of these wires is used to carry signals to the receiver, and the other is used only as ground reference.
- The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources. This results in a difference at the receiver.

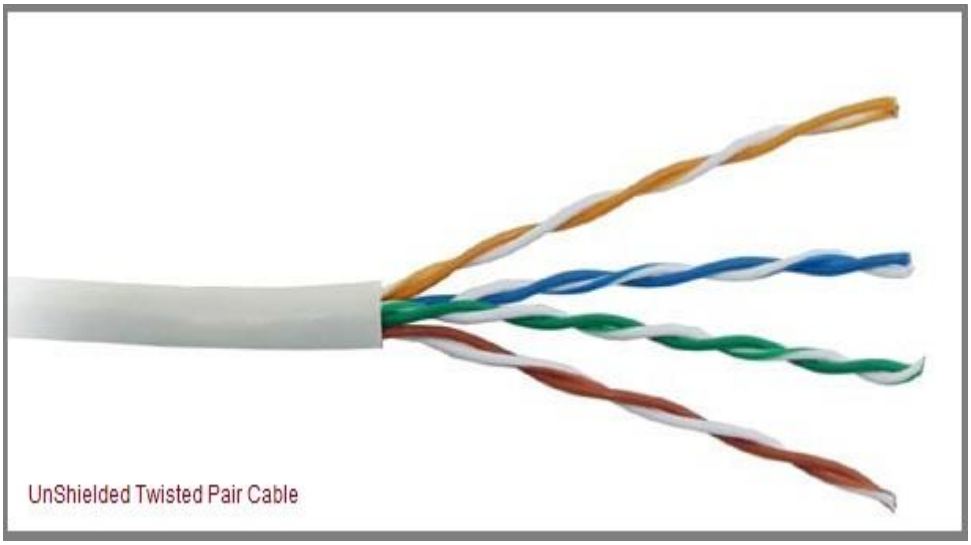
Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

Unshielded Twisted Pair Cable

- It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable.



Advantages of Unshielded Twisted Pair Cable

- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages of Unshielded Twisted Pair Cable

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

Shielded Twisted Pair

- A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

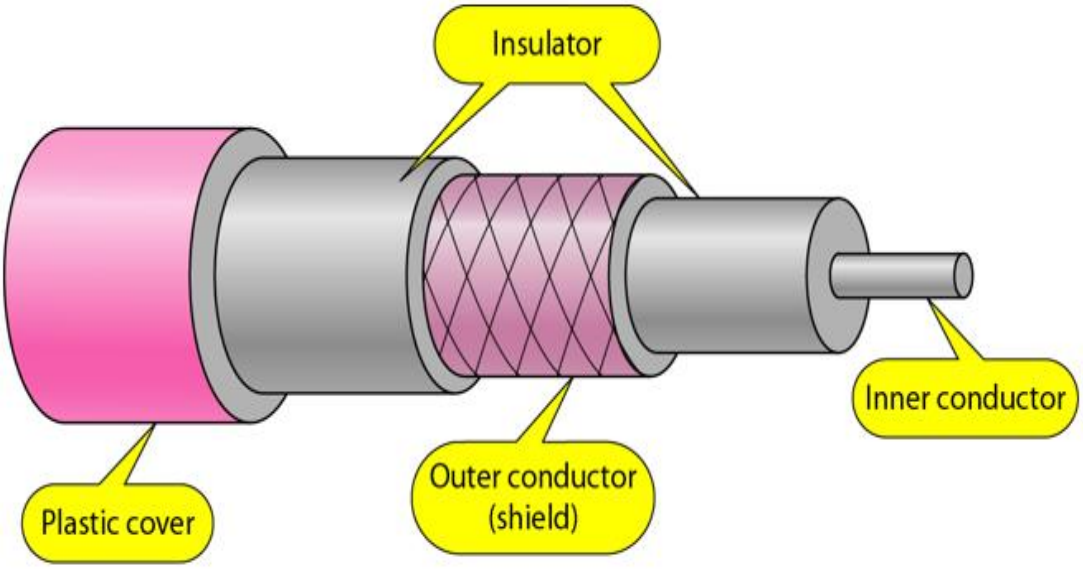
Applications of Shielded Twisted Pair Cable

- In telephone lines to provide voice and data channels. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.
- Local Area Network

1.5.3 Coaxial cable

Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.

- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- 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 separates 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).



Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages of Coaxial cable:

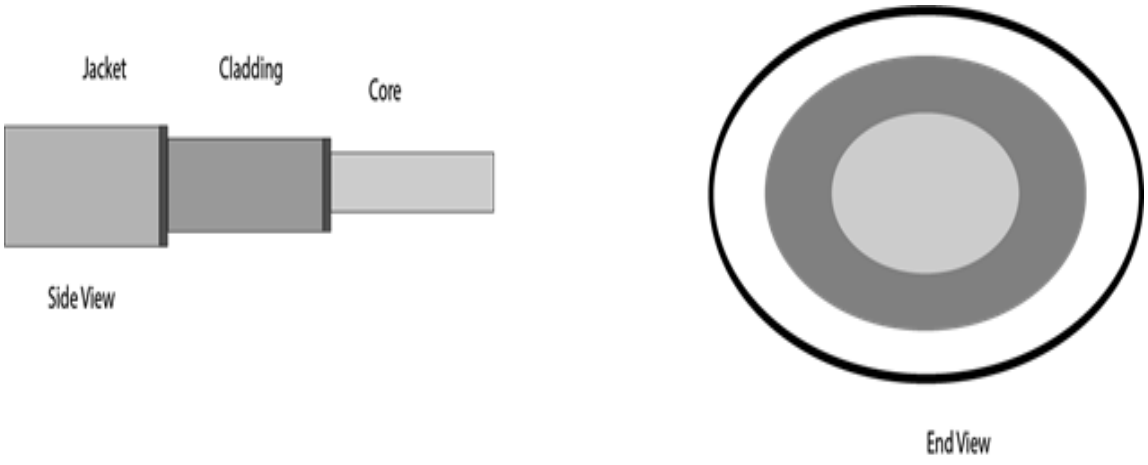
- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

Disadvantages of Coaxial cable:

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

1.5.4 Fibre Optic

- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the optical fibres 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.
- Fibre optics provides faster data transmission than copper wires.



Basic elements of Fibre optic cable:

- **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 fibre. The more the area of the core, the more light will be transmitted into the fibre.
- **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 fibre.
- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Following are the advantages of Fibre optic cable over copper:

- **Greater Bandwidth:** The Fibre optic cable provides more bandwidth as compared copper. Therefore, the Fibre optic carries more data as compared to copper cable.
- **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the Fibre optic cable to carry the signals at a higher speed.
- **Longer distances:** The Fibre optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The Fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

1.6 Cable Television

Many people already get their telephone and Internet service over the cable, and the cable operators are actively working to increase their market share.

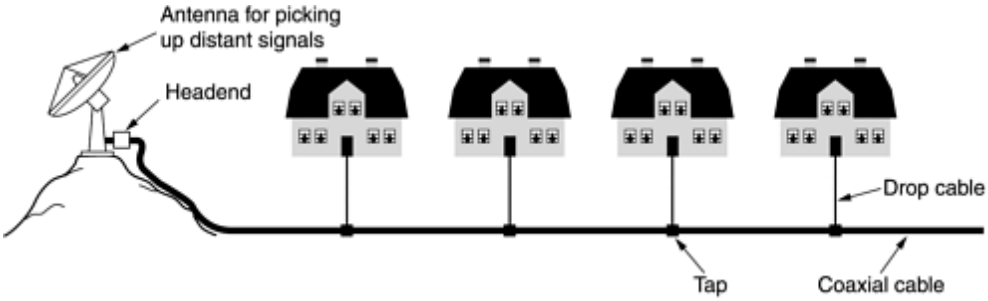
1.6.1 Community Antenna Television

- Cable television in their early days were called Community Antenna Television (CATV) or sometimes as Community Access Television.
- It was originally conceived as a method to provide cable TV services to rural areas and hilly terrains.
- The subscribers who want to avail the cable TV services need to pay a specified monthly subscription charge as well as an initial establishment charge.

System layout

- The system comprises of a big sized community antenna, installed on a hilltop that can receive broadcast signals from communication satellites.
- The signals received are amplified, corrected and strengthened by a device attached to the antenna, popularly referred to as headend.
- The modified signals are then transmitted by coaxial cables that are laid out in the locality. A drop cable connects the coaxial cables to individual homes and establishments.

An early cable television system.



1.6.2 Internet over Cable

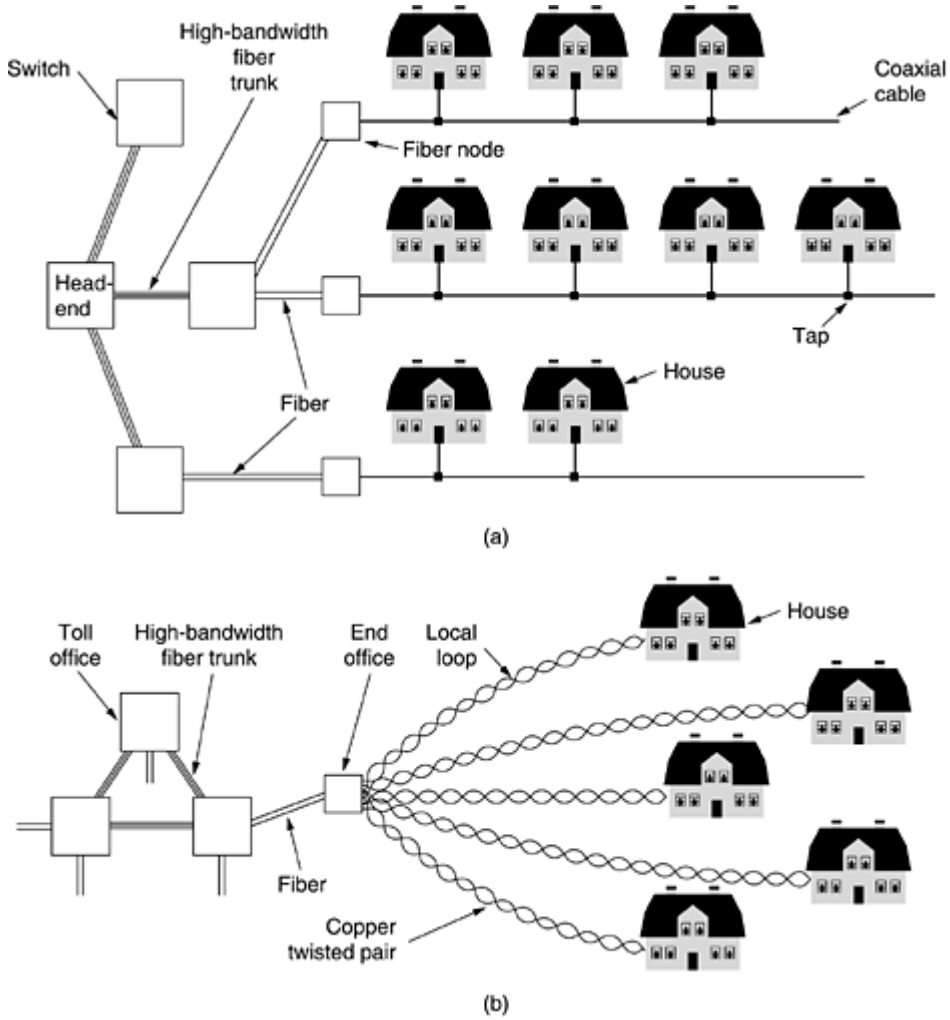
- Cable Internet is a category of broadband Internet access that uses the infrastructure of cable TV network to provide Internet services. Cable Internet provides connectivity from the Internet service provider (ISP) to the end users in a similar manner as digital subscriber line (DSL) and fiber-to-the-home (FTTH).
- Broadband cable Internet access has a cable modem termination system (CMTS) at a cable operator facility, called a headend.
- Headend is connected to switching centers by high bandwidth fiber trunk. Each switching center is connected to one or more fiber nodes through fiber optic cables.
- The local coaxial cable connects to the customer which has a cable modem to receive the services.

Features of Cable internet:

- Hybrid Fiber Coax (HFC) System: The system uses a combination of fiber cables and coaxial cables.
- Fiber cables are used for long haul connections, fiber trunks connect the headend with switching centres and fiber cables connect switching centre with fiber node. Coaxial cables run to the individual houses.

- The fiber nodes are responsible for optical – electrical conversion of signals.
- Cable TV networks were originally one – way traffic. So, they had one-way amplifiers. These are replaced with two-way amplifiers to enable both upstream and downstream traffic.
- Peak downstream bit rates can be as high as 1 Gbps, while upstream bit rates ranges from 384 Kbps to more than 20 Mbps. One downstream channel can be connected to hundreds of cable modems.

. (a) Cable television. (b) The fixed telephone system.



1.6.3 Spectrum Allocation

- Since the electromagnetic spectrum is a common resource, which is open for access by anyone, several national and international agreements have been drawn regarding the usage of the different frequency bands within the spectrum.

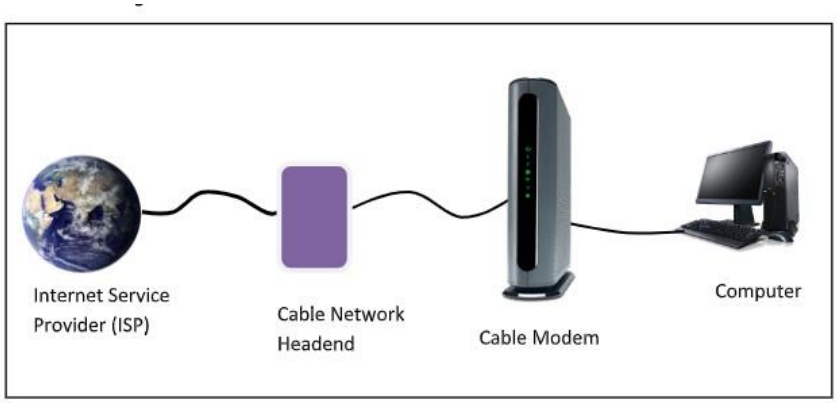
- The individual national governments allocate spectrum for applications such as AM/FM radio broadcasting, television broadcasting, mobile telephony, military communication, and government usage.
- Worldwide, an agency of the International Telecommunications Union Radio Communication **(ITU-R)** Bureau called World Administrative Radio Conference **(WARC)** tries to coordinate the spectrum allocation by the various national governments, so that communication devices that can work in multiple countries can be manufactured.

1.6.4 Cable Modems

- Cable modem is a hardware device that is used to connect the computer with the Internet Service Provider (ISP) through the local cable TV line.
- It has two interfaces – one to the cable TV network outlet and the other to a computer or television or set-top box.

Configuration

- Cable modems used to be proprietary in the initial days and had to be installed by the cable company.
- Nowadays, cable modems of open standards are available that can be personally installed by the user.
- The standard is called Data over Cable Service Interface Spectrum (DOSCIS). The modem to computer interface is normally Ethernet or USB.
- The interface between the modem and the cable network outlet supports FDM, TDM, and CDMA so that the bandwidth of the cable can be shared among the subscribers.



Connection establishment

- After a cable modem is plugged on to the cable TV network, it scans the downstream channels for a particular packet that is periodically sent over the network.
- On detecting it, the modem announces its presence over the network.
- If its authentication criteria are met, then it is assigned for both upstream and downstream communication.

Channels for communication

- For downstream data, 6HMz or 8MHz channels are used which are modulated using QAM-64. This gives the data rate of 36Mbps.
- For upstream data, there is more radio-frequency noise. Consequently, the data rate is around 9Mbps.

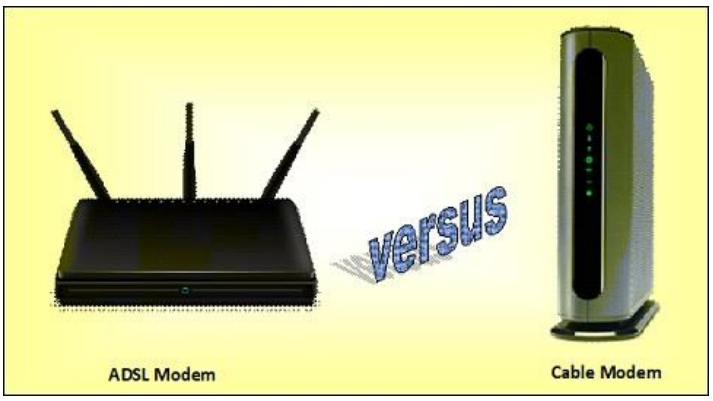
Communication method

- For sharing upstream data, time division multiplexing (TDM) is used. TDM divides the time in minislots, which are assigned to subscribers who want to send the data.
- When a computer has data to send, it sends data packets to the cable modem. The modem requests the number of minislots needed to send the data.
- If the request is granted, the modem receives an acknowledgment along with the allotted number of slots. The modem then transmits the data packets accordingly.

1.6.5 ADSL versus Cable

ADSL −Asymmetric Digital Subscriber Line (ADSL) is a type of broadband communications technology to transmit digital data at a high bandwidth on existing phone lines to homes and businesses.

Cable − Cable network is a system of providing varied services like television programming, FM programming, Internet and telephone services over existing cable TV network.



Comparison of ADSL and Cable network

- ADSL uses the existing telephone lines for providing data, voice and multimedia services, while cable uses existing cable TV networks to provide similar services.
- Both ADSL and cable networks use fiber optic cables in their backbone. However, in the customer end, cable network uses coaxial cables while ADSL use twisted pairs.
- Cable provide much high speed connection than ADSL. ADSL provides maximum speed of 200 Mbps, while cable modem can provide speed up to 1.2 Gbps.
- ADSL provides reasonably consistent bandwidth and speed of transmission. However, the parameters fluctuate significantly in case of cable connections, since it depends upon the number of users who are using the cable at a given instance of time.
- ADSL networks are more scalable in nature, as each user has a dedicated connection. If the number of users increases in the system, it does not have much impact on the existing users. On the other hand, cable lines are shared and so if more users are logged on, the performance decreases. This renders the cable system less scalable.
- In order to avail ADSL services, the distance between the subscriber and the end offices should be within a stipulated range. On the other hand, the distance from the headend of the cable provider and the subscriber does not pose as a hindrance for availing the services.
- The telephone system is more reliable and secure than the cable network system, since the former was designed for point - to - point communication while the latter was designed for broadcast services.
- In ADSL, subscribers can choose their own Internet service providers (ISPs). This facility is not available to cable users.