UNIT 1 Introductory Concept

CO 1 Explain Basic concept, OSI reference Model. Services .Role of each layer in OSI Model. TCP/IP. Network devices. Transmission Media, Analog and Digital Transmission

CO 2 Apply Channel allocation . Framing. Frame control and Error Control Techniques

CO 3 Describe the function of Network Layer, Logical addressing and Subletting, Routing Mechanism

CO 4 Explain the function of Session and Presentation Layer.

CO 5 Explain different Protocol used at different Application layer HTTP.SNMP..FTP.TELNET. VPN

Content :

- **Goal and Application of Computer Network**
- **Categories of Network**
- **Network Structure and Architecture**
- **Protocols and Standards**
- **OSI Reference Model**
- **TCP/IP Model**
- **Network Devices and Components**
- **Introduction of Physical Layer**
- **Network Topology Design**
- **Types of Connection**
- **Transmission Media**
- **Signal Transmission**
- **Switching Techniques**
- **Multiplexing**
- **ISP**

1.1 Introduction

What is Computer Network?

A computer network is a set of devices connected through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels.

Computer Network uses distributed processing in which task is divided among several computers. Instead, a single computer handles an entire task, each separate computer handles a subset.

1.2 Goals of Computer Network

The main goals of computer networks are as follows −

Resource Sharing

The main goal of the computer network is Resource Sharing. It is to create all the programs, data and hardware accessible to anyone on the network without considering the resource's physical area and the client.

Saving Money

The second goal of a computer network is saving money. Small computers have a much excellent value proportion than higher ones. Mainframes are approximately a method ten times quicker than the quickest single-chip microprocessors, but they cost a huge number of times more.

This imbalance has made numerous system designers build systems, including dynamic personal computers, one per customer, with data kept on at least one shared document server machines. This objective prompts networks for specific computers situated in a similar building, including a network is known as LAN (Local Area Network).

High Reliability

The third goal is to support high reliability by acquiring a different authority of supply. For example, all files can be recreated on a few machines, and thus if one of them is non existent, the additional copies could be available.

Improve Performance

The fourth goal of a computer network is to improve accessibility and the performance of the system. A system's performance can be improved by inserting one or more processors into it as its workload grows.

For example, if the system is full, replacing it with a larger one at a large expense, it is better to add more processors to it at less cost and less disruption to the user. This improves both accessibilities as well as the performance of a system.

Communication Medium

The fifth goal of the computer network offers a powerful communication medium. The different user on the network can immediately identify a document that has been refreshed on a network.

1.3 PROTOCOLS AND STANDARDS

In this section, we define two widely used terms: protocols and standards. First, we define protocol, which is synonymous with rule. Then we discuss standards, which are agreed-upon rules.

Protocols In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing

Syntax. The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself. O

Semantics. The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message? o

Timing. The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost

Standards Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes.

Standards provide guidelineto manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications. Data communication standards fall into two categories:

de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation"). o De facto. Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

De jure. Those standards that have been legislated by an officially recognized body are de jure standards.

Standards Organizations

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Standards Creation Committees While many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:

o **International Organization for Standardization (ISO).** The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.

o **International Telecommunication Union**-Telecommunication Standards Sector (ITU-T). By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT). This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication UnionTelecommunication Standards Sector (ITU-T).

o **American National Standards Institute (ANSI).** Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affiliated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.

o **Institute of Electrical and Electronics Engineers (IEEE**). The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communications.

o **Electronic Industries Association (EIA).** Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of

1.4 Application of Computer Network

Computer networks have become invaluable to organizations as well as individuals. Some of its main uses are as follows −

- **Information and Resource Sharing** − Computer networks allow organizations having units which are placed apart from each other, to share information in a very effective manner. Programs and software in any computer can be accessed by other computers linked to the network. It also allows sharing of hardware equipment, like printers and scanners among varied users.

- **Retrieving Remote Information** − Through computer networks, users can retrieve remote information on a variety of topics. The information is stored in remote databases to which the user gains access through information systems like the World Wide Web.
- **Speedy Interpersonal Communication** − Computer networks have increased the speed and volume of communication like never before. Electronic Mail (email) is extensively used for sending texts, documents, images, and videos across the globe. Online communications have increased by manifold times through social networking services.
- **E-Commerce** − Computer networks have paved way for a variety of business and commercial transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or sell items, pay bills, manage bank accounts, pay taxes, transfer funds and handle investments electronically.

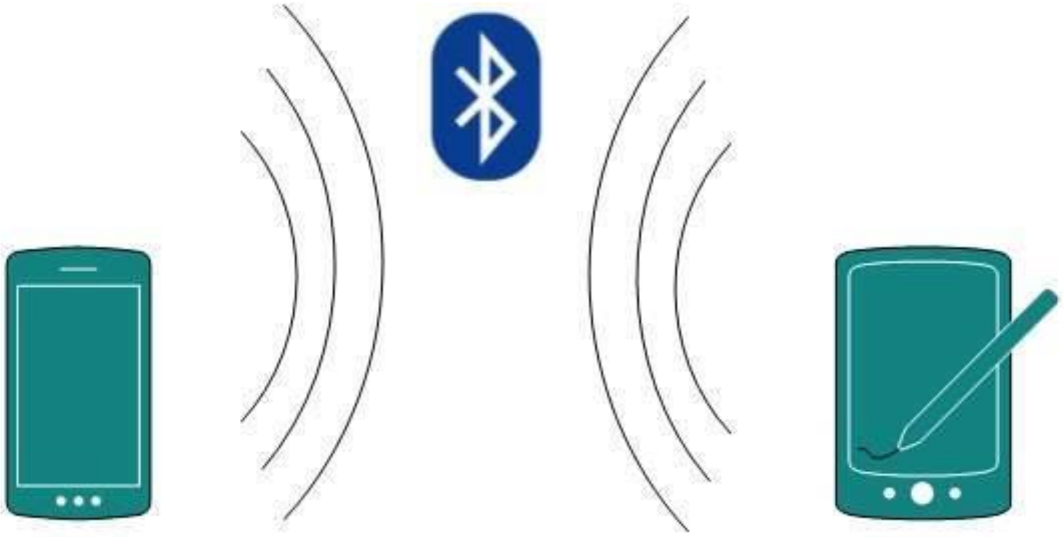
- **Highly Reliable Systems −** Computer networks allow systems to be distributed in nature, by the virtue of which data is stored in multiple sources. This makes the system highly reliable. If a failure occurs in one source, then the system will still continue to function and data will still be available from the other sources.
- **Cost–Effective Systems** − Computer networks have reduced the cost of establishment of computer systems in organizations. Previously, it was imperative for organizations to set up expensive mainframes for computation and storage. With the advent of networks, it is sufficient to set up interconnected personal computers (PCs) for the same purpose.
- **VoIP −** VoIP or Voice over Internet protocol has revolutionized telecommunication systems. Through this, telephone calls are made digitally using Internet Protocols instead of the regular analog phone lines.

1.5 Types of Computer Network

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

Personal Area Network

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

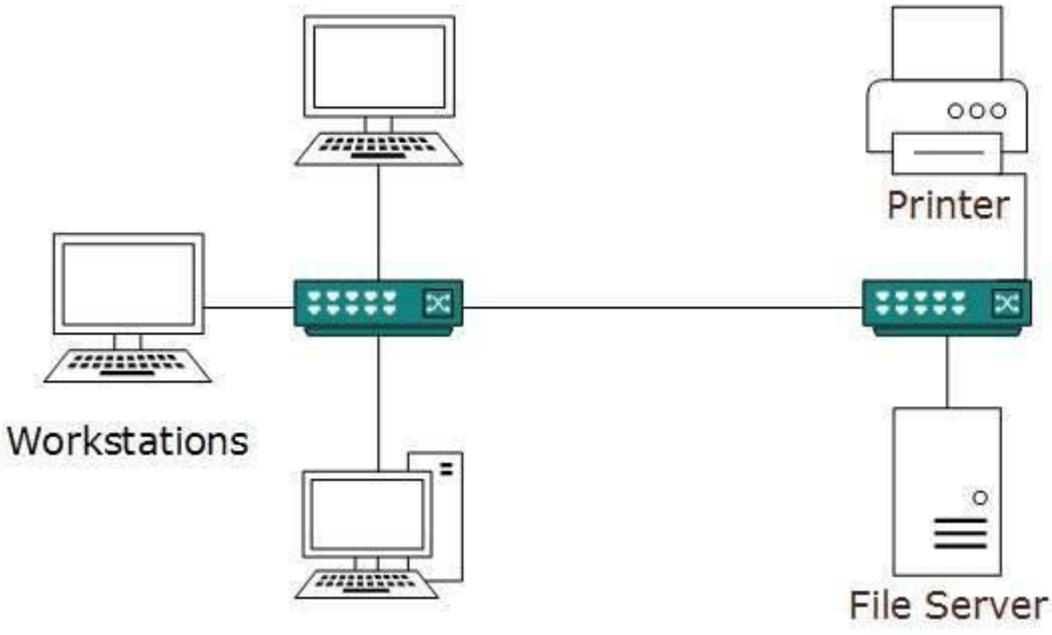


For example, Piconet is Bluetooth-enabled Personal Area Network which may contain up to 8 devices connected together in a master-slave fashion.

Local Area Network

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually,LAN covers an organization' offices, schools, colleges or universities. Number of systems connected in LAN may vary from as least as two to as much as 16 million.

LAN provides a useful way of sharing the resources between end users.The resources such as printers, file servers, scanners, and internet are easily sharable among computers.



LANs are composed of inexpensive networking and routing equipment. It may contains local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally.

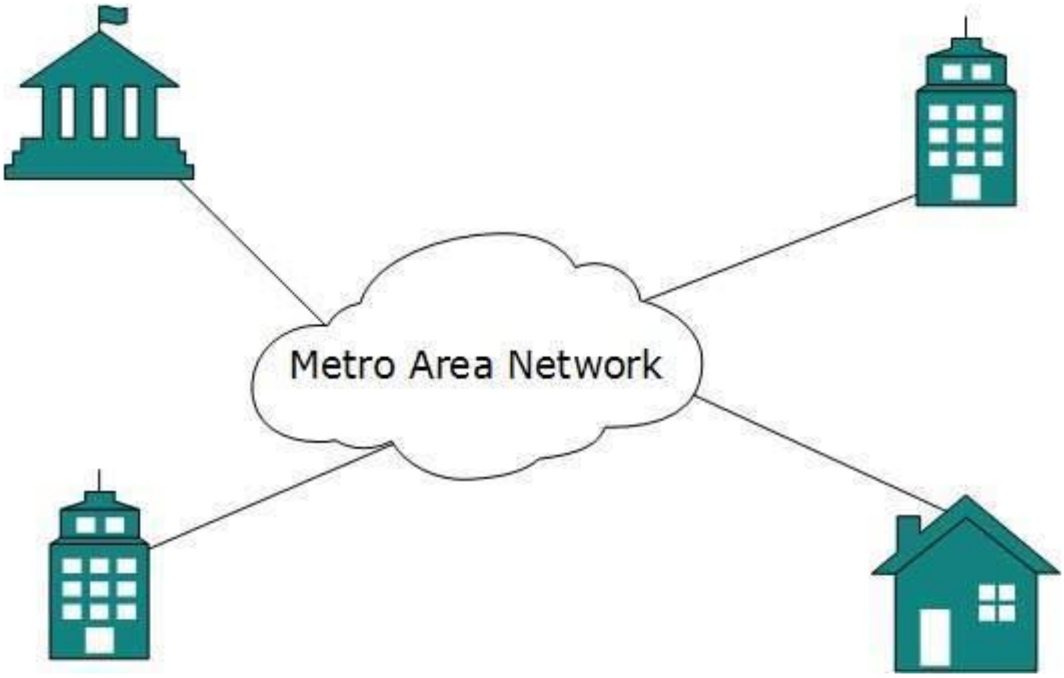
LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology, while Token-ring is rarely seen.

LAN can be wired,wireless, or in both forms at once.

Metropolitan Area Network

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet,Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).

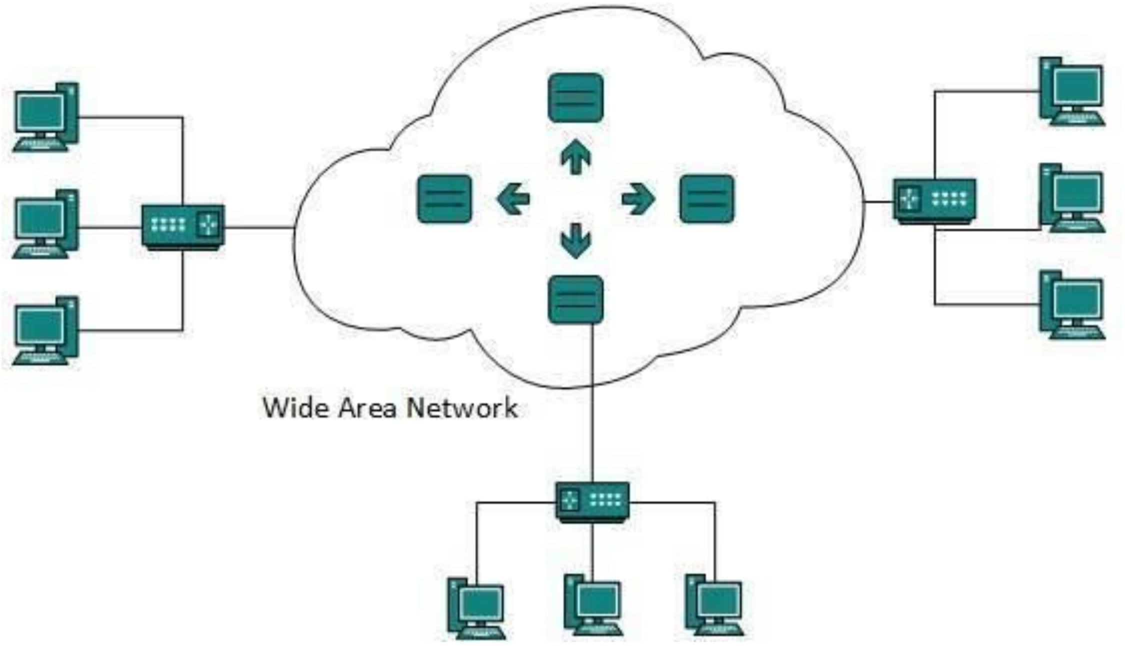
Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.



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

Wide Area Network

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



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

Internetwork

A network of networks is called an internetwork, or simply the internet. It is the largest network in existence on this planet.The internet hugely connects all WANs and it can have connection to LANs and Home networks. Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6.

Internet enables its users to share and access enormous amount of information worldwide. It uses WWW, FTP, email services, audio and video streaming etc. At huge level, internet works on Client-Server model.

Internet uses very high speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

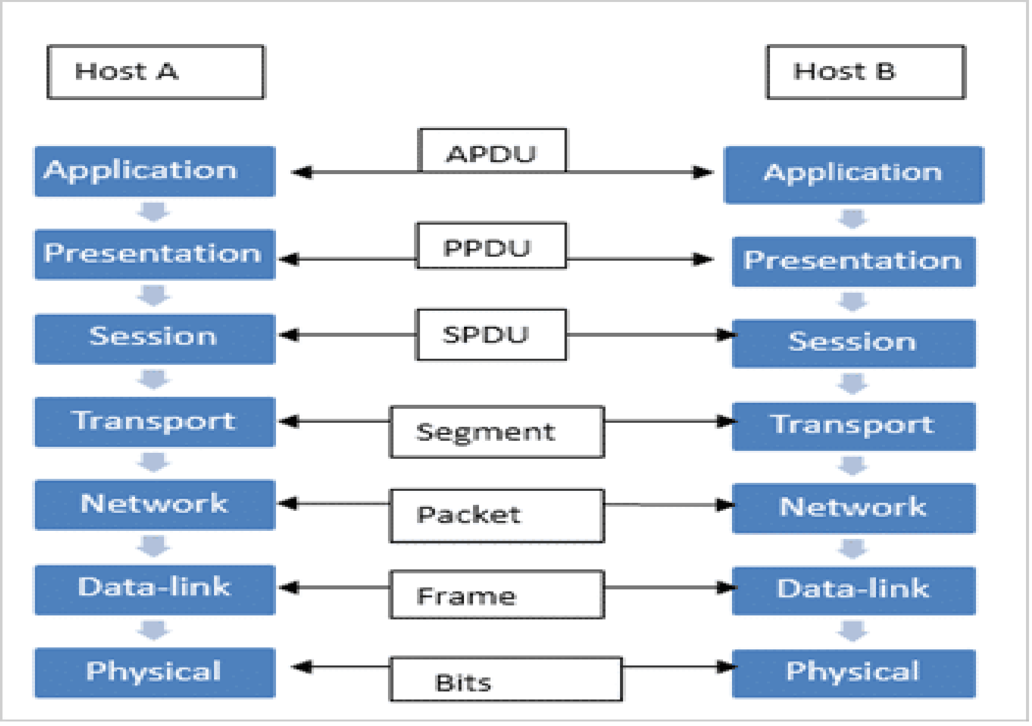
Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by client software known as Web Browsers. When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page. The communication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

Internet is serving many proposes and is involved in many aspects of life. Some of them are:

- Web sites
- E-mail
- Instant Messaging
- Blogging
- Social Media

- Marketing
- Networking
- Resource Sharing
- Audio and Video Streaming

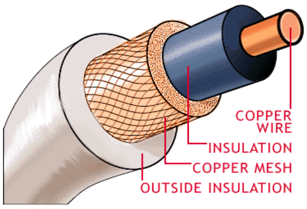
1.6 OSI Reference Model



1 **Physical Layer**

This layer is the lowest layer in the OSI model. It helps in the transmission of data between two machines that are communicating through a physical medium, which can be optical fibres, copper wire or wireless etc. The following are the main functions of the physical layer:

1. Hardware Specification: The details of the physical cables, network interface cards, wireless radios, etc are a part of this layer.



2 Encoding and Signalling: How are the bits encoded in the medium is also decided by this layer. For example, on the coppar wire medium, we can use different voltage levels for a certain time interval to represent '0' and '1'. We may use +5mV for 1nsec to represent '1' and -5mV for 1nsec to represent '0'. All the issues of modulation is dealt with in this layer. eg, we may use Binary phase shift keying for the representation of '1' and '0' rather than using different volatage levels if we have to transfer in RF waves.

3 Data Transmission and Reception: The transfer of each bit of data is the responsibility of this layer. This layer assures the transmission of each bit with a high probability. The transmission of the bits is not completely reliable as there is no error correction in this layer.

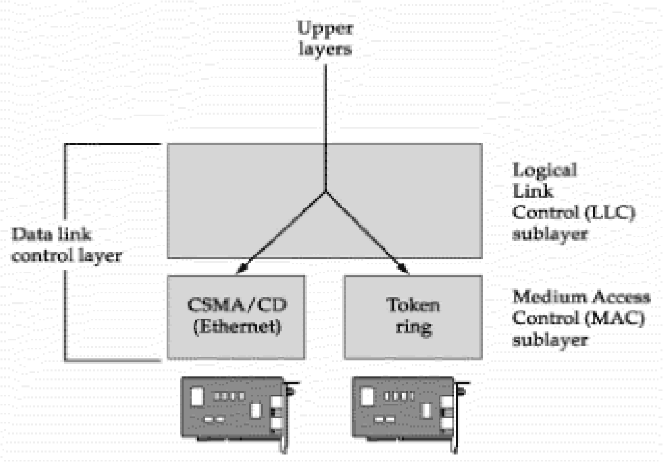
4 Topology and Network Design: The network design is the integral part of the physical layer. Which part of the network is the router going to be placed, where the switches will be used, where we will put the hubs, how many machines is each switch going to handle, what server is going to be placed where, and many such concerns are to be taken care of by the physical layer. The various kinds of topologies that we decide to use may be ring, bus, star or a hybrid of these topologies depending on our requirements.

2 Data Link Layer

This layer provides reliable transmission of a packet by using the services of the physical layer which transmits bits over the medium in an unreliable fashion. This layer is concerned with :

1. Framing : Breaking input data into frames (typically a few hundred bytes) and caring about the frame boundaries and the size of each frame.

2. Acknowledgment : Sent by the receiving end to inform the source that the frame was received without any error.
3. Sequence Numbering : To acknowledge which frame was received.
4. Error Detection : The frames may be damaged, lost or duplicated leading to errors.The error control is on link to link basis.
5. Retransmission : The packet is retransmitted if the source fails to receive acknowledgment.
6. Flow Control : Necessary for a fast transmitter to keep pace with a slow receiver.


Upper layers
Data link control layer
Logical Link Control (LLC) sublayer
CSMA/CD (Ethernet)
Token ring
Medium Access Control (MAC) sublayer

3 Network Layer

Its basic functions are routing and congestion control.
Routing: This deals with determining how packets will be routed (transferred) from source to destination. It can be of three types :

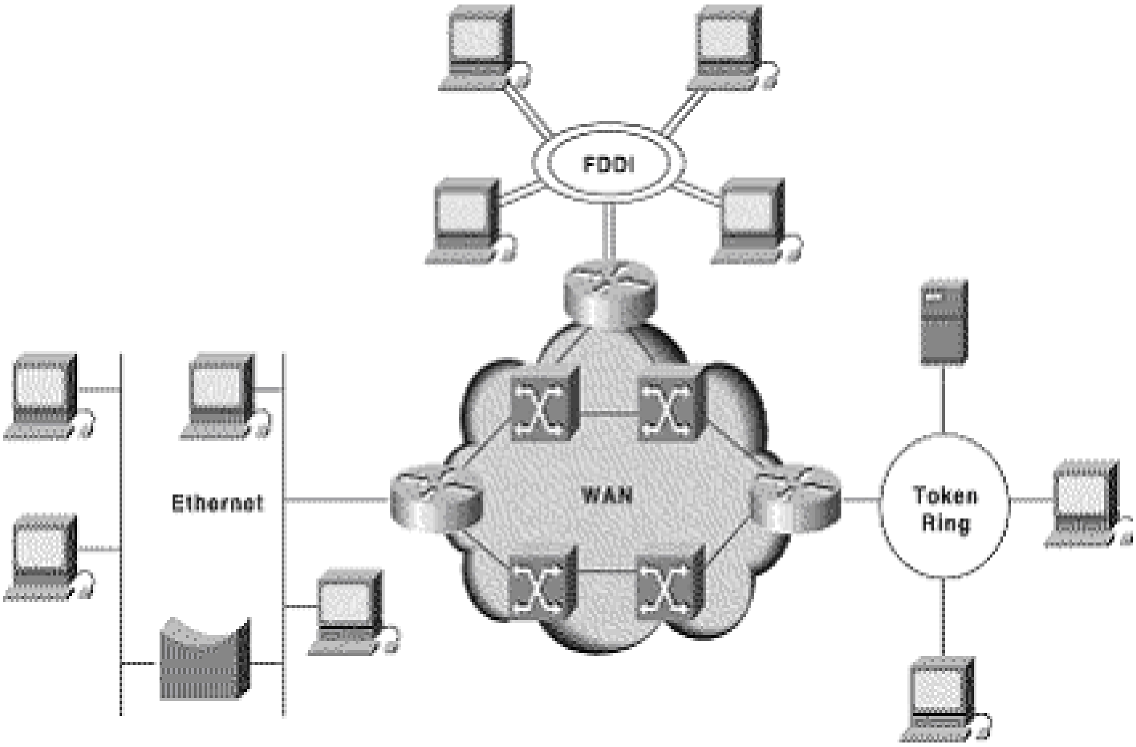
- Static : Routes are based on static tables that are "wired into" the network and are rarely changed.
- Dynamic : All packets of one application can follow different routes depending upon the topology of the network, the shortest path and the current network load.
- Semi-Dynamic : A route is chosen at the start of each conversation and then all the packets of the application follow the same route.

The services provided by the network can be of two types :

- **Connection less service:** Each packet of an application is treated as an independent entity. On each packet of the application the destination address is provided and the packet is routed.
- **Connection oriented service:** Here, first a connection is established and then all packets of the application follow the same route. To understand the above concept, we can also draw an analogy from the real life. Connection oriented service is modeled after the telephone system. All voice packets go on the same path after the connection is established till the connection is hung up. It acts like a tube ; the sender pushes the objects in at one end and the receiver takes them out in the same order at the other end. Connection less service is modeled after the postal system. Each letter carries the destination address and is routed independent of all the others. Here, it is possible that the letter sent first is delayed so that the second letter reaches the destination before the first letter.

Congestion Control: A router can be connected to 4-5 networks. If all the networks send packet at the same time with maximum rate possible then the router may not be able to handle all the packets and may drop some/all packets. In this context the dropping of the packets should be minimized and the source whose packet was dropped should be informed. The control of such congestion is also a function of the network layer. Other issues related with this layer are transmitting time, delays, jittering.

Internetworking: Internetworks are multiple networks that are connected in such a way that they act as one large network, connecting multiple office or department networks. Internetworks are connected by networking hardware such as routers, switches, and bridges. Internetworking is a solution born of three networking problems: isolated LANs, duplication of resources, and the lack of a centralized network management system. With connected LANs, companies no longer have to duplicate programs or resources on each network. This in turn gives way to managing the network from one central location instead of trying to manage each separate LAN. We should be able to transmit any packet from one network to any other network even if they follow different protocols or use different addressing modes.

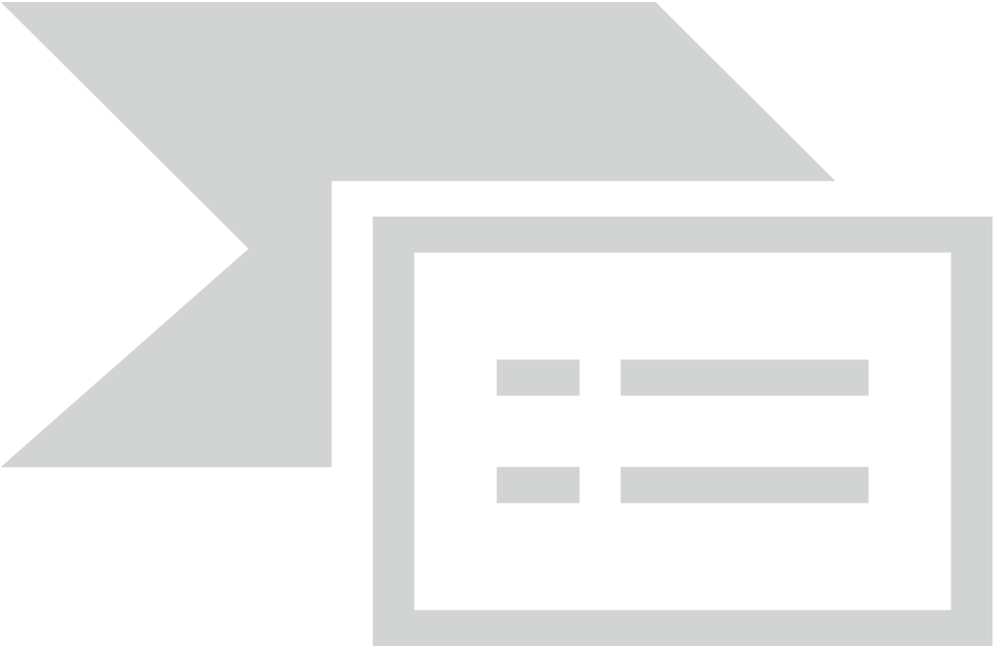


Network Layer does not guarantee that the packet will reach its intended destination. There are no reliability guarantees.

4 Transport Layer

Its functions are :

- **Multiplexing / Demultiplexing** : Normally the transport layer will create distinct network connection for each transport connection required by the session layer. The transport layer may either create multiple network connections (to improve throughput) or it may multiplex several transport connections onto the same network connection (because creating and maintaining networks may be expensive). In the latter case, demultiplexing will be required at the receiving end. A point to note here is that communication is always carried out between two processes and not between two machines. This is also known as process-to-process communication.
- **Fragmentation and Re-assembly :** The data accepted by the transport layer from the session layer is split up into smaller units (fragmentation) if needed and then passed to the network layer. Correspondingly, the data provided by the network layer to the transport layer on the receiving side is re-assembled.



- **Types of service :** The transport layer also decides the type of service that should be provided to the session layer. The service may be perfectly reliable, or may be reliable within certain tolerances or may not be reliable at all. The message may or may not be received in the order in which it was sent. The decision regarding the type of service to be provided is taken at the time when the connection is established.
- **Error Control** : If reliable service is provided then error detection and error recovery operations are also performed. It provides error control mechanism on end to end basis.
- **Flow Control** : A fast host cannot keep pace with a slow one. Hence, this is a mechanism to regulate the flow of information.
- **Connection Establishment** / Release: The transport layer also establishes and releases the connection across the network. This requires some sort of naming mechanism so that a process on one machine can indicate with whom it wants to communicate.

5 Session Layer

It deals with the concept of Sessions i.e. when a user logins to a remote server he should be authenticated before getting access to the files and application programs. Another job of session layer is to establish and maintain sessions. If during the transfer of data between two machines the session breaks down, it is the session layer which re-establishes the connection. It also ensures that the data transfer starts from where it

breaks keeping it transparent to the end user. e.g. In case of a session with a database server, this layer introduces check points at various places so that in case the connectoin is broken and reestablished, the transition running on the database is not lost even if the user has not committed. This activity is called Synchronization. Another function of this layer is Dialogue Control which determines whose turn is it to speak in a session. It is useful in video conferencing.

6 Presentation Layer

This layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different data representations to communicate data structures to be exchanged can be defined in abstract way along with standard encoding. It also manages these abstract data structures and allows higher level of data structures to be defined an exchange. It encodes the data in standard agreed way(network format). Suppose there are two machines A and B one follows 'Big Endian' and other 'Little Endian' for data representation. This layer ensures that the data transmitted by one gets converted in the form compatibale to other machine. This layer is concerned with the syntax and semantics of the information transmitted.In order to make it possible for computers with different data representations to communicate data structures to be exchanged can be defined in abstract way along with standard encoding. It also manages these abstract data structres and allows higher level of data structures to be defined an exchange. Other functions include compression, encryption etc.

7 Application Layer

The seventh layer contains the application protocols with which the user gains access to the network. The choice of which specific protocols and their associated functions are to be used at the application level is up to the individual user. Thus the boundary between the presentation layer and the application layer represents a separation of the protocols imposed by the network designers from those being selected and implemented by the network users. For example commonly used protocols are HTTP(for web browsing), FTP(for file transfer) etc.

Network Layers as in Practice

In most of the networks today, we do not follow the OSI model of seven layers. What is actually implemented is as follows. The functionality of Application layer and Presentation layer is merged into one and is called as the Application Layer. Functionalities of Session Layer is not implemented in most networks today. Also, the Data Link layer is split theoretically into MAC (Medium Access Control) Layer and LLC (Link Layer Control). But again in practice, the LLC layer is not implemented by most networks. So as of today, the network architecture is of 5 layers only.

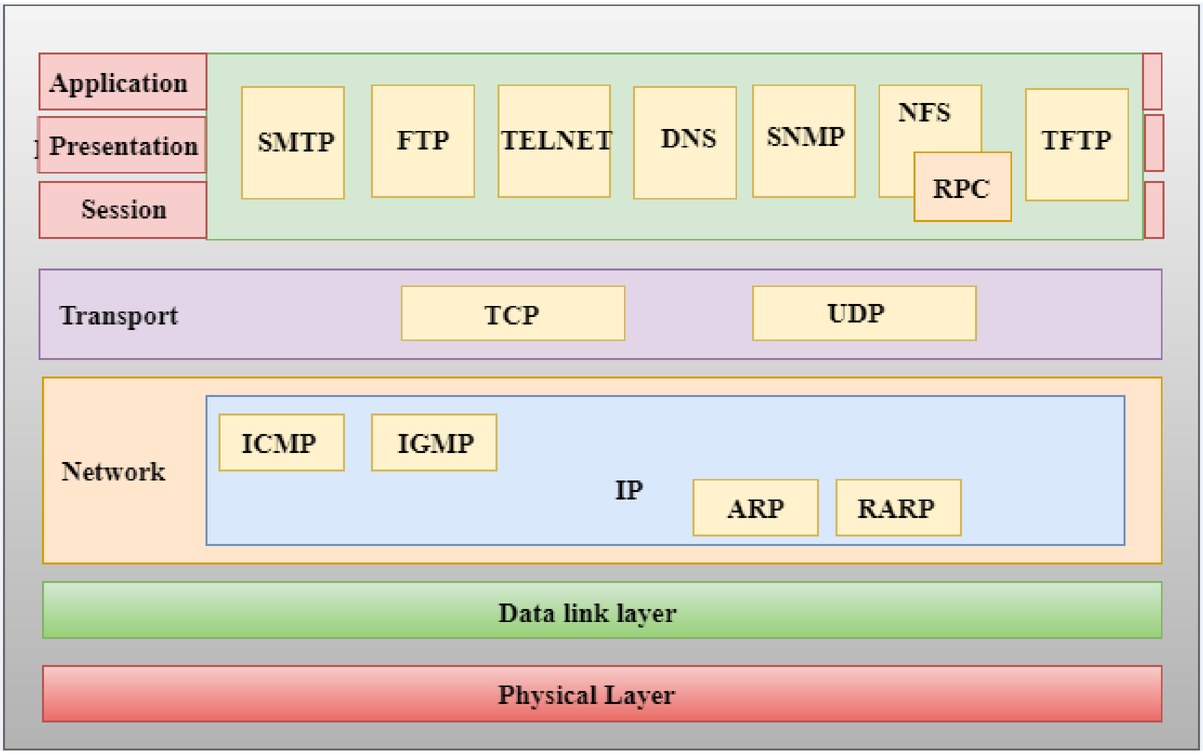
1.7 TCP/IP PROTOCOL SUITE

The TCPIIP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCPIIP taking care of part of the duties of the session layer. So in this book, we assume that the TCPIIP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCPIIP by a single layer called the application layer .

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.

- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.



Network Access 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.
- It defines how the data should be sent physically through the network.

- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.
- Internet Layer
- 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 route they take.

Following are the protocols used in this layer are:

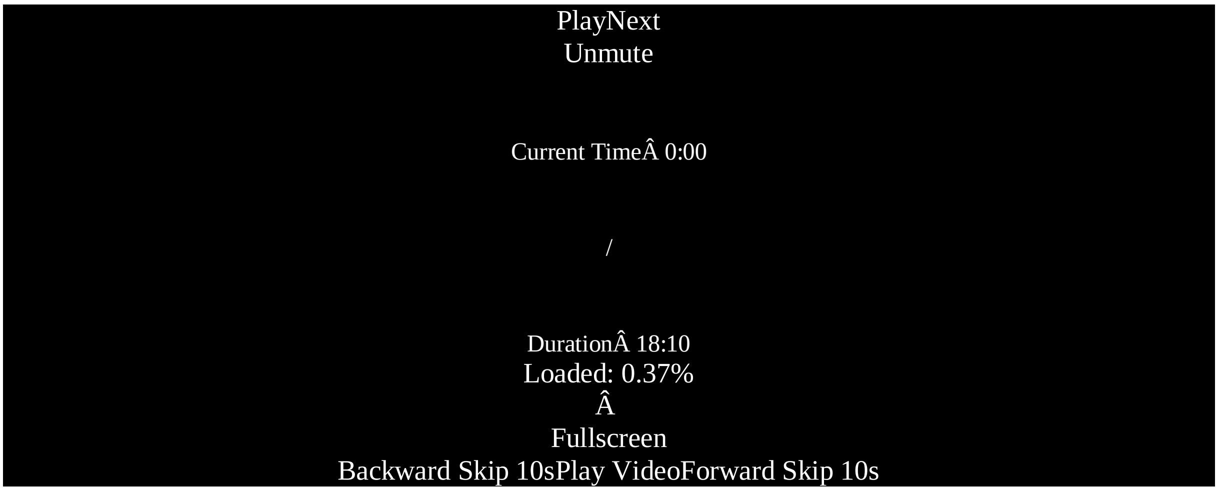
- IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- IP Addressing: This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- Host-to-host communication: It determines the path through which the data is to be transmitted.
- Data Encapsulation and Formatting: An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- Fragmentation and Reassembly: The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- Routing: When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant

network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol


PlayNext
Unmute

Current TimeÂ 0:00

/

DurationÂ 18:10
Loaded: 0.37%
Â
Fullscreen
Backward Skip 10sPlay VideoForward Skip 10s

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- The two terms are mainly associated with the ARP Protocol:
  - ARP request: When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - ARP reply: Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- ICMP stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:

  - 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.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

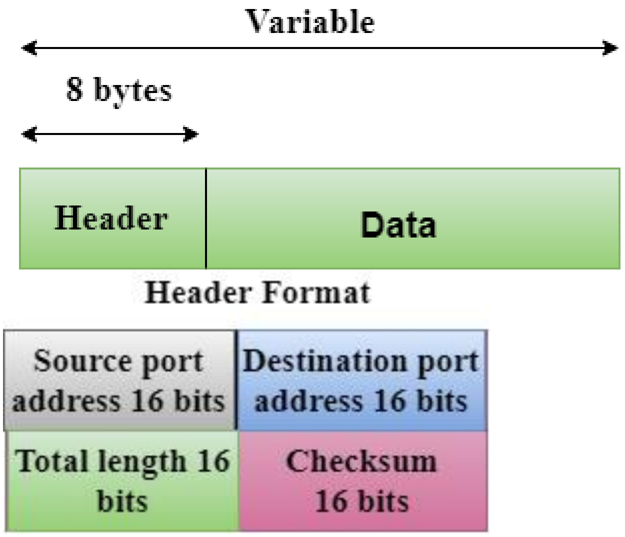
Transport Layer

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- The two protocols used in the transport layer are User Datagram protocol and Transmission control protocol.

- **User Datagram Protocol (UDP)**
  - It provides connectionless service and end-to-end delivery of transmission.
  - It is an unreliable protocol as it discovers the errors but not specify the error.
  - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
  - **UDP consists of the following fields:**

    Source port address: The source port address is the address of the application program that has created the message.
    Destination port address: The destination port address is the address of the application program that receives the message.
    Total length: It defines the total number of bytes of the user datagram in bytes.
    Checksum: The checksum is a 16-bit field used in error detection.

- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



Header Format

Source port address 16 bits	Destination port address 16 bits
Total length 16 bits	Checksum 16 bits

Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.

- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using HTTP protocol to interact with the network where HTTP protocol is an application layer protocol.

Following are the main protocols used in the 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. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP**: SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **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. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Physical Layer

Physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is recieved by the other side as 1 bit and not as 0 bit. In physical layer we deal with the communication medium used for transmission.

1.8 Types of Medium

Medium can be classified into 2 categories.

1. **Guided Media** : Guided media means that signals is guided by the prescence of physical media i.e. signals are under control and remains in the physical wire. For eg. copper wire.
2. **Unguided Media** : Unguided Media means that there is no physical path for the signal to propogate. Unguided media are essentially electro-magnetic waves. There is no control on flow of signal. For eg. radio waves.

Communication Links

In a nework nodes are connected through links. The communication through links can be classified as

1. Simplex : Communication can take place only in one direction. eg. T.V broadcasting.
2. Half-duplex : Communication can take place in one direction at a time. Suppose node A and B are connected then half-duplex communication means that at a time data can flow from A to B or from B to A but not simultaneously. eg. two persons talking to each other such that when speaks the other listens and vice versa.
3. Full-duplex : Communication can take place simultaneously in both directions. eg. A discussion in a group without discipline.

Links can be further classified as

1. Point to Point : In this communication only two nodes are connected to each other. When a node sends a packet then it can be received only by the node on the other side and none else.
2. Multipoint : It is a kind of sharing communication, in which signal can be recieved by all nodes. This is also called broadcast.

Generally two kind of problems are associated in transmission of signals.

1. Attenuation : When a signal transmits in a network then the quality of signal degrades as the signal travels longer distances in the wire. This is called attenuation. To improve quality of signal amplifiers are used at regular distances.
2. Noise : In a communication channel many signals transmits simultaneously, certain random signals are also present in the medium. Due to interference of these signals our signal gets disrupted a bit.

Bandwidth

Bandwidth simply means how many bits can be transmitted per second in the communication channel. In technical terms it indicates the width of frequency spectrum.

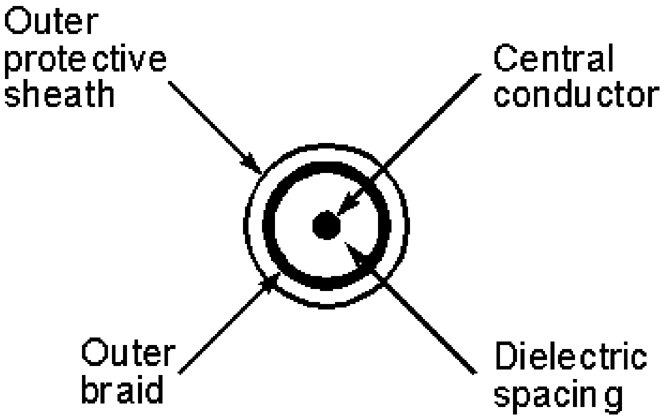
Transmission Media

Guided Transmission Media

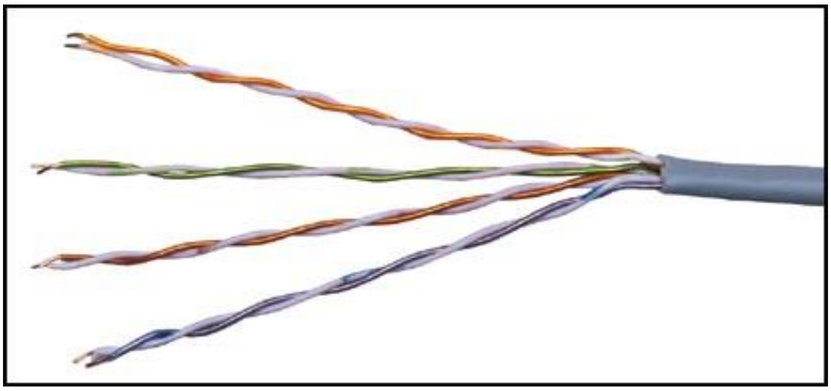
In Guided transmission media generally two kind of materials are used.

1. Copper
   - Coaxial Cable
   - Twisted Pair
2. Optical Fiber

1. Coaxial Cable: Coaxial cable consists of an inner conductor and an outer conductor which are seperated by an insulator. The inner conductor is usually copper. The outer conductor is covered by a plastic jacket. It is named coaxial because the two conductors are coaxial. Typical diameter of coaxial cable lies between 0.4 inch to 1 inch. The most application of coaxial cable is cable T.V. The coaxial cable has high bandwidth, attenuation is less.



1. **Twisted Pair**: A Twisted pair consists of two insulated copper wires, typically 1mm thick. The wires are twisted together in a helical form the purpose of twisting is to reduce cross talk interference between several pairs. Twisted Pair is much cheaper then coaxial cable but it is susceptible to noise and electromagnetic interference and attenuation is large.



Twisted Pair can be further classified in two categories:
Unshielded twisted pair: In this no insulation is provided, hence they are susceptible to interference.
Shielded twisted pair: In this a protective thick insulation is provided but shielded twisted pair is expensive and not commonly used.

The most common application of twisted pair is the telephone system. Nearly all telephones are connected to the telephone company office by a twisted pair. Twisted pair can run several kilometers without amplification, but for longer distances repeaters are needed. Twisted pairs can be used for both analog and digital transmission. The bandwidth depends on the thickness of wire and the distance travelled. Twisted pairs are generally limited in distance, bandwidth and data rate.

2. **Optical Fiber:** In optical fiber light is used to send data. In general terms presence of light is taken as bit 1 and its absence as bit 0. Optical fiber consists of inner core of either glass or plastic. Core is surrounded by cladding of the same material but of different refractive index. This cladding is surrounded by a plastic jacket which prevents optical fiber from electromagnetic interference and harshly environments. It uses the principle of total internal reflection to transfer data over optical fibers. Optical fiber is much better in bandwidth as compared to copper wire, since there is hardly any attenuation or electromagnetic interference in optical wires. Hence there is less requirement to improve quality of signal, in long distance transmission. Disadvantage of optical fiber is that end points are fairly expensive. (eg. switches)

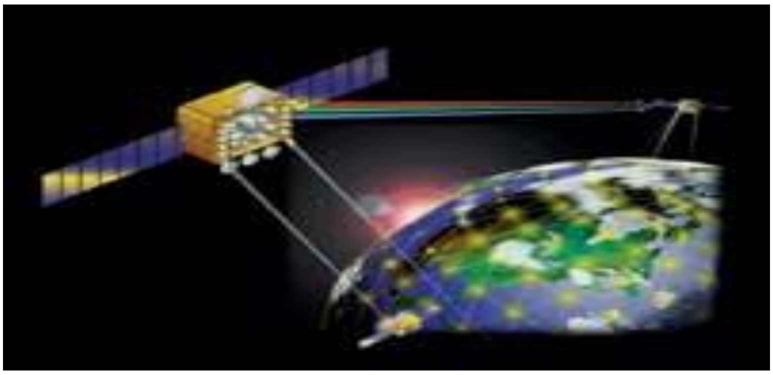
   Differences between different kinds of optical fibers:

   1. Depending on material
      - Made of glass
      - Made of plastic.
   2. Depending on radius
      - Thin optical fiber
      - Thick optical fiber
   3. Depending on light source
      - LED (for low bandwidth)

- Injection lased diode (for high bandwidth)

Wireless Transmission

1. **Radio**: Radio is a general term that is used for any kind of frequency. But higher frequencies are usually termed as microwave and the lower frequency band comes under radio frequency. There are many application of radio. For eg. cordless keyboard, wireless LAN, wireless ethernet. but it is limited in range to only a few hundred meters. Depending on frequency radio offers different bandwidths.
2. **Terrestrial microwave**: In terrestrial microwave two antennas are used for communication. A focused beam emerges from an antenna and is recieved by the other antenna, provided that antennas should be facing each other with no obstacle in between. For this reason antennas are situated on high towers. Due to curvature of earth terristial microwave can be used for long distance communication with high bandwidth. Telecom department is also using this for long distance communication. An advantage of wireless communication is that it is not required to lay down wires in the city hence no permissions are required.
3. **Satellite communication**: Satellite acts as a switch in sky. On earth VSAT(Very Small Aperture Terminal) are used to transmit and recieve data from satellite. Generally one station on earth transmitts signal to satellite and it is recieved by many stations on earth. Satellite communication is generally used in those places where it is very difficult to obtain line of sight i.e. in highly irregular terristial regions. In terms of noise wireless media is not as good as the wired media. There are frequency band in wireless communication and two stations should not be allowed to transmit simultaneously in a frequency band. The most promising advantage of satellite is broadcasting. If satellites are used for point to point communication then they are expensive as compared to wired media.



Digital Data Communication Techniques:

For two devices linked by a transmission medium to exchange data ,a high degree of co-operation is required. Typically data is transmitted one bit at a time. The timing (rate, duration, spacing) of these bits must be same for transmitter and receiver. There are two options for transmission of bits.

1. **Parallel** All bits of a byte are transferred simultaneously on separate parallel wires. Synchronization between multiple bits is required which becomes difficult over large distance. Gives large band width but expensive. Practical only for devices close to each other.
2. **Serial** Bits transferred serially one after other. Gives less bandwidth but cheaper. Suitable for transmission over long distances.

Transmission Techniques:

1. Asynchronous: Small blocks of bits (generally bytes) are sent at a time without any time relation between consecutive bytes .when no transmission occurs a default state is maintained corresponding to bit 1. Due to arbitrary delay between consecutive bytes, the time occurrences of the clock pulses at the receiving end need to be synchronized for each byte. This is achieved by providing 2 extra bits start and stop.

   Start bit: It is prefixed to each byte and equals 0. Thus it ensures a transition from 1 to 0 at onset of transmission of byte.The leading edge of start bit is used as a reference for generating clock pulses at required sampling instants. Thus each onset of a byte results in resynchronization of receiver clock.

   Stop bit: To ensure that transition from 1 to 0 is always present at beginning of a byte it is necessary that default state be 1. But there may be two bytes one immediately following the other and if last bit of first byte is 0, transition from 1 to 0 will not occur. Therefore a stop bit is suffixed to each byte equaling 1. It's duration is usually 1,1.5,2 bits.

   Asynchronous transmission is simple and cheap but requires an overhead of 3 bits i.e. for 7 bit code 2 (start, stop bits)+1 parity bit implying 30% overhead. However % can be reduced by sending larger blocks of data but then timing errors between receiver and sender can not be tolerated beyond [50/no. of bits in block] % (assuming sampling is done at middle of bit interval). It will not only result in incorrect sampling but also misaligned bit count i.e. a data bit can be mistaken for stop bit if receiver's clock is faster.

2. **Synchronous** - Larger blocks of bits are successfully transmitted.Blocks of data are either treated as sequence of bits or bytes. To prevent timing drift clocks at two ends need to be synchronized.This can done in two ways:
   1. Provide a separate clock line between receiver and transmitter. OR
   2. Clocking information is embedded in data signal i.e. biphase coding for digital signals.

Still another level of synchronization is required so that receiver determines beginning or end of block of data. Hence each block begins with a start code and ends with a stop code. These are in general same known as flag that is unique sequence of fixed no. of bits. In addition some control characters encompass data within these flags. Data +control information is called a frame. Since any arbitrary bit pattern can be transmitted there is no assurance that bit pattern for flag will not appear inside the frame thus destroying frame level synchronization. So to avoid this we use bit stuffing

Bit Stuffing: Suppose our flag bits are 01111110 (six 1's). So the transmitter will always insert an extra 0 bit after each occurrence of five 1's (except for flags). After detecting a starting flag the receiver monitors the bit stream . If pattern of five 1's appear, the sixth is examined and if it is 0 it is deleted else if it is 1 and next is 0 the combination is accepted as a flag. Similarly byte stuffing is used for byte oriented transmission. Here we use an escape sequence to prefix a byte similar to flag and 2 escape sequences if byte is itself a escape sequence.

1.9 Multiplexing

When two communicating nodes are connected through a media, it generally happens that bandwidth of media is several times greater than that of the communicating nodes. Transfer of a single signal at a time is both slow and expensive. The whole capacity of the link is not being utilized in this case. This link can be further exploited by sending several signals combined into one. This combining of signals into one is called multiplexing.

Frequency Division Multiplexing (FDM): This is possible in the case where transmission media has a bandwidth than the required bandwidth of signals to be transmitted. A number of signals can be transmitted at the same time. Each source is allotted a frequency range in which it can transfer it's signals, and a suitable frequency gap is given between two adjescent signals to avoid overlapping

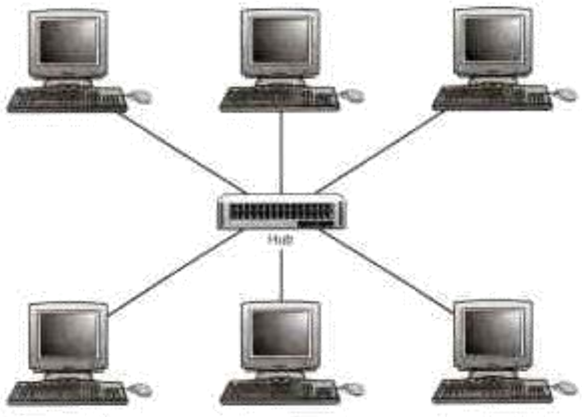
Time Division Multiplexing (TDM): This is possible when data transmission rate of the media is much higher than that of the data rate of the source. Multiple signals can be transmitted if each signal is allowed to be transmitted for a definite amount of time. These time slots are so small that all transmissions appear to be in parallel.

1. **Synchronous TDM**: Time slots are preassigned and are fixed. Each source is given it's time slot at every turn due to it. This turn may be once per cycle, or several turns per cycle ,if it has a high data transfer rate, or may be once in a no. of cycles if it is slow. This slot is given even if the source is not ready with data. So this slot is transmitted empty.
2. **Asynchronous TDM:** In this method, slots are not fixed. They are allotted dynamically depending on speed of sources, and whether they are ready for transmission.

1.10 Network Topologies

A network topology is the basic design of a computer network. It is very much like a map of a road. It details how key network components such as nodes and links are interconnected. A network's topology is comparable to the blueprints of a new home in which components such as the electrical system, heating and air conditioning system, and plumbing are integrated into the overall design. Taken from the Greek work "Topos" meaning "Place," Topology, in relation to networking, describes the configuration of the network; including the location of the workstations and wiring connections. Basically it provides a definition of the components of a Local Area Network (LAN). A topology, which is a pattern of interconnections among nodes, influences a network's cost and performance. There are three primary types of network topologies which refer to the physical and logical layout of the Network cabling. They are:

1. **Star Topology**: All devices connected with a Star setup communicate through a central Hub by cable segments. Signals are transmitted and received through the Hub. It is the simplest and the oldest and all the telephone switches are based on this. In a star topology, each network device has a home run of cabling back to a network hub, giving each device a separate connection to the network. So, there can be multiple connections in parallel.



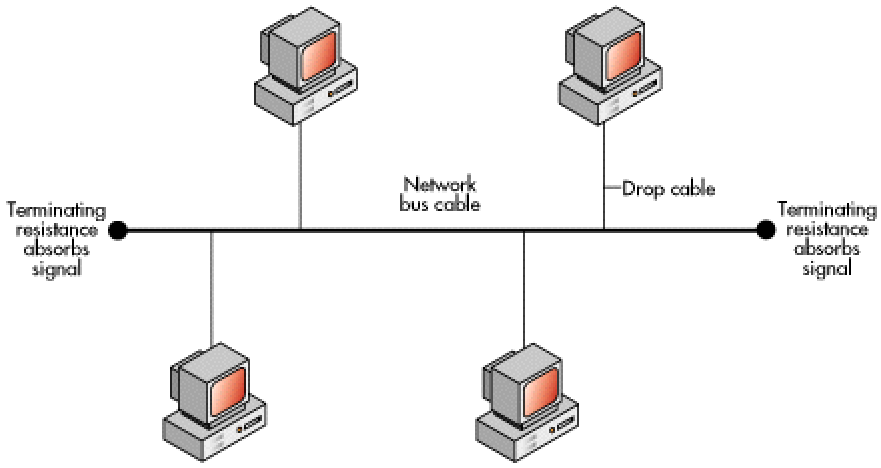
Advantages

- Network administration and error detection is easier because problem is isolated to central node
- Networks runs even if one host fails
- Expansion becomes easier and scalability of the network increases
- More suited for larger networks

Disadvantages

- Broadcasting and multicasting is not easy because some extra functionality needs to be provided to the central hub
- If the central node fails, the whole network goes down; thus making the switch some kind of a bottleneck
- Installation costs are high because each node needs to be connected to the central switch

2. **Bus Topology**: The simplest and one of the most common of all topologies, Bus consists of a single cable, called a Backbone, that connects all workstations on the network using a single line. All transmissions must pass through each of the connected devices to complete the desired request. Each workstation has its own individual signal that identifies it and allows for the requested data to be returned to the correct originator. In the Bus Network, messages are sent in both directions from a single point and are read by the node (computer or peripheral on the network) identified by the code with the message. Most Local Area Networks (LANs) are Bus Networks because the network will continue to function even if one computer is down. This topology works equally well for either peer to peer or client server.



The purpose of the terminators at either end of the network is to stop the signal being reflected back.

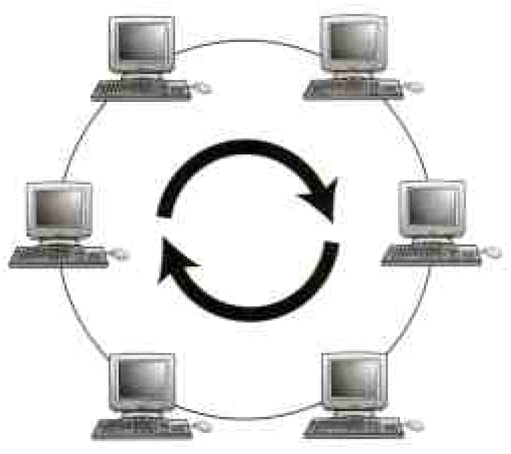
Advantages

- Broadcasting and multicasting is much simpler
- Network is redundant in the sense that failure of one node doesn't effect the network. The other part may still function properly
- Least expensive since less amount of cabling is required and no network switches are required
- Good for smaller networks not requiring higher speeds

Disadvantages

- Trouble shooting and error detection becomes a problem because, logically, all nodes are equal
- Less secure because sniffing is easier
- Limited in size and speed

3. **Ring Topology:** All the nodes in a Ring Network are connected in a closed circle of cable. Messages that are transmitted travel around the ring until they reach the computer that they are addressed to, the signal being refreshed by each node. In a ring topology, the network signal is passed through each network card of each device and passed on to the next device. Each device processes and retransmits the signal, so it is capable of supporting many devices in a somewhat slow but very orderly fashion. There is a very nice feature that everybody gets a chance to send a packet and it is guaranteed that every node gets to send a packet in a finite amount of time.



Advantages

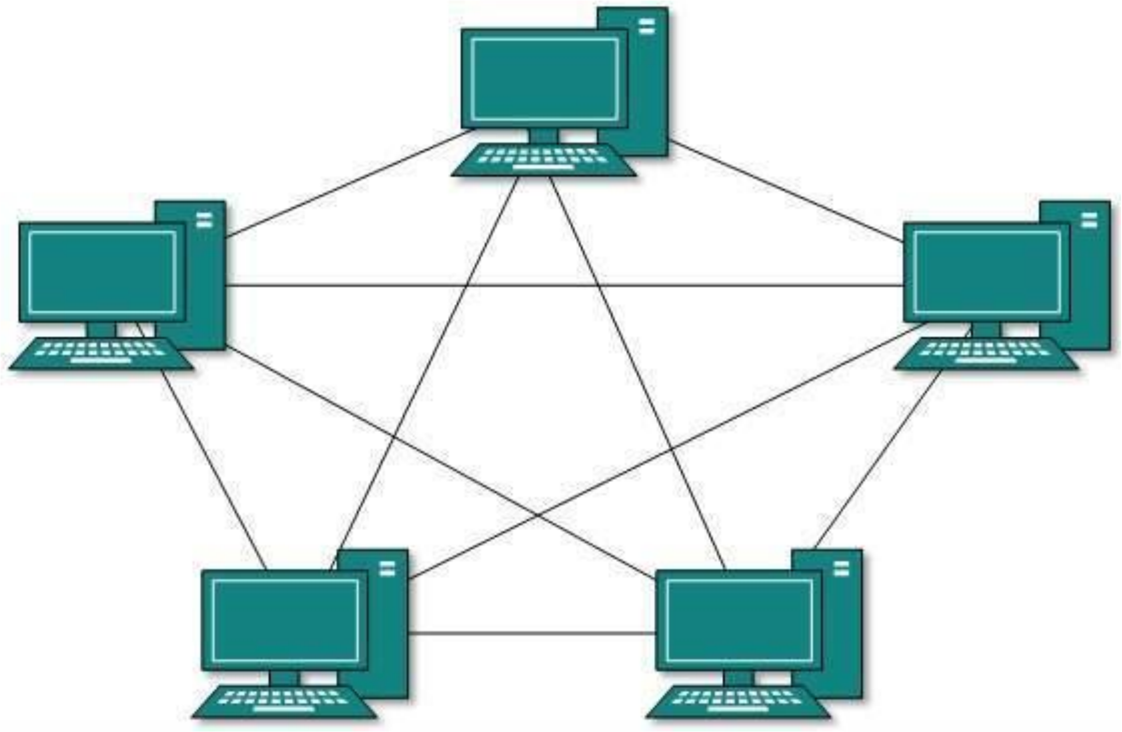
- Broadcasting and multicasting is simple since you just need to send out one message
- Less expensive since less cable footage is required
- It is guaranteed that each host will be able to transmit within a finite time interval
- Very orderly network where every device has access to the token and the opportunity to transmit
- Performs better than a star network under heavy network load

Disadvantages

- Failure of one node brings the whole network down
- Error detection and network administration becomes difficult
- Moves, adds and changes of devices can effect the network
- It is slower than star topology under normal load

4 Mesh Topology

In this type of topology, a host is connected to one or multiple hosts.This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.



Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

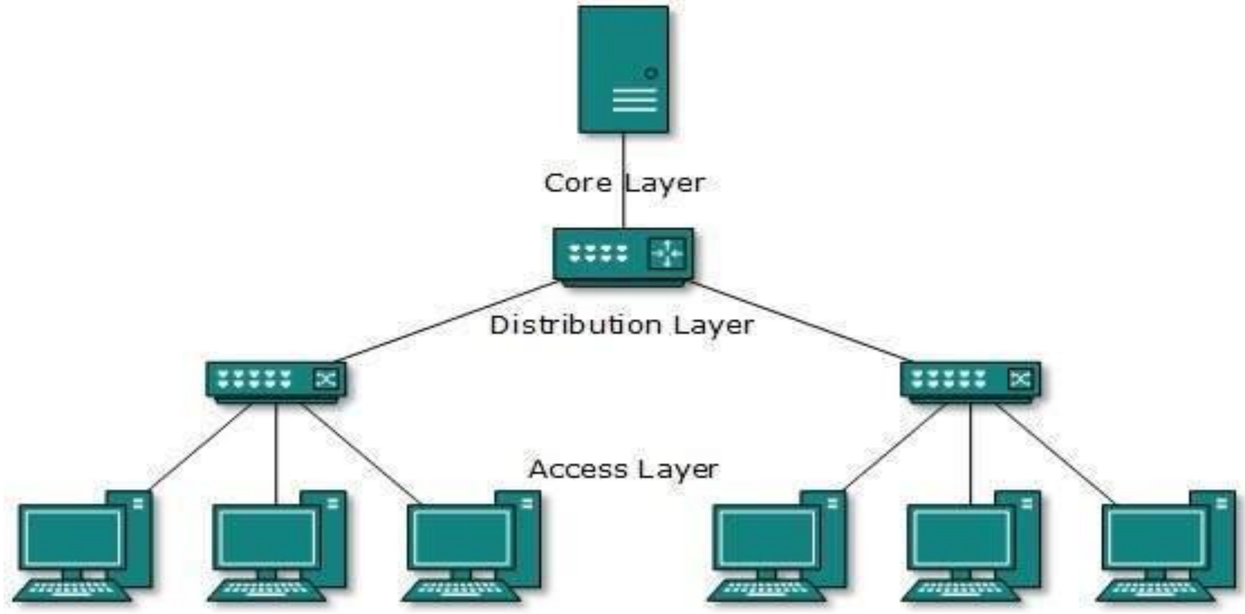
Full Mesh: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.

Partially Mesh: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

5 Tree Topology

Also known as Hierarchical Topology, this is the most common form of network topology in use presently.This topology imitates as extended Star topology and inherits properties of bus topology.

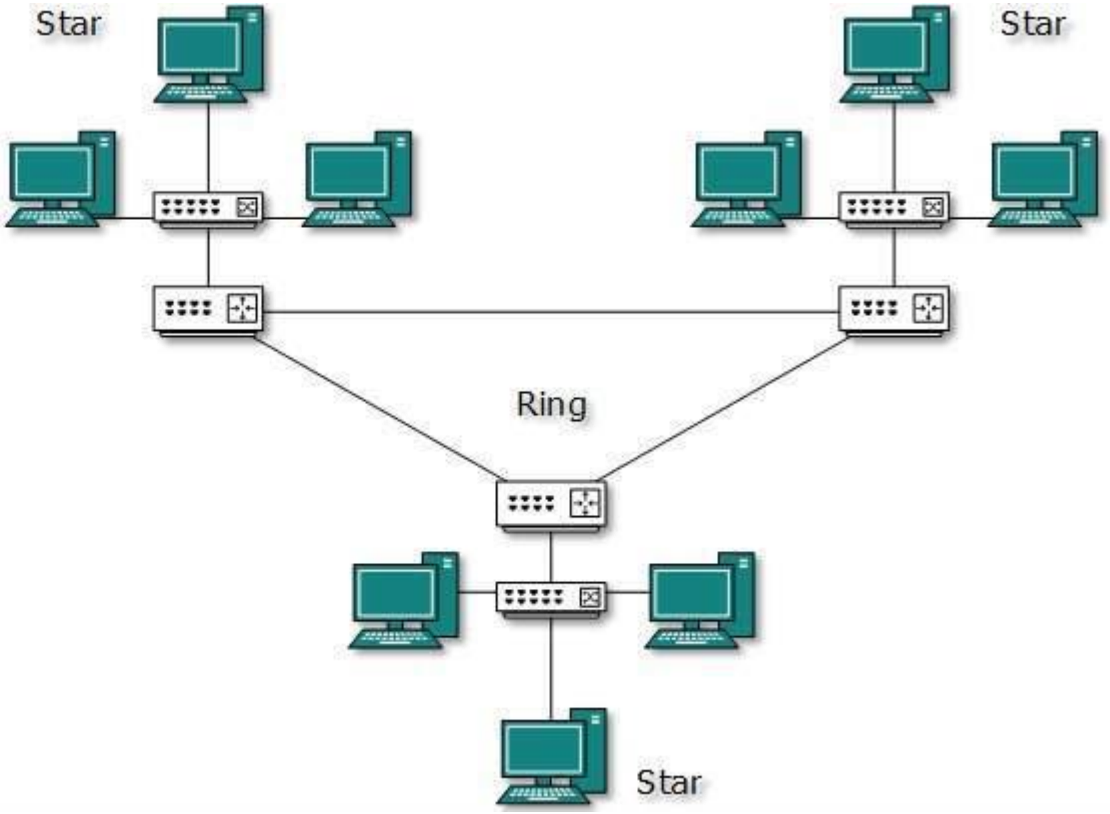
This topology divides the network in to multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.



All neighbouring hosts have point-to-point connection between them.Similar to the Bus topology, if the root goes down, then the entire network suffers even. Though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment.

6 Hybrid Topology

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.



3 The above picture represents an arbitrarily hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology

1.11 Signal Transmission

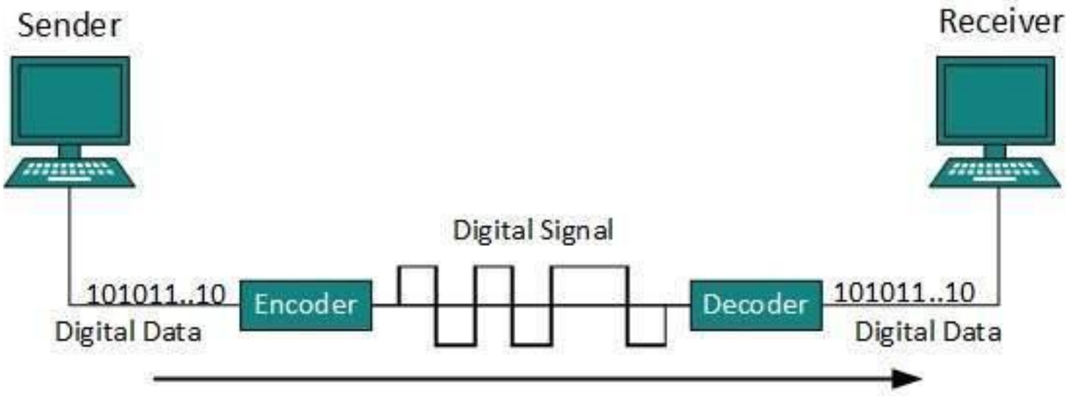
Data or information can be stored in two ways, analog and digital. For a computer to use the data, it must be in discrete digital form.Similar to data, signals can also be in analog and digital form. To transmit data digitally, it needs to be first converted to digital form.

Digital-to-Digital Conversion

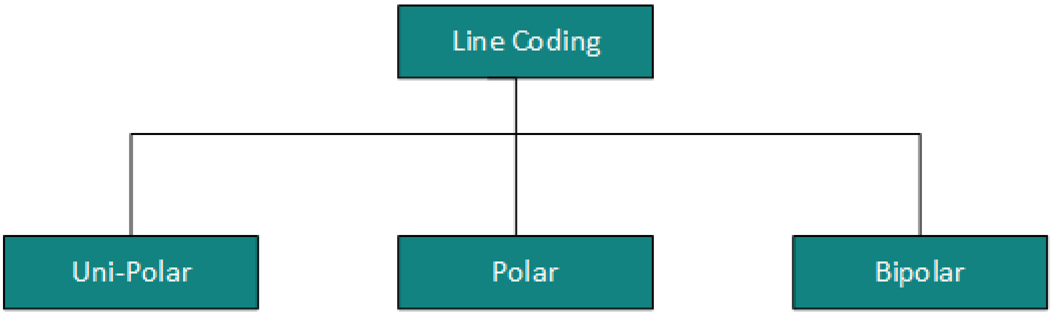
This section explains how to convert digital data into digital signals. It can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

2 Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format.It is represented (stored) internally as series of 1s and 0s.

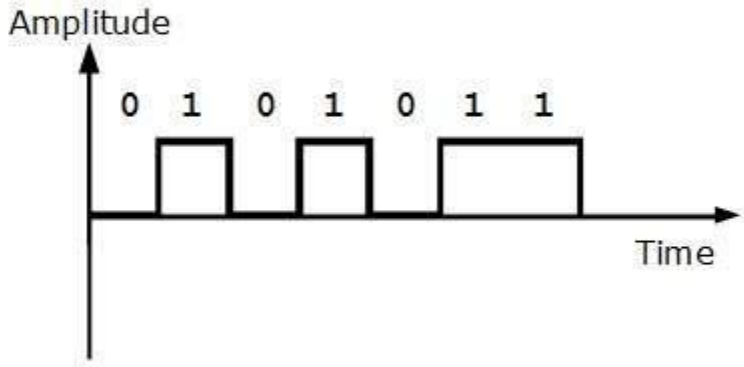


Digital signal is denoted by discreet signal, which represents digital data.There are three types of line coding schemes available:



Uni-polar Encoding

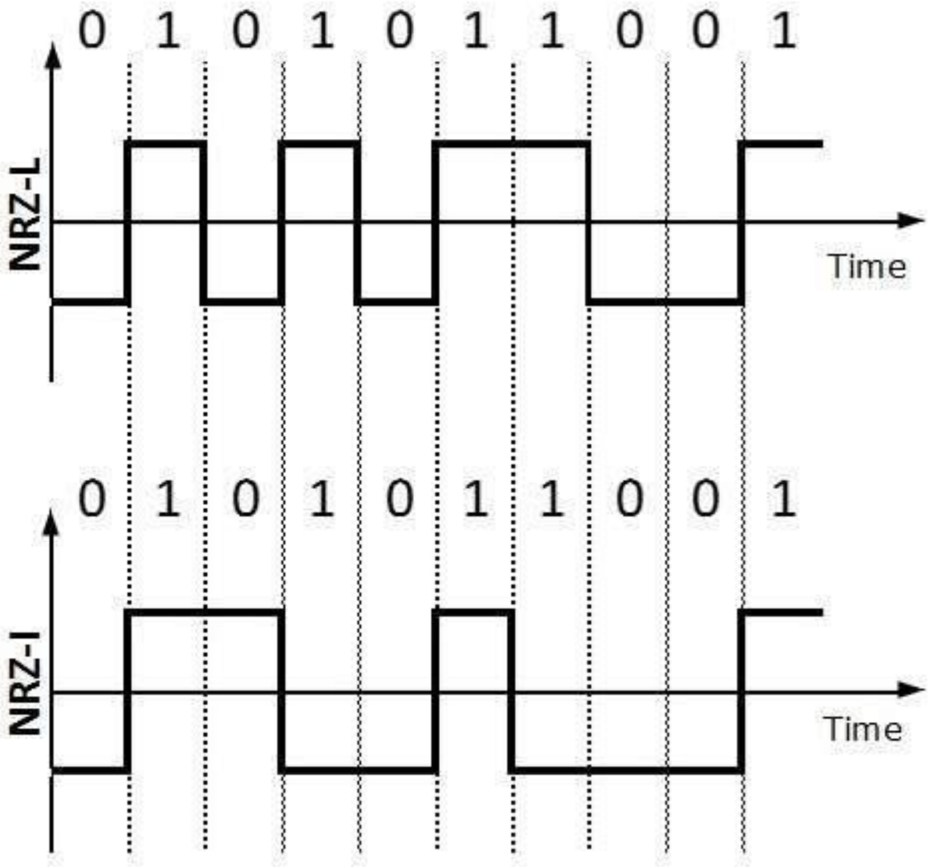
Unipolar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.



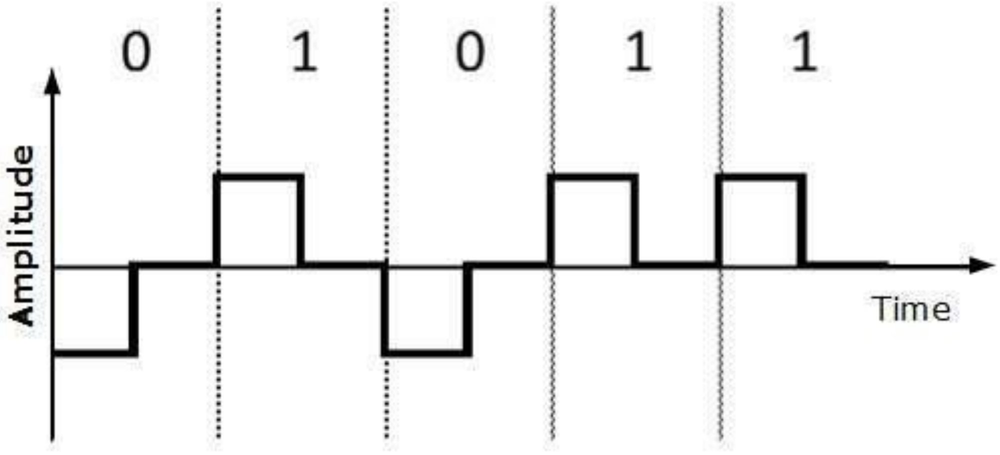
Polar Encoding

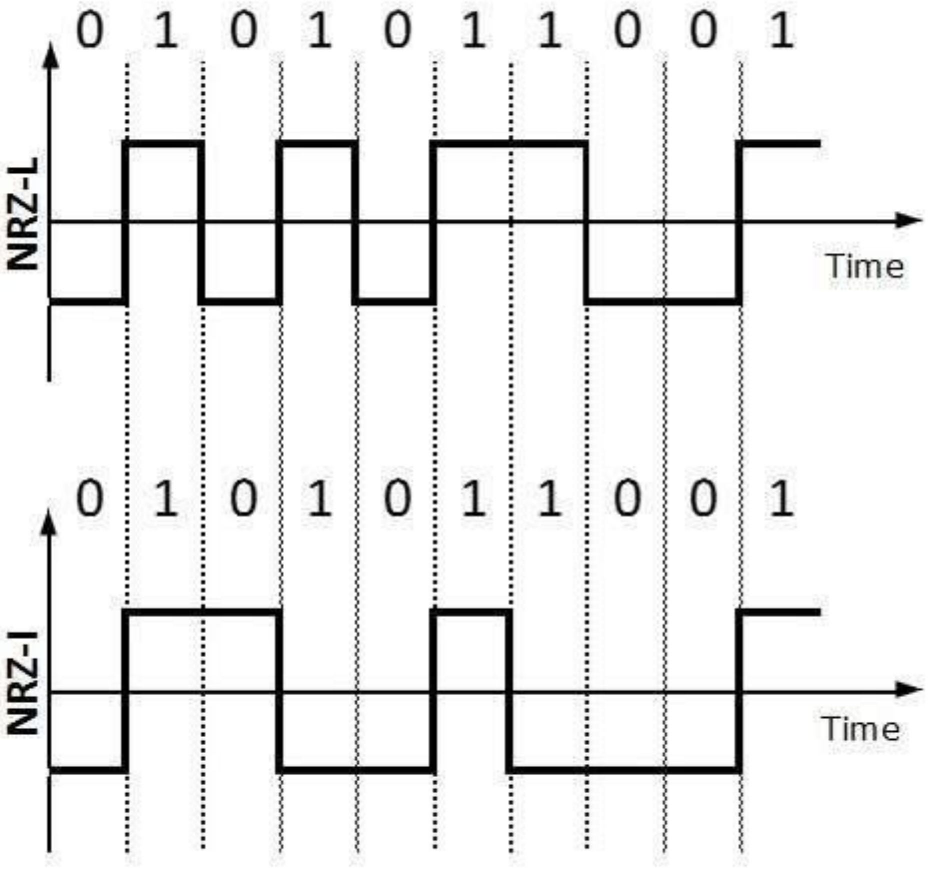
Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types:

- Polar Non-Return to Zero (Polar NRZ)
  It uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition.
  NRZ scheme has two variants: NRZ-L and NRZ-I.



- NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.
- Return to Zero (RZ)
  Problem with NRZ is that the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver's clock are not synchronized.

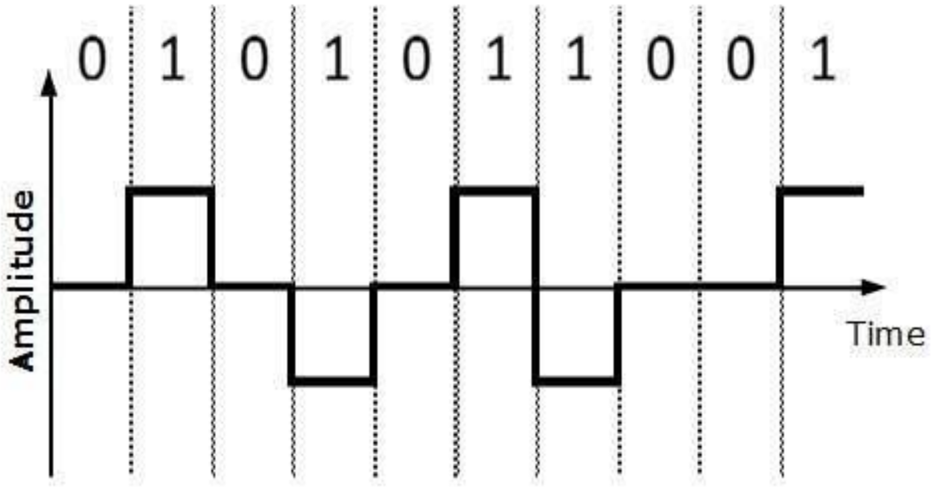




- RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.
- Manchester
  This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.
- Differential Manchester
  This encoding scheme is a combination of RZ and NRZ-I. It also transit at the middle of the bit but changes phase only when 1 is encountered.

Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.



Block Coding

To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding.

Block coding is represented by slash notation, mB/nB.Means, m-bit block is substituted with n-bit block where n > m. Block coding involves three steps:

Division,

Substitution

Combination.

After block coding is done, it is line coded for transmission.

Analog-to-Digital Conversion

Microphones create analog voice and camera creates analog videos, which are treated is analog data. To transmit this analog data over digital signals, we need analog to digital conversion.

Analog data is a continuous stream of data in the wave form whereas digital data is discrete. To convert analog wave into digital data, we use Pulse Code Modulation (PCM).

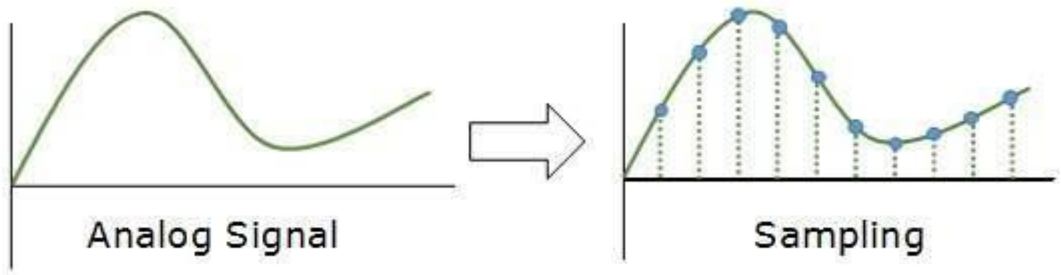
PCM is one of the most commonly used method to convert analog data into digital form. It involves three steps:

Sampling

Quantization

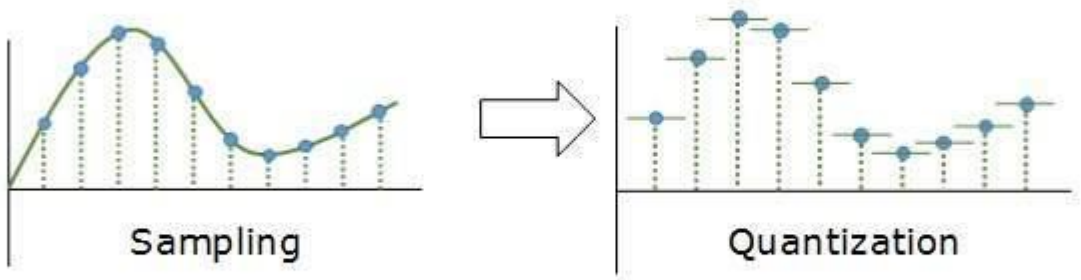
Encoding.

Sampling



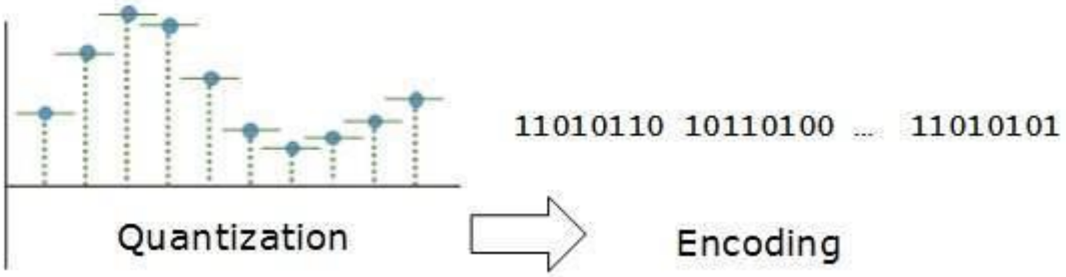
The analog signal is sampled every T interval. Most important factor in sampling is the rate at which analog signal is sampled. According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal.

Quantization



Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.

Encoding

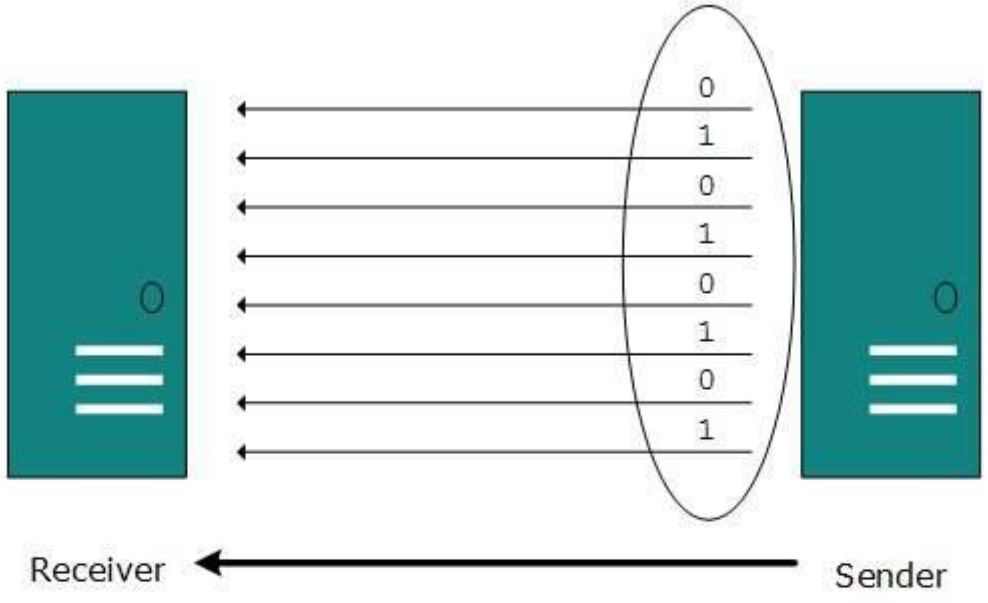


In encoding, each approximated value is then converted into binary format.

Transmission Modes

The transmission mode decides how data is transmitted between two computers.The binary data in the form of 1s and 0s can be sent in two different modes: Parallel and Serial.

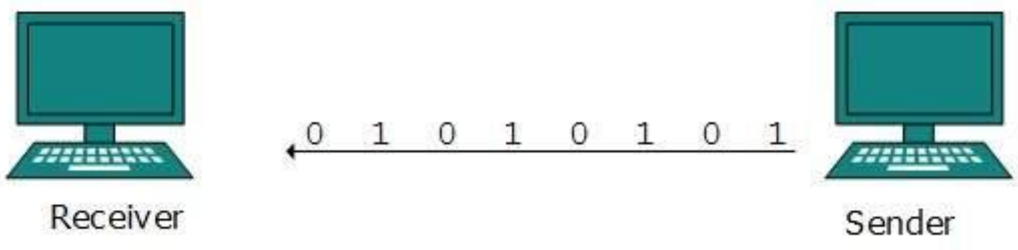
Parallel Transmission



The binary bits are organized in-to groups of fixed length. Both sender and receiver are connected in parallel with the equal number of data lines. Both computers distinguish between high order and low order data lines. The sender sends all the bits at once on all lines.Because the data lines are equal to the number of bits in a group or data frame, a complete group of bits (data frame) is sent in one go. Advantage of Parallel transmission is high speed and disadvantage is the cost of wires, as it is equal to the number of bits sent in parallel.

Serial Transmission

In serial transmission, bits are sent one after another in a queue manner. Serial transmission requires only one communication channel.



Serial transmission can be either asynchronous or synchronous.

Asynchronous Serial Transmission

It is named so because there'is no importance of timing. Data-bits have specific pattern and they help receiver recognize the start and end data bits.For example, a 0 is prefixed on every data byte and one or more 1s are added at the end.

Two continuous data-frames (bytes) may have a gap between them.

Synchronous Serial Transmission

Timing in synchronous transmission has importance as there is no mechanism followed to recognize start and end data bits.There is no pattern or prefix/suffix method. Data bits are sent in burst mode without maintaining gap between bytes (8-bits). Single burst of data bits may contain a number of bytes. Therefore, timing becomes very important.

It is up to the receiver to recognize and separate bits into bytes.The advantage of synchronous transmission is high speed, and it has no overhead of extra header and footer bits as in asynchronous transmission.

To send the digital data over an analog media, it needs to be converted into analog signal.There can be two cases according to data formatting.

Bandpass:The filters are used to filter and pass frequencies of interest. A bandpass is a band of frequencies which can pass the filter.

Low-pass: Low-pass is a filter that passes low frequencies signals.

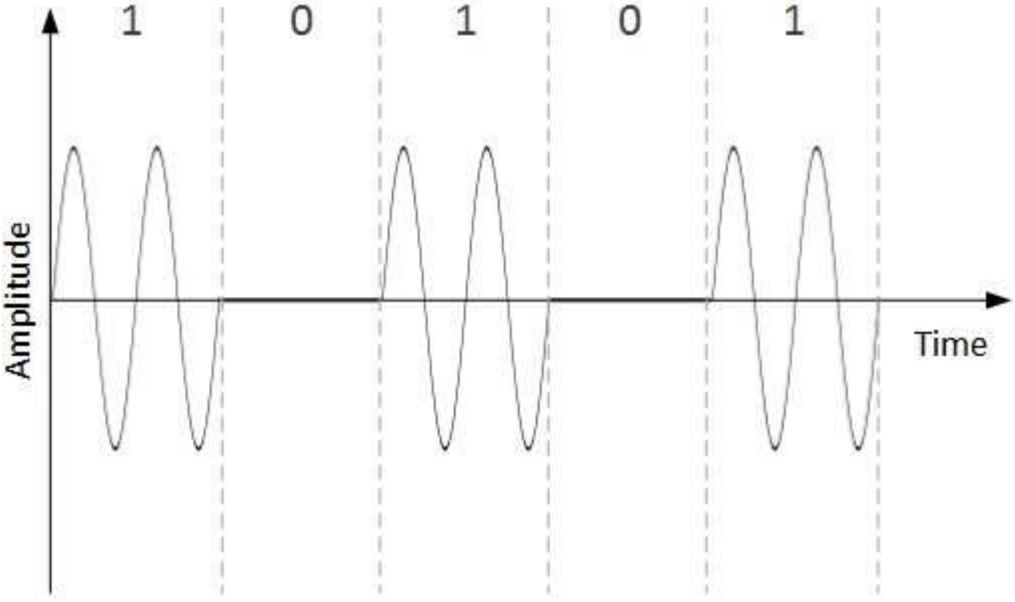
When digital data is converted into a bandpass analog signal, it is called digital-to-analog conversion. When low-pass analog signal is converted into bandpass analog signal, it is called analog-to-analog conversion.

Digital-to-Analog Conversion

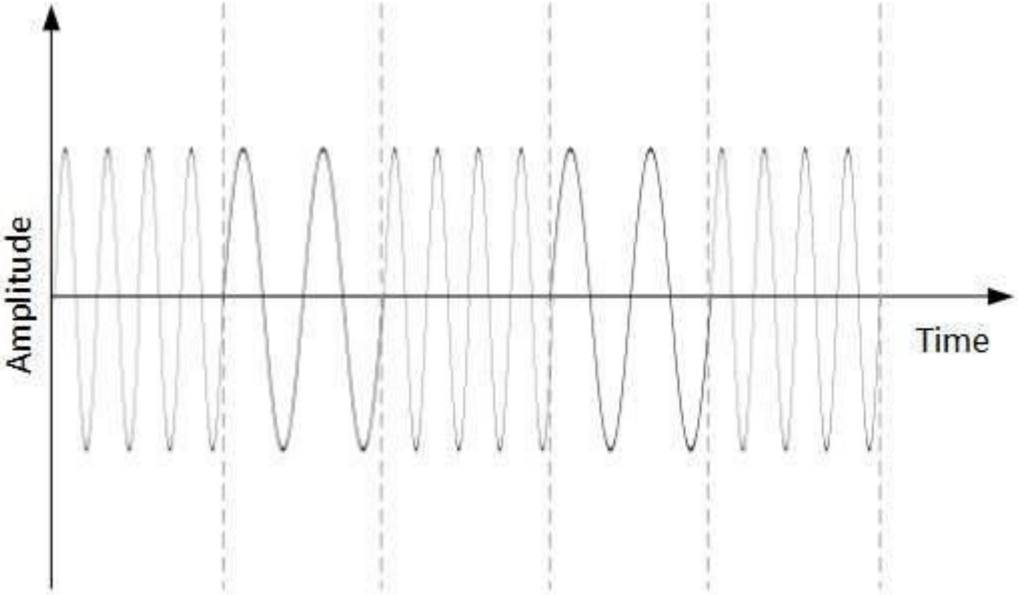
When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data.

An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

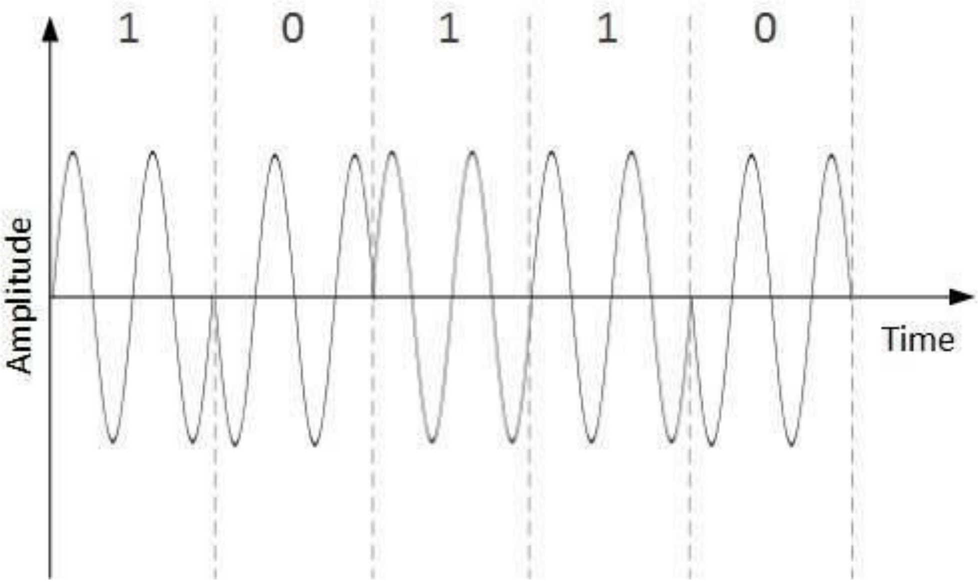
- Amplitude Shift Keying
  In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.



- When binary data represents digit 1, the amplitude is held; otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.
- Frequency Shift Keying
  In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.



- This technique uses two frequencies, f1 and f2. One of them, for example f1, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.
- Phase Shift Keying
  In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.



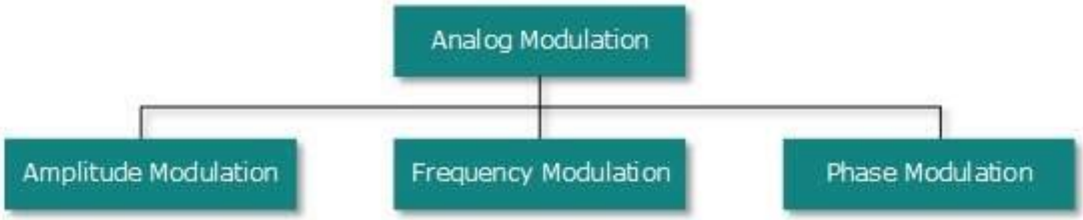
- When a new binary symbol is encountered, the phase of the signal is altered. Amplitude and frequency of the original carrier signal is kept intact.

Quadrature Phase Shift Keying

- QPSK alters the phase to reflect two binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two sub-streams. The serial data is converted in to parallel in both sub-streams and then each stream is converted to digital signal using NRZ technique. Later, both the digital signals are merged together.

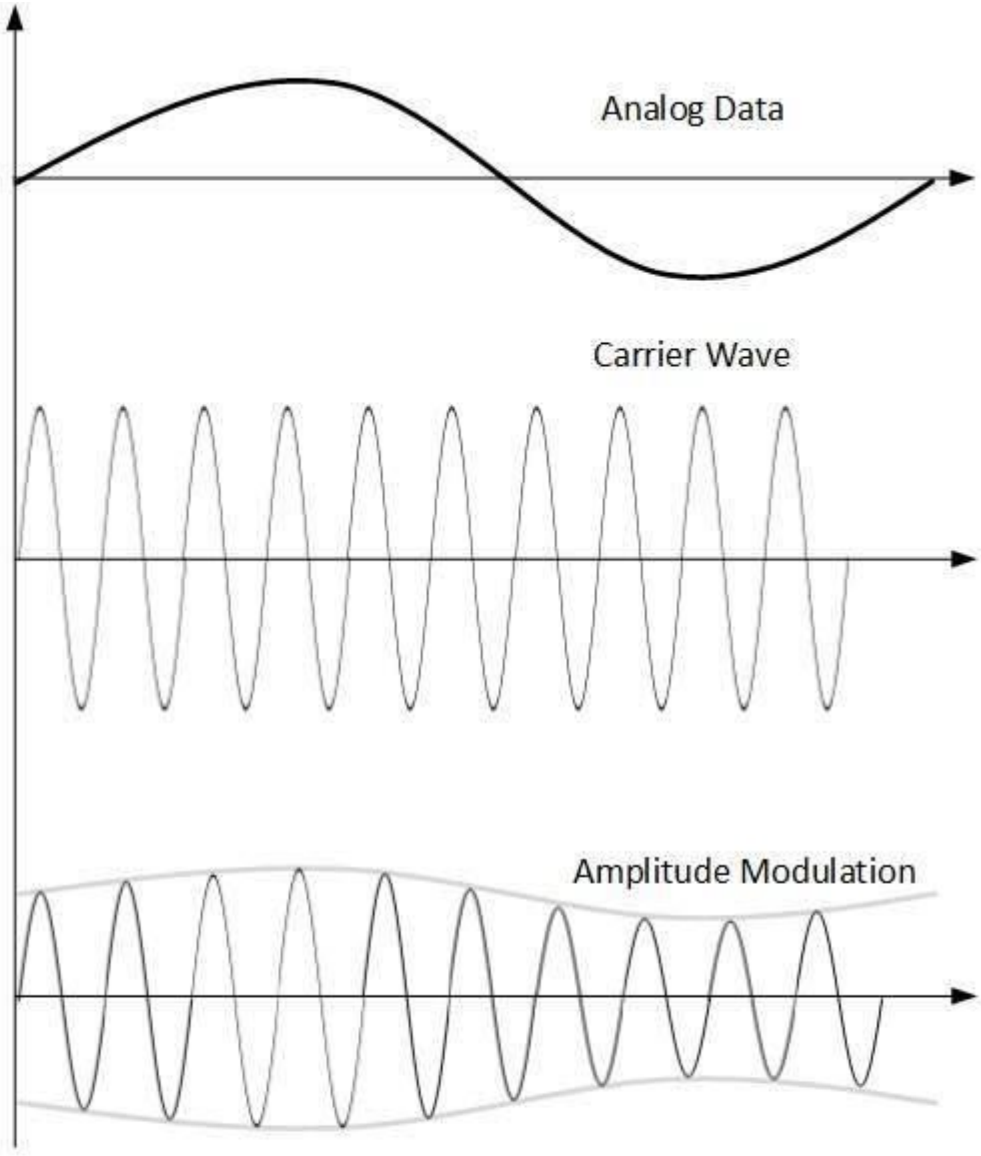
Analog-to-Analog Conversion

- Analog signals are modified to represent analog data. This conversion is also known as Analog Modulation. Analog modulation is required when bandpass is used. Analog to analog conversion can be done in three ways:



Amplitude Modulation

In this modulation, the amplitude of the carrier signal is modified to reflect the analog data

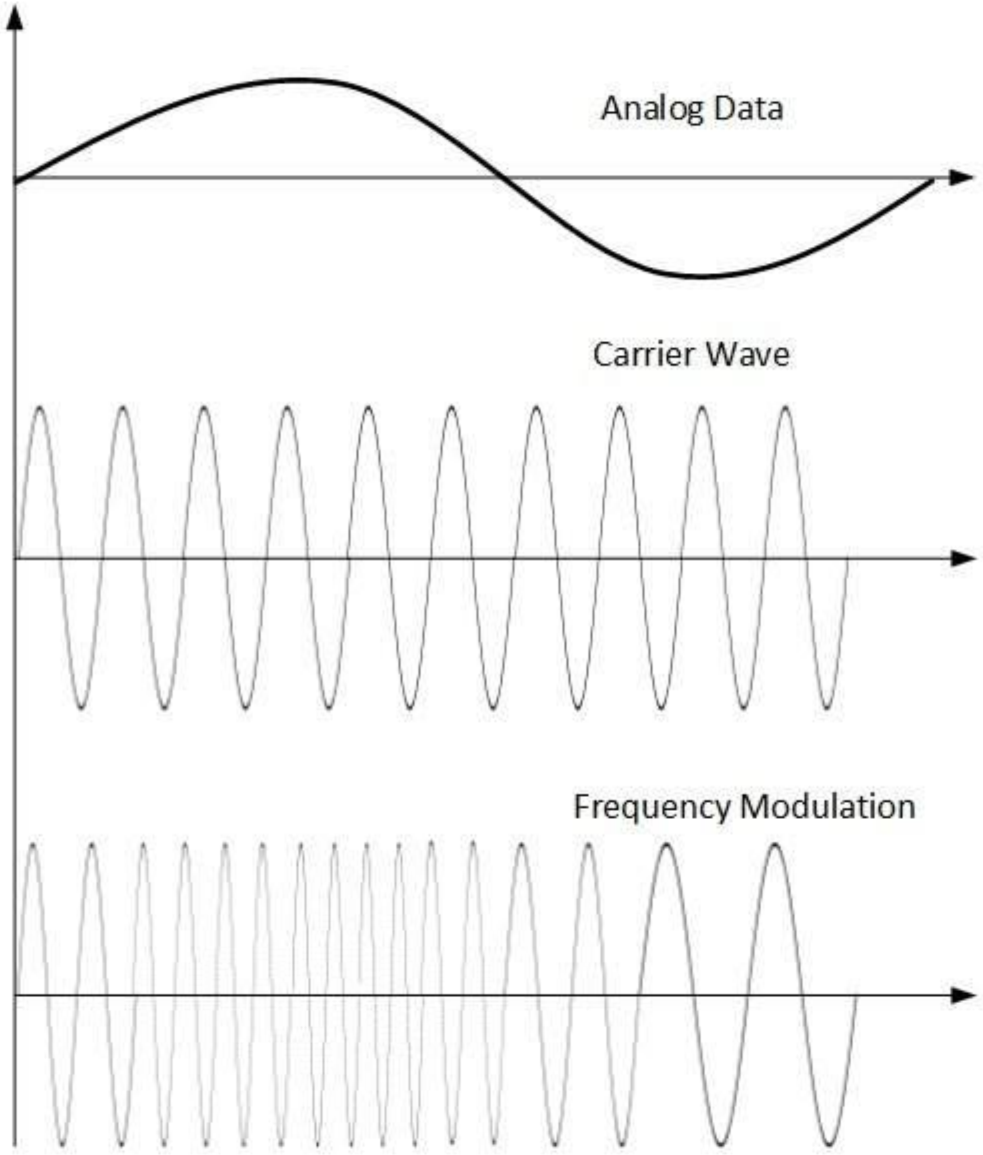


Amplitude modulation is implemented by means of a multiplier. The amplitude of modulating signal (analog data) is multiplied by the amplitude of carrier frequency, which then reflects analog data.

The frequency and phase of carrier signal remain unchanged.

- **Frequency Modulation**

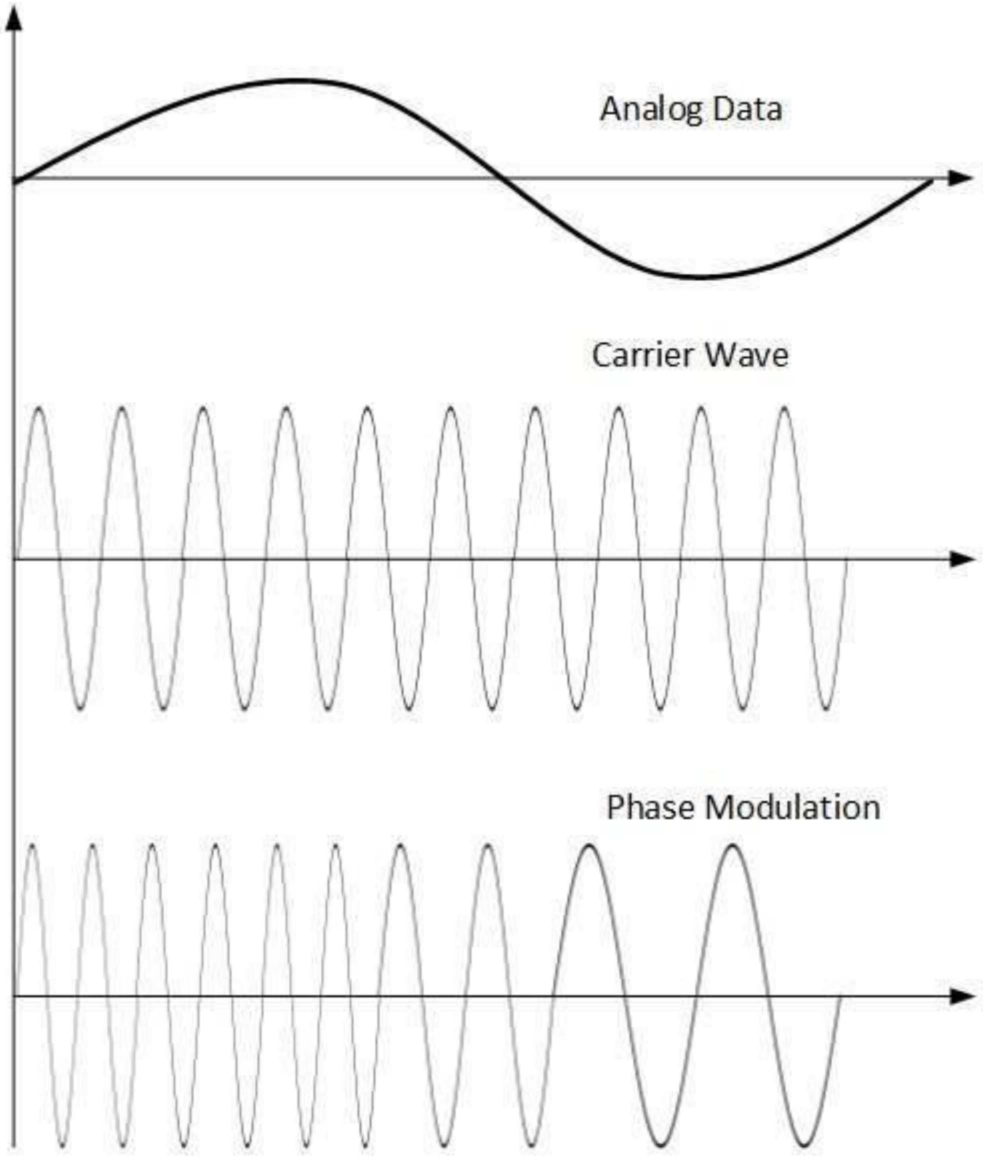
  In this modulation technique, the frequency of the carrier signal is modified to reflect the change in the voltage levels of the modulating signal (analog data).



The amplitude and phase of the carrier signal are not altered.

Phase Modulation

In the modulation technique, the phase of carrier signal is modulated in order to reflect the change in voltage (amplitude) of analog data signal.



Phase modulation is practically similar to Frequency Modulation, but in Phase modulation frequency of the carrier signal is not increased. Frequency of carrier is signal is changed (made dense and sparse) to reflect voltage change in the amplitude of modulating signal.

1.12 Internet Service Provider (ISP)

ISP stands for Internet Service Provider which is a term used to refer to a company that provides internet access to people who pay the company or subscribe to the company for the same. For their services, the customers have to pay the internet service provider a nominal fee which varies according to the amount of data they actually use or the data plan which they purchase. An Internet Service Provider is also known as an Internet Access Provider or an online service provider. An Internet Service Provider is a must if one wants to connect to the internet.

History

The first Internet Service Provider was Telenet. Telenet was the commercialized version of the ARPANET – a precursor to the internet, of sorts. Telenet was introduced in 1974. Since then, many Internet Service Providers have entered the scene and this was partly because of the proliferation of the internet as a commodity that fuelled the consumerist attitude of the people. Pretty soon, an Internet Service Provider called "The World" came to be in vogue and ever since it started serving its customers today in 1989 has cemented itself as the first archetypal Internet Service Provider. Examples of major Internet Service Providers include Google Fiber, Verizon, Jio, AT&T etc.

Characteristics

- **E-mail Account**: Many Internet Service Providers offer an e-mail address to their consumers.
- **User Support**: Professionals and an increasing number of lay users prefer an ISP that can provide them with customer support so that they have someone they can refer to if things go awry.
- **Access to high-speed internet**: Probably the most obvious item on this list as this feature of an Internet Service Provider lies literally in its name. Furthermore, the higher the speed an Internet Service Provider can offer one, the better it's standing in the market and the more customers it can attract.
- **Spam Blocker**: An Internet Service Provider that hinders its customers' productivity by way of not blocking spam and displaying frequent ads is not something that is generally favoured in the market today. Therefore, many of the Internet Service Providers offer spam blocking features to their customers.
- **Web Hosting**: Some of the ISPs offer web hosting services to their clientele as well.

Different types of ISP connections

- DSL
- Wi-Fi broadband
- mobile broadband
- fibre optic broadband
- cable broadband

List of ISP

- Reliance Jio
- Vodafone Idea
- Airtel
- BSNL
- Hathway

Advantages

- The customer need not then bother with either the technicalities or finances of investing and inventing a web browser to work with. An ISP can readily do all of this for its customers.
- Many ISPs, being professional companies, provide its clientele with high-speed internet and that is not possible if one decides to sidesteps these companies.
- ISPs offer a very high degree of reliability and availability

- The ISPs are secure – they offer a tremendous deal of protection against viruses and use only the latest software patches whilst operating and thereby, maintaining the integrity of the browser.
- User do not need to invest in user's own web server.
- ISP's should give the best uptime guarantee.

Disadvantages

- Because of the range of options available in the market and due to cut-throat competition, some of the ISPs have been accused of violating the customers' trust by way of inflated pricing, data losses, etc. It is true that using an ISP makes the customer entirely dependent on it.
- If an Internet Service Provider is stretched thin because of hosting too many sites on a shared server, it can compromise the quality of the customers' data by way of slow download rates and poor performance of websites.
- User need to trust user's ISP for uptime and security.
- ISP can directly affect user if the it gets blacklisted.