Computer Network:

Definition: Computer Network is a collection of two or more systems that are connected together for the purpose of communicating and sharing data in network.

NETWORK HARDWARE:

There is no generally accepted taxonomy into which all computer networks fit, but two dimensions stand out as important: transmission technology and scale. We will now examine each of these in turn.

Broadly speaking, there are two types of transmission technology that are in widespread use: **broadcast** links and **point-to-point** links.

Point-to-point links connect individual pairs of machines. To go from the source to the destination on a network made up of point-to-point links, short messages, called **packets** in certain contexts, 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. Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called **unicasting**.

In contrast, on a broadcast network, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others. An address field within each packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.

Broadcast systems usually 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, which known as **multicasting**.

An alternative criterion for classifying networks is by scale. Distance is important as a classification metric because different technologies are used at different scales.

In Fig. 1-6 we classify multiple processor systems by their rough physical size. At the top are the personal area networks, networks that are meant for one person. Beyond these come longer-range networks. These can be divided into local, metropolitan, and wide area networks, each with increasing scale. Finally, the connection of two or more networks is called an internetwork. The worldwide Internet is certainly the best-known (but not the only) example of an internetwork. Soon we will have even larger internetworks with the **Interplanetary Internet** that connects networks across space

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Figure 1-6. Classification of interconnected processors by scale.

Types of Networks:

- **Personal Area Networks (PAN)**
- **Local area networks (LAN)**
- **Wide area networks (WAN)**
- **Metro Politian area network (MAN)**
- **Internetworks**

PANs (**Personal Area Networks**) let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer. Without using wireless, this connection must be done with cables. So many new users have a hard time finding the right cables and plugging them into the right little holes (even though they are usually color coded) that most computer vendors offer the option of sending a technician to the user's home to do it. To help these users, some companies got together to design a short-range wireless network called **Bluetooth** to connect these components without wires. The idea is that if your devices have Bluetooth, then you need no cables. You just put them down, turn them on, and they work together. For many people, this ease of operation is a big plus.

In the simplest form, Bluetooth networks use the master-slave paradigm of Fig. 1-7. The system unit (the PC) is normally the master, talking to the mouse, keyboard, etc., as slaves. The master tells the slaves what addresses to use, when they can broadcast, how long they can transmit, what frequencies they can use, and so on.

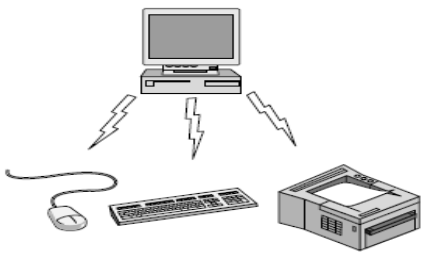


Figure 1-7. Bluetooth PAN configuration.

Local Area Networks: (LAN)

The next step up is the **LAN** (**Local Area Network**). A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory. LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information. When LANs are used by companies, they are called **enterprise networks**.

Wireless LANs are very popular these days, especially in homes, older office buildings, cafeterias, and other places where it is too much trouble to install cables. In these systems, every computer has a radio modem and an antenna that it uses to communicate with other computers. In most cases, each computer talks to a device in the ceiling as shown in Fig. 1-8(a). This device, called an **AP** (**Access Point**), **wireless router**, or **base station**, relays packets between the wireless computers and also between them and the Internet. Being the AP is like being the popular kid as school because everyone wants to talk to you. However, if other computers are close enough, they can communicate directly with one another in a peer-to-peer configuration.

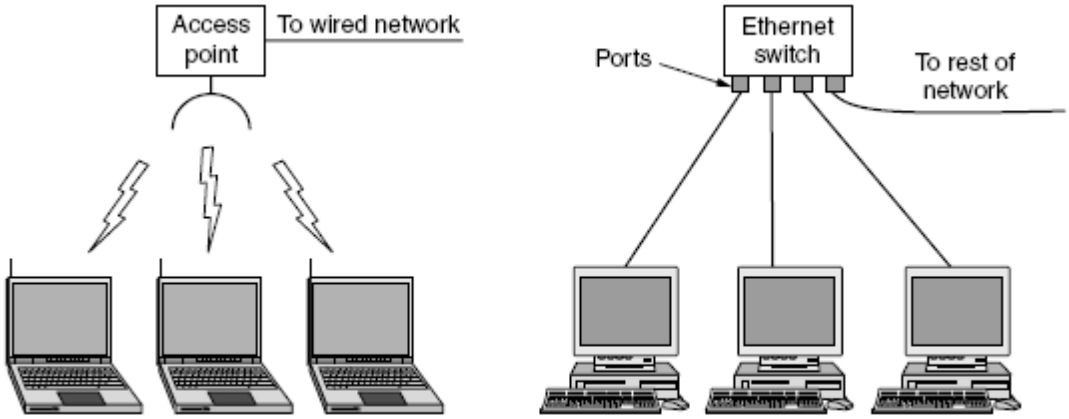


Figure 1-8. Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.

Metropolitan Area Networks:(MAN)

A **MAN** (**Metropolitan Area Network**) covers a city. The best-known examples of MANs are the cable television networks available in many cities. These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception. In those early systems, a large antenna was placed on top of a nearby hill and a signal was then piped to the subscribers' houses.

At first, these were locally designed, ad hoc systems. Then companies began jumping into the business, getting contracts from local governments to wire up entire cities. The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on. But from their inception until the late 1990s, they were intended for television reception only.

When the Internet began attracting a mass audience, the cable TV network operators began to realize that with some changes to the system, they could provide two-way Internet service in unused parts of the spectrum. At that point, the cable TV system began to morph from simply a way to distribute television to a metropolitan area network. To a first approximation, a MAN might

look something like the system shown in Fig. 1-9. In this figure we see both television signals and Internet being fed into the centralized **cable headend** for subsequent distribution to people's homes.

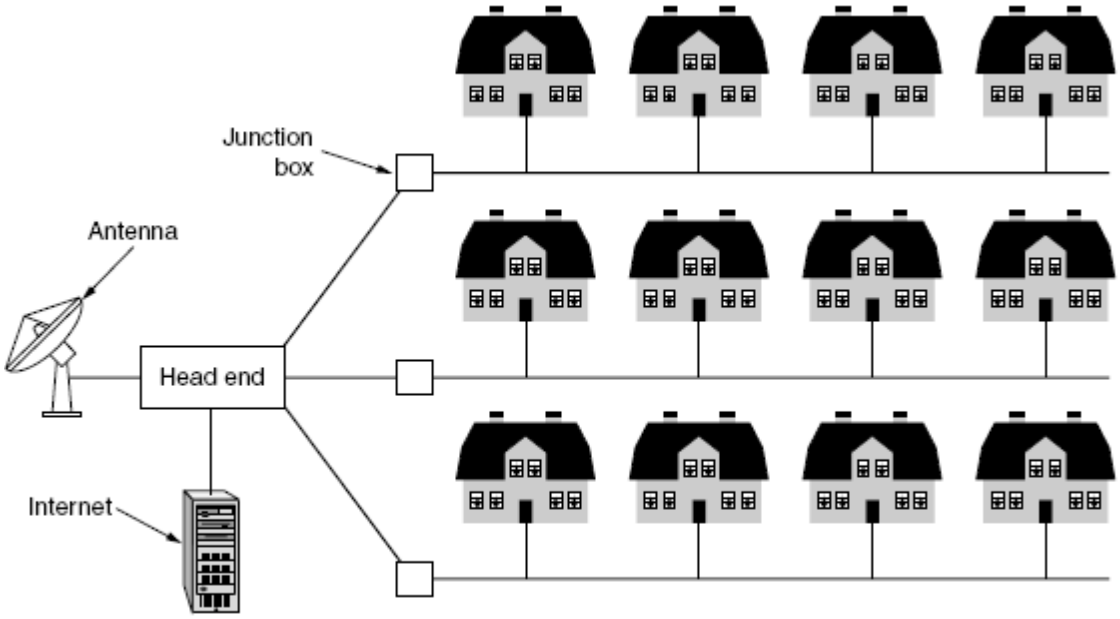


Figure 1-9. A metropolitan area network based on cable TV.

Wide Area Networks: (WAN)

A **WAN** (**Wide Area Network**) spans a large geographical area, often a country or continent. We will begin our discussion with wired WANs, using the example of a company with branch offices in different cities.

We will follow traditional usage and call these machines hosts. The rest of the network that connects these hosts is then called the **communication subnet**, or just **subnet** for short. The job of the subnet is to carry messages from host to host, just as the telephone system carries words (really just sounds) from speaker to listener.

In most WANs, the subnet consists of two distinct components: transmission lines and switching elements. **Transmission lines** move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Most companies do not have transmission lines lying about, so instead they lease the lines from a telecommunications company. **Switching elements**, or just **switches**, are specialized computers that connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them.

The variation is that the subnet may be run by a different company. The subnet operator is known as a **network service provider** and the offices are its customers. This structure is shown in Fig. 1-12. The subnet operator will connect to other customers too, as long as they can pay and it can provide service. Since it would be a disappointing network service if the customers could only send packets to each other, the subnet operator will also connect to other networks that are part of the Internet. Such a subnet operator is called an **ISP** (**Internet**

Service Provider) and the subnet is an **ISP network**. Its customers who connect to the ISP receive Internet service.

We can use the ISP network to preview some key issues that we will study in later chapters. In most WANs, the network contains many transmission lines, each connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers. There may be many paths in the network that connect these two routers. How the network makes the decision as to which path to use is called the **routing algorithm**. Many such algorithms exist. How each router makes the decision as to where to send a packet next is called the **forwarding algorithm**. Many of them exist too.

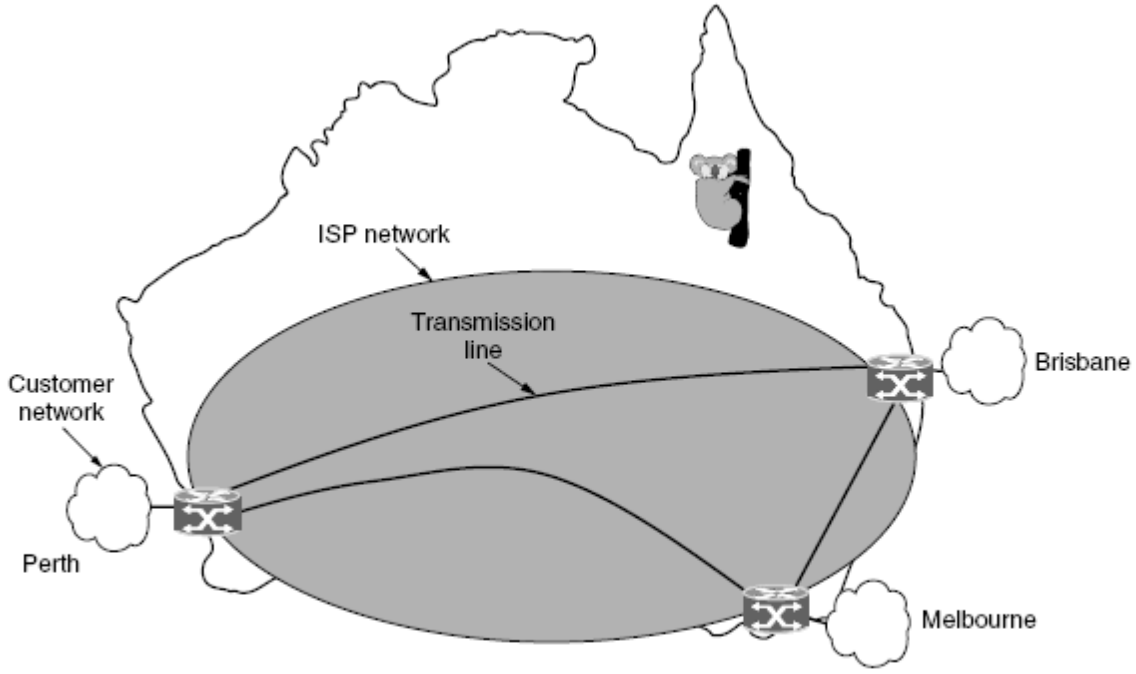


Figure 1-12. WAN using an ISP network.

Internetworks:

Many networks exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. The fulfillment of this desire requires that different, and frequently incompatible, networks be connected. A collection of interconnected networks is called an **internetwork** or **internet**. These terms will be used in a generic sense, in contrast to the worldwide Internet (which is one specific internet), which we will always capitalize. The Internet uses ISP networks to connect enterprise networks, home networks, and many other networks.

Subnets, networks, and internetworks are often confused. The term ‘‘subnet’’ makes the most sense in the context of a wide area network, where it refers to the collection of routers and communication lines owned by the network operator. As an analogy, the telephone system consists of telephone switching offices connected to one another by high-speed lines, and to houses and businesses by low-speed lines. These lines and equipment, owned and managed by the telephone company, form the subnet of the telephone system. The telephones themselves (the hosts in this analogy) are not part of the subnet.

Difference b/w LAN , WAN, MAN:

PARAMETERS	LAN	WAN	MAN
Ownership of network	Private	Private or public	Private or public
Geographical area covered	Small	Very large	Moderate
Design and maintenance	Easy	Not easy	Not easy
Communication medium	Coaxial cable	PSTN or satellite links	Coaxial cables, PSTN, optical fibre, cables, wireless
Bandwidth	Low	High	moderate
Data rates(speed)	High	Low	moderate

NETWORK SOFTWARE:

- **Protocol hierarchies**
- **Design issues for the layers**
- **Connection-oriented versus connectionless service**
- **Service primitives**

The first computer networks were designed with the hardware as the main concern and the software as an afterthought. This strategy no longer works. Network software is now highly structured.

Protocol Hierarchies:

- In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task.
- The main aim of the layered architecture work is to divide the design into different layers.
- 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 next layers.
- The basic elements of layered architecture are services, protocols, and interfaces .
    - Service: It is a set of actions that a layer provides to the next layer.
    - Protocol: It defines a set of rules of each layer .
    - Interface: It is a way through which the message is transferred from one layer to another layer.

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 while 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.

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 software processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol to talk to each other.

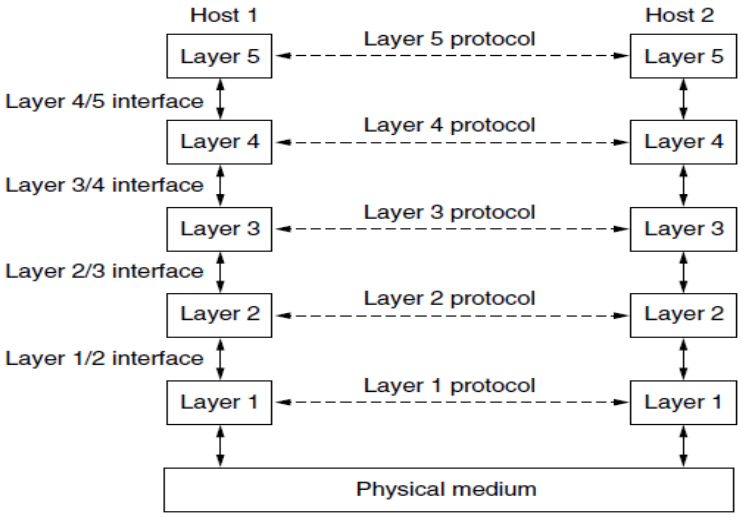


Figure 1-13. Layers, protocols, and interfaces.

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. When network designers decide how many layers to include in a network and what each one should do, one of the most important considerations is defining clean interfaces between the layers. Doing so, in turn, requires that each layer perform a specific collection of well-understood functions. In addition to minimizing the amount of information that must be passed between layers.

A set of layers and protocols is called a **network architecture**. The specification of an architecture must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol. Neither the details of the implementation nor the specification of the interfaces is part of the architecture because these are hidden away inside the machines and not visible from the outside. It is not even necessary that the interfaces on all machines in a network be the same, provided that each machine can correctly use all the protocols. A list of the protocols used by a certain system, one protocol per layer, is called a **protocol stack**.

Design Issues for the Layers:

Some of the key design issues that occur in computer networks will come up in layer after layer. Below, we will briefly mention the more important ones.

- Some of the key design issues that occur in computer networks .
- **"Reliability" is the design issue** of making a ***network that operates correctly*** **even though it is made up of a collection of components .**

Ex: Think about the bits of a packet traveling through the network.

- There is a chance that **some of these bits will be received damaged** (inverted) due to ***electrical noise, random wireless signals, hardware flaws, software bugs*** and so on. **How is it possible that we find and fix these errors?**

- **One mechanism for *finding errors"* in received information uses codes** for "**error detection**".

- **Information that is incorrectly received** then it can be **retransmitted until it is received correctly.** More powerful codes allow for "**error correction**". **Both of these mechanisms work by adding redundant information**.

- **Error detection** is the **detection** of **errors** caused by noise or other impairments during transmission from the transmitter to the receiver.
- **"flow control"** is the process of managing the rate of ***data transmission between two nodes*** to prevent a ***fast sender from a slow receiver .***
- **Feedback from the receiver to the sender is often used.** This subject is called **flow control**.
- **Flow control** should be **distinguished(different)**from ***congestion control***, (which is used for controlling the ***flow of data when congestion has actually occurred.)***
- Sometimes the problem is that the network is oversubscribed because too **many computers want to send messages at that time too much traffic, and the network cannot deliver it all.**
- This overloading of the network is called "**congestion".**

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.

Connection-Oriented Versus Connectionless Service:

Layers can offer two different types of service to the layers above them: connection-oriented and connectionless. In this section we will look at these two types and examine the differences between them.

Connection-oriented service is modeled after the telephone system. To talk to someone, you pick up the phone, dial the number, talk, and then hang up. Similarly, to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection. The essential aspect of a connection is that it acts like a tube: the sender pushes objects (bits) in at one end, and the receiver takes them out at the other end. In most cases the order is preserved so that the bits arrive in the order they were sent.

In some cases when a connection is established, the sender, receiver, and subnet conduct a **negotiation** about the parameters to be used, such as maximum message size, quality of service required, and other issues. Typically, one side makes a proposal and the other side can accept it, reject it, or make a counterproposal. A **circuit** is another name for a connection with associated resources, such as a fixed bandwidth. This dates from the telephone network in which a circuit was a path over copper wire that carried a phone conversation.

In contrast to connection-oriented service, **connectionless** service is modeled after the postal system. Each message (letter) carries the full destination address, and each one is routed through the intermediate nodes inside the system independent of all the subsequent messages. There are different names for messages in different contexts; a **packet** is a message at the network layer. When the intermediate nodes receive a message in full before sending it on to the next node, this is called **store-and-forward switching**. The alternative, in which the onward transmission of a message at a node starts before it is completely received by the node, is called **cut-through switching**. Normally, when two messages are sent to the same destination, the first one sent will be the first one to arrive. However, it is possible that the first one sent can be delayed so that the second one arrives first.

Connection-oriented Vs Connection-less Services

CONNECTION-ORIENTED SERVICE	CONNECTION-LESS SERVICE
Connection-oriented services involve the establishment and termination of the connection before transmitting data.	**Connection-less services** involve the no need to establishment the connection before transmitting data.
Connection-oriented Service is feasible.	Connection-less Service is not feasible.
In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give the guarantee of reliability.
In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets follow the same route may or may not.
Connection-oriented Services requires a bandwidth of high range.	Connection-less Service requires a bandwidth of low range.
Resource Allocation Need to be allocated.	Need not to be allocated.

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Text messaging
	Request-reply	Database query

Figure 1-16. Six different types of service.

Service Primitives:

A service is formally specified by a set of **primitives** (operations) available to user processes 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 connectionless service. As a minimal example of the service primitives that might provide a reliable byte stream, consider the primitives listed in Fig. 1-17. They will be familiar to fans of the Berkeley socket interface, as the primitives are a simplified version of that interface.

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
ACCEPT	Accept an incoming connection from a peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Figure 1-17. Six service primitives that provide a simple connection-oriented service.

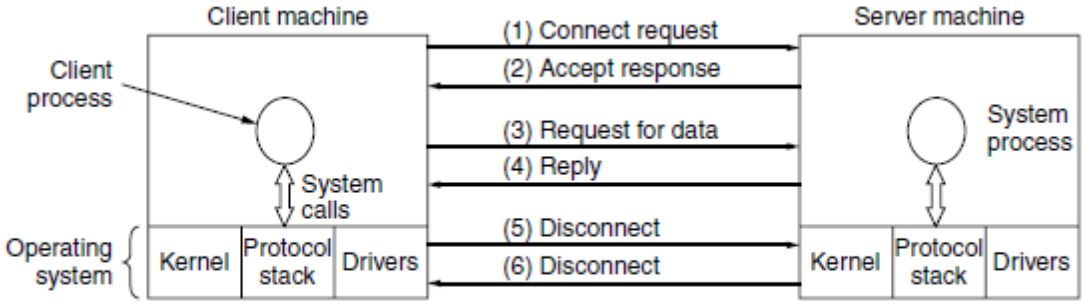


Figure 1-18. A simple client-server interaction using acknowledged datagrams.

Reference Model:

Reference Model offers a means of standardization which is acceptable worldwide. Since people using the computer network are located over a wide physical range and their network devices might have heterogeneous architecture. In order to provide communication among heterogeneous devices, we need a standardized model i.e. a reference model, which would provide us way how these devices can communicate regardless their architecture.

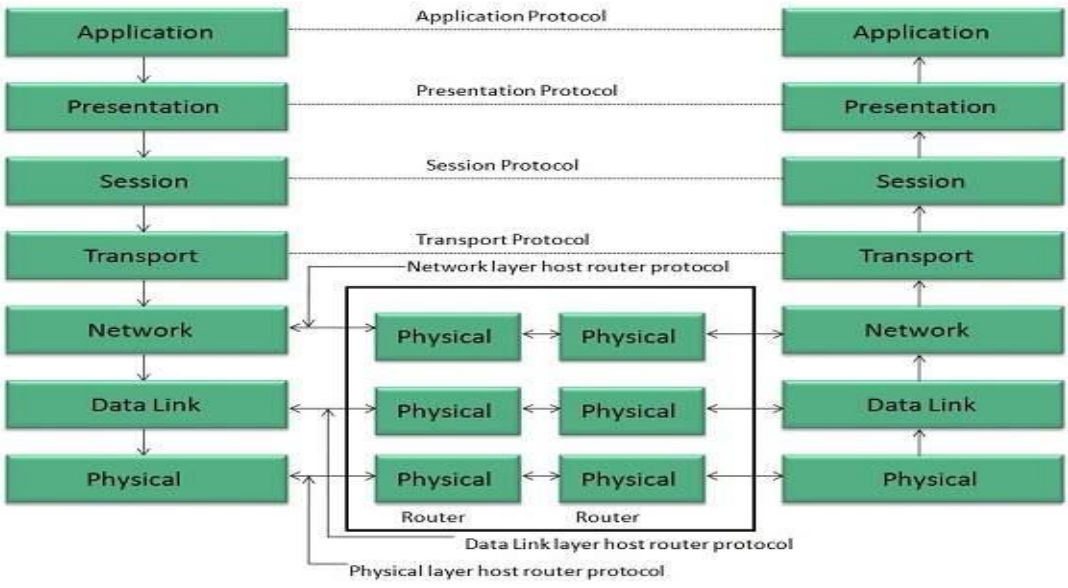
We have two reference models such as **OSI** model and **TCP/IP** reference model, however, the OSI model is a hypothetical one but the TCP/IP is absolutely practical model.

ISO- OSI Reference Model:

OSI is acronym of Open System Interface. This model is developed by the International organization of Standardization (ISO) and therefore also referred as ISO-OSI Model.

The OSI model consists of seven layers as shown in the following diagram. Each layer has a specific function, however each layer provide services to the layer above.

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



Physical Layer:

- Physical Layer is the lowest layer of the OSI Model.
- It is responsible for transmission and reception of the unstructured raw data over network.
- It performs *Encoding and Decoding mechanisms.*(bits will be encoded conversion of bits)
- It converts the digital/analog bits into electrical signal or optical signals.
- Data transfer in the form of bits.
- Deciding whether the connection is simplex, half duplex or full duplex.

Data Link Layer:

- Data link layer synchronizes the information which is to be transmitted over the physical layer.
- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- Data transfer in the form of frames.
- Transmitting and receiving data frames sequentially is managed by this layer.
- This layer sends and expects acknowledgements for frames received and sent respectively.
- Enables error detection, and error correction bits to the data which are to be transmitted.

Network Layer:

- 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 the shortest path to transmit the packet, from the number of routes available.
- (Ip address (source address +destination address)) + port address + fragments)
- It acts as a network controller.
- It manages the Subnet traffic.
- It decides by which route data should take.
- Data transfer in the form of packets.
- It performs Routing: The network layer protocols determine which route is suitable from source to destination.

Transport Layer:

- It decides if the data transmission should take parallel paths or single path.
- It is responsible for end to end data transfer with the help of segments(fragmentation)(every fragmentation port address will be added).
- It performs multiplexing, splitting on the data. (port address + fragments)
- It breaks the data groups into smaller units so that they are handled more efficiently by the network layer.
- It also provides flow and error control , sequence numbering and message acknowledgement with Reliable data delivery.

- Data broken into datagrams.(Self-contained packet of data that carries with it the source and destination information for correct routing.).

Session Layer:

The Session layer performs the following functions:

- **Synchronization :** This layer allows a **process to add checkpoints(** based on check points to reduce errors) which are considered as synchronization points into the data.
- These **synchronization helps to identify the error so that the data is re-synchronized properly.**
- **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.
- **To Establish, manage and terminate the sessions.**

Presentation Layer:

The Presentation layer performs the following functions:

- Presentation layer is also called the **Translation layer**.
- To **translate should be done encrypt ,decrypt (plaintext and cipher text)and compress the data.**

The functions of the presentation layer are :

Translation

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.

Compression: Reduces the number of bits that need to be transmitted on the network.

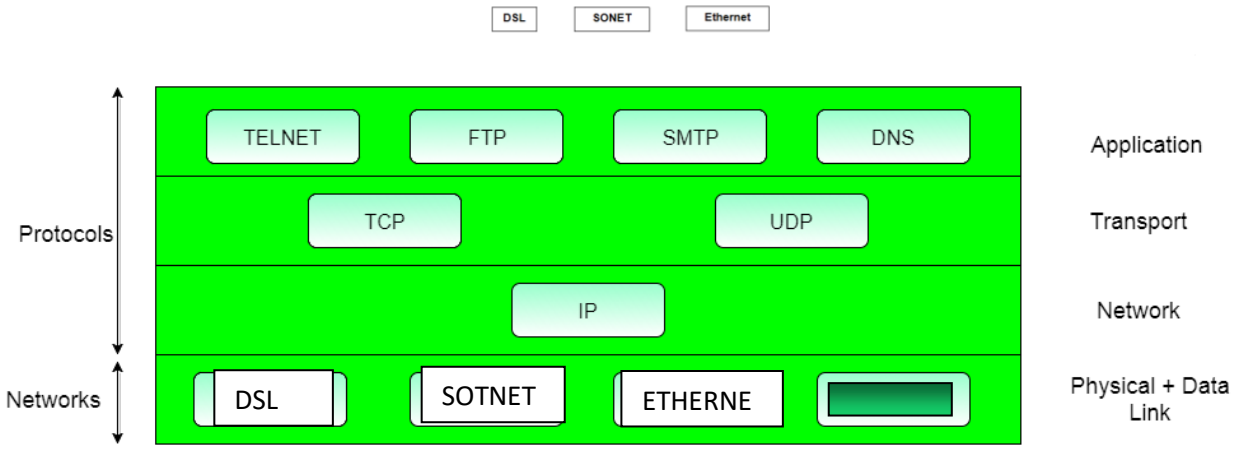
Application Layer:

The Application layer performs the following functions:

- At the very top of the OSI Reference Model stack of layers.
- It allow to access network resources.
- In Applications are directly communicated with network the Data with the help of web browsers.
- It provides different services such as **manipulation of information** in several ways, **retransferring the files , distributing the results etc over a network.**
- This layer performs **authentication details to perform transactions.**

TCP/IP Model:

- TCP/IP model is practical model and is used in the Internet. TCP/IP is acronym of Transmission Control Protocol and Internet Protocol.
- The TCP/IP model combines the two layers (Physical and Data link layer) into one layer i.e. Host-to-Network layer. The following diagram shows the various layers of TCP/IP model:
    - **Link layer or Host to network.**
    - **Internet layer**
    - **Transport layer**
    - **Application layer**



Application Layer:

- This layer is same as that of the OSI model and performs the following functions:
- It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.
- The functions such as LOGIN or password checking are also performed by the application layer.
- Protocols used: TELNET, FTP, SMTP, HTTP,SNMP are the protocols employed in this layer.

Protocols in application layer:

HTTP: HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video.

SMTP: SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

DNS: DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely.

TELNET: It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer.

FTP: FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Transport Layer:

- It does the same functions as that of transport layer in OSI model. Here are the key points regarding transport layer:
- It uses TCP and UDP protocol for end to end transmission.
- TCP is connection oriented protocol , TCP also handles flow control.
- The UDP is connection less protocols.
- Segments and splitting of data.
- Decides data transfer either single path or multiple paths.
- Header information added , transmitting error free end to end data delivery.
- Protocols used: TCP/IP and UDP protocols in this layer.

Internet Layer:

The function of this layer is to allow the host to insert **packets** into network and then make them ***travel independently to the destination*.** However, **the order of receiving the packets from the sequence they were sent.(packet delivery , routing, congestion control).**

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the **independent route they take.**

Protocols used:

IP (Internet protocol) Path selection , routing and addressing

- ICMP (Internet Control Message Protocol)
- **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
- **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.

Host-to-Network Layer:

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- Used for **physical transmission of data.**
- This layer is mainly responsible for the physical transmission of the data between two devices on the network.
- Defines **protocols to connect host.**

Ethernet : Ethernet is a family of computer networking technologies commonly used in local area networks, metropolitan area networks and wide area networks

DSL: DSL stands for Digital Subscriber Line. Users get a high speed bandwidth connection over a network.

SONET: Synchronous optical network is a communication protocol . that is used to transmit a large amount of data over a large distances using optical fiber.

Difference b/w OSI Reference model vs TCP/IP :

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.

11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

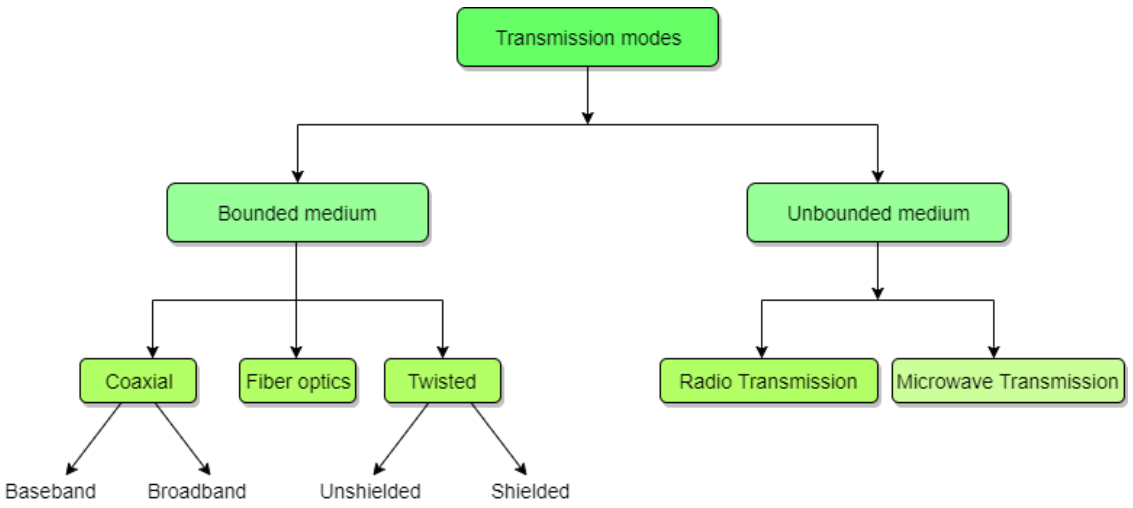
Difference b/w TCP vs UDP:

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
TCP is a connection-oriented protocol.	UDP is the connection less protocol.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
TCP is heavy-weight.	UDP is lightweight.
TCP doesn't supports Broadcasting.	UDP supports Broadcasting.

Unit-1 –ii part:

Transmission Mediums in Computer Networks:

- **Media** is the general term used to describe the **data path** forms the **physical channel b/w sender and receiver.**
- **Data is represented by computers** and other telecommunication devices **using signals**.
- **Signals are transmitted** in the form of **electromagnetic signals travel from one device to another.**
- Electromagnetic energy (includes electrical and magnetic fields) consists of power, voice, visible light, radio waves etc.
- **Different types of transmission media** used for **different data transmission rates** and long distances.
- **Higher bandwidth transmission media support higher data rates.**



Factors to be considered while selecting a Transmission Medium

1. Transmission Rate
2. Cost and Ease of Installation
3. Resistance to Environmental Conditions
4. Distances

Bounded or Guided Transmission Media:

Guided media, which are those that provide a conduit from one device to another, include **Twisted-Pair Cable**, **Coaxial Cable**, and **Fiber-Optic Cable**.

Depending on the type of transmission medium it can be classified into 3 types.

1. **Twisted-Pair Cable**
2. **Coaxial Cable**, and
3. **Fiber-Optic Cable**.

A signal travelling along any of these media is directed and contained by the **physical connection** limits of the medium.

- **"Twisted-pair"** and "**coaxial cable"** use metallic (copper) conductors that ***accept and transport signals in the form of electric current.***
- **"Fiber-Optical"** 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.**
- Its frequency range is 0 to 3.5 kHz.
- A twisted pair consists of **two insulated copper wires arranged in regular spiral pattern.**
- **A wire pair acts as single communication link.**
- **One of these wires is used to carry signals to the receiver, and the other is used only as ground reference.**
- Twisted pair cables **transmits both analog and digital signals.**
- **For *Analog signals* Amplifiers are require every 5 to 6 km.**
- **For *Digital signals* repeaters are require every 2 to 3 km.**
- Most commonly used medium for in the **Telephone network.**

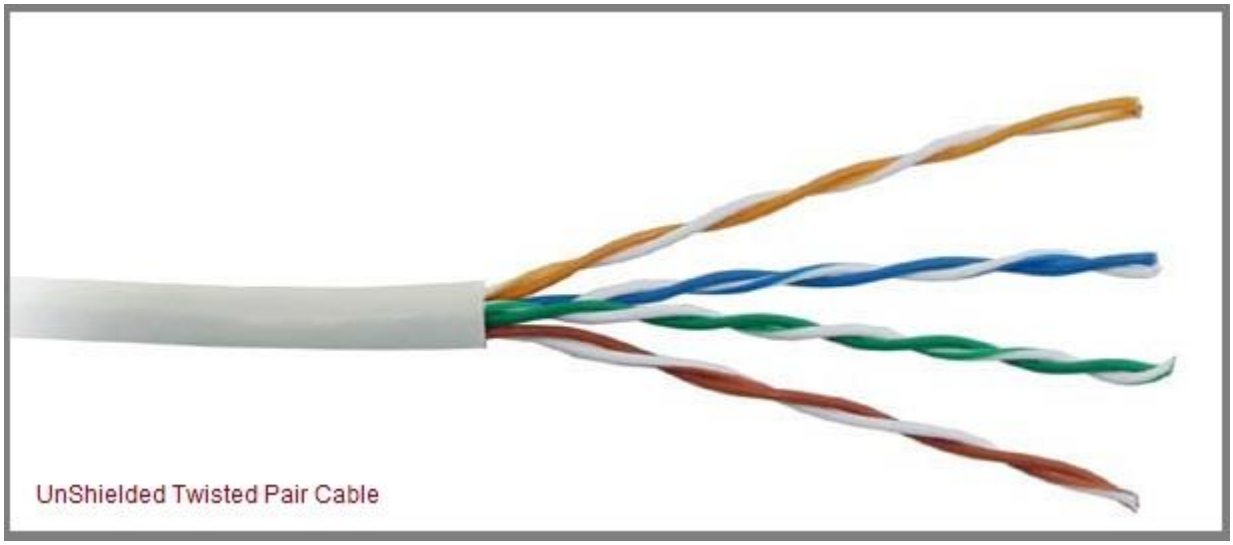
2 TYPES OF TWISTED PAIR CABLES

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

Unshielded Twisted Pair Cable

- UTP is a set of twisted pair of cables .
- 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 color plastic insulator.**
- It is **Least expensive** of all the transmission media **commonly used in LAN**.
- UTP cables consist of 2 or 4 pairs of twisted cable.
- It can be divided into different Categories
- **Category 5**: it supports upto100 mbps.
- **Cat 4:** it supports 16 mbps Data transfer rate.
- **Category 3**: it supports 10 mbps.
- **Cat2**: it supports 4 mbps Data transfer rate.
- **Category 1**: Mostly used in telephone system , it is suitable for voice and low speed of data communication.

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 Cable:

- This **cable has a protective covering which encases each pair of insulated conductors**.
- STP provides **better performance at Lower data rates.**
- **STP is easy to install.**
- **Cost is moderately expensive.**
- **High rate Data transfer rate** up to **150 mbps.**
- **Distance 500 meters max.**
- Electromagnetic noise penetration(forcedly moving) is prevented by metal casing.
- It is faster than unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

Applications of Shielded Twisted Pair Cable

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

Advantages of Shielded Twisted Pair Cable

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signaling 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.

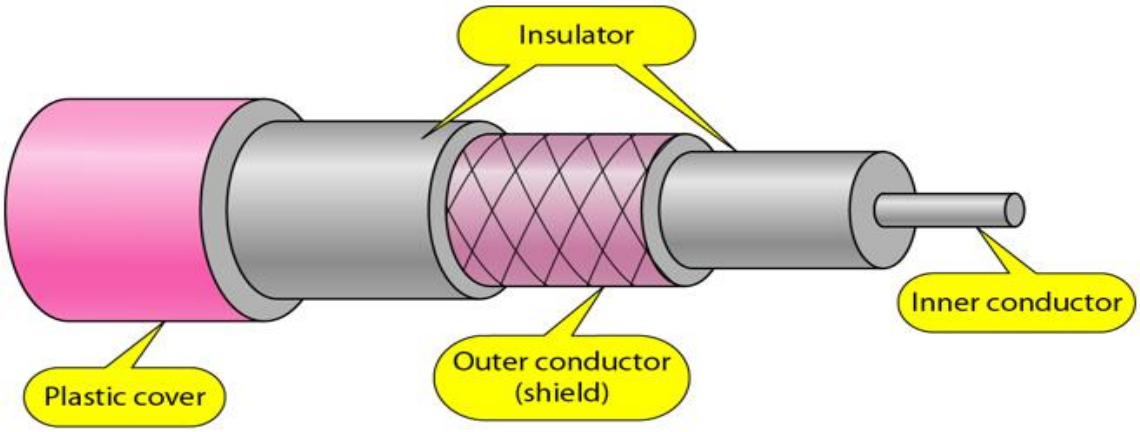
Coaxial Cable:

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as center 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.



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.

Performance of Coaxial Cable

We can measure the performance of a coaxial cable in same way as that of Twisted Pair Cables. From the below figure, it can be seen that the attenuation is much higher in coaxial cable than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

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.

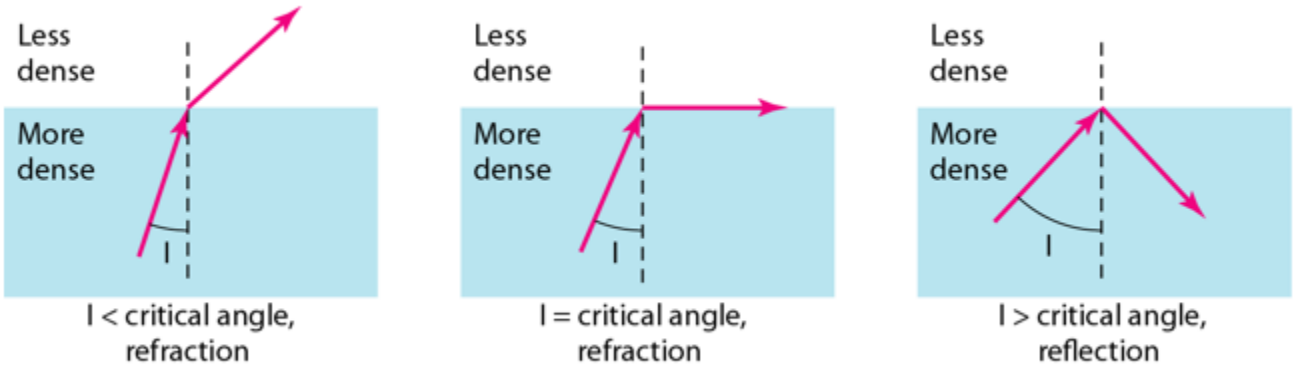
For better understanding we first need to explore several aspects of the **nature of light**.

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

- Light is an electro magnetic signal and it can be modulated (balance or adjust) by information.
- The frequency of light is extremely high , it can be accommodate **wide bandwidth of information and also high data rate** to achieve excellent reliability.
- FOC t**ransmits lights signals rather than electric signals.**
- **Each fiber has Inner core of glass or plastic that conducts light.**
- A cable may contain a single fiber but often fibers are bundled together in the center of the cable.
- FOC may be multimode or single mode. **Multi mode fibers use multiple light paths**

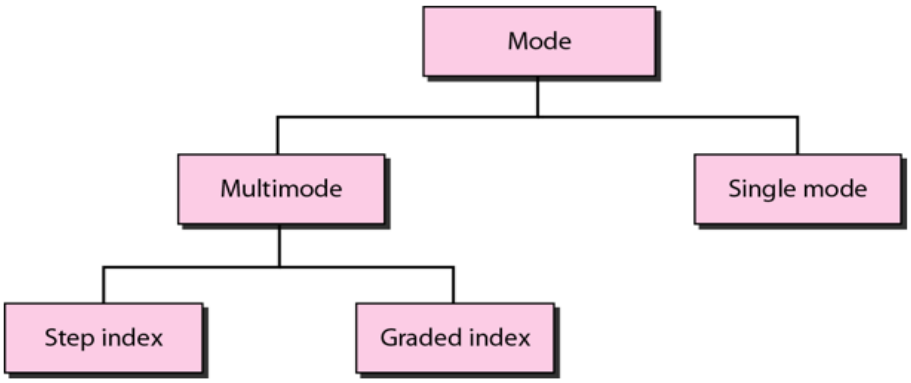
where as **single mode fibers allow single light path.**

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



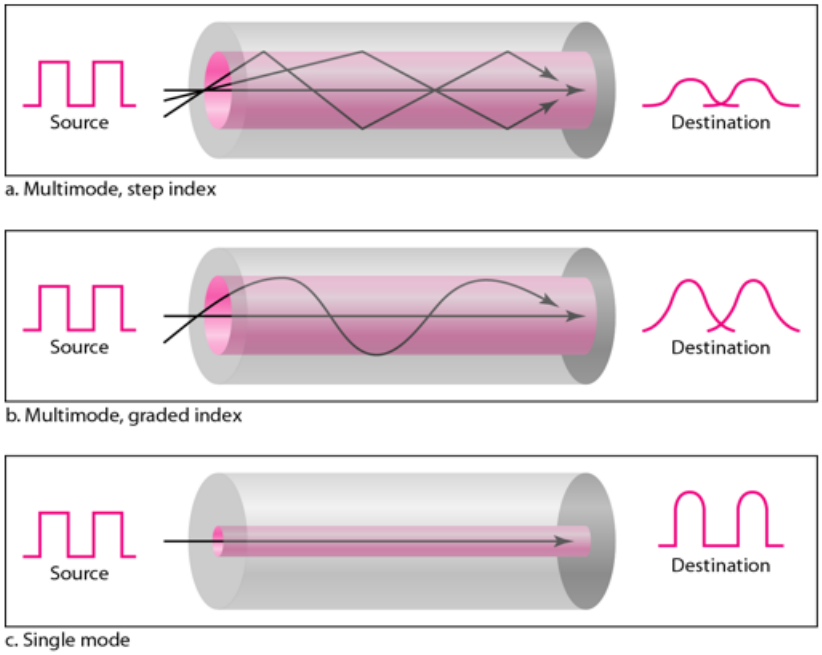
Propagation Modes of Fiber Optic Cable:

Current technology supports two modes(**Multimode** and **Single mode**) for propagating light along optical channels, each requiring fibre with different physical characteristics. Multimode can be implemented in two forms: **Step-index** and **Graded-index**.



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.



- In **multimode step-index fibre**, the density of the core remains constant from the centre to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. The term step-index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fibre.

- In **multimode graded-index fibre**, this distortion gets decreases through the cable. The word index here refers to the index of refraction. This index of refraction is related to the density. A graded-index fibre, therefore, is one with varying densities. Density is highest at the centre of the core and decreases gradually to its lowest at the edge.

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.

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.

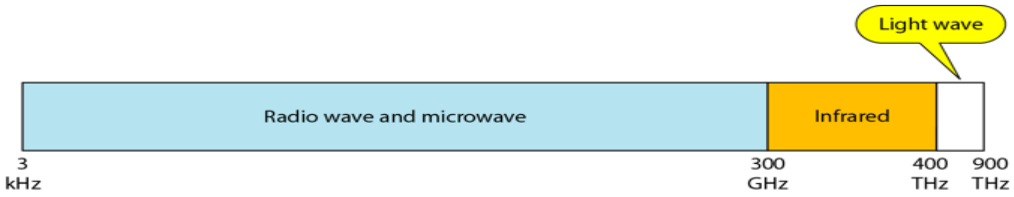
Applications of Fibre Optic Cable

- 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.**
- **These signal energy propagates through air.**
- **Un guided media is mainly used for broadcasting purpose.**
- **This signals propagates in unguided media in the form of electromagnetic waves.**
- 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.**

Examples : Microwaves or radio links, infrared



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.

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

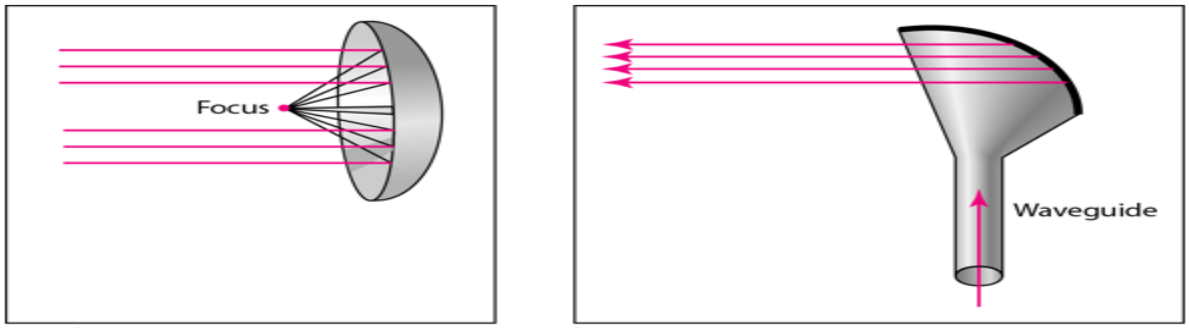
Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves. Micro waves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious 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