Unit - I

Computer Networks

The term "computer network" to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used.

Distributed system and Computer Network

There is considerable confusion in the literature between a computer network and a distributed system. The key distinction is that in a distributed system, a collection of independent computers appears to its users as a single coherent system. Usually, it has a single model or paradigm that it presents to the users. Often a layer of software on top of the operating system, called middleware, is responsible for implementing this model. A well-known example of a distributed system is the World Wide Web, in which everything looks like a document (Web page).

Applications of Computer Networks

1. **Business Applications**: The issue here is resource sharing, and the goal is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user. An obvious and widespread example is having a group of office workers share a common printer. None of the individuals really needs a private printer, and a high-volume networked printer is often cheaper, faster, and easier to maintain than a large collection of individual printers.
2. **Home Applications**: Access to remote information, Person-to-person communication, Interactive entertainment, Electronic commerce.

Electronic commerce : Example

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on line
P2P	Peer-to-peer	File sharing

3. **Mobile Applications**: Mobile computers, such as notebook computers and personal digital assistants (PDAs), are one of the fastest-growing segments of the computer industry. Many owners of these computers have desktop machines back at the office and want to be connected to their home base even when away from home or en route. Since having a wired connection is impossible in cars and airplanes, there is a lot of interest in wireless networks. For instance, Wireless parking meters have advantages for both users and city governments. The meters could accept credit or debit cards with instant verification over the wireless link. When a meter expires, it could check for the presence of a car (by bouncing a signal off it) and report the expiration to the police. It has been estimated that city governments in the U.S. alone could collect an additional $10 billion this way (Harte et al., 2000). Furthermore, better parking

enforcement would help the environment, as drivers who knew their illegal parking was sure to be caught might use public transport instead.

Transmission Technology

1. Broad cast systems:Broadcast systems generally also allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting. Some broadcast systems also support transmission to a subset of the machines, something known as multicasting. One possible scheme is to reserve one bit to indicate multicasting. The remaining n - 1 address bits can hold a group number. Each machine can "subscribe" to any or all of the groups. When a packet is sent to a certain group, it is delivered to all machines subscribing to that group.

2. Point-to-Point networks :Point-to-Point networks consist of many connections between individual pairs of machines. To go from the source to the destination, a packet on this type of network may have to first visit one or more intermediate machines. Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point networks. As a general rule (although there are many exceptions), smaller, geographically localized networks tend to use broadcasting, whereas larger networks usually are point-to-point. Point-to-point transmission with one sender and one receiver is sometimes called unicasting.

Network Hardware

Networking hardware, also known as network equipment or computer networking devices, are physical devices which are required for communication and interaction between devices on a computer network. Specifically, they mediate data in a computer network.

Typical core network devices include:

- Gateway: an interface providing a compatibility between networks by converting transmission speeds, protocols, codes, or security measures.
- Router: a networking device that forwards data packets between computer networks. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.
- Switch: a device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device. Unlike less advanced network hubs, a network switch forwards data only to one or multiple devices that need to receive it, rather than broadcasting the same data out of each of its ports.
- Bridge: a device that connects multiple network segments.
- Repeater: an electronic device that receives a signal and retransmits it at a higher level or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances.
- Repeater hub: for connecting multiple Ethernet devices together and making them act as a single network segment. It has multiple input/output (I/O) ports, in which a signalintroduced at the input of any port appears at the output of every port except the original incoming. Hubs are now largely obsolete, having been replaced by network switchesexcept in very old installations or specialized applications.

Hybrid network devices include:

- Multilayer switch: a switch that, in addition to switching on OSI layer 2, provides functionality at higher protocol layers.
- Protocol converter: a hardware device that converts between two different types of transmission, for interoperation.
- Bridge router (brouter): a device that works as a bridge and as a router. The brouter routes packets for known protocols and simply forwards all other packets as a bridge would.

Hardware or software components which typically sit on the connection point of different networks (for example, between an internal network and an external network) include:

- Proxy server: computer network service which allows clients to make indirect network connections to other network services.
- Firewall: a piece of hardware or software put on the network to prevent some communications forbidden by the network policy. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.
- Network address translator (NAT): network service (provided as hardware or as software) that converts internal to external network addresses and vice versa.

Other hardware devices used for establishing networks or dial-up connections include:

- Multiplexer: a device that selects only one signal from several electrical input signals.
- Network interface controller (NIC): a device connecting a computer to a wire-based computer network.
- Wireless network interface controller: a device connecting the attached computer to a radio-based computer network.
- Modem: device that modulates an analog "carrier" signal (such as sound) to encode digital information, and that also demodulates such a carrier signal to decode the transmitted information. Used (for example) when a computer communicates with another computer over a telephone network.
- ISDN terminal adapter (TA): a specialized gateway for ISDN.
- Line driver: a device to increase transmission distance by amplifying the signal; used in base-band networks only.

Network Software

Network software encompasses a broad range of software used for design, implementation, and operation and monitoring of computer networks. Traditional networks were hardware based with software embedded. With the advent of Software – Defined Networking (SDN), software is separated from the hardware thus making it more adaptable to the ever-changing nature of the computer network.

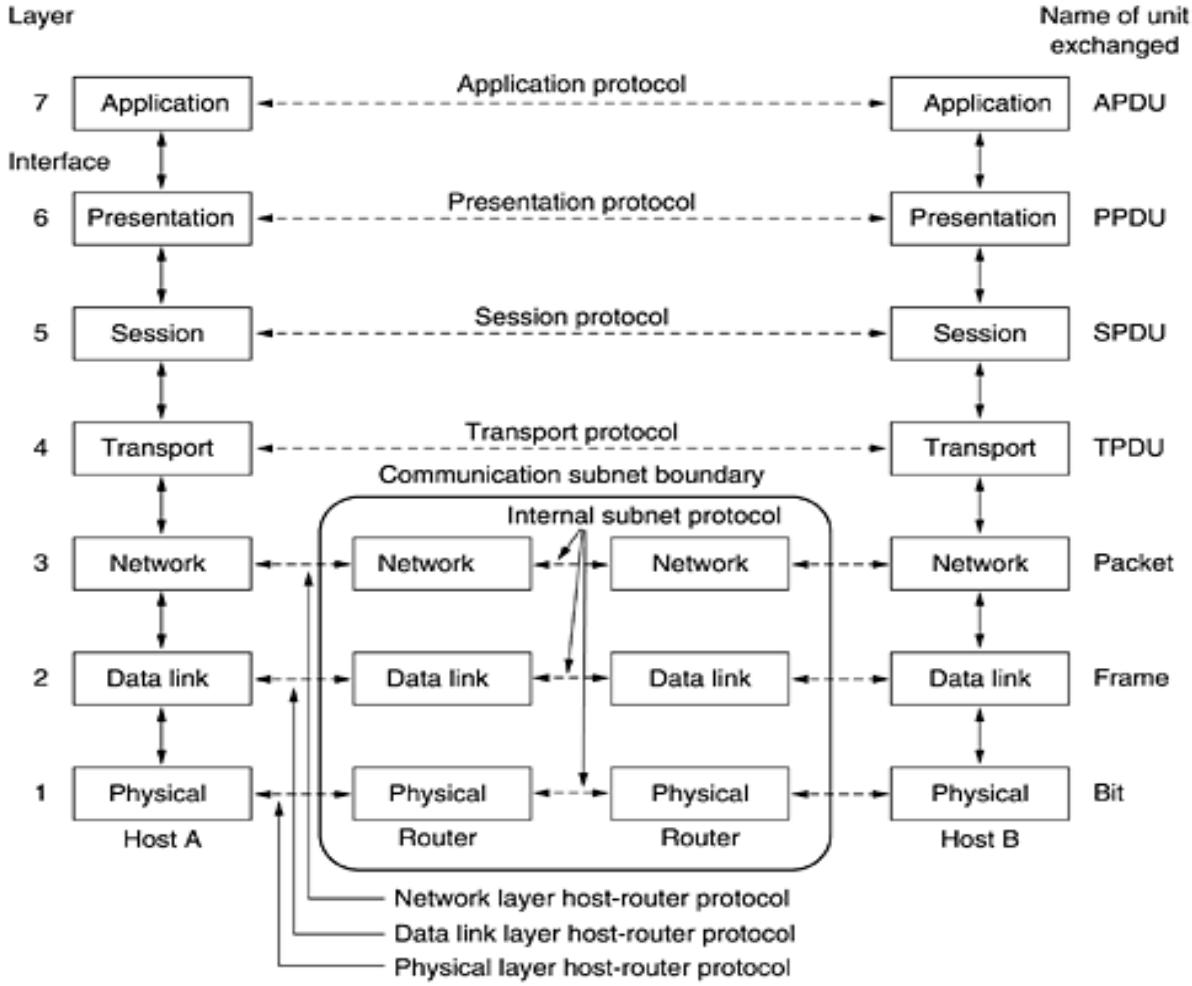
Functions of Network Software :

1. Helps to set up and install computer networks
2. Enables users to have access to network resources in a seamless manner
3. Allows administrations to add or remove users from the network
4. Helps to define locations of data storage and allows users to access that data
5. Helps administrators and security system to protect the network from data breaches, unauthorized access and attacks on a network
6. Enables network virtualizations

OSI Reference Model

OSI (Open Systems Interconnection) is a reference model for how applications communicate over a network.A reference model is a conceptual framework for understanding relationships.

The purpose of the OSI reference model is to guide vendors and developers so the digital communication products and software programs they create can interoperate, and to facilitate a clear framework that describes the functions of a networking or telecommunication system.



Physical Layer:The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits.It is responsible for the actual physical connection between the devices. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

Functions of Physical Layer:

1. Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
4. Transmission mode: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

Data Link Layer: The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer. When a packet arrives in a network, it is the

responsibility of DLL to transmit it to the Host using its MAC address. Data Link Layer is divided into two sub layers :

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

Packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.The functions of the data Link layer are :

1. Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. Physical addressing: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. Flow Control: The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. Access control: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

NetworkLayer: Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by network layer.
The functions of the Network layer are :

1. Routing: The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
2. Logical Addressing: In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

Transport Layer: Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End delivery of the complete message. Transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if
Error is found.

Senders side: Transport layer receives the formatted data from the upper layers, performs Segmentation and also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the network layer.

Receiver side :Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.
The functions of the transport layer are :

1. Segmentation and Reassembly: This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. Service Point Addressing: In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer :

1. Connection Oriented Service: It is a three phase process which include Connection Establishment, Data Transfer and Termination. In this type of transmission the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
2. Connection less service: It is a one phase process and includes Data Transfer. In this type of transmission the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.

Session Layer: The session layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
The functions of the session layer are :

1. Session establishment, maintenance and termination: The layer allows the two processes to establish, use and terminate a connection.
2. Synchronization : This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. Dialog Controller : The session layer determines which device will communicate first and the amount of data that will be sent.

Presentation Layer: Presentation layer is also called the Translation layer.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
The functions of the presentation layer are :

1. Translation : For example, ASCII to EBCDIC.
2. Encryption/ Decryption : Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. Compression: Reduces the number of bits that need to be transmitted on the network.

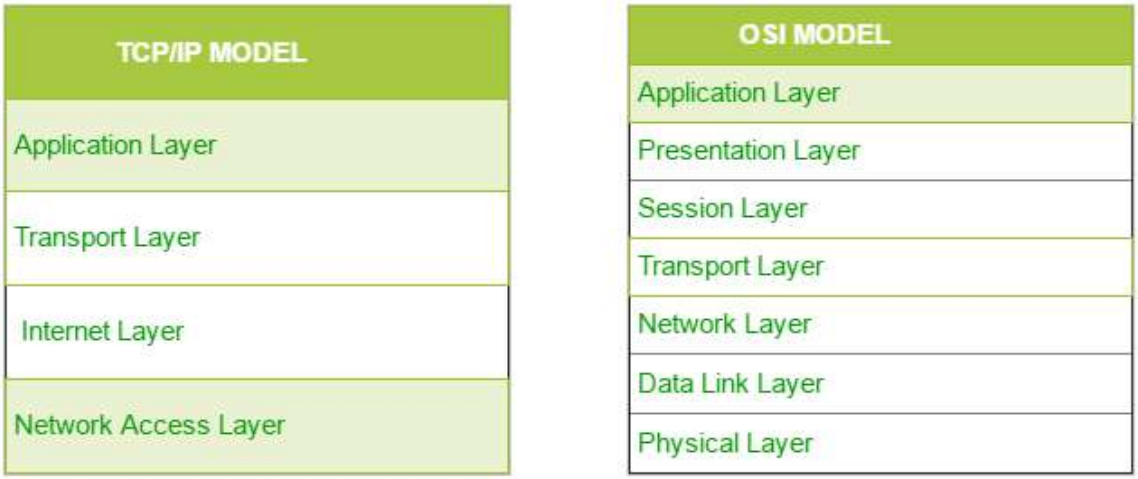
Application Layer: At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as window for the application services to access the network and for displaying the received information to the user.
Ex: Application – Browsers, Skype Messenger etc.
The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

TCP/IP Reference Model

The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer



1. **Network Access Layer :**
This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.
2. **Internet Layer :**
This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :
IP – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
ICMP – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
ARP – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.
3. **Host-to-Host Layer:**
This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :
Transmission Control Protocol (TCP) – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also

has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.

User Datagram Protocol (UDP) – On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. **Process Layer :**

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

HTTP and HTTPS – HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.

SSH – SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.

NTP – NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

ATM (Asynchoronous Transmission Mode)

- Broadband ISDN (B-ISDN) is a set of communication protocols which are designed to transport a wide range of services simultaneously.
- The purpose of B-ISDN is to simplify and reduce the cost of communication between the interconnecting LAN's, multimedia conferencing, interactive games, image transmission etc.
- B-ISDN is the low-level MAC(Media Access control) protocol for transferring the actual data.

The ATM (Asynchronous Transfer Mode) was designed with an aim to provide:

1. High speed data rate.
2. Low error rate between two or more switching centers.
3. Digital voice and videos.
4. Low operating cost.

Features of ATM

- Flexibility and versatility of voice, videos and images can be transmitted simultaneously over a single or integrated corporate network.
- Higher transmission capability.
- It provides support for virtual networks.

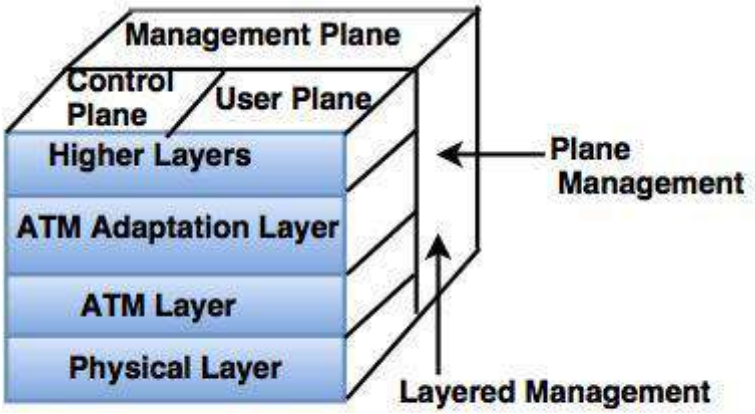
ATM supports four different types of bit rate:

1. Constant bit rate (CBR) : CBR traffic is derived from the source, where the information is transmitted at a constant rate. Example: Telephonic speech without silencer.

2. Variable Bit Rate (VBR) :Variable traffic is derived from a variable source. Example: Compressed voice or video with silence suppression.
3. Available Bit Rate (VBR) :When a carrier has allocated the necessary bandwidth on the links to carry CBR traffic and minimum VBR is guaranteed. The ABR is the mechanism to share the remaining bandwidth fairly between the links.
4. Unspecified Bit Rate (UBR)

- In UBR, there is no guarantee about the bandwidth traffic delay and loss. The control of flow in UBR can be provided from the end device.
- The protocol which performs the operation of braking frames into the cells is known as ATM Adaptation Layer (AAL).
- Cells carrying speech and video must be received in the order they were sent. This is known as preserving data integrity and it is a function of ATM layer.
- Any link which preserves the order of data entering and leaving is known as channel.
- In ATM protocols, an end-to end connection is established before traffic and starts to flow. Then ,the traffic follows the same path through the network to achieve a true quality of service.
- The connection-less services are implemented with the help of AAL.

Architecture of ATM



ATM Architecture

1**. Physical layer**

- Physical layer is a point-to-point transfer mechanism at the top of hardware (it may be wire also).
- Physical layer adds its own information to each cell which is transmitted for link management.

Physical layer performs four functions:
i) Physical layer converts bits into cells.
ii) It transmits and receives the bits on physical medium.
iii) Tracks the cell boundaries.
iv) Packaging of cell into frames.

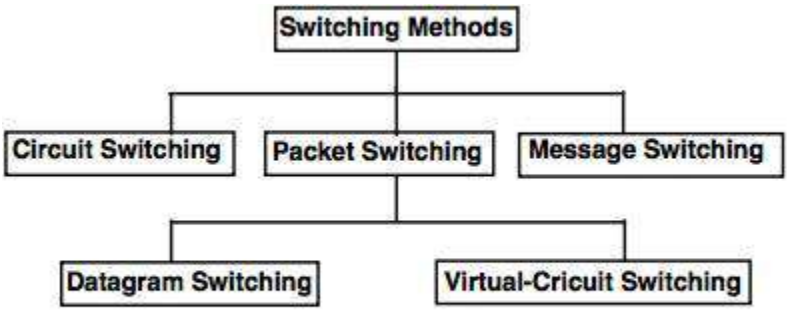
2**. ATM layer**

- ATM layer provides the routing information to the data cells.
- ATM interfaces with the AAL and the Physical layer.
- Functions of ATM layer are under the network management, signaling and OAM protocol.

3. **ATM Adaptation Layer**

- AAL provides the flexibility of a single communication process to carry the multiple types of traffic such as data, voice, video and multimedia.
- AAL is divided into two major parts.
- Upper part of the AAL is called as the convergence sublayer. Its task is to provide the interface to the application. The lower part of the AAL is called as the segmentation and reassembly (SAR) sublayer. It can add headersand trailers to the data units given to it by the convergence sublayer to form cell payloads.

SWITCHING



Types of Switching

Circuit Switching

- Circuit switched network consists of a set of switches connected by physical links.
- In circuit switched network, two nodes communicate with each other over a dedicated communication path.
- There is a need of pre-specified route from which data will travel and no other data is permitted.
- Before starting communication, the nodes must make a reservation for the resources to be used during the communication.
- In this type of switching, once a connection is established, a dedicated path exists between both ends until the connection is terminated.

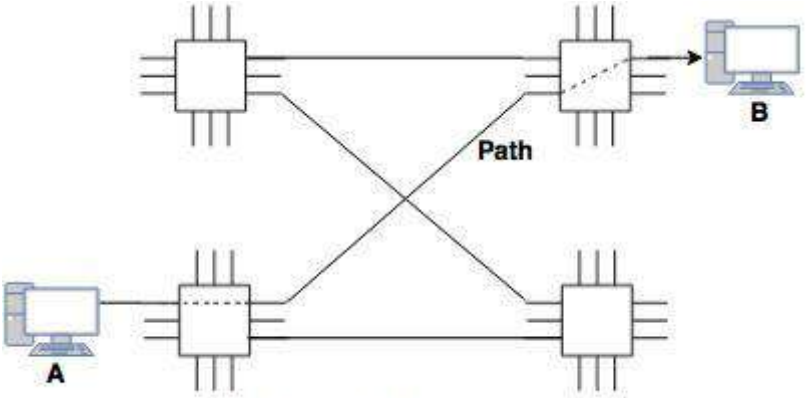


Fig: Circuit Switching

- The end systems, such as telephones or computers are directly connected to a switch.
- When system A needs to communicate with system B, system A needs to request a connection to system B that must be accepted by all switches as well as by B itself.

- This is called as **setup phase** in which a circuit is reserved on each link, and the combination of circuits or channels defines a dedicated path.
- After the establishment of the dedicated circuit, the data transfer can take place.
- After all data has been transferred, the circuit is torn down.

Packet Switching

- In packet switching, messages are divided into packets of fixed or variable size.
- The size of packet is decided by the network and the governing protocol.
- Resource allocation for a packet is not done in packet switching.
- Resources are allocated on demand.
- The resource allocation is done on first-come, first-served basis.
- Each switching node has a small amount of buffer space to hold packets temporarily.
- If the outgoing line is busy, the packet stays in queue until the line becomes available.

Packet switching method uses two routing methods:

1. Datagram Packet Switching

- Datagram packet switching is normally implemented in the network layer.
- In datagram network, each packet is routed independently through the network.
- Each packet carries a header that contains the full information about the destination.
- When the switch receives the packet, the destination address in the header of the packet is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.

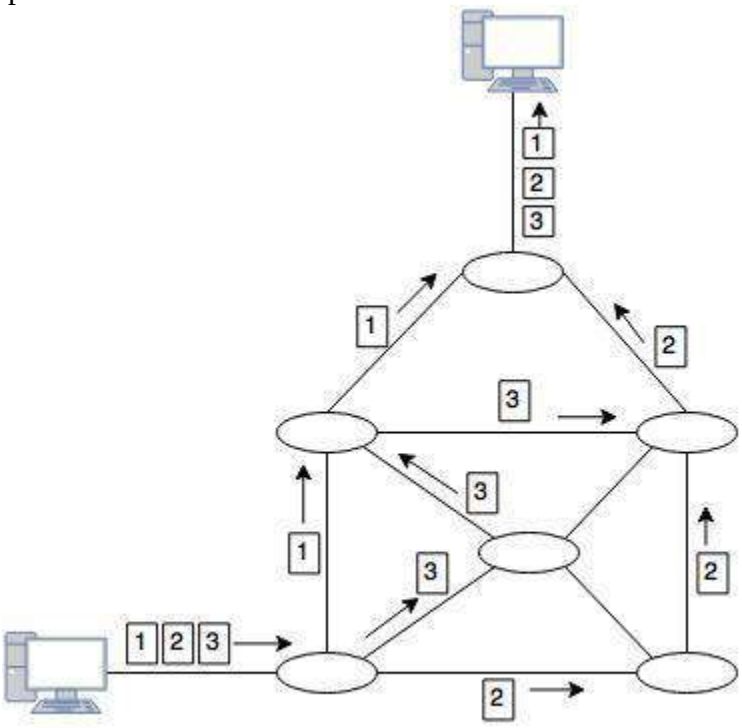


Fig: Datagram Packet Switching

2. Virtual Circuit Packet Switching

- Virtual circuit packet switching is normally done at the data link layer.
- Virtual circuit packet switching establishes a fixed path between a source and a destination to transfer the packets.
- It is also called as **connection oriented network.**

A source and destination have to go through three phases in a virtual circuit packet switching:

I. Setup phase

ii. Data transfer phase
iii. Connection release phase

- A logical connection is established when a sender sends a setup request to the receiver and the receiver sends back an acknowledgement to the sender if the receiver agree.
- All packets belonging to the same source and destination travel the same path.
- The information is delivered to the receiver in the same order as transmitted by the sender.

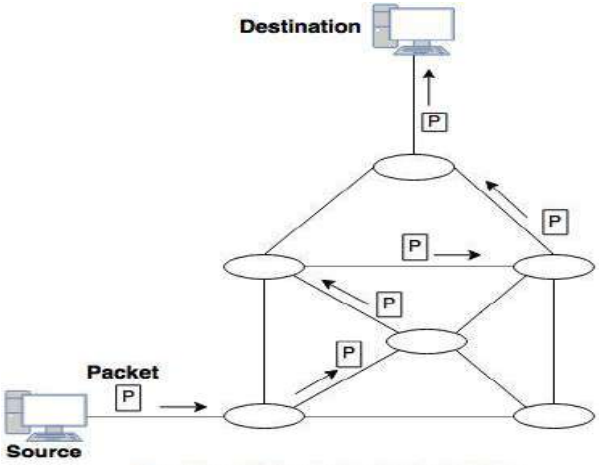


Fig: Virtual Circuit Packet Switching

Message Switching

- In message switching, it is not necessary to establish a dedicated path between transmitter and receiver.
- In this, each message is routed independently through the network.
- Each message carries a header that contains the full information about the destination.
- Each intermediate device receives the whole message and buffers it until there are resources available to transfer it to the next hop.
- If the next hop does not have enough resources to accommodate large size message, the message is stored and switch waits.
- For this reason a message switching is sometimes called as **Store and Forward Switching**.
- Message switching is very slow because of store-and-forward technique.
- Message switching is not recommended for real time applications like voice and video.

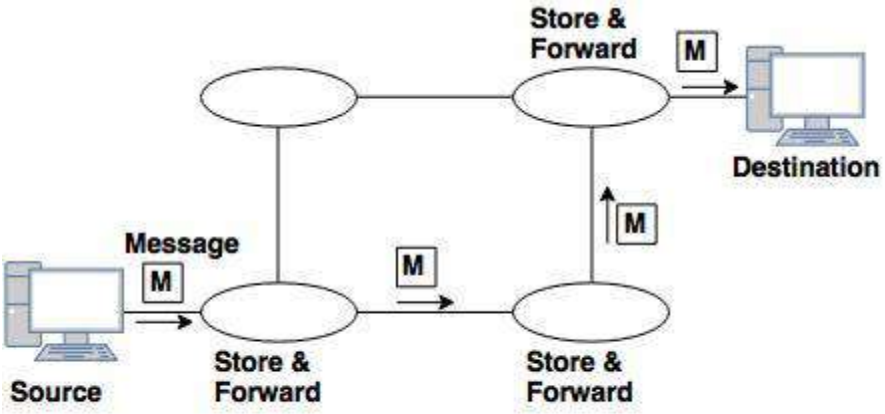
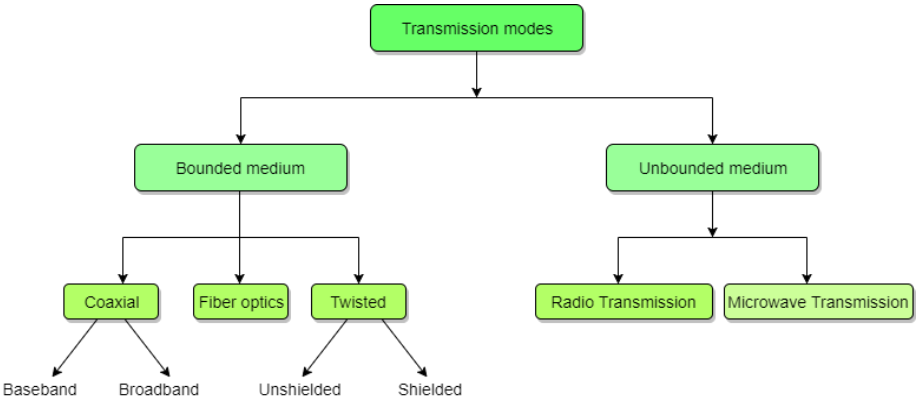


Fig: Message Switching

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.



Guided Media

Guided media, which are those that provide a conduit from one device to another, include **Twisted-Pair Cable**, **Coaxial Cable**, and **Fibre-Optic Cable**.A signal travelling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. **Optical fibre** is a cable that accepts and transports signals in the form of light.

Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 μs/km.
- Repeater spacing is 2km.

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.

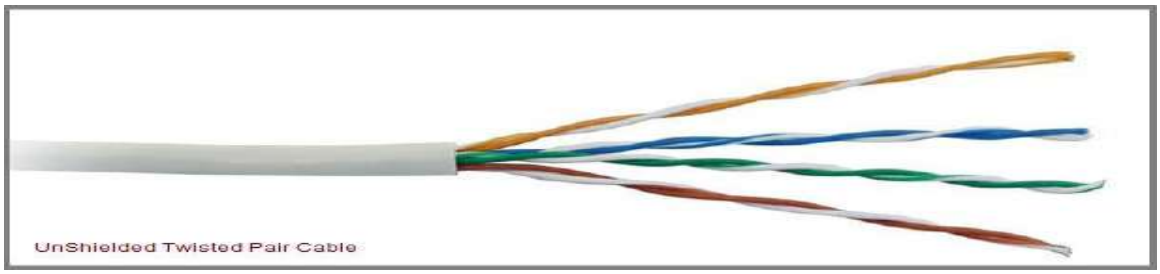
Twisted Pair is of two types:

- **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. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.



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.

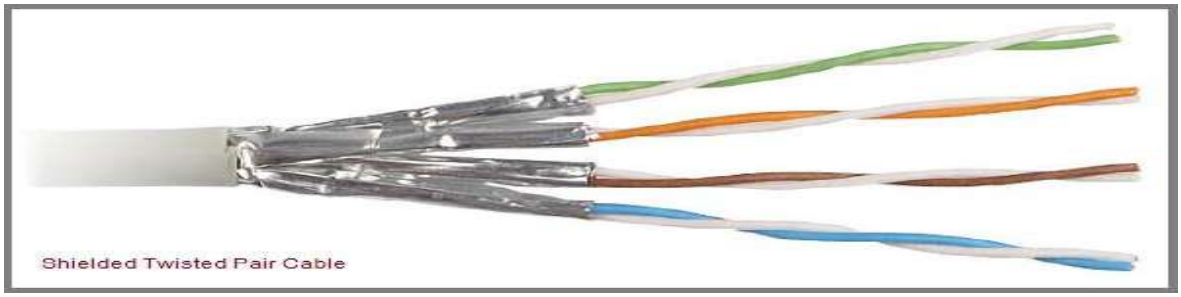
It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages of Unshielded Twisted Pair Cable

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

Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk (explained in KEY TERMS Chapter).It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.



Advantages of Shielded Twisted Pair Cable

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages of Shielded Twisted Pair Cable

- Difficult to manufacture
- Heavy

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, such as 10Base-T and 100Base-T, also use twisted-pair cables.

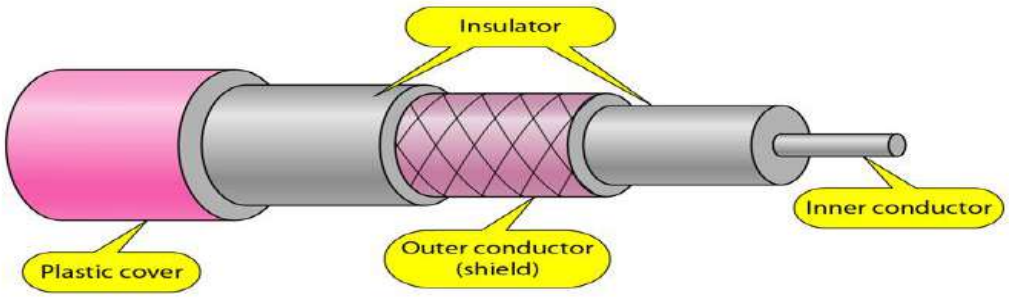
Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.

Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.



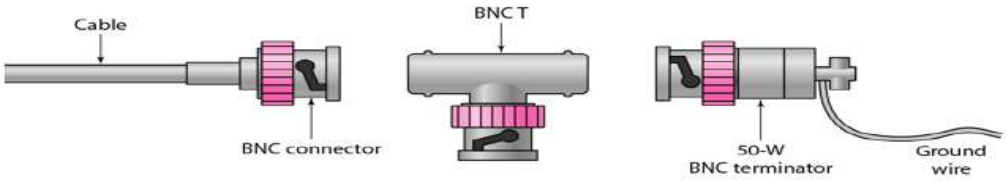
Coaxial Cable Standards

Coaxial cables are categorized by their Radio Government(RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and the type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function, as shown in the table below:

Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayonet Neill-Concelman (BNC) connector. The below figure shows 3 popular types of these connectors: the BNC Connector, the BNC T connector and the BNC terminator.



The BNC connector is used to connect the end of the cable to the device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

There are two types of Coaxial cables:

1. BaseBand

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

2. BroadBand

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages of Coaxial Cable

- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.
- The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages of Coaxial Cable

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

Applications of Coaxial Cable

- Coaxial cable was widely used in analog telephone networks, where a single coaxial network could carry 10,000 voice signals.
- Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Cable TV uses RG-59 coaxial cable.
- In traditional Ethernet LANs. Because of it high bandwidth, and consequence high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs. The 10Base-2, or Thin Ethernet, uses RG-58 coaxial cable with BNC connectors to transmit data at 10Mbps with a range of 185 m.

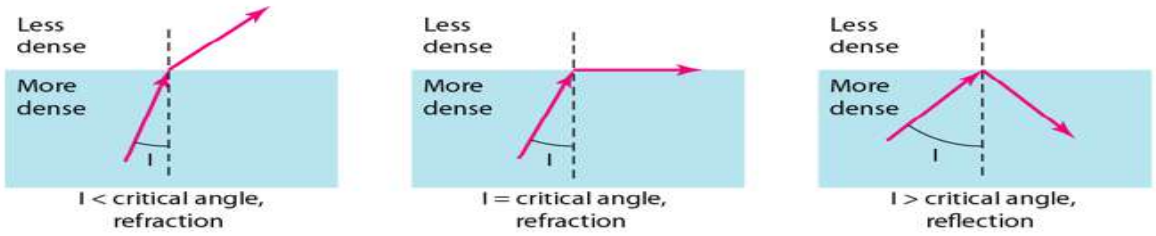
Fiber Optic Cable

A fibre-optic cable is made of glass or plastic and transmits signals in the form of light.

For better understanding we first need to explore several aspects of the **nature of light**.

Light travels in a straight line as long as it is mobbing through a single uniform substance. If ray of light travelling through one substance suddenly enters another substance (of a different density), the ray changes direction.

The below figure shows how a ray of light changes direction when going from a more dense to a less dense substance.



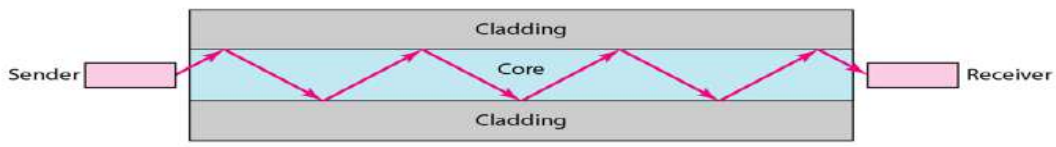
Bending of a light ray

As the figure shows:

- If the **angle of incidence I**(the angle the ray makes with the line perpendicular to the interface between the two substances) is **less** than the **critical angle**, the ray **refracts** and moves closer to the surface.
- If the angle of incidence is **greater** than the critical angle, the ray **reflects**(makes a turn) and travels again in the denser substance.
- If the angle of incidence is **equal** to the critical angle, the ray refracts and **moves parallel** to the surface as shown.

Note: *The critical angle is a property of the substance, and its value differs from one substance to another.*

Optical fibres use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



Internal view of an Optical fibre

Propagation Modes of Fiber Optic Cable

Current technology supports two modes(**Multimode** and **Single mode**) for propagating light along optical channels, each requiring fibre with different physical characteristics.

Multimode Propagation Mode

Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core as shown in the below figure.

Single Mode

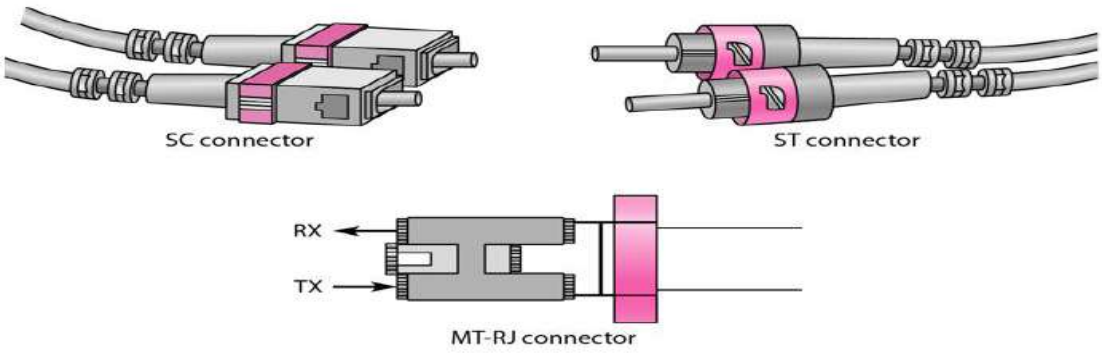
Single mode uses step-index fibre and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single-mode fibre itself is manufactured with a much smaller diameter than that of multimode fibre, and with substantially lower density.
The decrease in density results in a critical angle that is close enough to 90 degree to make the propagation of beams almost horizontal.

Fibre Sizes for Fiber Optic Cable

Optical fibres are defined by the ratio of the diameter or their core to the diameter of their cladding, both expressed in micrometers.

Fibre Optic Cable Connectors

There are three types of connectors for fibre-optic cables, as shown in the figure below.



The **Subscriber Channel(SC)** connector is used for cable TV. It uses push/pull locking system. The **Straight-Tip(ST)** connector is used for connecting cable to the networking devices. MT-RJ is a connector that is the same size as RJ45.

Advantages of Fibre Optic Cable

Fibre optic has several advantages over metallic cable:

- Higher bandwidth
- Less signal attenuation
- Immunity to electromagnetic interference

- Resistance to corrosive materials
- Light weight
- Greater immunity to tapping

Disadvantages of Fibre Optic Cable

There are some disadvantages in the use of optical fibre:

- Installation and maintenance
- Unidirectional light propagation
- High Cost

Performance of Fibre Optic Cable

Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer(actually one tenth as many) repeaters when we use the fibre-optic cable.

Applications of Fibre Optic Cable

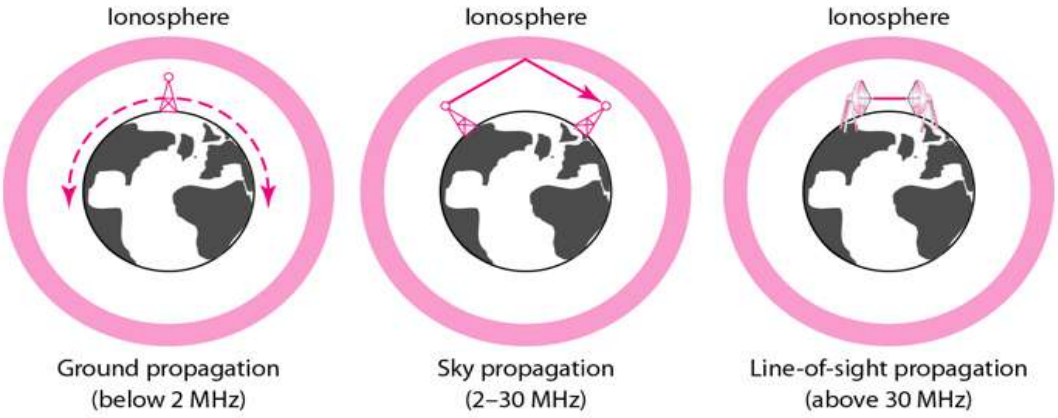
- Often found in backbone networks because its wide bandwidth is cost-effective.
- Some cable TV companies use a combination of optical fibre and coaxial cable thus creating a hybrid network.
- Local-area Networks such as 100Base-FX network and 1000Base-X also use fibre-optic cable.

UnBounded or UnGuided Transmission Media

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

The below figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.

Unguided signals can travel from the source to the destination in several ways: **Gound propagation**, **Sky propagation** and **Line-of-sight propagation** as shown in below figure.



Propagation Modes

- **Ground Propagation:** In this, radio waves travel through the lowest portion of the atmosphere, hugging the Earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.
- **Sky Propagation:** In this, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to Earth. This type of transmission allows for greater distances with lower output power.
- **Line-of-sight Propagation:** in this type, very high-frequency signals are transmitted in straight lines directly from antenna to antenna.

We can divide wireless transmission into three broad groups:

1. Radio waves
2. Micro waves
3. Infrared waves

Radio Waves

Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves.

Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna send waves that can be received by any receiving antenna. The omnidirectional property has disadvantage, too. The radio waves

transmitted by one antenna are susceptible to interference by another antenna that may send signal suing the same frequency or band.

Radio waves, particularly with those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

Omnidirectional Antenna for Radio Waves

Radio waves use omnidirectional antennas that send out signals in all directions.

Applications of Radio Waves

- The omnidirectional characteristics of radio waves make them useful for multicasting in which there is one sender but many receivers.
- AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

Micro Waves

Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves. Micro waves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

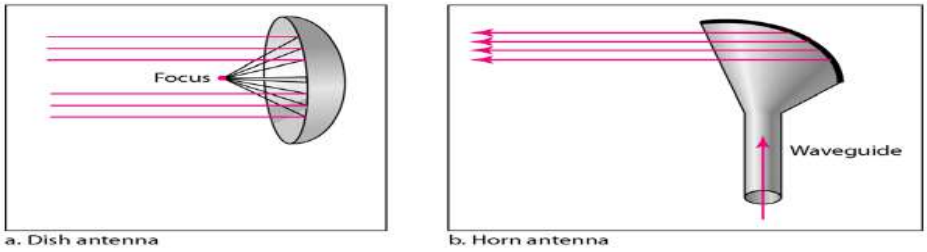
The following describes some characteristics of microwaves propagation:

- Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside the buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore, wider sub-bands can be assigned and a high date rate is possible.

- Use of certain portions of the band requires permission from authorities.

Unidirectional Antenna for Micro Waves

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: **Parabolic Dish** and **Horn**.



a. Dish antenna b. Horn antenna

A parabolic antenna works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.

A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by the curved head. Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

Applications of Micro Waves

Microwaves, due to their unidirectional properties, are very useful when unicast(one-to-one) communication is needed between the sender and the receiver. They are used in cellular phones, satellite networks and wireless LANs.

There are 2 types of Microwave Transmission :

1. Terrestrial Microwave
2. Satellite Microwave

Advantages of Microwave Transmission

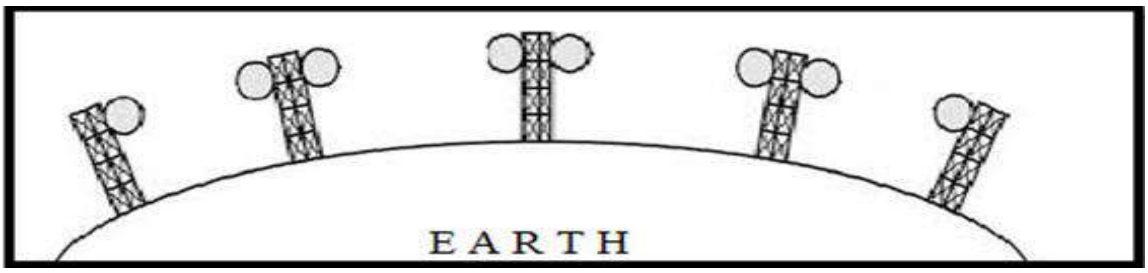
- Used for long distance telephone communication
- Carries 1000's of voice channels at the same time

Disadvantages of Microwave Transmission

- It is very costly

Terrestrial Microwave

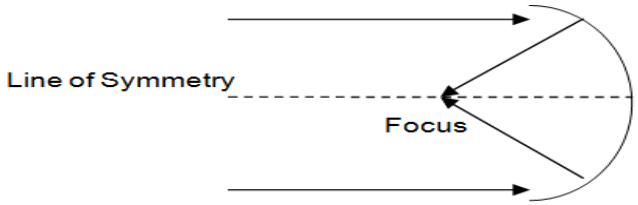
For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna .The signal received by an antenna can be converted into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world



There are **two types of antennas** used for terrestrial microwave communication :

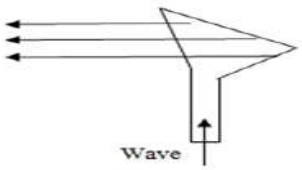
1. Parabolic Dish Antenna

In this every line parallel to the line of symmetry reflects off the curve at angles in a way that they intersect at a common point called focus. This antenna is based on geometry of parabola.



2. Horn Antenna

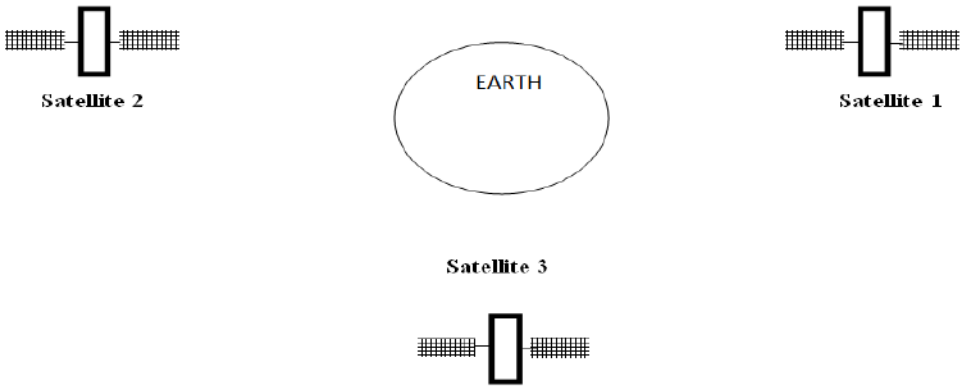
It is a like gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.



Satellite Microwave

This is a microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles carry them.

These are positioned 36000 Km above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.



Features of Satellite Microwave

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for orbiting satellite is difficult.

Advantages of Satellite Microwave

- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
- A single microwave relay station which is visible from any point.

Disadvantages of Satellite Microwave

- Satellite manufacturing cost is very high
- Cost of launching satellite is very expensive
- Transmission highly depends on whether conditions, it can go down in bad weather

Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another, a short-range communication system in on room cannot be affected by another system in the next room.

When we use infrared remote control, we do not interfere with the use of the remote by our neighbours. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications of Infrared Waves

- The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.
- The Infrared Data Association(IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mouse, PCs and printers.
- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.