Lecture Notes on

4AID4-07

Data Communication and Computer Networks

Unit 1 and 2

Department of Artificial Intelligence & Data Science

Jaipur Engineering College & Research Centre, Jaipur

Neelkamal Chaudhary

Assistant Professor

AI&DS

Vision of the Institute

To become a renowned centre of outcome based learning and work toward academic, professional, cultural and social enrichment of the lives of individuals and communities.

Mission of the Institute

M1: Focus on evaluation of learning outcomes and motivate students to inculcate research aptitude by project based learning.
M2: Identify, based on informed perception of Indian, regional and global needs, the areas of focus and provide platform to gain knowledge and solutions.
M3: Offer opportunities for interaction between academia and industry.
M4: Develop human potential to its fullest extent so that intellectually capable and imaginatively gifted leaders can emerge in a range of professions.

Vision Of The Department

To prepare students in the field of Artificial Intelligence and Data Science for competing with the global perspective through outcome based education, research and innovation.

Mission Of The Department

1. To impart outcome based education in the area of AI&DS.
2. To provide platform to the experts from institutions and industry of repute to transfer the knowledge to students for providing competitive and sustainable solutions.
3. To provide platform for innovation and research.

Program Outcomes (PO)

1. **Engineering knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and Artificial Intelligence & Data Science specialization to the solution of complex Artificial Intelligence & Data Science problems.
2. **Problem analysis**: Identify, formulate, research literature, and analyze complex Artificial Intelligence & Data Science problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions**: Design solutions for complex Artificial Intelligence & Data Science problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of Artificial Intelligence & Data Science experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex Artificial Intelligence & Data Science activities with an understanding of the limitations.
6. **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional Artificial Intelligence & Data Science practice.
7. **Environment and sustainability**: Understand the impact of the professional Artificial Intelligence & Data Science in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the Artificial Intelligence & Data Science practice.
9. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings in Artificial Intelligence & Data Science
10. **Communication**: Communicate effectively on complex Artificial Intelligence & Data Science activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance**: Demonstrate knowledge and understanding of the Artificial Intelligence & Data Science and management principles and apply these to one" s own work, as a

member and leader in a team, to manage projects and in multidisciplinary environments.

12. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change in Artificial Intelligence & Data Science.

Program Educational Objectives (PEO)

PEO1: To provide students with the fundamentals of Engineering Sciences with more emphasis in Artificial Intelligence & Data Science by way of analyzing and exploiting engineering challenges.

PEO2: To train students with good scientific and engineering knowledge so as to comprehend, analyze, design, and create novel products and solutions for the real life problems in Artificial Intelligence & Data Science

PEO3: To inculcate professional and ethical attitude, effective communication skills, teamwork skills, multidisciplinary approach, entrepreneurial thinking and an ability to relate engineering issues with social issues for Artificial Intelligence & Data Science.

PEO4: To provide students with an academic environment aware of excellence, leadership, written ethical codes and guidelines, and the self-motivated life-long learning needed for a successful professional career in Artificial Intelligence & Data Science.

PEO5: To prepare students to excel in Industry and Higher education by Educating Students along with High moral values and Knowledge in Artificial Intelligence & Data Science.

COURSE OUTCOME: After studying this subject, student will be able

CO-1	Understand the principles of Network Protocols and OSI and TCP/IP model.
CO-2	Analyze and implement the concepts of various protocols of Error Detection and Correction
CO-3	Analyze and apply the concept of various Routing algorithms and principles of reliable data transfers along with transactional TCP and associated congestion control.
C0-4	Classify role of application layer, its various elements like WWW, DNS FTP and network security.

CO_PO Mapping

SUBJECT CODE	subject name		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
4AID4-07	Data Communication and Computer Networks	CO1:	3	3	3	2	2	1	1	1	1	1	1	3
		CO2:	3	3	3	3	1	1	1	1	1	2	1	3
		CO3:	3	3	3	2	1	1	1	1	1	2	1	3
		CO4:	3	3	3	2	1	1	1	1	1	1	1	3

Syllabus

4AID4-07: Data Communication and Computer Networks

Credit: 3 **Max. Marks: 100(IA:30,ETE:70)**

3L+0T+0P **End Term Exam: 3 Hours**

SN	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	1
2	Introductory Concepts: Network hardware, Network software, topologies, Protocols and standards, OSI model, TCP model, TCP/IP model, Physical Layer: Digital and Analog Signals, Periodic Analog Signals, Signal Transmission, Limitations of Data Rate, Digital Data Transmission, Performance Measures, Line Coding, Digital Modulation, Media and Digital Transmission System	7
3	Data Link Layer: Error Detection and Correction, Types of Errors, Two dimensional parity check, Detection verses correction, Block Coding, Linear Block Coding, Cyclic Codes, Checksum, Standardized Polynomial Code, Error Correction Methods, Forward Error Correction, Protocols: Stop and wait, Go-back-N ARQ, Selective Repeat ARQ, Sliding window, Piggy backing, Pure ALOHA, Slotted ALOHA, CSMA/CD, CSMA/CA	9
4	Network Layer: Design issues, Routing algorithms: IPV4, IPV6, Address mapping:ARQ,RARQ,Congestion control, Unicast,Multicast, Broadcast routing protocols, Quality of Service, Internetworking	8
5	Transport Layer: Transport service, Elements of transport protocols, User Datagram Protocol, Transmission Control Protocol, Quality of service, Leaky Bucket and Token Bucket algorithm	8
6	Application Layer**:** WWW, DNS, Multimedia, Electronic mail, FTP, HTTP, SMTP, Introduction to network security	7
	Total	40

A system of interconnected computers and computerized peripherals such as printers is called computer network. This interconnection among computers facilitates information sharing among them. Computers may connect to each other by either wired or wireless media.

Classification of Computer Networks

Computer networks are classified based on various factors. They include:

- Geographical span
- Inter-connectivity
- Administration
- Architecture

Geographical Span

Geographically a network can be seen in one of the following categories:

- It may be spanned across your table, among Bluetooth enabled devices,Ranging not more than few meters.
- It may be spanned across a whole building, including intermediate devices toconnect all floors.
- It may be spanned across a whole city.
- It may be spanned across multiple cities or provinces.
- It may be one network covering whole world.

Inter-Connectivity

Components of a network can be connected to each other differently in some fashion.By connectedness we mean either logically, physically, or both ways.

- Every single device can be connected to every other device on network, makingthe network mesh.
- All devices can be connected to a single medium but geographicallydisconnected, created bus-like structure.
- Each device is connected to its left and right peers only, creating linearstructure.

- All devices connected together with a single device, creating star-like structure.
- All devices connected arbitrarily using all previous ways to connect each other, resulting in a hybrid structure.

Administration

From an administrator's point of view, a network can be private network which belongs a single autonomous system and cannot be accessed outside its physical or logical domain. A network can be public, which is accessed by all.

Network Architecture

Computer networks can be discriminated into various types such as Client-Server, peer-to-peer or hybrid, depending upon its architecture.

- There can be one or more systems acting as Server. Other being Client, requests the Server to serve requests. Server takes and processes request on behalf of Clients.
- Two systems can be connected Point-to-Point, or in back-to-back fashion. They both reside at the same level and called peers.
- There can be hybrid network which involves network architecture of both the above types.

Network Applications

Computer systems and peripherals are connected to form a network. They provide numerous advantages:

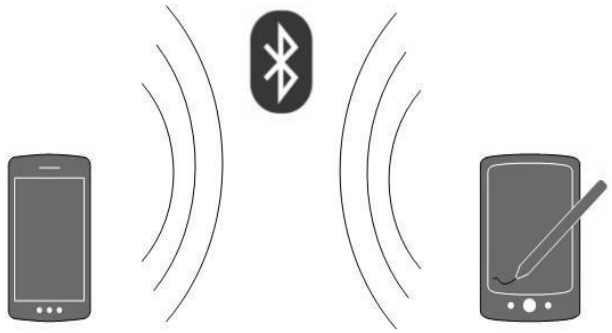
- Resource sharing such as printers and storage devices
- Exchange of information by means of e-Mails and FTP
- Information sharing by using Web or Internet
- Interaction with other users using dynamic web pages
- IP phones
- Video conferences
- Parallel computing
- Instant messaging

2. TYPES OF COMPUTER NETWORKS

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

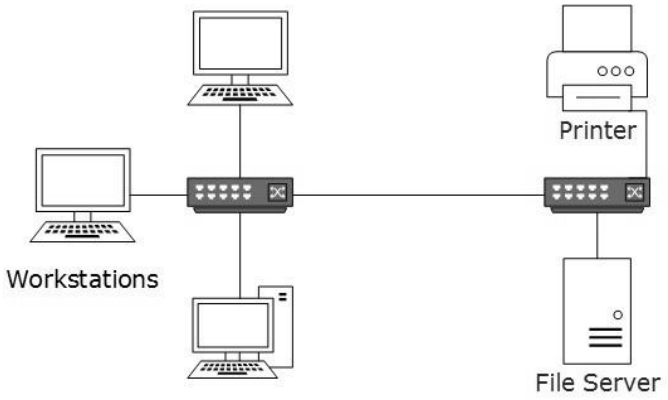
A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers,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



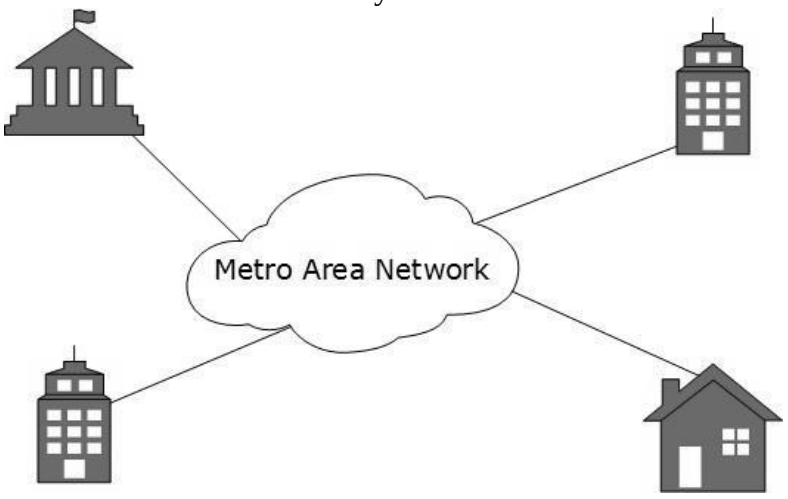
LANs are composed of inexpensive networking and routing equipment. It may contains local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally.LAN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

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

MetropolitanAreaNetwork

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).

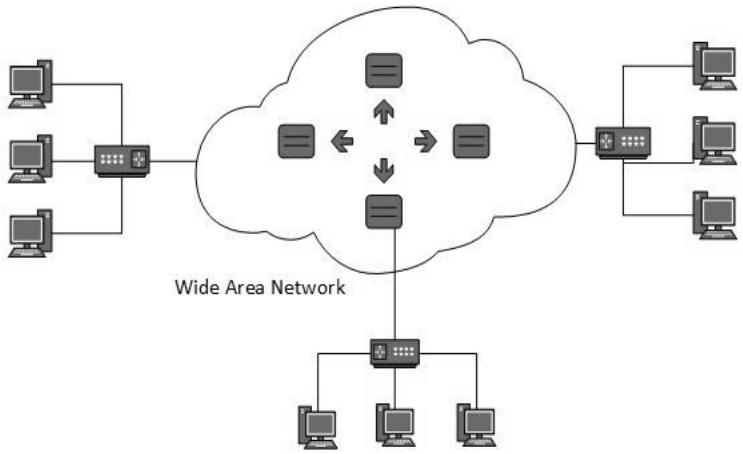
Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.



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

3. NETWORK LAN TECHNOLOGIES

Let us go through various LAN technologies in brief:

Ethernet

Ethernet is a widely deployed LAN technology. This technology was invented by BobMetcalfe and D.R. Boggs in the year 1970. It was standardized in IEEE 802.3 in 1980.

Ethernet shares media. Network which uses shared media has high probability of data collision. Ethernet uses Carrier Sense Multi Access/Collision Detection (CSMA/CD) technology to detect collisions. On the occurrence of collision in Ethernet, all its hosts roll back, wait for some random amount of time, and then re-transmit the data.

Ethernet connector is network interface card equipped with 48-bits MAC address. This helps other Ethernet devices to identify and communicate with remote devices in Ethernet.

Traditional Ethernet uses 10BASE-T specifications. The number 10 depicts 10MBPS speed, BASE stands for baseband, and T stands for Thick Ethernet. 10BASE-T Ethernet provides transmission speed up to 10MBPS and uses coaxial cable or Cat-5 twisted pair cable with RJ-5 connector. Ethernet follows Star topology with segment length up to 100 meters. All devices are connected to a hub/switch in a star fashion.

Fast-Ethernet

To encompass need of fast emerging software and hardware technologies, Ethernet extends itself as Fast-Ethernet. It can run on UTP, Optical Fiber, and wirelessly too. It can provide speed up to 100MBPS. This standard is named as 100BASE-T in IEEE
803.2 using Cat-5 twisted pair cable. It uses CSMA/CD technique for wired media sharing among the Ethernet hosts and CSMA/CA (CA stands for Collision Avoidance)technique for wireless Ethernet LAN.

Fast Ethernet on fiber is defined under 100BASE-FX standard which provides speed up to 100MBPS on fiber. Ethernet over fiber can be extended up to 100 meters in half-duplex mode and can reach maximum of 2000 meters in full-duplex over multimode fibers.

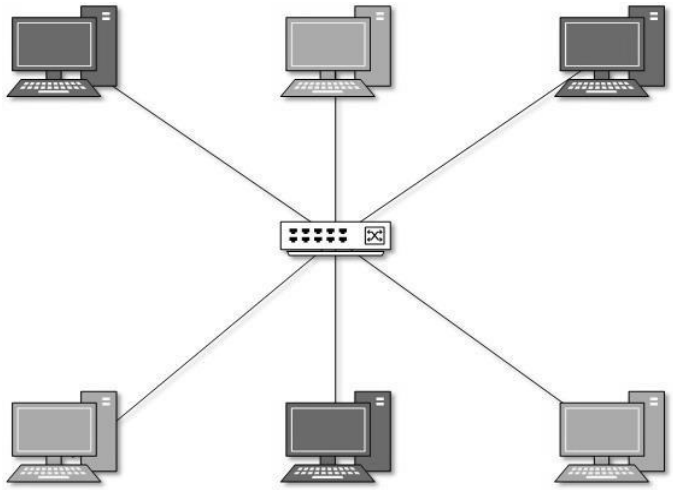
Giga-Ethernet

After being introduced in 1995, Fast-Ethernet retained its high speed status only for three years till Giga-Ethernet introduced. Giga-Ethernet provides speed up to 1000 mbits/seconds. IEEE802.3ab standardizes Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables. IEEE802.3ah defines Giga-Ethernet over Fiber.

VirtualLAN

LAN uses Ethernet which in turn works on shared media. Shared media in Ethernet create one single Broadcast domain and one single Collision domain. Introduction of switches to Ethernet has removed single collision domain issue and each device connected to switch works in its separate collision domain. But even Switches cannot divide a network into separate Broadcast domains.

Virtual LAN is a solution to divide a single Broadcast domain into multiple Broadcast domains. Host in one VLAN cannot speak to a host in another. By default, all hosts are placed into the same VLAN.



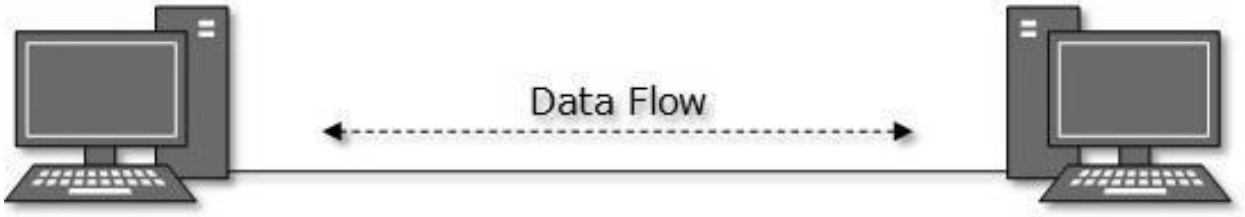
In this diagram, different VLANs are depicted in different color codes. Hosts in one VLAN, even if connected on the same Switch cannot see or speak to other hosts in different VLANs. VLAN is Layer-2 technology which works closely on Ethernet. To route packets between two different VLANs, a Layer-3 device such as Router is required.

4. COMPUTER NETWORK TOPOLOGIES

A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or differentin a same network.

Point-to-Point

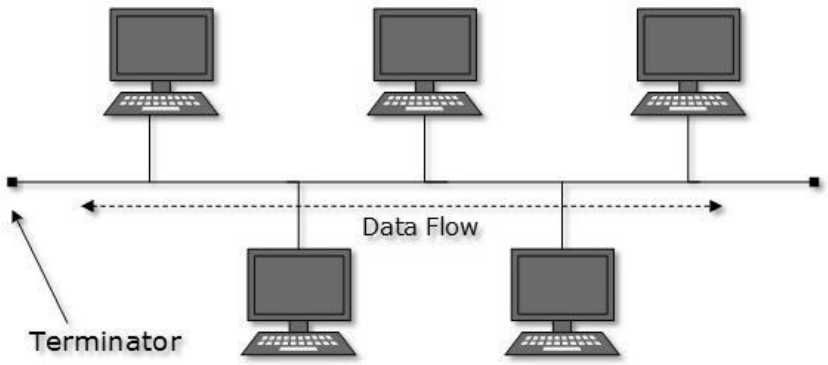
Point-to-point networks contains exactly two hosts such as computer, switches, routers, or servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice versa.



If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.

BusTopology

In case of Bus topology, all devices share single communication line or cable. Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.

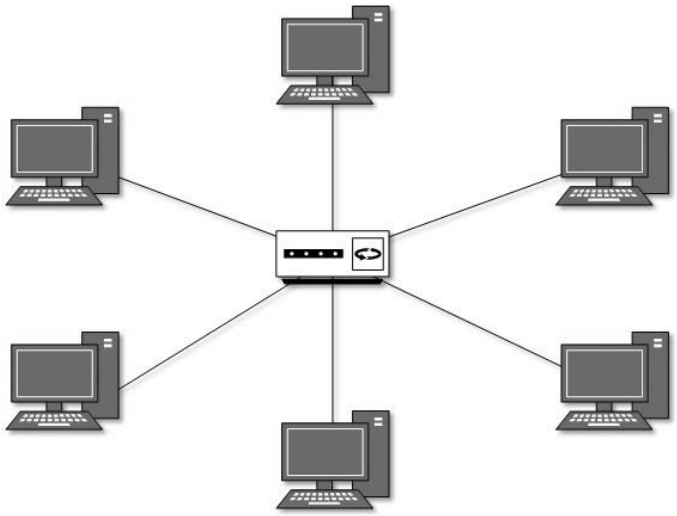


Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the datafrom the line.

StarTopology

All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

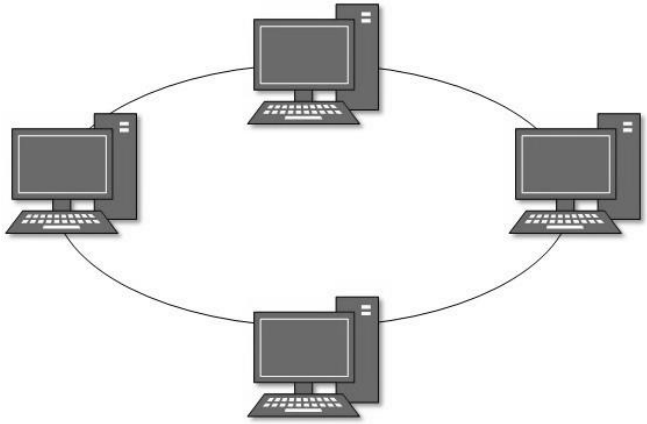
- Layer-1 device such as hub or repeater
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway



As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts takes place through only the hub. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

RingTopology

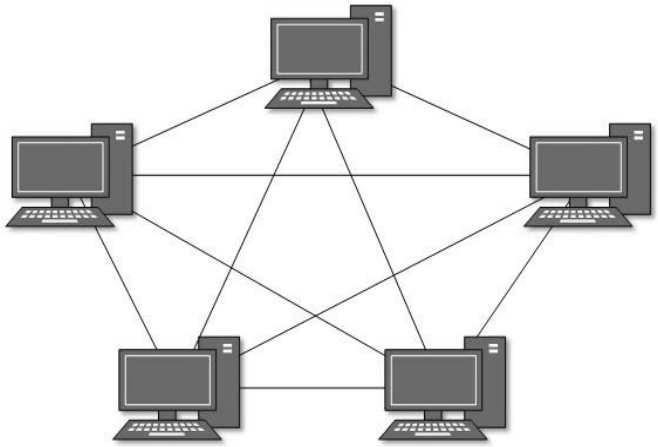
In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need onlyone more extra cable.



Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

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 with 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:

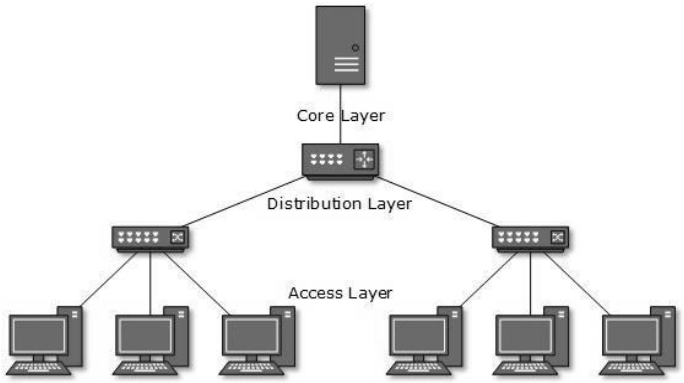
- **Full Mesh:** All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.
- **Partially Mesh:** Not all hosts have point-to-point connection to 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.

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 into 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 treefrom which all nodes fork.



All neighboring 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.

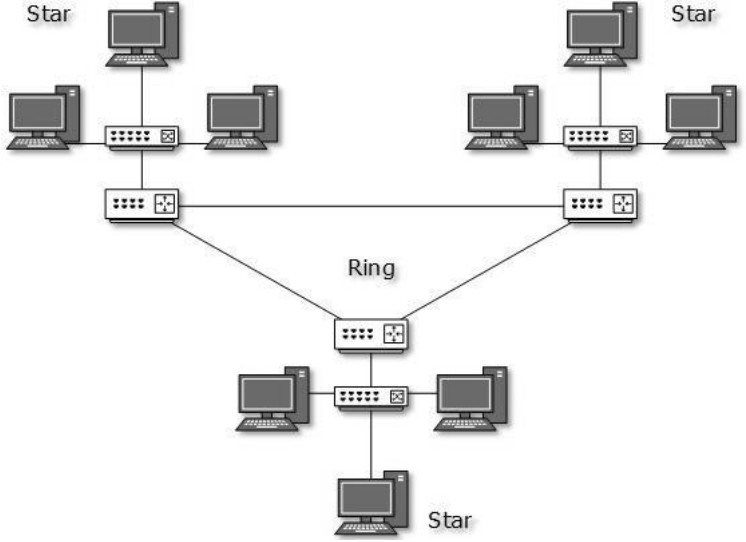
DaisyChain

This topology connects all the hosts in a linear fashion. Similar to Ring topology, all hosts are connected to two hosts only, except the end hosts. Means, if the end hosts in daisy chain are connected then it represents Ring topology.

Each link in daisy chain topology represents single point of failure. Every link failure splits the network into two segments. Every intermediate host works as relay for itsimmediate hosts.

HybridTopology

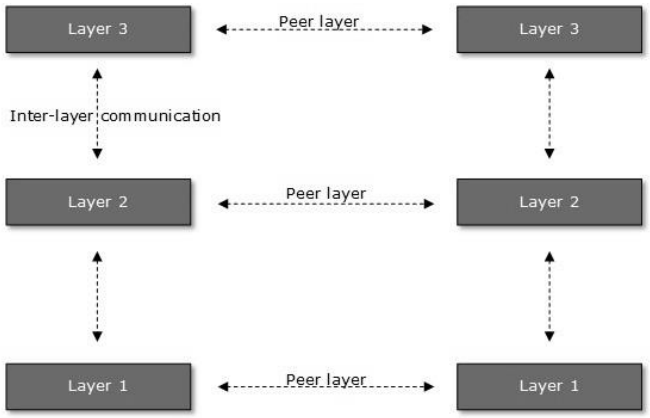
A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporatingtopologies.



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.

Layered Tasks

In layered architecture of Network Model, one whole network process is divided into small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work.

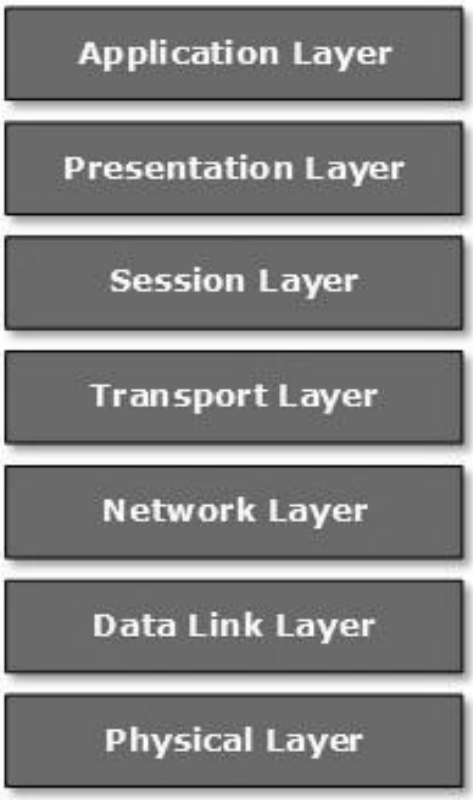


In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. The task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by the topmost layer, it is passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and passes on to lower layer. If the task is initiated by lowermost layer, then the reverse path is taken.

Every layer clubs together all procedures, protocols, and methods which it requires to execute its piece of task. All layers identify their counterparts by means of encapsulation header and tail.

OSIModel

Open System Interconnect is an open standard for all communication systems. OSI model is



established by International Standard Organization (ISO). This model has seven layers:

Application Layer: This layer is responsible for providing interface to the application user. This layer encompasses protocols which directly interact withthe user.

Presentation Layer: This layer defines how data in the native format of remote host should be presented in the native format of host.

Session Layer: This layer maintains sessions between remote hosts. For example, once user/password authentication is done, the remote host maintains this session for a while and does not ask for authentication again inthat time span.

Transport Layer: This layer is responsible for end-to-end delivery between hosts.

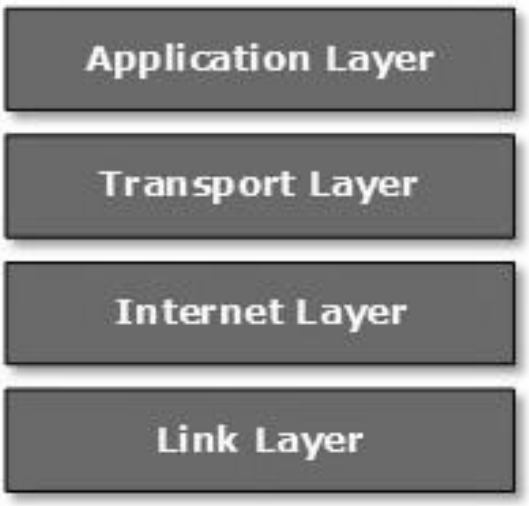
Network Layer: This layer is responsible for address assignment and uniquelyaddressing hosts in a network.

Data Link Layer: This layer is responsible for reading and writing data fromand onto the line. Link errors are detected at this layer.

Physical Layer: This layer defines the hardware, cabling, wiring, poweroutput, pulse rate etc.

InternetModel

Internet uses TCP/IP protocol suite, also known as Internet suite. This defines Internet Model which contains four layered architecture. OSI Model is general communication model but Internet Model is what the internet uses for all its communication. The internet is independent of its underlying network architecture sois its Model. This model has the following layers:



Application Layer: This layer defines the protocol which enables user to interact with the network. For example, FTP, HTTP etc.

Transport Layer: This layer defines how data should flow between hosts. Major protocol at this layer is Transmission Control Protocol (TCP). This layer ensures data delivered between hosts is in-order and is responsible for end- to-end delivery.

Internet Layer: Internet Protocol (IP) works on this layer. This layer facilitates host addressing and recognition. This layer defines routing.

Link Layer: This layer provides mechanism of sending and receiving actual data. Unlike its OSI Model counterpart, this layer is independent of underlying network architecture and hardware.

During initial days of internet, its use was limited to military and universities for research and development purpose. Later when all networks merged together and formed internet, the data used to travel through public transit network. Common people may send the data that can be highly sensitive such as their bank credentials, username and passwords, personal documents, online shopping details, or confidential documents.

All security threats are intentional i.e. they occur only if intentionally triggered. Security threats can be divided into the following categories:

Interruption

Interruption is a security threat in which availability of resources is attacked. For example, a user is unable to access its web-server or the web-server is hijacked.

Privacy-Breach

In this threat, the privacy of a user is compromised. Someone, who is not the authorized person is accessing or intercepting data sent or received by the original authenticated user.

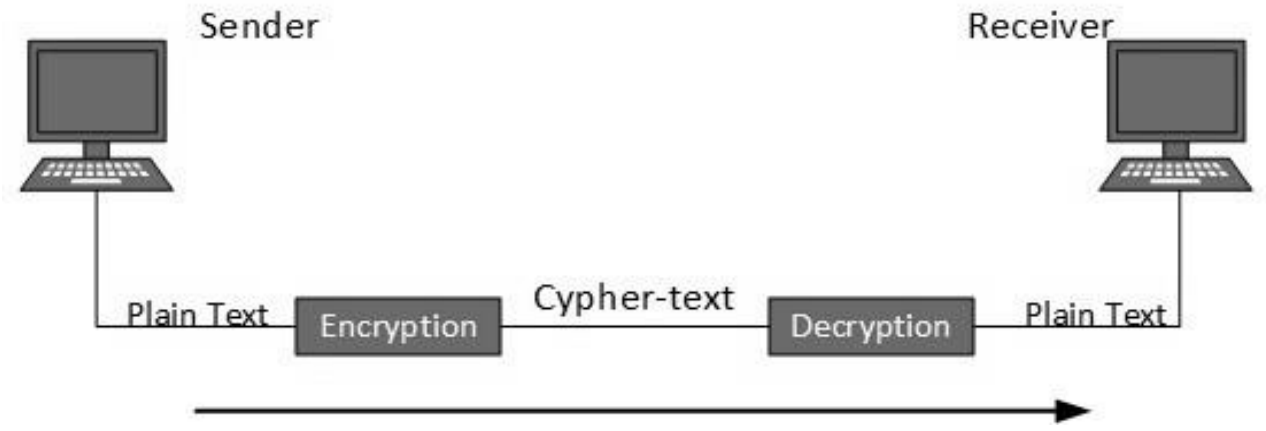
Integrity

This type of threat includes any alteration or modification in the original context of communication. The attacker intercepts and receives the data sent by the sender and the attacker then either modifies or generates false data and sends to the receiver. The receiver receives the data assuming that it is being sent by the original Sender.

Authenticity

This threat occurs when an attacker or a security violator poses as a genuine person and accesses the resources or communicates with other genuine users.

No technique in the present world can provide 100% security. But steps can be taken to secure data while it travels in unsecured network or internet. The most widely usedtechnique is Cryptography.



Cryptography is a technique to encrypt the plain-text data which makes it difficult to understand and interpret. There are several cryptographic algorithms available present day as described below:

- Secret Key
- Public Key
- Message Digest

SecretKeyEncryption

Both sender and receiver have one secret key. This secret key is used to encrypt the data at sender's end. After the data is encrypted, it is sent on the public domain to the receiver. Because the receiver knows and has the Secret Key, the encrypted datapackets can easily be decrypted.

Example of secret key encryption is Data Encryption Standard (DES). In Secret Key encryption, it is required to have a separate key for each host on the network makingit difficult to manage.

PublicKeyEncryption

In this encryption system, every user has its own Secret Key and it is not in the shared domain. The secret key is never revealed on public domain. Along with secret key, every user has its own but public key. Public key is always made public and is used by Senders to encrypt the data. When the user receives the encrypted data, hecan easily decrypt it by using its own Secret Key.

Example of public key encryption is Rivest-Shamir-Adleman (RSA)..

MessageDigest

In this method, actual data is not sent; instead a hash value is calculated and sent. The other end user, computes its own hash value and compares with the one just received. If both hash values are matched, then it is accepted; otherwise rejected.

Example of Message Digest is MD5 hashing. It is mostly used in authentication where user password is cross checked with the one saved on the server.

PHYSICAL LAYER INTRODUCTION

Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network model which actually deals with the physical connectivity of two different stations. This layer defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.

Physical layer provides its services to Data-link layer. Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data. The binary data is then sent over the wired or wireless media.

Signals

When data is sent over physical medium, it needs to be first converted into electromagnetic signals. Data itself can be analog such as human voice, or digital such as file on the disk. Both analog and digital data can be represented in digital oranalog signals.

Digital Signals

Digital signals are discrete in nature and represent sequence of voltage pulses. Digital signals are used within the circuitry of a computer system.

Analog Signals

Analog signals are in continuous wave form in nature and represented by continuous electromagnetic waves.

Transmission Impairment

When signals travel through the medium, they tend to deteriorate. This may have many reasons as given:

Attenuation

For the receiver to interpret the data accurately, the signal must be sufficiently strong. When the signal passes through the medium, it tends to get weaker. As it covers distance, it loses strength.

Dispersion

As signal travels through the media, it tends to spread and overlaps. The amount of dispersion depends upon the frequency used.

Delay distortion

Signals are sent over media with pre-defined speed and frequency. If the signal speedand frequency do not match, there are possibilities that signal reaches destination in

arbitrary fashion. In digital media, this is very critical that some bits reach earlier than the previously sent ones.

Noise

Random disturbance or fluctuation in analog or digital signal is said to be Noise in signal, which may distort the actual information being carried. Noise can be characterized in one of the following class:

Thermal Noise

Heat agitates the electronic conductors of a medium which may introduce noise in the media. Up to a certain level, thermal noise is unavoidable.

Intermodulation

When multiple frequencies share a medium, their interference can cause noise in the medium. Intermodulation noise occurs if two different frequencies are sharing a medium and one of them has excessive strength or the component itself is not functioning properly, then the resultant frequency may not be delivered as expected.

Crosstalk

This sort of noise happens when a foreign signal enters into the media. This is because signal in one medium affects the signal of second medium.

Impulse

This noise is introduced because of irregular disturbances such as lightening, electricity, short-circuit, or faulty components. Digital data is mostly affected by thissort of noise.

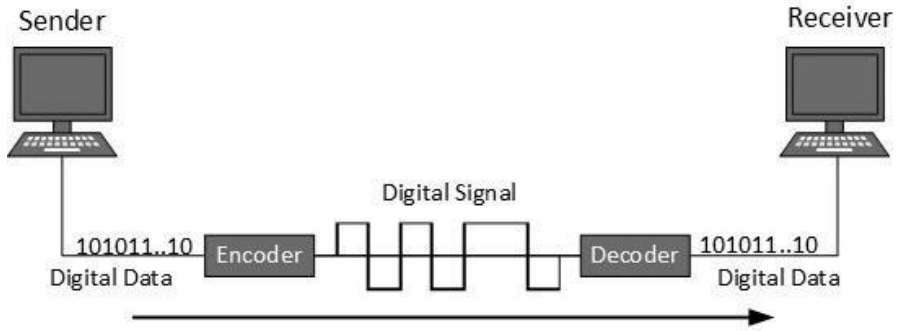
Data or information can be stored in two ways, analog and digital. For a computer touse the data, it must be in discrete digital form. Similar to data, signals can also be in analog and digital form. To transmit data digitally, it needs to be first converted todigital form.

Digital-to-DigitalConversion

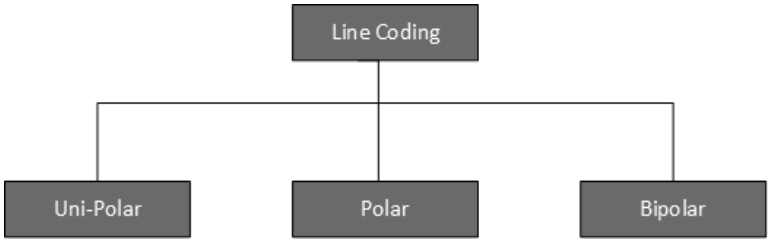
This section explains how to convert digital data into digital signals. It can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

LineCoding

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.

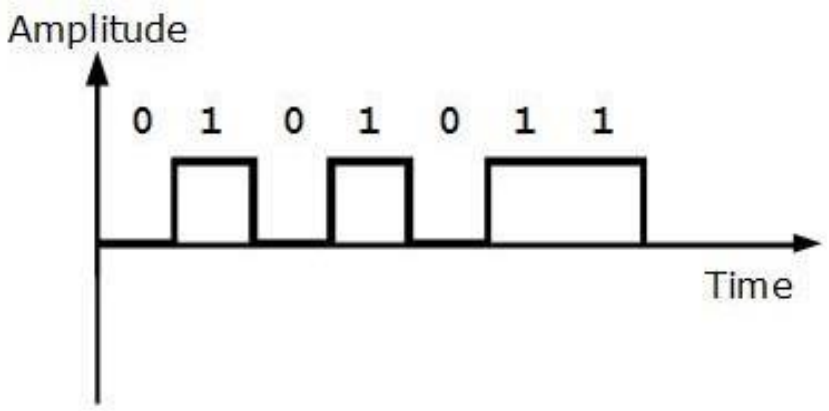


Digital signal is denoted by discreet signal, which represents digital data. There are three types of line coding schemes available:



UnipolarEncoding

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.



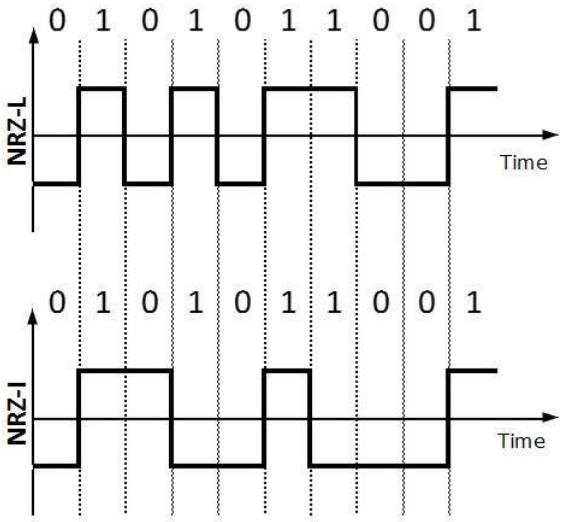
PolarEncoding

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.

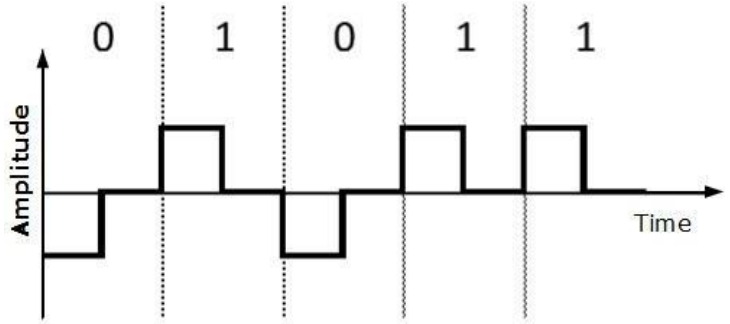
NRZ scheme has two variants: NRZ-L and NRZ-I.



NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-Ichanges voltage when a 1 is encountered.

Return to Zero (RZ)

Problem with NRZ is that the receiver cannot conclude when a bit ended and whenthe 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

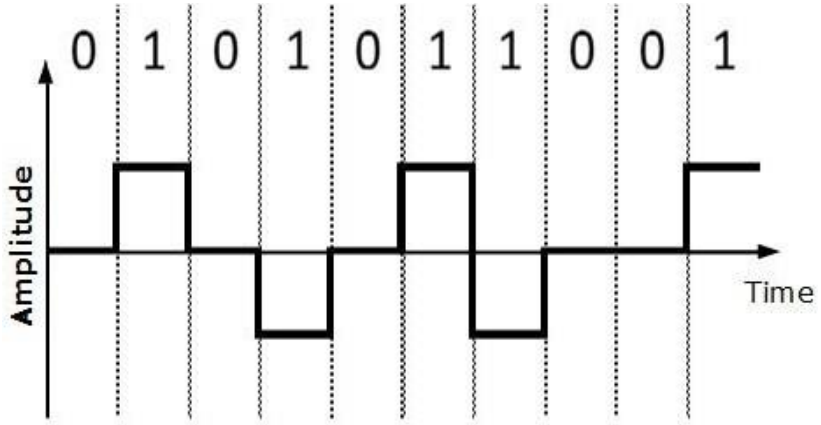
This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.

Differential Manchester

This encoding scheme is a combination of RZ and NRZ-I. It also transits at the middle of the bit but changes phase only when 1 is encountered.

BipolarEncoding

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.



BlockCoding

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:

1. Division
2. Substitution
3. Combination.

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

Analog-to-DigitalConversion

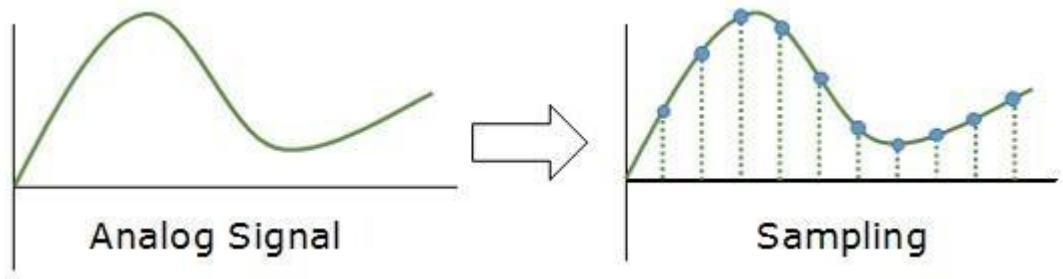
Microphones create analog voice and camera creates analog videos, which are treated is analog data. To transmit this analog data over digital signals, we need analog to digital conversion.

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:

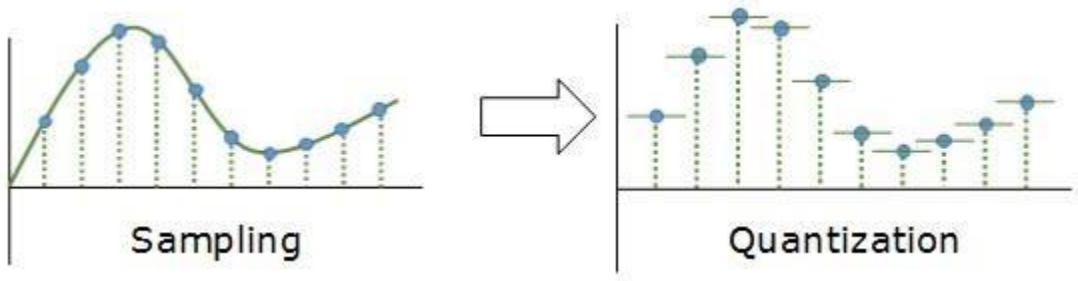
- Sampling
- Quantization
- Encoding.

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.

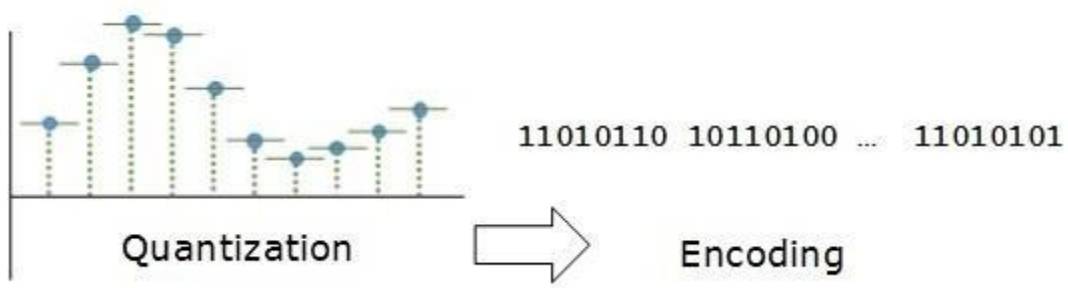
Quantization



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

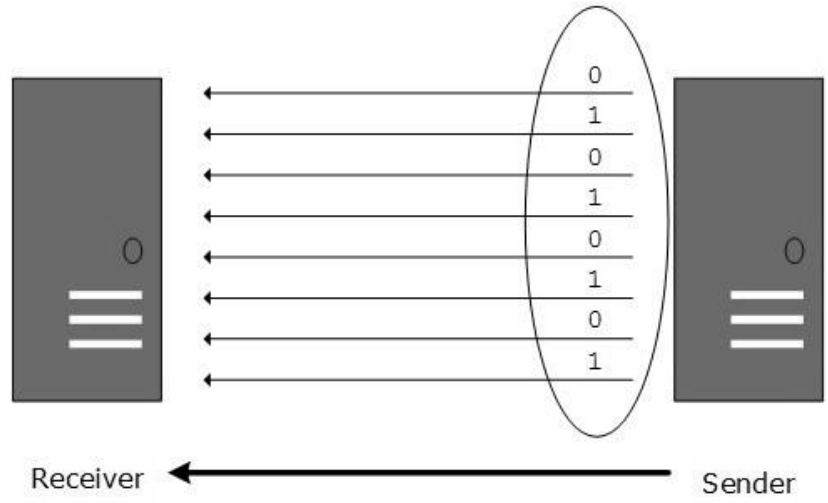


In encoding, each approximated value is then converted into binary format.

TransmissionModes

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

Parallel Transmission

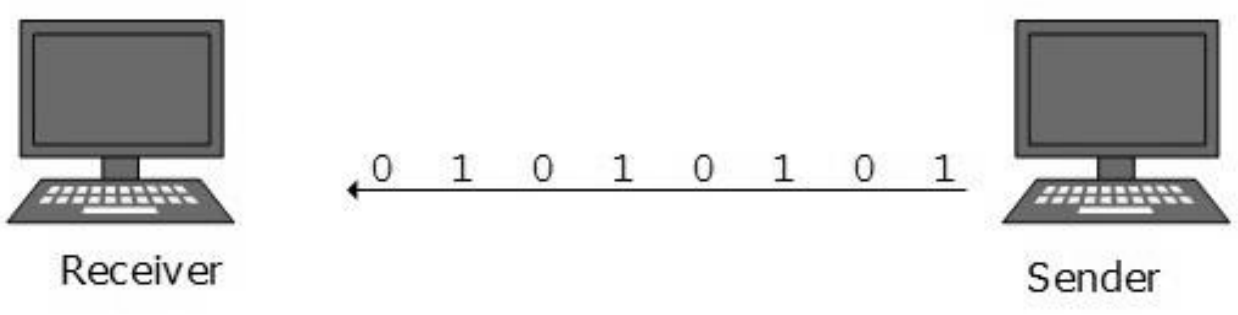


The binary bits are organized into groups of fixed length. Both sender and receiver are connected in parallel with the equal number of data lines. Both computers distinguish between high order and low order data lines. The sender sends all the bitsat once on all lines. Because the data lines are equal 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.

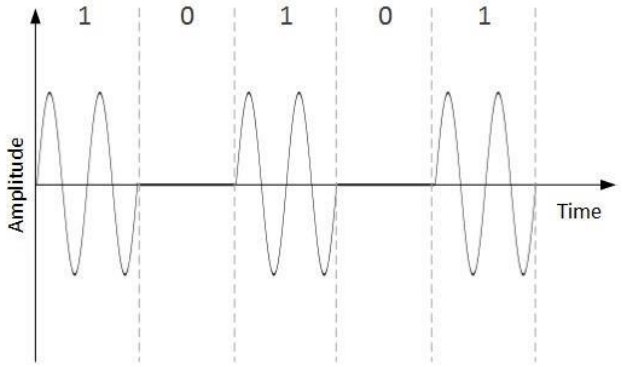
Digital-to-AnalogConversion

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

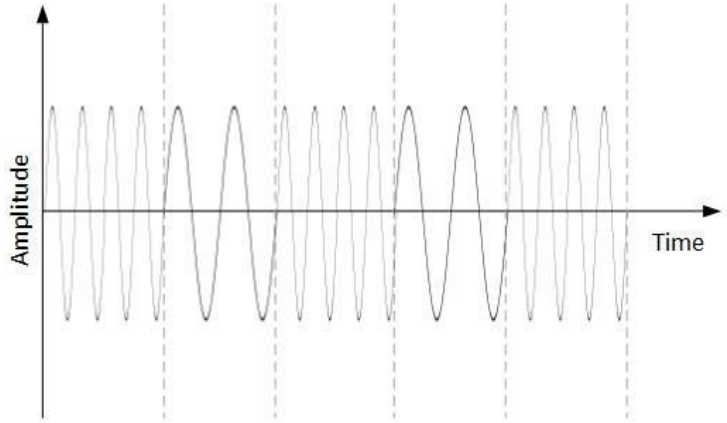
In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.



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

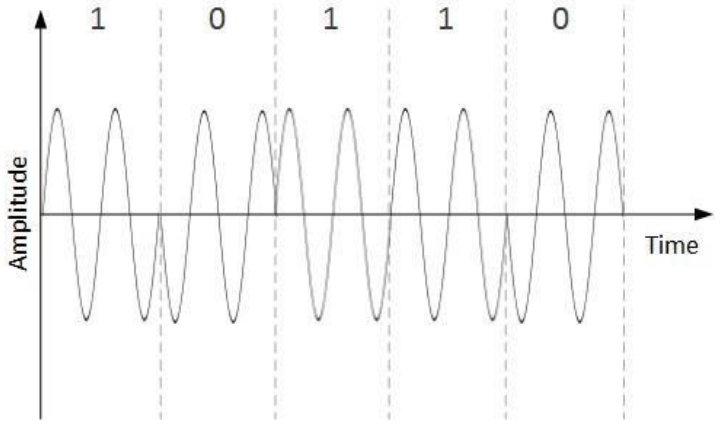
In this conversion technique, the frequency of the analog carrier signal is modified toreflect binary data.



This technique uses two frequencies, f1 and f2. One of them, for example f1, ischosen 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 reflectthe binary data.



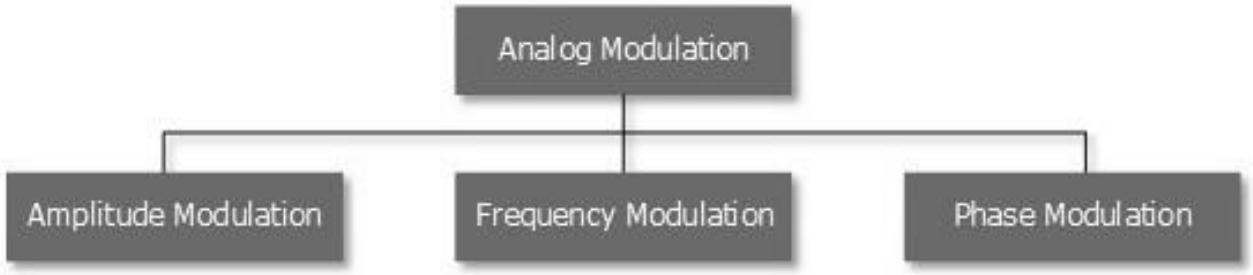
When a new binary symbol is encountered, the phase of the signal is altered.Amplitude and frequency of the original carrier signal is kept intact.

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.

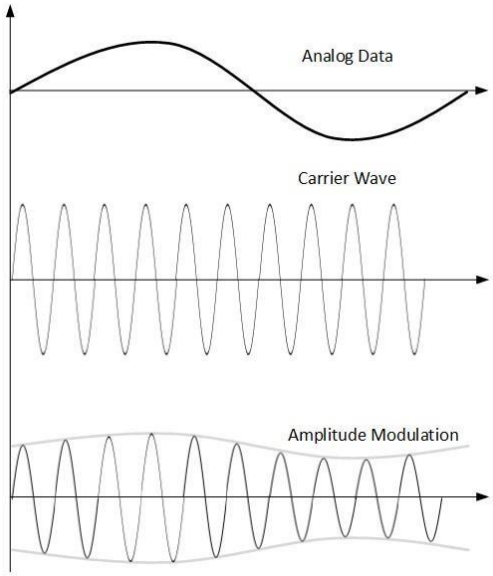
Analog-to-Analog Conversion

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.

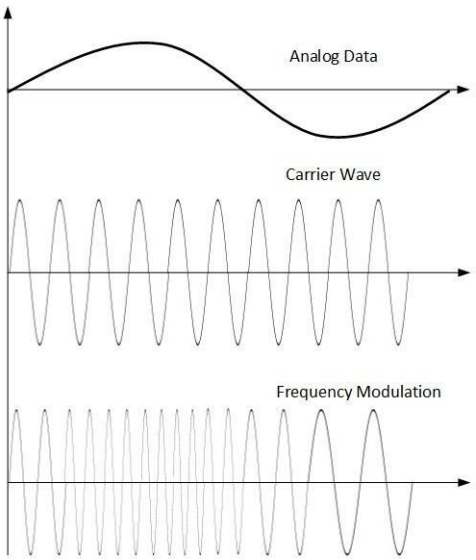


Amplitude modulation is implemented by means of a multiplier. The amplitude of modulating signal (analog data) is multiplied by the amplitude of carrier frequency, which then reflects analog data.

The frequency and phase of carrier signal remain unchanged.

Frequency Modulation

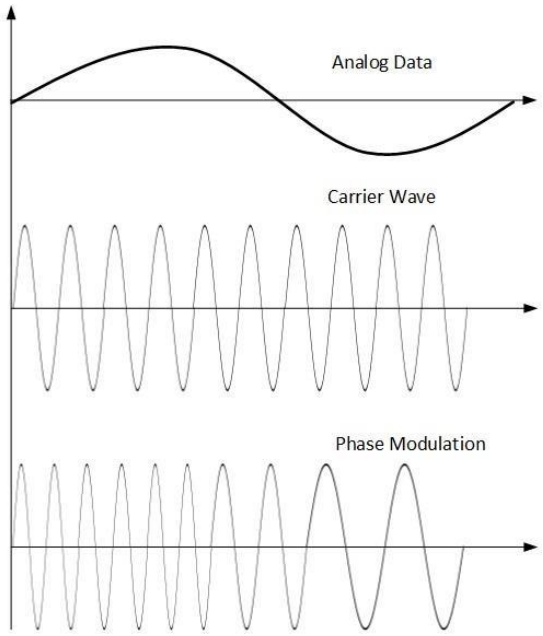
In this modulation technique, the frequency of the carrier signal is modified to reflect the change in the voltage levels of the modulating signal (analog data).



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 toreflect 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 amplitudeof modulating signal.