Computer Networks

Course Code: CSE3003

Ms. Shubhra dwivedi
Assistant Professor
School - SCOPE
VIT-AP Amaravati
Shubhra.d@vitap.ac.in

Introduction

Course Objectives

- To introduce basic concepts in Computer Networks
- To expose state-of-the-art technologies in computer network protocols, architectures, and applications.

Expected Course Outcomes

On completion of the course, students will have the ability to

- Independently understand basic computer network technology.
- Enumerate the layers of the OSI model and TCP/IP. Explain the function(s) of each layer.
- Understand and building the skills of subnetting and routing mechanisms.
- To assist in network design and implementation.

Textbooks

1. **"Computer Networking: A Top-Down Approach", James F. Kurose, Keith W. Ross, Pearson, 7th Edition, 2017.**
2. **"Computer and Communication Networks", Nader. F. Mir, Pearson Prentice Hall Publishers, Second Edition, 2015.**
3. **"Data Communications And Networking (SIE)", Behrouz Forouzan, Tata McGraw-Hill Education, 5th Edition, 2015.**
4. **"Computer Networks", Andrew S. Tanenbaum, David J. Wetherall, 5th Edition, 2011.**
5. **"Data and Computer Communications", William Stallings, Pearson Prentice Hall Publishers, 10th edition, 2013**

Contents

- Introduction and Course outline
- Short History
- Progress and application
- Internet
- Network architecture
- Networking devices
- OSI Model
- TCP/IP Protocol stack
- Networking in different OS.

Computer network

- A digital network that provides resource sharing between two nodes is called Computer Network.
- In a computer network, multiple computers get connected with each other to share data or information.

OR

- A computer network is a system of interconnected computers and peripheral devices. For example, it may connect computers, printers, scanners and cameras.
- A computer network can be established through both cable or wireless media.
- Computer networks nowadays support various applications such as the World Wide Web, digital audio, digital video, etc.

ARPANET - the First Network

ARPANET − Advanced Research Projects Agency Network:

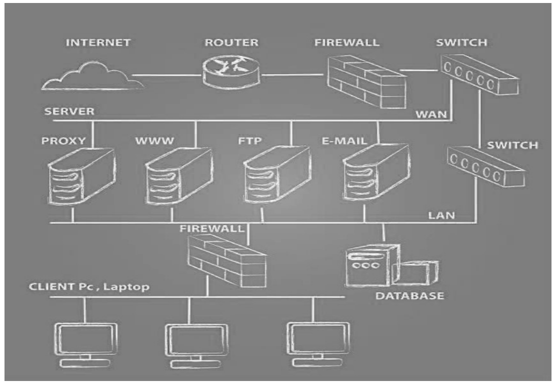
The **ARPANET**,one of the earliest computer networks, was proposed by Leonard Kleinrock in 1961, in his paper titled **"Information Flow in Large Communication Nets."**

•It was a network established by the US Department of Defense (DOD).

•The work for establishing the network started in the early 1960s and DOD sponsored major research work, which resulted in development on initial protocols, languages and frameworks for network communication.

•It had four nodes at University of California at Los Angeles (UCLA), Stanford Research Institute (SRI), University of California at Santa Barbara (UCSB) and University of Utah.

•On October 29, 1969, the first message was exchanged between UCLA and SRI. E-mail was created by Roy Tomlinson in 1972 at Bolt Beranek and Newman, Inc. (BBN) after UCLA was connected to BBN.



Internet

•ARPANET expanded to connect DOD with those universities of the US that were carrying out defense-related research.

•It covered most of the major universities across the country.

•The concept of networking got a boost when University College of London (UK) and Royal Radar Network (Norway) connected to the ARPANET and a network of networks was formed.

•The term **Internet** was coined by Vinton Cerf, Yogen Dalal and Carl Sunshine of Stanford University to describe this network of networks.

•Together they also developed protocols to facilitate information exchange over the Internet. Transmission Control Protocol (TCP) still forms the backbone of networking.

Telenet & World Wide Web

Telenet

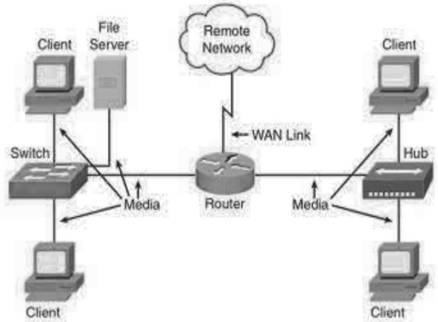
•Telenet was the first commercial adaptation of ARPANET introduced in 1974. With this the concept of Internet Service Provider (ISP) was also introduced.

•The main function of an ISP is to provide uninterrupted Internet connection to its customers at affordable rates.

World Wide Web

- With commercialization of internet, more and more networks were developed in different part of the world.
- Each network used different protocols for communicating over the network. This prevented different networks from connecting together seamlessly.
- In the 1980s, Tim Berners-Lee led a group of Computer scientists at CERN, Switzerland, to create a seamless network of varied networks, called the World Wide Web (WWW).
- World Wide Web is a complex web of websites and web pages connected together through hypertexts. Hypertext is a word or group of words linking to another web page of the same or different website. When the hypertext is clicked, another web page opens.

Overview of Network Components



Brief history

The History about Computer Network...

1971 ARPANET has 15 sites, 23 hosts

1972 **FTP** is outlined in 1972;
E-mail is created in 1972 by Ray Tomlinson of BBN;
Telnet protocol is proposed in his year.

1974 Vinton Cerf, propose the Transmission Control Protocol (**TCP**) in the paper, "A Protocol for Packet Network **Internet**working", which introduce the term **Internet**.

1977 The first **wireless** gateway is connected to ARPANET, which transmits packet over radio waves.

1978 Vinton Cerf, launch the plan for Internet Protocol (**IP**), which is proposed as a routing function that is separated from TCP.

1982 **TCP and IP** are adopted as the main protocol suite for ARPANET

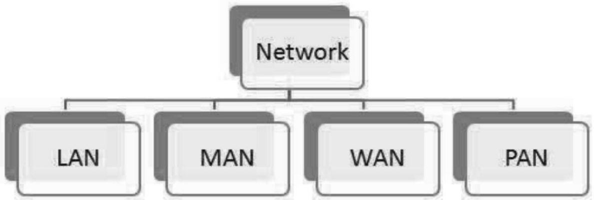
Brief history

- ARPANET finished the transition to using TCP/IP in 1983.
- Paul Mockapetris and Jon Postel implement the first DNS in 1983.
- The NSFNET (National Science Foundation Network) came online in 1986. It was a backbone for ARPANET, before eventually replacing ARPANET in the early 1990s.
- Tim Berners-Lee, a British scientist, invented the World Wide Web (WWW) in 1989, while working at CERN.
- The first version of the 802.11 standard for Wi-Fi is introduced in June 1997, providing transmission speeds up to 2 Mbps.
- The Wired Equivalent Privacy (WEP) encryption protocol for Wi-Fi is introduced in September 1999, for use with 802.11b.

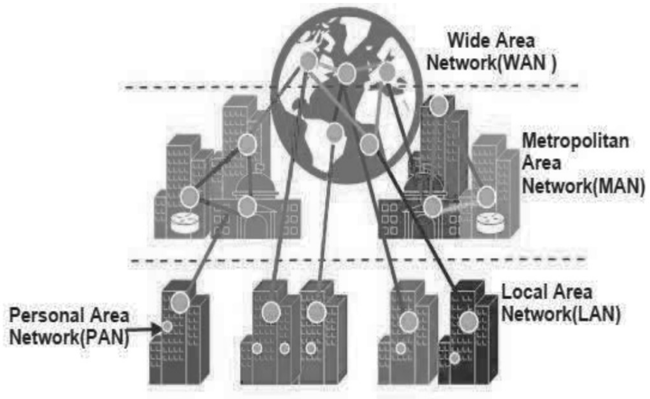
Applications

- **E-mail**
- **Searchable Data (Web Sites)**
- **E-Commerce**
- **News Groups**
- **Internet Telephony (VoIP)**
- **Video Conferencing**
- **Chat Groups**
- **Instant Messengers**
- **Internet Radio**

Types of Computer Networks



LAN, MAN, WAN and PAN



LAN, MAN, WAN and PAN

- Network in small geographical Area (Room, Building or a Campus) is called LAN (Local Area Network)
- Network in a City is call MAN (Metropolitan Area Network)
- Network spread geographically (Country or across Globe) is called WAN (Wide Area Network)
- A personal area **network** (**PAN**) is a computer **network** for interconnecting devices centered on an individual person's workspace. A **PAN** provides data transmission among devices such as computers, smartphones, tablets and personal digital assistants.

LAN, MAN, WAN and PAN

DISTINGUISH BETWEEN LAN,WAN,MAN

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

Internet

- A network of networks is called an internetwork, or simply the internet. It is the largest network in existence on this planet.
- Internet is a world-wide global system of interconnected computer networks.
- Internet uses the standard Internet Protocol (TCP/IP).
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
- For example, a DNS server will resolve a name http://www.xxx.com to a particular IP address to uniquely identify the computer on which this website is hosted.
- Internet is accessible to every user all over the world.

Internet Connectivity

We will discuss how to connect to internet i.e. internet service providers, software and hardware requirements, configuring internet connection etc.

Internet backbone:
- A set of high-speed networks that carry Internet traffic.
- These networks are provided by companies such as AT&T(*American Telephone and Telegraph*), GTE(**General Telephone & Electronics Corporation**), and IBM.

Internet service provider (ISP): A company that provides other companies or individuals with access to the Internet.

NIXI (National Internet Exchange of India):
The **National Internet Exchange of India** (**NIXI**) is a non-profit Company incorporated under Section 25 of the India Companies Act, 1956 (now section 8 under Companies Act 2013) with an objective of facilitating improved internet services in the country.

Connection Types:

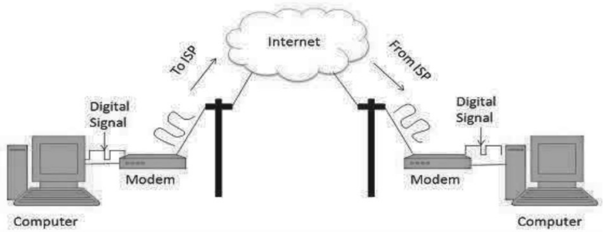
There exist several ways to connect to the internet. Following are these connection types available:

- Dial-up Connection
- ISDN
- DSL
- Cable TV Internet connections
- Satellite Internet connections
- Wireless Internet Connections

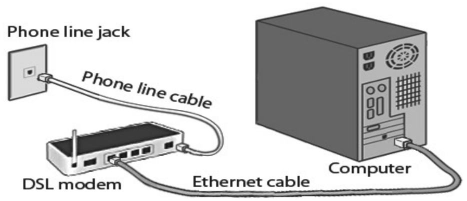
Dial-up Connection:

- Dial-up connection uses telephone line to connect PC to the internet.
- It requires a modem to setup dial-up connection. This modem works as an interface between PC and the telephone line.
- There is also a communication program that instructs the modem to make a call to specific number provided by an ISP.

Dial-up connection uses either of the following protocols:
1.Serial Line Internet Protocol (SLIP)
2.Point to Point Protocol (PPP)
The following diagram shows the accessing internet using modem:



Digital subscriber line (DSL):
- Transmit data over telephone lines.
- DSL service can be delivered simultaneously with wired telephone service on the same telephone line.
- Asymmetric DSL (ADSL), the most commonly used DSL technology for internet access.
- In Symmetric DSL (SDSL) upstream and downstream data rates are same.



ISDN

ISDN is acronym of **Integrated Services Digital Network.** It establishes the connection using the phone lines which carry digital signals instead of analog signals.

There are two techniques to deliver ISDN services:

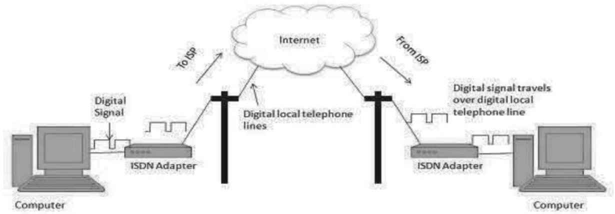
•Basic Rate Interface (BRI)

•Primary Rate Interface (PRI)

Key points:

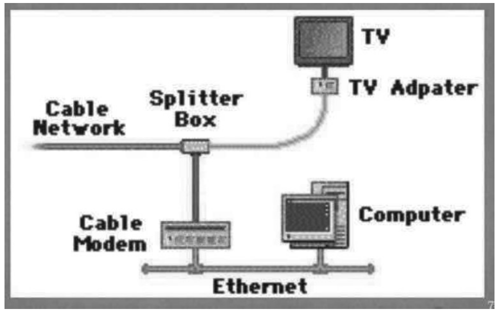
- The BRI configuration provides **two data** or bearer channels at **64 Kbits/sec** speed and one control or delta channel at **16 Kbits/sec**. The ISDN BRI interface is commonly used by smaller organizations or home users or within a local group, limiting a smaller area.

•The Primary Rate Interface or Primary Rate Access, simply called the ISDN PRI connection is used by enterprises and offices. The PRI configuration is based on T-carrier or T1 in the US, Canada and Japan countries consisting of **23 data** or bearer channels and one control or delta channel, with 64kbps speed for a bandwidth of 1.544 M bits/sec.The following diagram shows accessing internet using ISDN connection:



Cable TV Internet Connection:

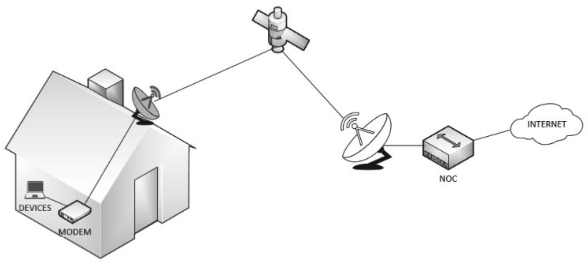
Cable TV Internet connection is provided through Cable TV lines. It uses coaxial cable which is capable of transferring data at much higher speed than common telephone line.



Satellite Internet Connection

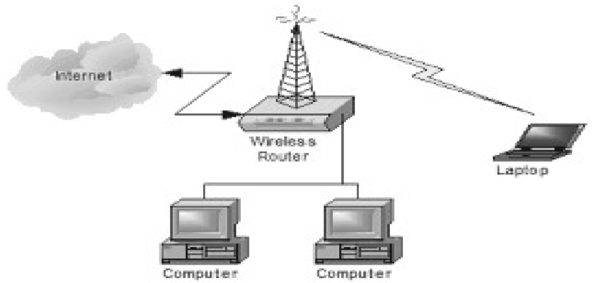
- Satellite Internet connection offers high speed connection to the internet. There are two types of satellite internet connection: one way connection or two way connection.
- In one way connection, we can only download data but if we want to upload, we need a dialup access through ISP over telephone line.
- In two way connection, we can download and upload the data by the satellite. It does not require any dialup connection.

The following diagram shows how internet is accessed using satellite internet connection:



Wireless Internet Connection

Wireless Internet Connection makes use of radio frequency bands to connect to the internet and offers a very high speed. The wireless internet connection can be obtained by either WiFi or Bluetooth.



Computer Networks

Course Code: CSE3003

Ms. Shubhra dwivedi

Assistant Professor

School - SCOPE

VIT-AP Amaravati

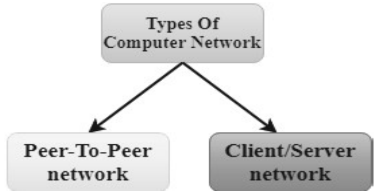
Shubhra.d@vitap.ac.in

Computer Network Architecture

- A Computer Network Architecture is a design in which all computers in a computer network are organized.
- A architecture defines how the computers should get connected to get the maximum advantages of a computer network such as better response time, security, scalability etc.

The two types of network architectures are used:

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

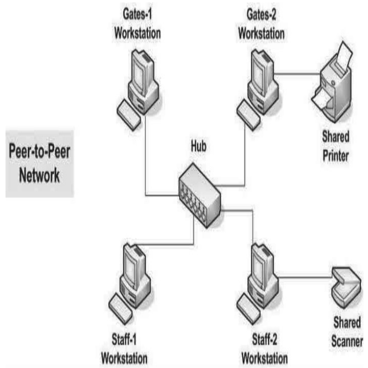


Peer-To-Peer network

- In peer to peer architecture all the computers in a computer network are connected with every computer in the network.
- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Every computer in the network use the same resources as other computers.
- There is no central computer that acts as a server rather all computers acts as a server for the data that is stored in them.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

P2P Networks Example

- Many Linux operating systems are distributed via BitTorrent downloads using P2P transfers. Such examples are Ubuntu, Linux Mint, and Manjaro.
- In Windows 7 and Windows 8.1, when you create an ad-hoc network between two computers, you create a peer-to-peer network between them.



Advantages of a Peer to Peer Architecture

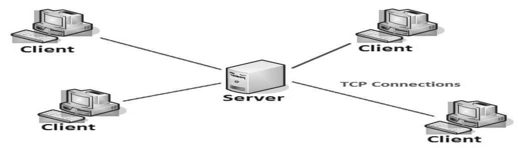
1. Less costly as there is no central server that has to take the backup.
2. In case of a computer failure all other computers in the network are not affected and they will continue to work as same as before the failure.
3. Installation of peer to peer architecture is quite easy as each computer manages itself.

Disadvantages of a Peer to Peer Architecture

1. Each computer has to take the backup rather than a central computer and the security measures are to be taken by all the computers separately.
2. Scalability is a issue in a peer to Peer Architecture as connecting each computer to every computer is a headache on a very large network.

Client/Server network

- In Client Server architecture a central computer acts as a hub and serves all the requests from client computers.
- All the shared data is stored in the server computer which is shared with the client computer when a request is made by the client computer.
- All the communication takes place through the server computer, for example if a client computer wants to share the data with other client computer then it has to send the data to server first and then the server will send the data to other client.



Client/Server network

The client-server architecture on the web:

- A specific set of languages along with a communication standard, exclusively a protocol for the interaction of two systems. The most popular are the HTTP and HTTPS (Hyper Text Transfer Protocol Secure).
- Mechanism and protocol for requesting the required aspects from the server. That could be in any structure of formatted data. Mainly implemented and popular formats are done in XML and JSON.
- Next, the server responds by sending a reply in a structure of formatted data, (usually XML or JSON).

Advantages Of Client/Server network:

1. Data backup is easy and cost effective as there is no need to manage the backup on each computer.
2. Performance is better as the response time is greatly improves because the server is more powerful computer than the other computers in the network.
3. Security is better as unauthorised access are denied by server computer and all the data goes through the server.
4. Scalability is not an issue in this Architecture as large number of computers can be connected with server.

Disadvantages Of Client/Server network:

1. In case of server failure entire network is down.
2. Server maintenance cost is high as the server is the main component in this Architecture
3. Cost is high as the server needs more resources to handle that many client requests and to be able to hold large amount of data.

Networking devices

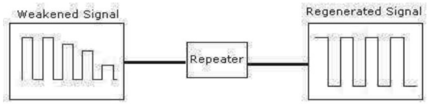
- Repeater
- Hub
- Bridge
- Switch
- Router
- Gateway
- Modem
- Network Interface Card (NIC)

Repeater

- A repeater operates at the physical layer.
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- An important point to be noted about repeaters is that they do not amplify the signal. It means:

When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

- Repeaters cannot connect dissimilar networks.
- They cannot reduce network traffic or congestion.



Properties of Repeater

Properties of Repeater

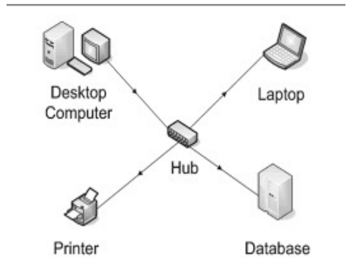
- 2 ports repeater
- Forwarding
- No filtering
- Collision domain(A **collision domain** is a network segment connected by a shared medium or through repeaters where simultaneous data transmissions **collide** with one another.
- Uses at physical layer

Hub

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.

Properties of Hub

- Multiport repeater
- Forwarding
- No filtering
- Collision domain
- Uses at physical layer



Hub

There are two types of the Hub.

- **Passive Hub**: It forwards data signals in the same format in which it receives them. It does not change the data signal in any manner.

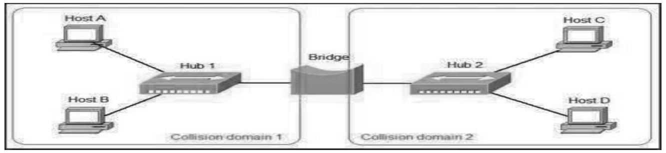
- **Active Hub**: It also works same as the passive Hub works. But before forwarding the data signals, it regenerates them. Due to this added feature, the active Hub is also known as the repeater.

Bridge

- A bridge operates at data link layer.
- A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination.
- It is also used for interconnecting two LANs working on the same protocol.
- It has a single input and single output port, thus making it a 2 port device. Basic functions of the Bridge are the following: -

1. Connecting network architectures working on same protocol.
2. Forwarding
3. Filtering
4. Collision domain

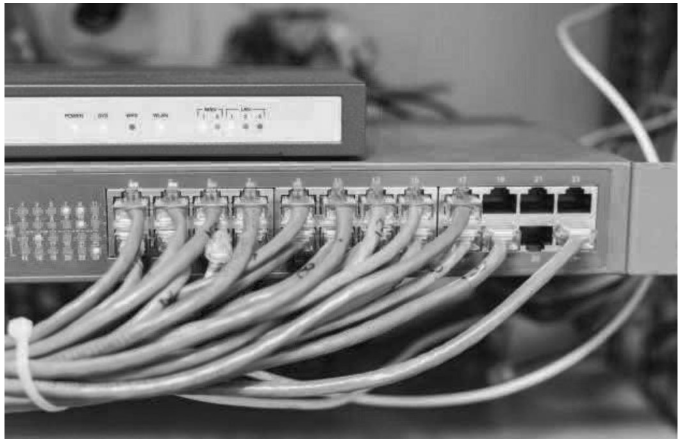
- Bridge data unit protocol (spanning tree protocol(STP)- It is a network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them.)



Switch

- Switch is a network device that connects other devices to Ethernet(**Ethernet is a family of wired computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN).**) networks through twisted pair cables.
- It uses packet switching technique to receive, store and forward data packets on the network.
- The switch maintains a list of network addresses of all the devices connected to it.
- On receiving a packet, it checks the destination address and transmits the packet to the correct port. Before forwarding, the packets are checked for collision and other network errors. The data is transmitted in full duplex mode.
- A switch is a data link layer device.
- Each switch has a dynamic table (called the **MAC address table**) that maps MAC addresses to ports.

Switch



Router

- A router is a network layer hardware device that transmits data from one LAN to another if both networks support the same set of protocols. So a router is typically connected to at least two LANs and the internet service provider (ISP).
- It receives its data in the form of packets, which are data frames with their destination address added.
- Router also strengthens the signals before transmitting them. That is why it is also called repeater.
- A router inspects a given data packet's destination Internet Protocol address (IP address), calculates the best way for it to reach its destination and then forwards it accordingly.
- Hundreds of routers might forward a single packet as it moves from one network to the next on the way to its final destination.
- Static and Dynamic routers are mainly use in CN.

Gateway

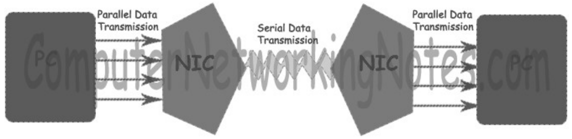
- Gateway is a network device used to connect two or more dissimilar networks. In networking parlance, networks that use different protocols are dissimilar networks.
- A gateway usually is a computer with multiple NICs connected to different networks.
- As networks connect to a different network through gateways, these gateways are usually hosts or end points of the network.
- They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters and can operate at any network layer.
- Gateways are generally more complex than switch or router.
- For basic Internet connections at home, the gateway is the Internet Service Provider that gives you access to the entire Internet.
- **Gateway** uses **packet switching** technique to transmit data from one network to another. In this way it is similar to a **router**, the only difference being router can transmit data only over networks that use same protocols.

Modem

- Modem is a device that enables a computer to send or receive data over telephone or cable lines.
- The data stored on the computer is digital whereas a telephone line or cable wire can transmit only analog data.
- The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices − modulator and demodulator.
- The modulator converts digital data into analog data when the data is being sent by the computer. The demodulator converts analog data signals into digital data when it is being received by the computer.
- For example, a cable Modem and DSL modem are two examples of these types of Modems.
- Modem speed is measured in bps and Kbps, which is the speed the modem can send and receive data.

Network Interface Card (NIC)

- A NIC or Ethernet card is a computer expansion card for connecting to a network (e.g., home network or Internet) using an Ethernet cable with an RJ-45 connector.
- A NIC converts parallel data stream into the serial data stream and the serial data stream into the parallel data stream.
- Typically all modern PCs have the integrated NICs in the motherboards. If additional NICs are required, they are also available as add-on devices separately.



Network Topology

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 different in a same network.

1. **Physical Topology :**

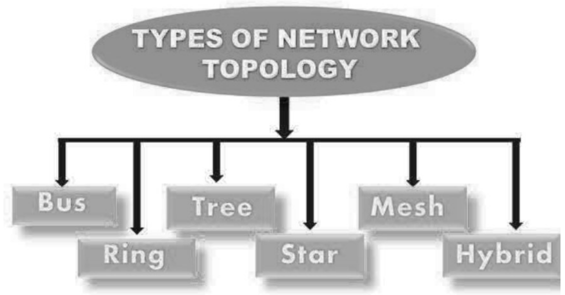
Physical topology indicates arrangement of different elements of a network. It reflects physical layout of devices and cables to a form a connected network.

2. Logical Topology :

Logical Topology reflects arrangement of devices and their communication. It is the transmission of data over physical topology. It is independent of physical topology, irrespective of arrangements of nodes.

Types of Network Topology

1.Bus Topology
2.Star Topology
3.Ring Topology
4.Mesh Topology
5.Tree Topology
6.Hybrid Topology



Bus Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.

Features of Bus Topology

- It transmits data only in one direction.
- Every device is connected to a single cable

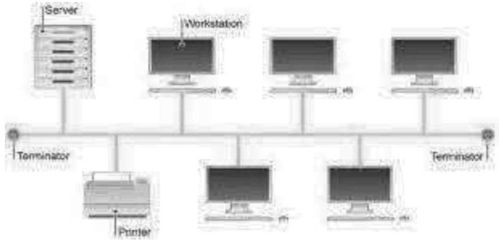
Advantages of Bus Topology

- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Bus Topology

Disadvantages of Bus Topology

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.



Star Topology

All the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

Features of Star Topology

- Every node has its own dedicated connection to the hub.
- Hub acts as a repeater for data flow.
- Can be used with twisted pair, Optical Fibre or coaxial cable.

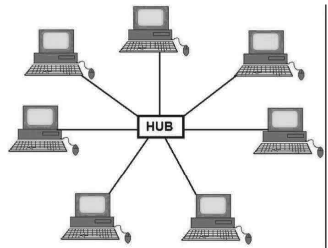
Advantages of Star Topology

- Fast performance with few nodes and low network traffic.
- Only that node is affected which has failed, rest of the nodes can work smoothly.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.

Star Topology

Disadvantages of Star Topology

- Cost of installation is high.
- Expensive to use.
- If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the hub that is it depends on its capacity



Ring Topology

It forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

Features of Ring Topology

- A number of repeaters are used for Ring topology with large number of nodes.
- The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
- In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
- Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Ring Topology

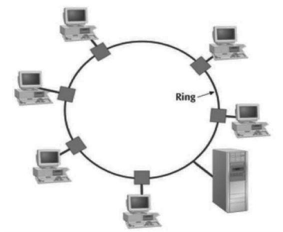
Advantages of Ring Topology

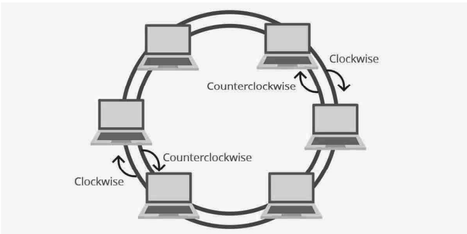
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand

Disadvantages of Ring Topology

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network.

Ring Topology





Uni-directional

Bi-directional

Mesh Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

- Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. We can even have routing logic, to re-configure the failed nodes.

- Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

Mesh Topology

Types of Mesh Topology

- **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
- **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

- Fully connected.
- Robust.
- Not flexible.

Mesh Topology

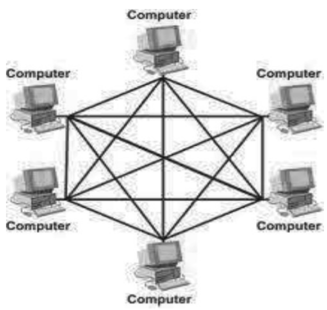
Advantages of Mesh Topology

- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

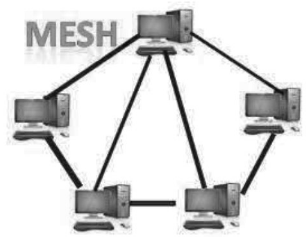
Disadvantages of Mesh Topology

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

Mesh Topology



Full Mesh Topology



Partial Mesh Topology

Tree Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

Features of Tree Topology

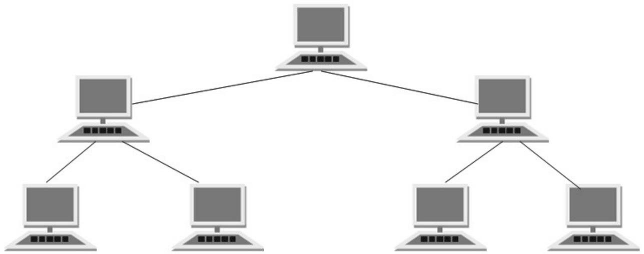
- Ideal if workstations are located in groups.
- Used in Wide Area Network.

Advantages of Tree Topology

- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Tree Topology

Disadvantages of Tree Topology
•Heavily cabled.
•Costly.
•If more nodes are added maintenance is difficult.
•Central hub fails, network fails.



Hybrid Topology

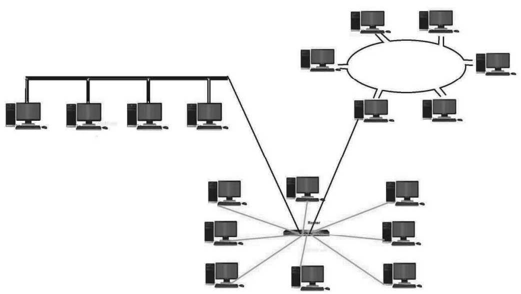
Hybrid topology combines two or more topologies.
• For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

Features of Hybrid Topology
- It is a combination of two or topologies
- Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology
- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

Hybrid Topology

Disadvantages of Hybrid Topology
- Complex in design.
- Costly.



Computer Networks

Course Code: CSE3003

Ms. Shubhra dwivedi
Assistant Professor
School - SCOPE
VIT-AP Amaravati
Shubhra.d@vitap.ac.in

OSI Model

OSI (**Open System Interconnection)** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

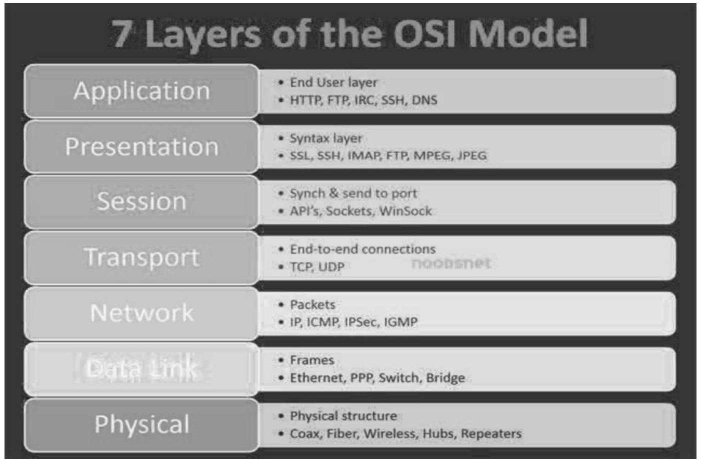
OSI Model

The OSI model is divided into two layers: upper layers and lower layers.

- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.

- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

OSI Model



OSI Model

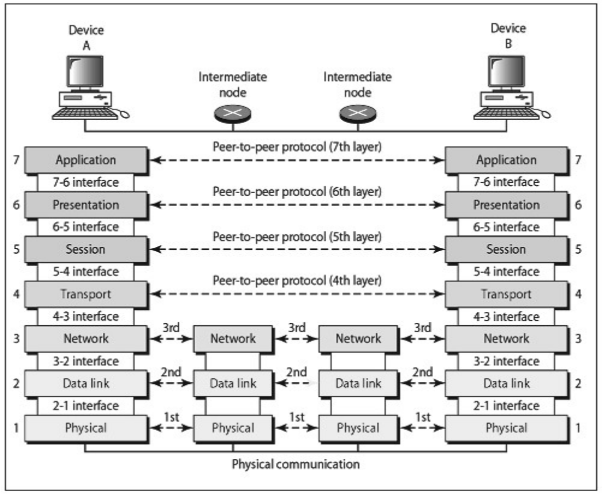
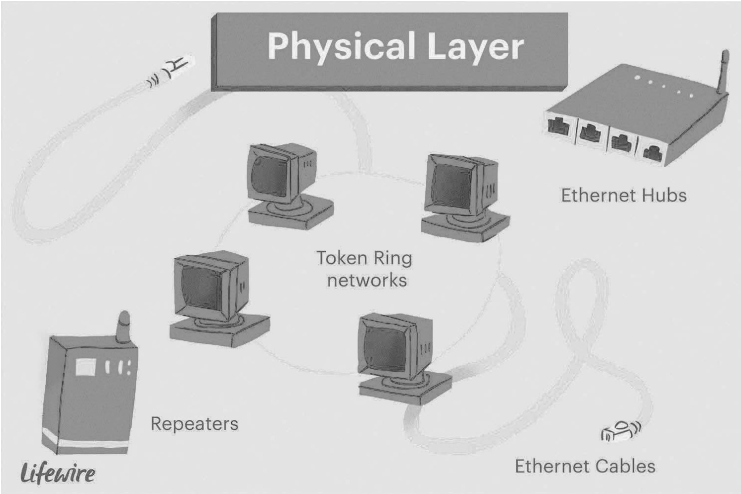
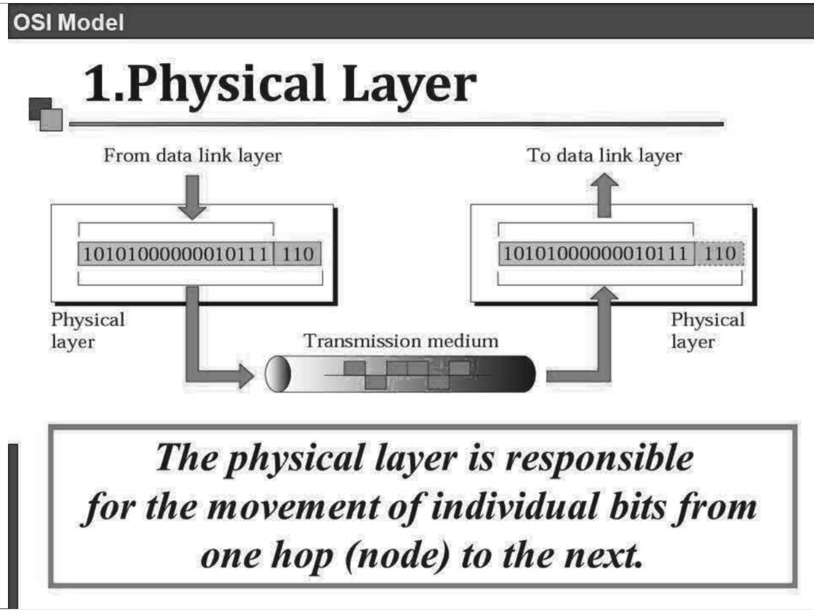


Fig: Communication & Interfaces in the OSI model

OSI Model





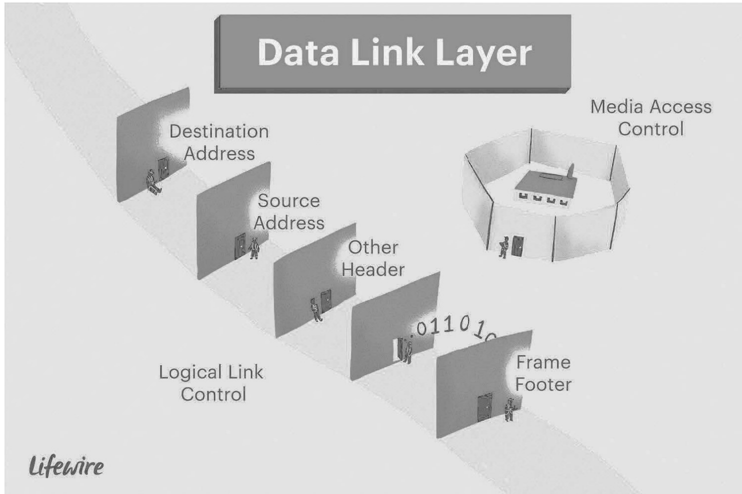
Physical Layer

- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

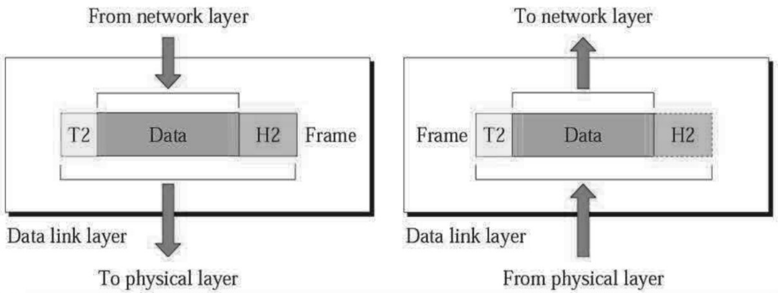
- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting
  the information.

OSI Model



OSI Model

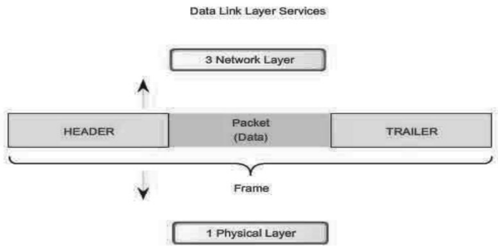
2.Data Link Layer



The data link layer is responsible for moving frames from one hop (node) to the next.

Data Link Layer

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.



Data Link Layer

It contains two sub-layers:

Logical Link Control Layer

- The uppermost sublayer, LLC, multiplexes protocols running at the top of the data link layer, and optionally provides flow control, acknowledgment, and error notification.
- The LLC provides addressing and control of the data link.
- It specifies which mechanisms are to be used for addressing stations over the transmission medium and for controlling the data exchanged between the originator and recipient machines. It identifies the address of the network layer protocol from the header.

Media Access Control Layer

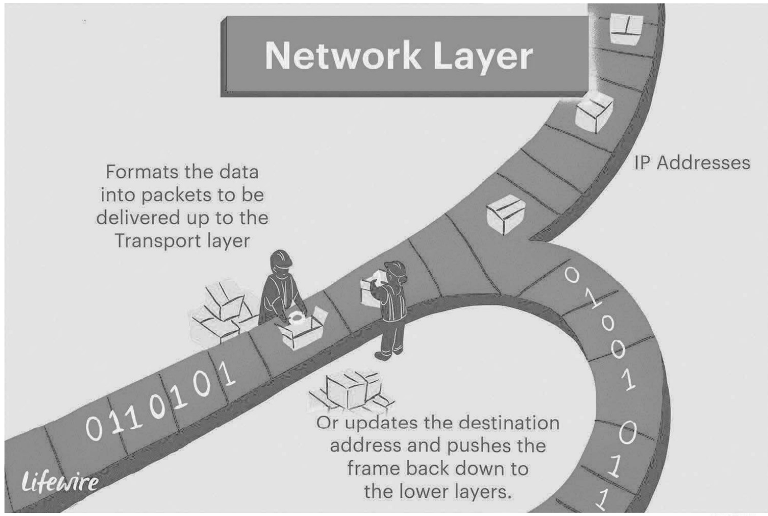
- MAC may refer to the sublayer that determines who is allowed to access the media at any one time (e.g. CSMA/CD). Other times it refers to a frame structure delivered based on MAC addresses inside.

Functionality of Data-link Layer

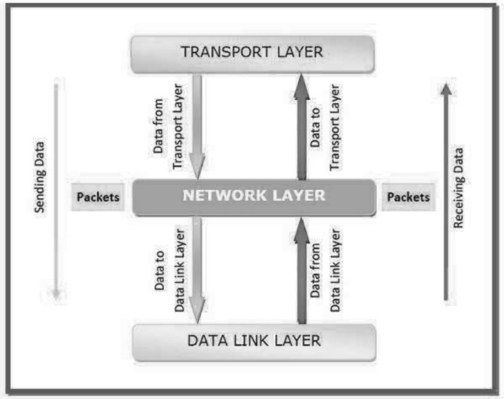
Data link layer does many tasks on behalf of upper layer. These are:

- **Framing:** Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver’ end, data link layer picks up signals from hardware and assembles them into frames.
- **Physical Addressing:** The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.
- **Synchronization:** When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.
- **Error Control:** Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.
- **Flow Control:** Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.

OSI Model



Network layer



Network Layer

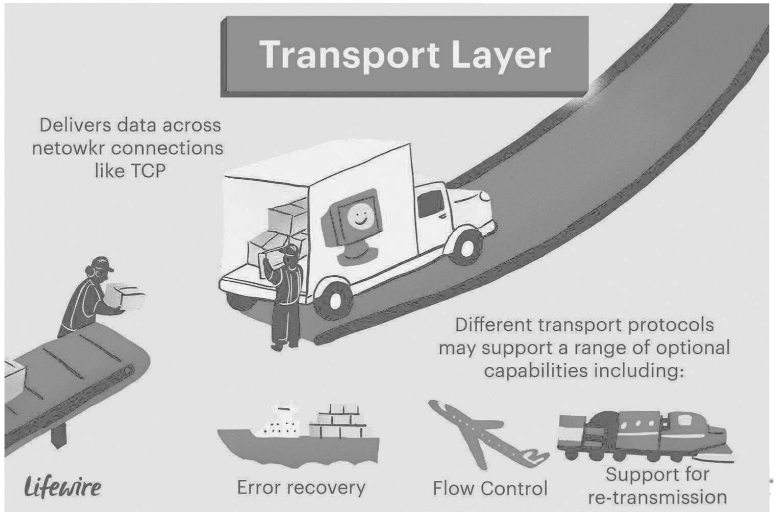
- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Network layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Network Layer

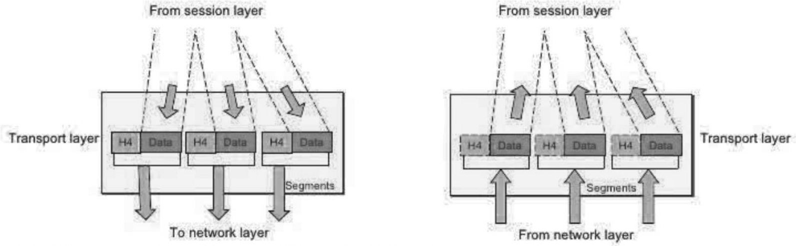
Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the packet. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the data from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

OSI Model



Transport Layer (Process to Process)



- The transport layer is responsible for the delivery of a message from one process to another
- Concerned:
  - Service-point addressing (Port address)
  - Segmentation and reassembly (Sequence number)
  - Connection control (Connectionless or connection oriented)
  - Flow control (end to end)
  - Error Control (Process to Process)

Transport Layer

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

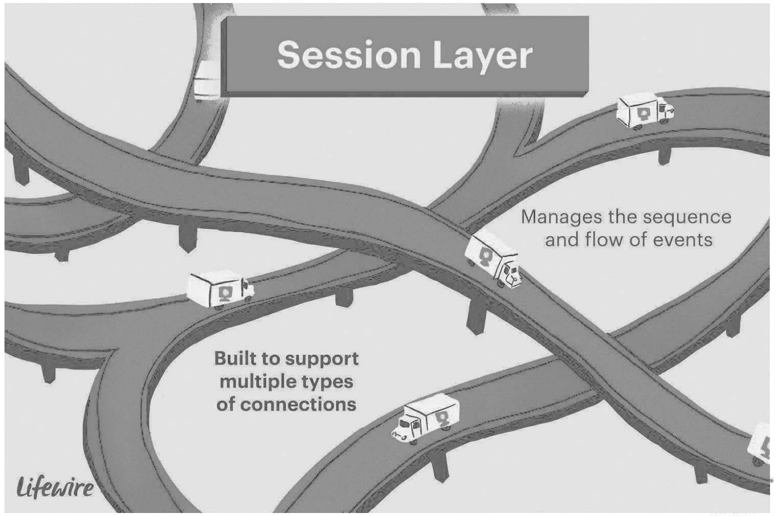
- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a reliable connection between hosts.
- **User Datagram Protocol**
  - It is an unreliable transport protocol.

Transport Layer

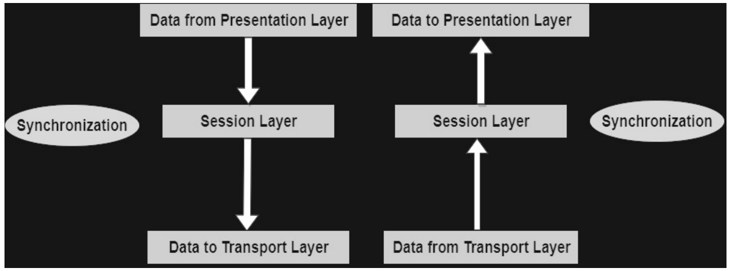
Functions of Transport Layer:

- **Service-point addressing:** The transport layer adds the header that contains the address known as a service-point address or port address.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control.

OSI Model



Session Layer

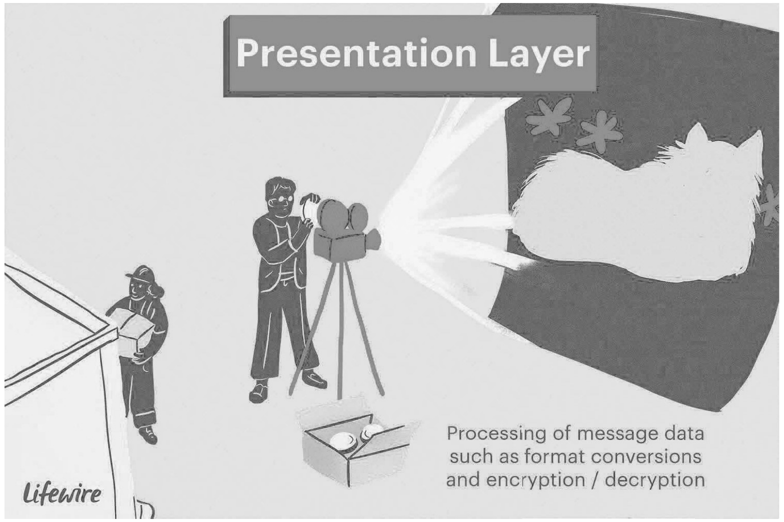


- It is a layer 5 in the OSI model.
- It is responsible for establishing, managing, synchronizing and terminating sessions between end-user application processes.

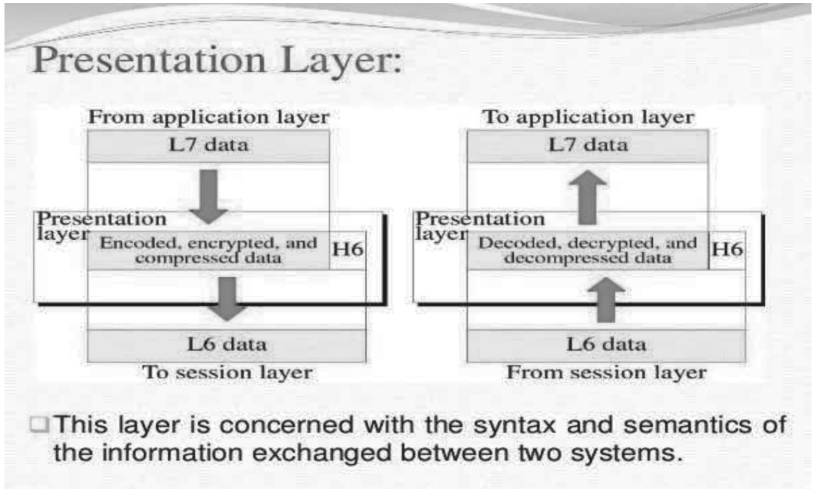
Functions of Session Layer

- **Dialog Control :** This layer allows two systems to start communication with each other in half-duplex or full-duplex.
- **Token Management:** This layer prevents two parties from attempting the same critical operation at the same time.
- **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into stream of data. **Example:** If a system is sending a file of 800 pages, adding checkpoints after every 50 pages is recommended. This ensures that 50 page unit is successfully received and acknowledged. This is beneficial at the time of crash as if a crash happens at page number 110; there is no need to retransmit 1 to100 pages.

OSI Model



Presentation Layer



Presentation Layer

- The primary goal of this layer is to take care of the syntax and semantics of the information exchanged between two communicating systems.
- Presentation layer takes care that the data is sent in such a way that the receiver will understand the information(data) and will be able to use the data.
- Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role translator.
- **Functions of Presentation Layer**

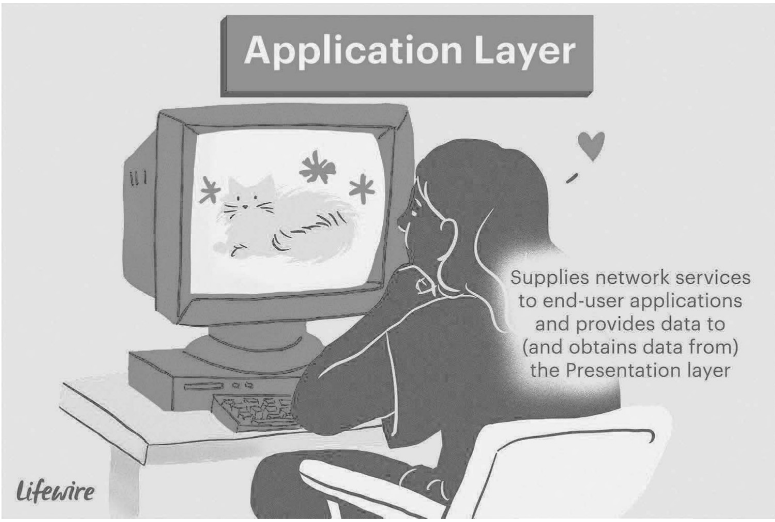
Translation: Before being transmitted, information in the form of characters and numbers should be changed to bit streams. The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods. It translates data between the formats the network requires and the format the computer.

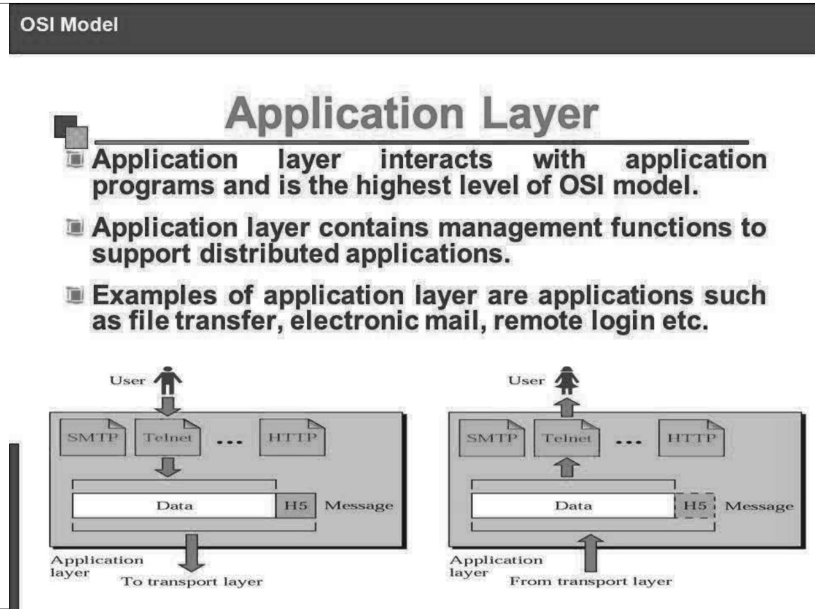
Encryption: It carries out encryption at the transmitter and decryption at the receiver.

Compression: It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of Data compression is to reduce the number of bits to be 0transmitted. It is important in transmitting multimedia such as audio, video, text etc.

VIT AP AMARAVATI

OSI Model





Application Layer

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- This layer provides the network services to the end-users.
- Other Application protocols that are used are: File Transfer Protocol(FTP), Trivial File Transfer Protocol(TFTP), Simple Mail Transfer Protocol(SMTP), TELNET, Domain Name System(DNS) etc.

Functions of Application Layer

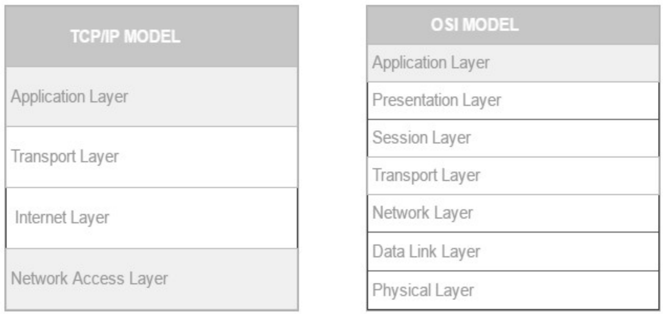
- Mail Services: This layer provides the basis for E-mail forwarding and storage.
- Network Virtual Terminal: It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.
- Directory Services: This layer provides access for global information about various services.
- File Transfer, Access and Management (FTAM): It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.

TCP/IP Protocol stack

- The OSI Model is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.
- TCP/IP model was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

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

The diagrammatic comparison of the TCP/IP and OSI model is as follows :



Application Layer

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI model, which is closest to the end-user. It means the OSI application layer allows users to interact with other software application.

Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model.

Example of the application layer is an application such as file transfer, email, remote login, etc.

The function of the Application Layers are:

- Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
- It allows users to log on to a remote host
- This layer provides various e-mail services
- This application offers distributed database sources and access for global information about various objects and services.

Transport Layer

Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system. It is hosted using single or multiple networks, and also maintains the quality of service functions.

It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation.

The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.
Important functions of Transport Layers:

- It divides the message received from the application layer into segments and numbers them to make a sequence.
- Transport layer makes sure that the message is delivered to the correct process on the destination machine.
- It also makes sure that the entire message arrives without any error else it should be retransmitted.

Internet Layer

An internet layer is a third layer of the TCP/IP model. It is also known as a network layer. The main work of this layer is to send the packets from any network, and any computer still they reach the destination irrespective of the route they take.

The Internet layer offers the functional and procedural method for transferring variable length data sequences from one node to another with the help of various networks.

Layer-management protocols that belong to the network layer are:

- Routing protocols
- Multicast group management
- Network-layer address assignment.

The Network Access Layer

Network Interface Layer is the four-layer of TCP/IP model. This layer is also called a network access layer. It helps you to defines details of how data should be sent using the network.

It also includes how bits should optically be signaled by hardware devices which directly interfaces with a network medium, like coaxial, optical fiber, or twisted-pair cables.

This layer defines how the data should be sent physically through the network. This layer is responsible for the transmission of the data between two devices on the same network.

Here, are some important differences between the OSI and TCP/IP model:

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

Advantages of the TCP/IP model

- It helps you to establish/set up a connection between different types of computers.
- It operates independently of the operating system.
- It supports many routing-protocols.
- It enables the internetworking between the organizations.
- TCP/IP model has a highly scalable client-server architecture.
- It can be operated independently.

Disadvantages of the TCP/IP model

- TCP/IP is a complicated model to set up and manage.
- The shallow/overhead of TCP/IP is higher-than IPX (Internetwork Packet Exchange).
- In this, model the transport layer does not guarantee delivery of packets.
- Replacing protocol in TCP/IP is not easy.
- It has no clear separation from its services, interfaces, and protocols.

Networking in different OS

- Short for network operating system, NOS is the software that allows multiple computers to communicate, share files and hardware devices with one another.
- A NOS is a specialized operating system for a network device such as a router, switch or firewall.
- Earlier versions of Microsoft Windows and Apple operating systems were not designed for single computer usage and not network usage.
- The first network operating system was Novell NetWare, released in 1983. After Netware, other network operating systems were released, including Banyan VINES and Microsoft Windows NT. Some examples of other network operating systems include Windows 2000, Microsoft Windows XP, Sun Solaris, and Linux.

Features of NOS

- Basic operating system features support like protocol support, processor support, hardware detection and multiprocessing support for applications
- Security features like authentication, restrictions, authorizations and access control
- Features for file, Web service, printing and replication
- Directory and name services management
- User management features along with provisions for remote access and system management
- Internetworking features like routing and WAN ports
- Clustering capabilities

Common tasks of NOS

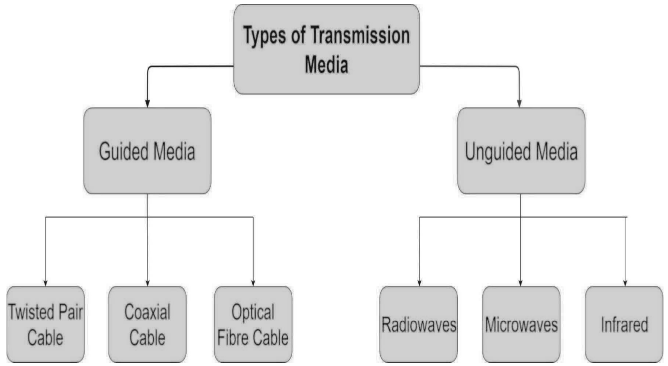
- User administration
- System maintenance activities like backup
- Tasks associated with file management
- Security monitoring on all resources in the network
- Setting priority to print jobs in the network

Computer Networks

Course Code: CSE3003
Module2: Guided and unguided media, analog and digital communication, transmission impairments

Ms. Shubhra dwivedi
Assistant Professor
School - SCOPE
VIT-AP Amaravati
Shubhra.d@vitap.ac.in

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



1. Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.
Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

Unshielded Twisted Pair (UTP):

This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.
Advantages:

- Least expensive
- Easy to install
- High-speed capacity
- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

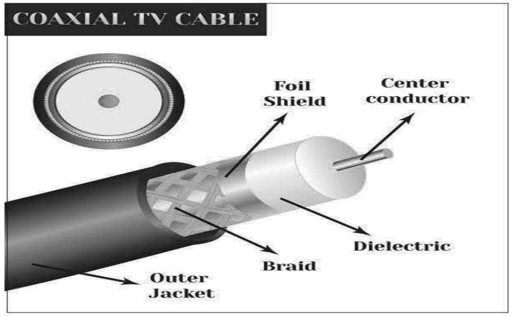
Shielded Twisted Pair (STP):

This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.
Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster
- Comparatively difficult to install and manufacture
- More expensive
- Bulky

(ii) Coaxial Cable –

It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.



Advantages of Coaxial Cables

These are the advantages of coaxial cables −

- Excellent noise immunity
- Signals can travel longer distances at higher speeds, e.g. 1 to 2 Gbps for 1 Km cable
- Can be used for both analog and digital signals
- Inexpensive as compared to fibre optic cables
- Easy to install and maintain

Disadvantages of Coaxial Cables

These are some of the disadvantages of coaxial cables −

- Expensive as compared to twisted pair cables
- Not compatible with twisted pair cables

Optical Fibre

Thin glass or plastic threads used to transmit data using light waves are called optical fibre. Light Emitting Diodes (LEDs) or Laser Diodes (LDs) emit light waves at the source, which is read by a detector at the other end. Optical fibre cable has a bundle of such threads or fibres bundled together in a protective covering. Each fibre is made up of these three layers, starting with the innermost layer −

- Core made of high quality silica glass or plastic
- Cladding made of high quality silica glass or plastic, with a lower refractive index than the core
- Protective outer covering called buffer

Note that both core and cladding are made of similar material. However, as refractive index of the cladding is lower, any stray light wave trying to escape the core is reflected back due to total internal reflection.

Optical fibre is rapidly replacing copper wires in telephone lines, internet communication and even cable TV connections because transmitted data can travel very long distances without weakening. Single node fibre optic cable can have maximum segment length of 2 kms and bandwidth of up to 100 Mbps. Multi-node fibre optic cable can have maximum segment length of 100 kms and bandwidth up to 2 Gbps.

Advantages of Optical Fibre

Optical fibre is fast replacing copper wires because of these advantages that it offers −

- High bandwidth
- Immune to electromagnetic interference
- Suitable for industrial and noisy areas
- Signals carrying data can travel long distances without weakening

Disadvantages of Optical Fibre

Despite long segment lengths and high bandwidth, using optical fibre may not be a viable option for every one due to these disadvantages −

- Optical fibre cables are expensive
- Sophisticated technology required for manufacturing, installing and maintaining optical fibre cables
- Light waves are unidirectional, so two frequencies are required for full duplex transmission

2. Unguided Media:

It is also referred to as Wireless or Unbounded transmission media.No physical medium is required for the transmission of electromagnetic signals.

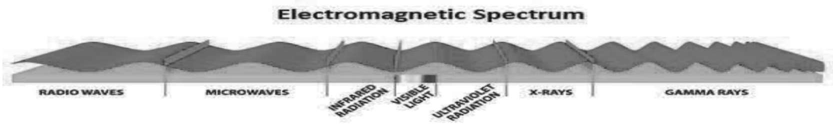
Features:

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 types of Signals transmitted through unguided media:

(i)Infrared

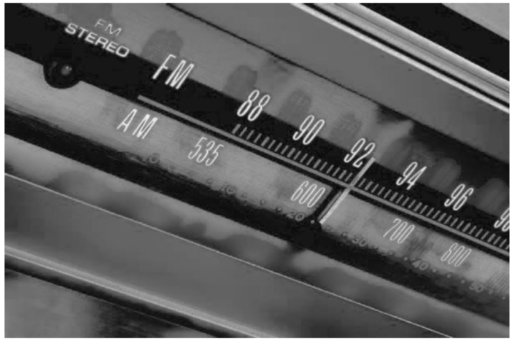
Low frequency infrared waves are used for very short distance communication like TV remote, wireless speakers, automatic doors, hand held devices etc. Infrared signals can propagate within a room but cannot penetrate walls. However, due to such short range, it is considered to be one of the most secure transmission modes. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.



(ii)Radio Wave

Transmission of data using radio frequencies is called radio-wave transmission. We all are familiar with radio channels that broadcast entertainment programs. Radio stations transmit radio waves using transmitters, which are received by the receiver installed in our devices.

Both transmitters and receivers use antennas to radiate or capture radio signals. These radio frequencies can also be used for direct voice communication within the allocated range. This range is usually 10 miles. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radiowaves for transmission.



Advantages of Radio Wave

These are some of the advantages of radio wave transmissions −

- Inexpensive mode of information exchange
- No land needs to be acquired for laying cables
- Installation and maintenance of devices is cheap

Disadvantages of Radio Wave

These are some of the disadvantages of radio wave transmissions −

- Insecure communication medium
- Prone to weather changes like rain, thunderstorms, etc.

(ii) Microwaves

The microwave is the electromagnetic waves with frequency ranging from ‘1 to 300 GHz’. The microwaves are unidirectional in nature and due to which it propagates in line-of-sight mode. In line-of-sight propagation, the source transmitting antenna and the receiving antenna needs to aligned to each other in such a way that they must be facing each other which enables point-to-point transmission.

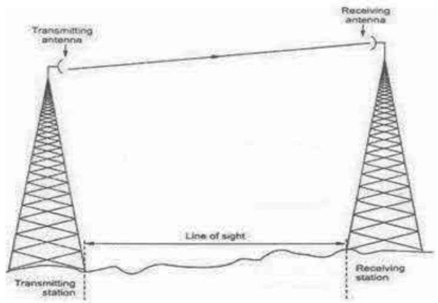
The microwave transmission can be classified into two types:

Terrestrial Microwave Transmission

In terrestrial microwave transmission, the transmitting and receiving antenna both are fixed on the ground and the signal wave is transmitted using the line of sight propagation mode. It is mostly used for telecommunication.

Satellite Microwave Transmission

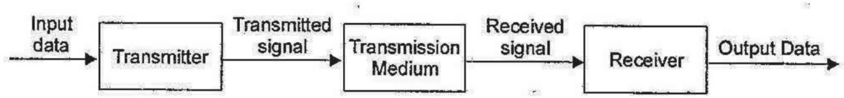
In satellite microwave transmission the electromagnetic wave is transmitted by the source transmitting antenna (earth station) which is received by satellite which amplifies the signal and rebroadcast it to the receiver antenna (earth station). Satellite microwave transmission is mostly used for television, long-distance telecommunication, and global positioning system.



BASIS FOR COMPARISON	GUIDED MEDIA	UNGUIDED MEDIA
Basic	The signal requires a physical path for transmission.	The signal is broadcasted through air or sometimes water.
Alternative name	It is called wired communication or bounded transmission media.	It is called wireless communication or unbounded transmission media.
Direction	It provides direction to signal for travelling.	It does not provide any direction.
Types	Twisted pair cable, coaxial cable and fibre optic cable.	Radio wave, microwave and infrared.

Data Communication

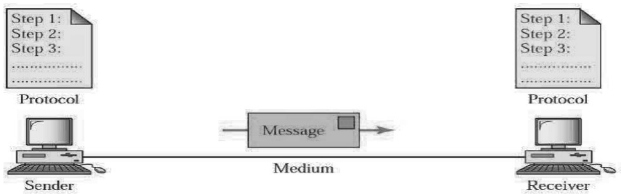
- **Data communication** refers to the exchange of **data** between a source and a receiver via form of **transmission** media such as a wire cable.
- Components of data communication



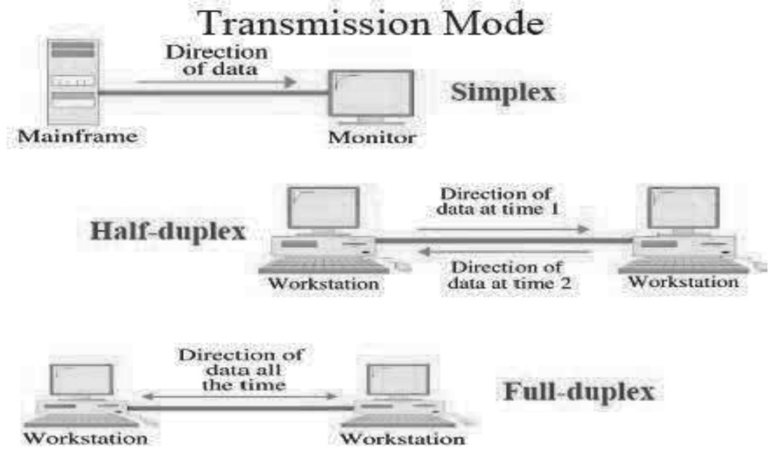
Simple Data Communicative System

Components of Data Communication

- Transmitter
- Receiver
- Medium
  - Guided medium
    - e.g. twisted pair, optical fiber
  - Unguided medium
    - e.g. air, water, vacuum



Transmission Mode

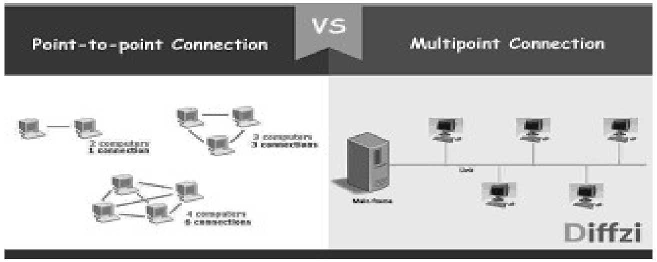


Transmission Mode

- Simplex
  - One direction
    e.g. Television
- Half duplex
  - Either direction, but only one way at a time
    e.g. police radio
- Full duplex
  - Both directions at the same time
    e.g. telephone

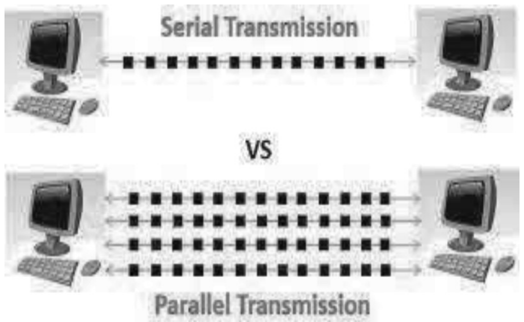
Types of Connection

- Point-to-point
  - Direct link
  - Only 2 devices share link
- Multi-point
  - More than two devices share the link



Methods to Transmit data

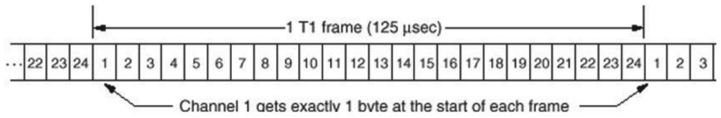
- **Serial** data transmission sends data bits one after another over a single channel.
- **Parallel** data transmission sends multiple data bits at the same time over multiple channels.



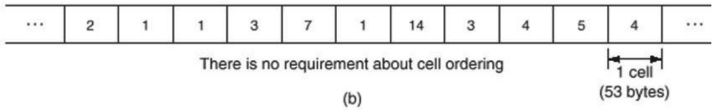
Synchronous and Asynchronous Transmission

- **Synchronous transmissions** are **synchronized** by an external clock.
  e. g. realtime streaming media, for example IP telephony, IP-TV and video conferencing.
- A**synchronous transmissions** are **synchronized** by special signals along the **transmission** medium.
  e. g. file **transfer**, email and the World Wide Web.

Synchronous Vs. Asynchronous Data Transmission



Synchronous Transmission in a T1 Line

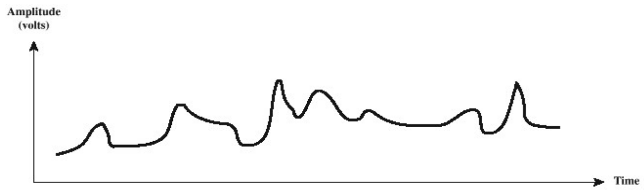


Asynchronous Transmission in an ATM Line

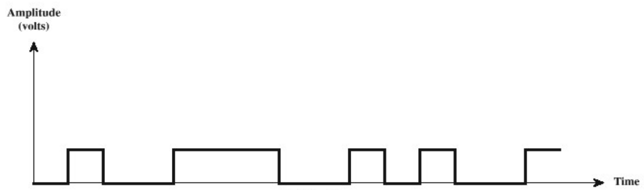
Time domain concepts

- Continuous signal
  - Varies in a smooth way over time
- Discrete signal
  - Maintains a constant level then changes to another constant level
- Periodic signal
  - Pattern repeated over time
- Aperiodic signal
  - Pattern not repeated over time

Continuous & Discrete Signals

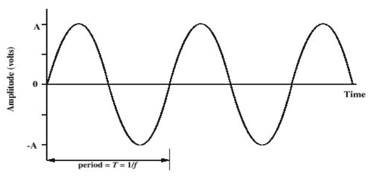


(a) Continuous

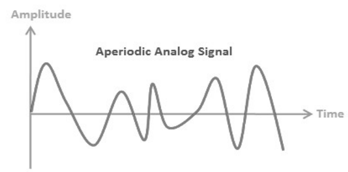


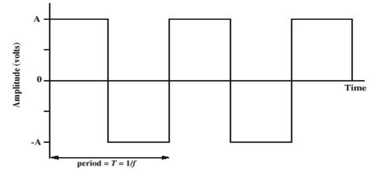
(b) Discrete

Periodic & Aperiodic Signals

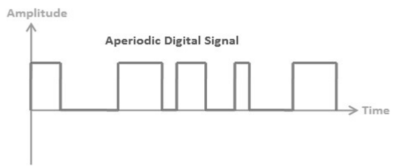


(a) Sine wave





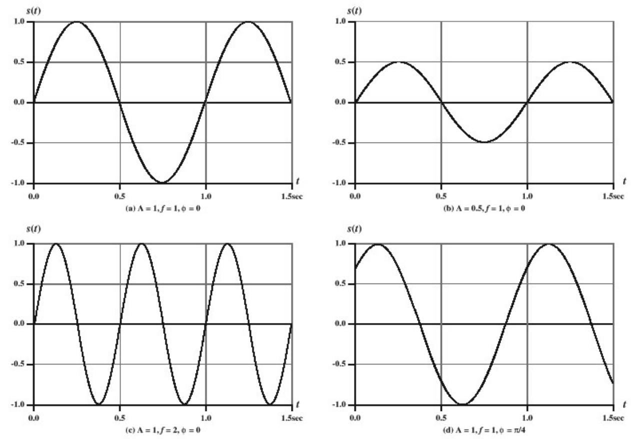
(b) Square wave



Sine Wave

- Peak Amplitude (A)
  - maximum strength of signal
  - volts
- Frequency (f)
  - Rate of change of signal
  - Hertz (Hz) or cycles per second
  - Period = time for one repetition (T)
  - T = 1/f
- Phase (ϕ)
  - Relative position in time

Varying Sine Waves



Wavelength

- Distance occupied by one cycle
- Distance between two points of corresponding phase in two consecutive cycles
- λ
- Assuming signal velocity v
  - $\lambda = vT$
  - $\lambda f = v$
  - c = $3*10^8$ ms^{-1} (speed of light in free space)

Frequency Domain Concepts

- Spectrum
  - range of frequencies contained in signal
- Absolute bandwidth
  - width of spectrum
- Effective bandwidth
  - Often just *bandwidth*
  - Narrow band of frequencies containing most of the energy
- DC Component : Component of zero frequency

When the voltage level in a digital signal is constant for a while, the spectrum creates very low frequencies, called **DC components**, that present **problems** for a system that cannot pass low frequencies.

Bandwidth, Throughput and Data Rate

- **What is Bandwidth?**
  Bandwidth is the measurement of the ability of an electronic communications device or system to send and receive information.

- **What is Throughput?**
  Throughput is the amount of data that enters and goes through a system.

- **What is Data Rate?**
  Data rate is the speed at which data is transferred between two devices, measured in mega bits per second (Mbps or mbps).

Analog and Digital Data Transmission

- Data
  - Entities that convey meaning
- Signals
  - Electric or electromagnetic representations of data
- Transmission
  - Communication of data by propagation and processing of signals

Data

- Analog
  - Continuous values within some interval
  - e.g. sound, video

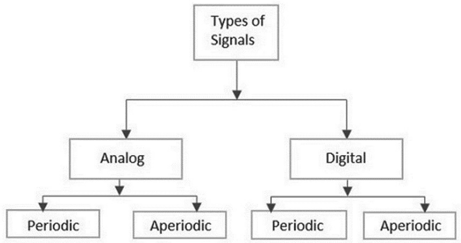
- Digital
  - Discrete values
  - e.g. text, integers

Types of Signals

- Conveying an information by some means such as gestures, sounds, actions, etc., can be termed as signaling. Hence, a signal can be a source of energy which transmits some information. This signal helps to establish a communication between the sender and the receiver.

- An electrical impulse or an electromagnetic wave which travels a distance to convey a message, can be termed as a signal in communication systems.

- Depending on their characteristics, signals are mainly classified into two types: Analog and Digital. Analog and Digital signals are further classified, as shown in the following figure.



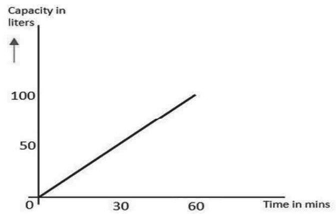
Analog Signal

A continuous time varying signal, which represents a time varying quantity can be termed as an Analog Signal. This signal keeps on varying with respect to time, according to the instantaneous values of the quantity, which represents it.

Example

Let us consider a tap that fills a tank of 100 liters capacity in an hour (6 AM to 7 AM). The portion of filling the tank is varied by the varying time. Which means, after 15 minutes (6:15 AM) the quarter portion of the tank gets filled, whereas at 6:45 AM, 3/4th of the tank is filled.

If we try to plot the varying portions of water in the tank according to the varying time, it would look like the following figure.



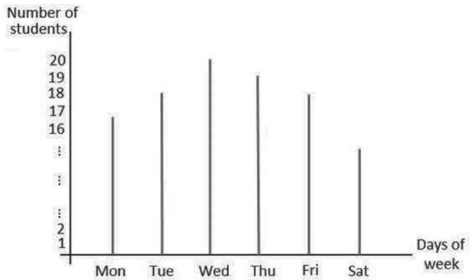
As the result shown in this image varies (increases) according to time, this time varying quantity can be understood as Analog quantity. The signal which represents this condition with an inclined line in the figure, is an Analog Signal. The communication based on analog signals and analog values is called as Analog Communication.

Digital Signal

A signal which is discrete in nature or which is non-continuous in form can be termed as a Digital signal. This signal has individual values, denoted separately, which are not based on the previous values, as if they are derived at that particular instant of time.

Example

Let us consider a classroom having 20 students. If their attendance in a week is plotted, it would look like the following figure.



In this figure, the values are stated separately. For instance, the attendance of the class on Wednesday is 20 whereas on Saturday is 15. These values can be considered individually and separately or discretely, hence they are called as discrete values.

The binary digits which has only 1s and 0s are mostly termed as digital values. Hence, the signals which represent 1s and 0s are also called as digital signals. The communication based on digital signals and digital values is called as Digital Communication.

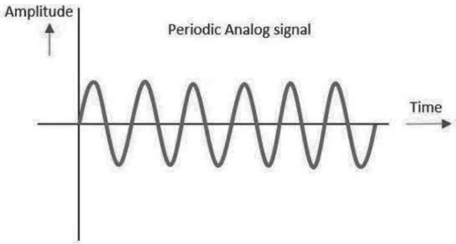
Periodic Signal

Any analog or digital signal, that repeats its pattern over a period of time, is called as a Periodic Signal. This signal has its pattern continued repeatedly and is easy to be assumed or to be calculated.

Example

If we consider a machinery in an industry, the process that takes place one after the other is a continuous procedure. For example, procuring and grading the raw material, processing the material in batches, packing a load of products one after the other, etc., follows a certain procedure repeatedly.

Such a process whether considered analog or digital, can be graphically represented as follows.



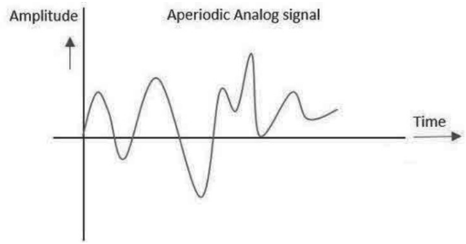
Aperiodic Signal

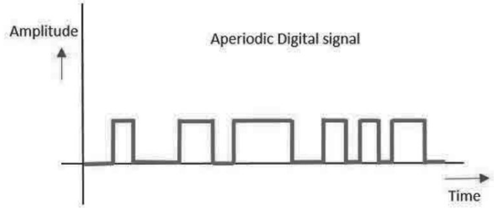
Any analog or digital signal, that doesn't repeat its pattern over a period of time is called as Aperiodic Signal. This signal has its pattern continued but the pattern is not repeated. It is also not so easy to be assumed or to be calculated.

Example

The daily routine of a person, if considered, consists of various types of work which take different time intervals for different tasks. The time interval or the work doesn't continuously repeat. For example, a person will not continuously brush his teeth from morning to night, that too with the same time period.

Such a process whether considered analog or digital, can be graphically represented as follows.

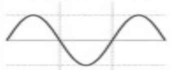




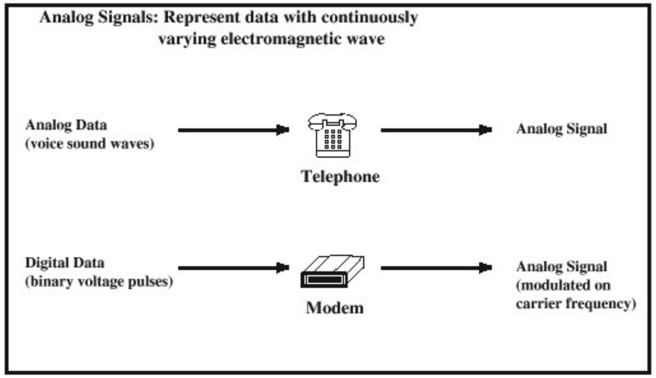
In general, the signals which are used in communication systems are analog in nature, which are transmitted in analog or converted to digital and then transmitted, depending upon the requirement.

Analog and Digital Signals

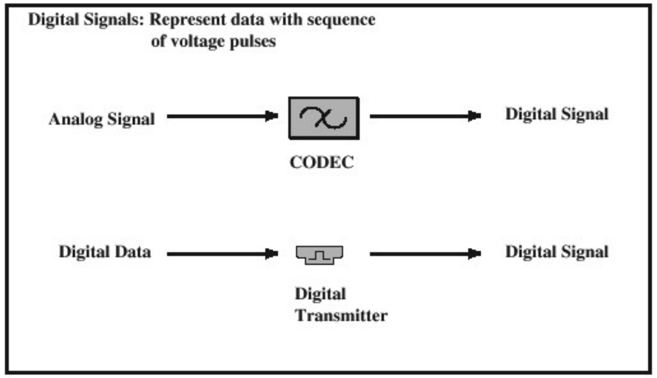
Table 1: Analog vs. Digital Waves Structure and Function

	Analog	Digital
Signal	Analog signals are continuous signals	Digital signals are discrete (binary) signals
Waves	Denoted by sine (curvy) waves 	Denoted by square (block) waves 
Examples	Human voice in air, record player, cassette tape, VHS tapes	Computers, CDs, DVDs, mP3s, digital photos, and cell phones
Uses	Can be used in analog devices only	Used in computing and digital electronics

Analog Signals Carrying Analog and Digital Data

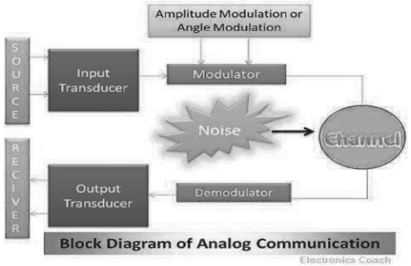


Digital Signals Carrying Analog and Digital Data



1. Analog Communication :

- In analog communication, the data is transferred from transmitter and receiver with the help of analog signal. Analog signal possesses continuous varying amplitude with time. Any type of data such as voice, sound etc. can be transferred through an analog signal.
- Firstly, the data needs to be converted into electrical form. As voice, sound is non-electric in nature, it can be converted into electric form with the help of transducer. Then this signal is passed through the communication channel.
- Analog communication is appropriate for short distance communication. Although, we can also use it for long distance communication with the help of analog modulation technique such as amplitude modulation and angle modulation.



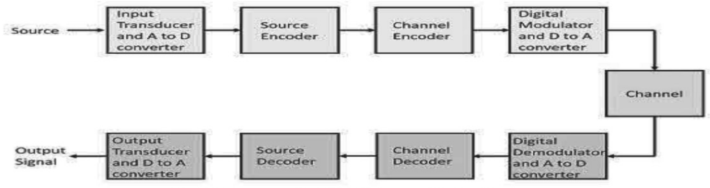
- Modulation is the process of multiplying the low-frequency information signal with a high-frequency carrier signal. Then, this signal is transmitted through the channel. Thus, one modulator is required at the transmitter end, and one demodulator is connected at receiving end for retrieving the original signal.
- The major drawback of Analog Communication is that the strength of the signal starts diminishing with the increase in the distance travelled. Thus, the signal to noise ratio starts getting degrade. Moreover, noise affects the Analog signal more than digital signal because analog signal is a continuous time-varying signal.

2. Digital Communication :

In digital communication, the message signal are transmitted in digital form that means digital communication involves transmission of data or information in digital form.

Model of a Digital Communication:

The overall purpose of these systems are to message or sequence of symbols that are coming out from the source to the destination point at a very high data rate and accuracy as possible. The source and destination points are physically separated in the space and a communication channel is used to connect the source and the destination. In digital communication the digital transmission data can be broken into packets as discrete messages which is not allowed in analog communication. The below figure illustrates the Digital Communication System :



Basic Elements of a Digital Communication System

Following are the sections of the digital communication system.
Source
The source can be an analog signal. Example: A Sound signal

Input Transducer
This is a transducer which takes a physical input and converts it to an electrical signal (Example: microphone). This block also consists of an analog to digital converter where a digital signal is needed for further processes. A digital signal is generally represented by a binary sequence.

Source Encoder
The source encoder compresses the data into minimum number of bits. This process helps in effective utilization of the bandwidth. It removes the redundant bits unnecessary excess bits,i.e.,zeroes.

Channel Encoder
The channel encoder, does the coding for error correction. During the transmission of the signal, due to the noise in the channel, the signal may get altered and hence to avoid this, the channel encoder adds some redundant bits to the transmitted data. These are the error correcting bits.

Digital Modulator
The signal to be transmitted is modulated here by a carrier. The signal is also converted to analog from the digital sequence, in order to make it travel through the channel or medium.

Channel
The channel or a medium, allows the analog signal to transmit from the transmitter end to the receiver end.

Digital Demodulator
This is the first step at the receiver end. The received signal is demodulated as well as converted again from analog to digital. The signal gets reconstructed here.

Channel Decoder
The channel decoder, after detecting the sequence, does some error corrections. The distortions which might occur during the transmission, are corrected by adding some redundant bits. This addition of bits helps in the complete recovery of the original signal.

Source Decoder
The resultant signal is once again digitized by sampling and quantizing so that the pure digital output is obtained without the loss of information. The source decoder recreates the source output.

Output Transducer
This is the last block which converts the signal into the original physical form, which was at the input of the transmitter. It converts the electrical signal into physical output (Example: loud speaker).

Output Signal
This is the output which is produced after the whole process. Example − The sound signal received.

Advantages of Digital Transmission

As the signals are digitized, there are many advantages of digital communication over analog communication, such as −

- The effect of distortion, noise, and interference is much less in digital signals as they are less affected.
- Digital circuits are more reliable.
- Digital circuits are easy to design and cheaper than analog circuits.
- The hardware implementation in digital circuits, is more flexible than analog.
- The occurrence of cross-talk is very rare in digital communication.
- The signal is un-altered as the pulse needs a high disturbance to alter its properties, which is very difficult.
- Signal processing functions such as encryption and compression are employed in digital circuits to maintain the secrecy of the information.
- The probability of error occurrence is reduced by employing error detecting and error correcting codes.
- Spread spectrum technique is used to avoid signal jamming.
- Combining digital signals using Time Division Multiplexing TDM is easier than combining analog signals using Frequency Division Multiplexing FDM.
- The configuring process of digital signals is easier than analog signals.
- Digital signals can be saved and retrieved more conveniently than analog signals.
- Many of the digital circuits have almost common encoding techniques and hence similar devices can be used for a number of purposes.
- The capacity of the channel is effectively utilized by digital signals.

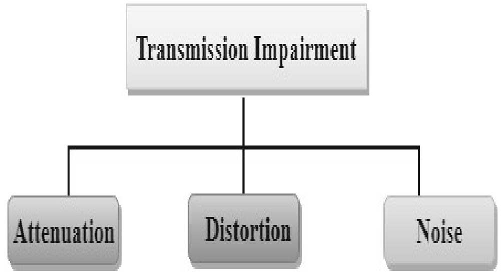
Key Differences Between Analog and Digital Communication

- **Bandwidth:** This factor creates the key difference between Analog and digital communication. Analog signal requires less bandwidth for the transmission while digital signal requires more bandwidth for the transmission.
- **Power Requirement:** Power requirement in case of digital communication is less a compared to Analog communication. Since the bandwidth requirement in digital systems is more thus, they consume less power. And Analog communication system requires less bandwidth thus more power.
- **Fidelity:** Fidelity is a factor which creates a crucial difference between Analog and digital communication. Fidelity is the ability of the receiver which receives the output exactly in coherence with that of transmitted input. Digital communication offers more fidelity as compared to Analog Communication.
- **Hardware Flexibility:** The hardware of analog communication system is not as flexible as digital communication. The equipment used in digital technology are compact in size and consumes less power.
- **Error Rate:** Error rate is another significant difference which separates Analog and Digital Communication. In Analog instruments, there is an error due to parallax or other kinds of observational method.
- **Synchronization:** Digital communication system offers to synchronize which is not effective in analog communication. Thus, synchronization also creates a key difference between Analog and Digital Communication.
- **Cost:** Digital communication equipments are costly and digital signal require more bandwidth for transmission.

TRANSMISSION IMPAIRMENT

- Signals travel through transmission media, which are not perfect.
- Imperfection causes signal impairment.
- Signal at the beginning of the medium is not the same as the signal at the end of the medium.
- What is sent is not what is received.
- Three causes of impairment are attenuation, distortion, and noise

Causes of impairment



Attenuation

- ***Attenuation means a loss of energy.***
- ***When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium.***
- ***A wire carrying electric signals gets warm, if not hot, after a while.***
- ***Electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.***

Attenuation

- Attenuation: signal strength falls off with distance.
- Depends on medium
  - For guided media, the attenuation is generally exponential and thus is typically expressed as a constant number of decibels per unit distance.
  - For unguided media, attenuation is a more complex function of distance and the makeup of the atmosphere.
- Three considerations for the transmission engineer:
  1. A received signal must have **sufficient strength** so that the electronic circuitry in the receiver can detect the signal.
  2. The signal must maintain a level **sufficiently higher than noise** to be received without error.

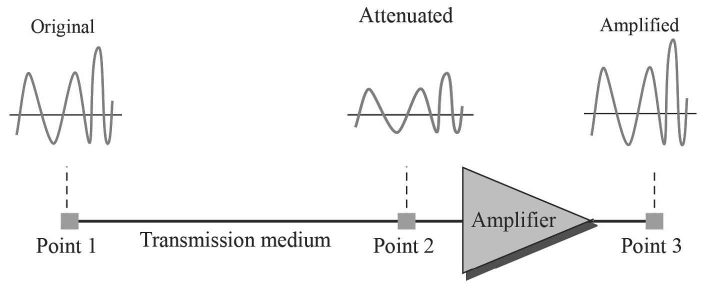
These two problems are dealt with by the use of amplifiers or repeaters.

Attenuation Distortion

3. Attenuation is often an increasing function of frequency. This leads to attenuation distortion:
   - some frequency components are attenuated more than other frequency components.

Attenuation distortion is particularly noticeable for analog signals: the attenuation varies as a function of frequency, therefore the received signal is distorted, reducing intelligibility.

Figure 3.27: ***Attenuation and amplification***



Example

Suppose a signal travels through a transmission medium and its power is reduced to one half. This means that P2 = 0.5 P1. In this case, the attenuation (loss of power) can be calculated as

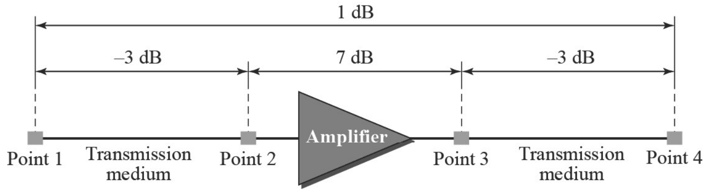
$$\boxed{10 \log_{10} P_2/P_1 = 10 \log_{10} (0.5\, P_1)/P_1 = 10 \log_{10} 0.5 = 10 \times (-0.3) = -3 \text{ dB.}}$$

A loss of 3 dB (−3 dB) is equivalent to losing one-half the power.

Example

A signal travels through an amplifier, and its power is increased 10 times. This means that $P_2 = 10P_1$. In this case, the amplification (gain of power) can be calculated as

$$10 \log_{10} \frac{P_2}{P_1} = 10 \log_{10} \frac{10P_1}{P_1} = 10 \log_{10} 10 = 10(1) = 10 \text{ dB}$$



Example

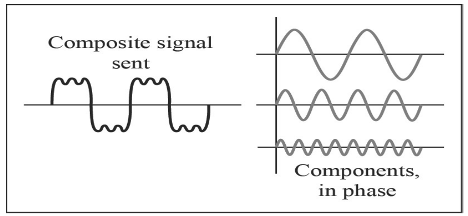
One reason that engineers use the decibel to measure the changes in the strength of a signal is that decibel numbers can be added (or subtracted) when we are measuring several points (cascading) instead of just two. In previous slide, a signal travels from point 1 to point 4. The signal is attenuated by the time it reaches point 2. Between points 2 and 3, the signal is amplified. Again, between points 3 and 4, the signal is attenuated. We can find the resultant decibel value for the signal just by adding the decibel measurements between each set of points. In this case, the decibel value can be calculated as

$$\mathbf{dB = -3 + 7 - 3 = +1}$$

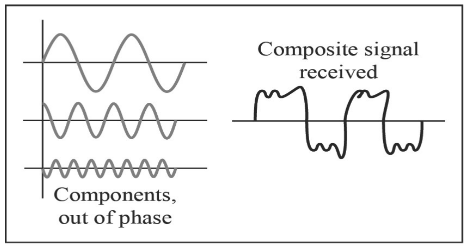
Distortion

- Distortion means that the signal changes its form or shape.
- Distortion can occur in a composite signal made of different frequencies.
- Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination.
- Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration.

Distortion



At the sender



At the receiver

Delay distortion-digital

- Some of the signal components of one bit position will spill over into other bit positions,
- cause intersymbol interference,
- major limitation to maximum bit rate over a transmission channel.

Noise

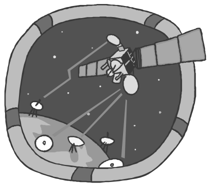
unwanted signals inserted between transmitter and receiver

is the major limiting factor in communications system performance

Categories of Noise

Thermal noise

- due to thermal agitation of electrons
- uniformly distributed across bandwidths
- Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter.
- referred to as white noise



Intermodulation noise

- produced by nonlinearities in the transmitter, receiver, and/or intervening transmission medium
- effect is to produce signals at a frequency that is the sum or difference of the two original frequencies

Categories of Noise

Impulse Noise:

- caused by external electromagnetic interferences
- noncontinuous, consisting of irregular pulses or spikes
- short duration and high amplitude
- minor annoyance for analog signals but a major source of error in digital data

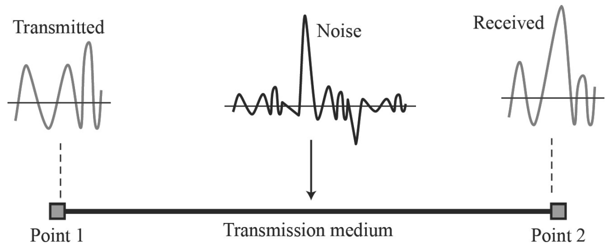
Crosstalk:

- a signal from one line is picked up by another
- can occur by electrical coupling between nearby twisted pairs or when microwave antennas pick up unwanted signals

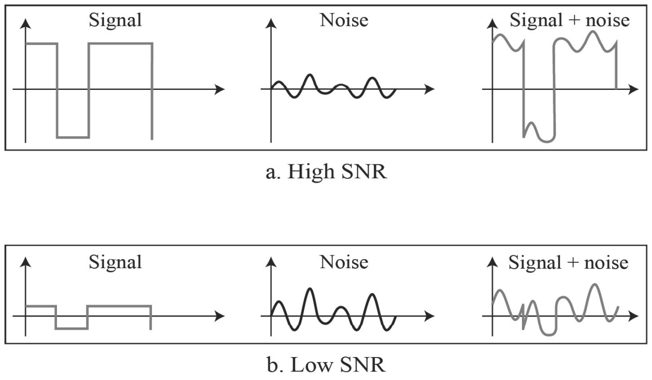
Induced noise

- **Induced noise** comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna.

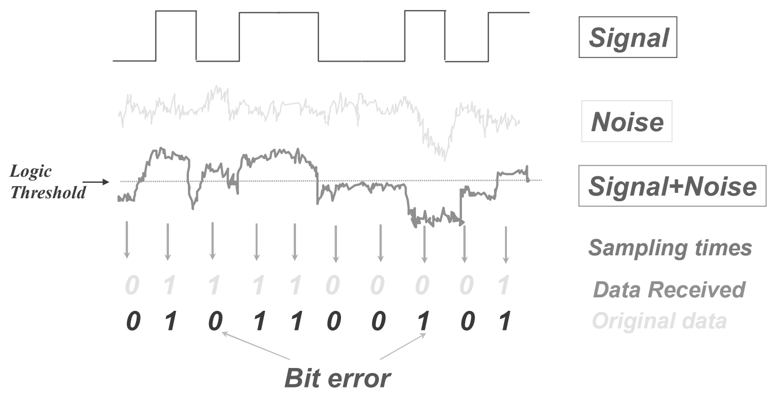
Noise



Two cases of SNR: a high SNR and a low SNR



Effect of noise



Signal to Noise Ratio (SNR)

- **Noise effects**
  - distorts a transmitted signal
  - attenuates a transmitted signal
- **signal-to-noise ratio to quantify noise: S/N**
- **usually expressed using dB**

$$SNR_{dB} = 10 \log_{10} \frac{S}{N}$$

S= average signal power

N= noise power

Example

The power of a signal is 10 mW and the power of the noise is 1 μW; what are the values of SNR and SNR_{dB}?

Solution

The values of SNR and SNR_{dB} can be calculated as follows:

$$SNR = (10{,}000\ \mu w) / (1\ \mu w) = 10{,}000 \quad SNR_{dB} = 10 \log_{10} 10{,}000 = 10 \log_{10} 10^4 = 40$$

An SNR greater than 40 dB is considered excellent, whereas a SNR below 15 dB may result in a slow, unreliable connection

Channel Capacity

- The maximum rate at which data can be transmitted over a given communication path, or channel, under given conditions.
- 4 related factors: **data rate, bandwidth, noise, error rate**
- Our goal: get as high a data rate as possible at a particular limit of error rate for a given bandwidth.
- The main constraint on achieving this efficiency is noise.

Channel Capacity (cont.)

- Data rate
  - In bits per second
  - Rate at which data can be communicated
- Bandwidth
  - In cycles per second of Hertz
  - Constrained by transmitter and medium
- Noise
  - Average level of noise over the communication path
- Error rate
  - Error: 1 becomes 0; 0 becomes 1
  - At a given noise level, higher data rate ⇒ higher error rate

DATA RATE LIMITS

A very important consideration in data communications is how fast we can send data, in bits per second. over a channel. Data rate depends on three factors:

- 1. The bandwidth available
- 2. The level of the signals we use
- 3. The quality of the channel (the level of noise)
- Two theoretical formulas were developed to calculate the data rate: one by Nyquist for a noiseless channel, another by Shannon for a noisy channel.

Noiseless Channel: Nyquist Bit Rate

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

$$\textbf{BitRate} = \textbf{2 x bandwidth x} \log_2 L$$

In this formula, bandwidth is the bandwidth of the channel, L is the number of signal levels used to represent data, and BitRate is the bit rate in bits per second.

Units of Bit Rate

- 1 bps
- 1 kbps = 1000 bps
- 1 Mbps = 1,000,000 bps
- 1 Gbps = 1,000,000,000 bps
- 1 Tbps = 1,000,000,000,000 bps

Time units

milli-	m	$0.001 = 1 \times 10^{-3}$
micro-	μ^*	$0.000\,001 = 1 \times 10^{-6}$
nano-	n	$0.000\,000\,001 = 1 \times 10^{-9}$

Example

Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as

$$\text{BitRate} = 2 \times 3000 \times \log_2 2 = 6000 \text{ bps}$$

Example

Consider the same noiseless channel transmitting a signal with four signal levels (for each level, we send 2 bits). The maximum bit rate can be calculated as

$$\text{BitRate} = 2 \times 3000 \times \log_2 4 = 12{,}000 \text{ bps}$$

Example

We need to send 265 kbps over a noiseless channel with a bandwidth of 20 kHz. How many signal levels do we need?

Solution

We can use the Nyquist formula as shown:

$$265{,}000 = 2 \times 20{,}000 \times \log_2 L \longrightarrow \log_2 L = 6.625 \longrightarrow L = 2^{6.625} = 98.7 \text{ levels}$$

Since this result is not a power of 2, we need to either increase the number of levels or reduce the bit rate. If we have 128 levels, the bit rate is 280 kbps. If we have 64 levels, the bit rate is 240 kbps.

Noisy Channel: Shannon Capacity

In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944,Claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel:

$$\textit{Capacity} = \textit{bandwidth} * \log_2 (1 + \textit{SNR})$$

In this formula, bandwidth is the bandwidth of the channel, SNR is the signal-tonoise ratio, and capacity is the capacity of the channel in bits per second. Note that in the Shannon formula there is no indication of the signal level, which means that no matter how many levels we have, we cannot achieve a data rate higher than the capacity of the channel. In other words, the formula defines a characteristic of the channel, not the method of transmission.

Example

Consider an extremely noisy channel in which the value of the signal-to-noise ratio is almost zero. In other words, the noise is so strong that the signal is faint. For this channel the capacity C is calculated as

$$C = B \log_2 (1 + \text{SNR}) = B \log_2(1 + 0) = B \log_2 1 = B \times 0 = 0$$

This means that the capacity of this channel is zero regardless of the bandwidth. In other words, we cannot receive any data through this channel.

Example

We can calculate the theoretical highest bit rate of a regular telephone line. A telephone line normally has a bandwidth of 3000 Hz (300 to 3300 Hz) assigned for data communications. The signal-to-noise ratio is usually 3162. For this channel the capacity is calculated as

$$C = B \log_2 (1 + \text{SNR}) = 3000 \log_2(1 + 3162) = 3000 \times 11.62 = 34{,}860 \text{ bps}$$

This means that the highest bit rate for a telephone line is 34.860 kbps. If we want to send data faster than this, we can either increase the bandwidth of the line or improve the signal-to-noise ratio.

Example

The signal-to-noise ratio is often given in decibels. Assume that $\text{SNR}_{\text{dB}} = 36$ and the channel bandwidth is 2 MHz. The theoretical channel capacity can be calculated as

$$\text{SNR}_{\text{dB}} = 10 \log_{10}\text{SNR} \longrightarrow \text{SNR} = 10^{\text{SNR}_{\text{dB}}/10} \longrightarrow \text{SNR} = 10^{3.6} = 3981$$

$$C = B \log_2(1 + \text{SNR}) = 2 \times 10^6 \times \log_2 3982 = 24 \text{ Mbps}$$

When the SNR is very high, we can assume that SNR + 1 is almost the same as SNR. In these cases, the theoretical channel capacity can be simplified

$C = B * \text{SNR}_{\text{dB}} / \mathbf{3}$

$$C = 2 \text{ MHz} \times (36 / 3) = 24 \text{ Mbps}$$

For example, we can calculate the theoretical capacity of the previous example as

Example

We have a channel with a 1-MHz bandwidth. The SNR for this channel is 63. What are the appropriate bit rate and signal level?

Solution

First, we use the Shannon formula to find the upper limit.

$$C = B \log_2(1 + \text{SNR}) = 10^6 \log_2(1 + 63) = 10^6 \log_2 64 = 6 \text{ Mbps}$$

The Shannon formula gives us 6 Mbps, the upper limit. For better performance we choose something lower, 4 Mbps. Then we use the Nyquist formula to find the number of signal levels.

$$4 \text{ Mbps} = 2 \times 1 \text{ MHz} \times \log_2 L \longrightarrow L = 4$$

PERFORMANCE

Up to now, we have discussed the tools of transmitting data (signals) over a network and how the data behave. One important issue in networking is the performance of the network—how good is it? In this section, we introduce terms that we need for future chapters.

Bandwidth

One characteristic that measures network performance is bandwidth. However, the term can be used in two different contexts with two different measuring values: bandwidth in hertz and bandwidth in bits per second..

Bandwidth in Hertz

Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass. For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

Bandwidth in Bits per Seconds

The term bandwidth can also refer to the number of bits per second that a channel, a link, or even a network can transmit. For example, one can say the bandwidth of a Fast Ethernet network (or the links in this network) is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

Relationship

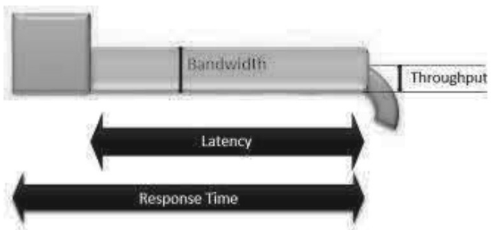
There is an explicit relationship between the bandwidth in hertz and bandwidth in bits per seconds. Basically, an increase in bandwidth in hertz means an increase in bandwidth in bits per second.

Example

The bandwidth of a subscriber line is 4 kHz for voice or data.
The bandwidth of this line for data transmission
can be up to 56,000 bps using a sophisticated modem to change the digital signal to analog.

If the telephone company improves the quality of the line and increases the bandwidth to 8 kHz, we can send 112,000 bps by using the same technology.

Throughput



The throughput is a measure of how fast we can actually send data through a network. Although, at first glance, bandwidth in bits per second and throughput seem the same, they are different. A link may have a bandwidth of B bps, but we can only send T bps through this link with T always less than B.

For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.

Example

A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution

We can calculate the throughput as

$$\text{Throughput} = (12{,}000 \times 10{,}000) / 60 = 2 \text{ Mbps}$$

The throughput is almost one-fifth of the bandwidth in this case.

Latency(delay)

The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. We can say that latency is made of four components: propagation time, transmission time, queuing time and processing delay.

$$\textbf{Latency} = \textbf{propagation time} + \textbf{transmission time} + \textbf{queuing time} + \textbf{processing delay}$$

Propagation Time

Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.

$$Propagation\ time = \frac{Distance}{Propagation\ speed}$$

The propagation speed of electromagnetic signals depends on the medium and on the frequency of the signaL For example, in a vacuum, light is propagated with a speed $of\ 3 * 10^8\ mfs$. It is lower in air; it is much lower in cable.

Transmission Time

In data communications we don't send just 1 bit, we send a message. The first bit may take a time equal to the propagation time to reach its destination; the last bit also may take the same amount of time. However, there is a time between the first bit leaving the sender and the last bit arriving at the receiver. The first bit leaves earlier and arrives earlier; the last bit leaves later and arrives later. The time required for transmission of a message depends on the size of the message and the bandwidth of the channel.

$$Transmission\ time\ = \frac{Message\ size}{Bandwidth}$$

Queuing Time

The third component in latency is the queuing time, the time needed for each intermediate or end device to hold the message before it can be processed. The queuing time is not a fixed factor; it changes with the load imposed on the network. When there is heavy traffic on the network, the queuing time increases. An intermediate device, such as a router, queues the arrived messages and processes them one by one. If there are many messages, each message will have to wait.

Example

What is the propagation time if the distance between the two points is 12,000 km? Assume the propagation speed to be 2.4×10^8 m/s in cable.

Solution

We can calculate the propagation time as

$$\text{Propagation tIme} = \frac{12000 \text{ x } 1000}{2.4\text{X}10^8} = 50 \text{ ms}$$

The example shows that a bit can go over the Atlantic Ocean in only 50 ms if there is a direct cable between the source and the destination.

Example

What are the propagation time and the transmission time for a 2.5-KB (kilobyte) message if the bandwidth of the network is 1 Gbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4×10^8 m/s.

Solution

We can calculate the propagation and transmission time as

$$\text{Propagation time} = (12{,}000 \times 1000) / (2.4 \times 10^8) = 50 \text{ ms}$$

$$\text{Transmission time} = (2500 \times 8) / 10^9 = 0.020 \text{ ms}$$

Note that in this case, because the message is short and the bandwidth is high, the dominant factor is the propagation time, not the transmission time.

Example

What are the propagation time and the transmission time for a 5-MB (megabyte) message (an image) if the bandwidth of the network is 1 Mbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4×10^8 m/s.

Solution

We can calculate the propagation and transmission times as

$$\text{Propagation time} = (12{,}000 \times 1000) / (2.4 \times 10^8) = 50 \text{ ms}$$

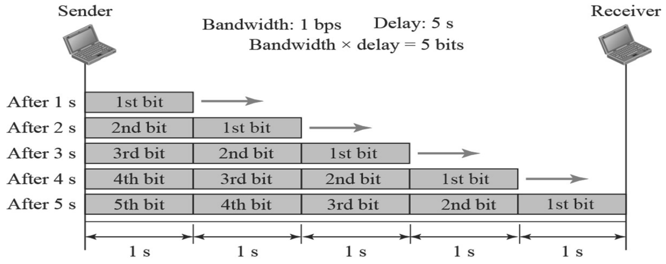
$$\text{Transmission time} = (5{,}000{,}000 \times 8) / 10^6 = 40 \text{ s}$$

We can calculate the propagation and transmission times as

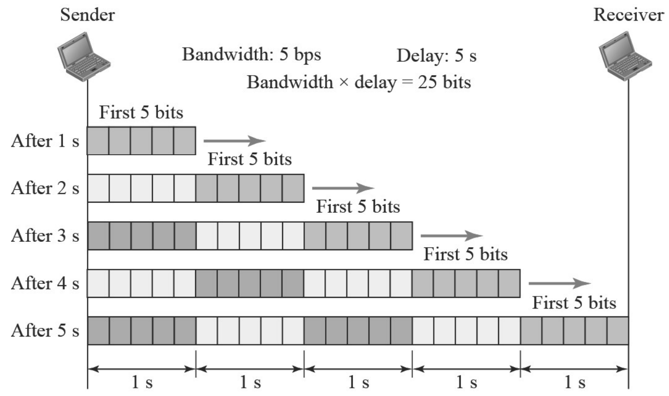
Bandwidth-Delay Product

Bandwidth and delay are two performance metrics of a link.

Filling the links with bits for Case 1:Let us assume that we have a link with a bandwidth of 1 bps (unrealistic, but good for demonstration purposes). We also assume that the delay of the link is 5 s (also unrealistic). We want to see what the bandwidth-delay product means in this case. Looking at figure, we can say that this product 1 x 5 is the maximum number of bits that can fill the link. There can be no more than 5 bits at any time on the link.



Filling the pipe with bits for Case 2

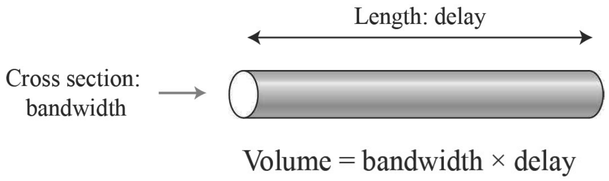


The bandwidth-delay product defines the number of bits that can fill the link.

Concept of bandwidth-delay product

Example

We can think about the link between two points as a pipe. The cross section of the pipe represents the bandwidth, and the length of the pipe represents the delay. We can say the volume of the pipe defines the bandwidth-delay product, as shown in Figure 3.34.



Fundamentals of Computer Networks

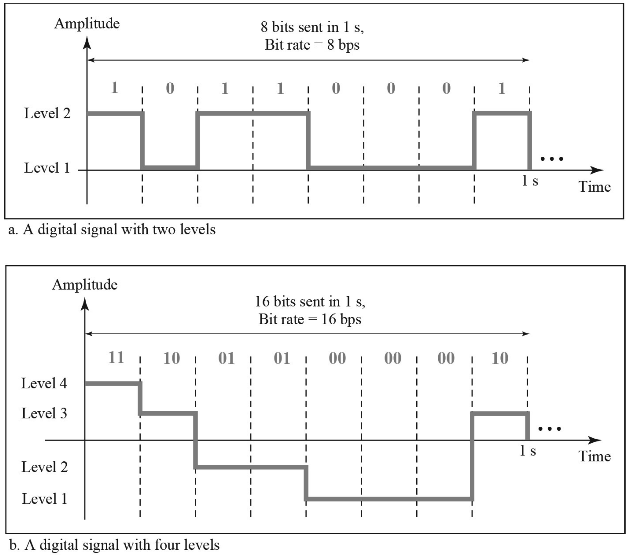
Course Code: CSE3003

Dr. Shubhra dwivedi
Assistant Professor
School - SCOPE
VIT-AP Amaravati

DIGITAL SIGNALS

In addition to being represented by an analog signal, information can also be represented by a digital signal. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage. A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level.

Figure 3.16 *Two digital signals: one with two signal levels and the other with four signal levels*



Example 3.16

A digital signal has eight levels. How many bits are needed per level? We calculate the number of bits from the formula

$$\boxed{\text{Number of bits per level} = \log_2 8 = 3}$$

Each signal level is represented by 3 bits.

Example 3.17

A digital signal has nine levels. How many bits are needed per level? We calculate the number of bits by using the formula. Each signal level is represented by 3.17 bits. However, this answer is not realistic. The number of bits sent per level needs to be an integer as well as a power of 2. For this example, 4 bits can represent one level.

Example 3.18

Bit Rate: The bit rate is the number of bits sent in Is, expressed in bits per second (bps).

Assume we need to download text documents at the rate of 100 pages per sec. What is the required bit rate of the channel?

Solution

A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires 8 bits (ascii), the bit rate is

$$\boxed{100 \times 24 \times 80 \times 8 = 1{,}636{,}000 \text{ bps} = 1.636 \text{ Mbps}}$$

Example 3.19

A digitized voice channel, as we will see in Chapter 4, is made by digitizing a 4-kHz bandwidth analog voice signal. We need to sample the signal at twice the highest frequency (two samples per hertz). We assume that each sample requires 8 bits. What is the required bit rate?

Solution

The bit rate can be calculated as

$$\boxed{2 \times 4000 \times 8 = 64{,}000 \text{ bps} = 64 \text{ kbps}}$$

Example 3.20

What is the bit rate for high-definition TV (HDTV)?

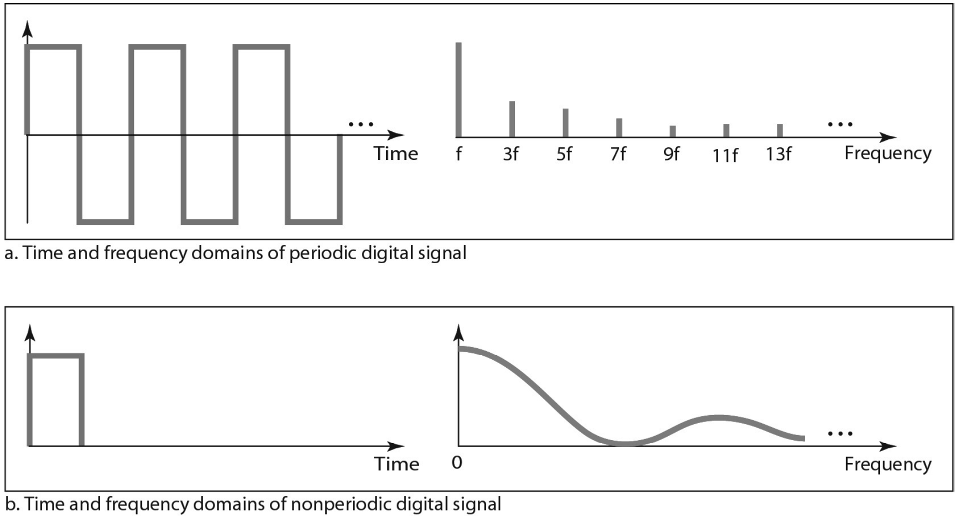
Solution

HDTV uses digital signals to broadcast high quality video signals. The HDTV screen is normally a ratio of 16 : 9. There are 1920 by 1080 pixels per screen, and the screen is renewed 30 times per second. Twenty-four bits represents one color pixel.

$$\boxed{1920 \times 1080 \times 30 \times 24 = 1{,}492{,}992{,}000 \text{ or } 1.5 \text{ Gbps}}$$

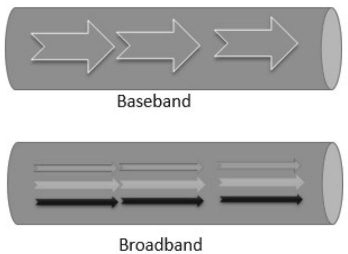
The TV stations reduce this rate to 20 to 40 Mbps through compression.

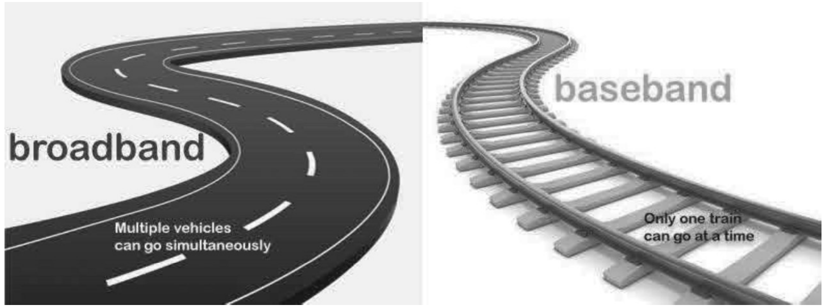
Figure 3.17 *The time and frequency domains of periodic and nonperiodic digital signals*



Transmission of Digital Signals

- We can transmit a digital signal by using one of two different approaches:
- 1. baseband transmission.
- 2. broadband transmission (using modulation).





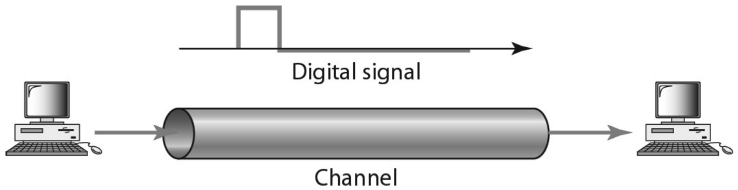
baseband

- binary values directly as pulses of different voltage levels
- repeaters in order to travel longer distances
- bidirectional communication
- transmits only a single data stream at a time, it is possible to transmit signals of multiple nodes simultaneously. Combine all the signals into a single data stream- multiplexing is used.
- Time Division Multiplexing (TDM).

Baseband

- mainly used in Ethernet networks to exchange data between nodes.
- This technology can be used on all three popular cable media types of Ethernet; coaxial, twisted-pair, fiber-optic

Figure 3.18 ***Baseband transmission***



Baseband transmission means sending a digital signal over a channel without changing the digital signal to an analog signal

Figure 3.19 *Bandwidths of two low-pass channels*

between CPU and memory, it
is not possible between two devices

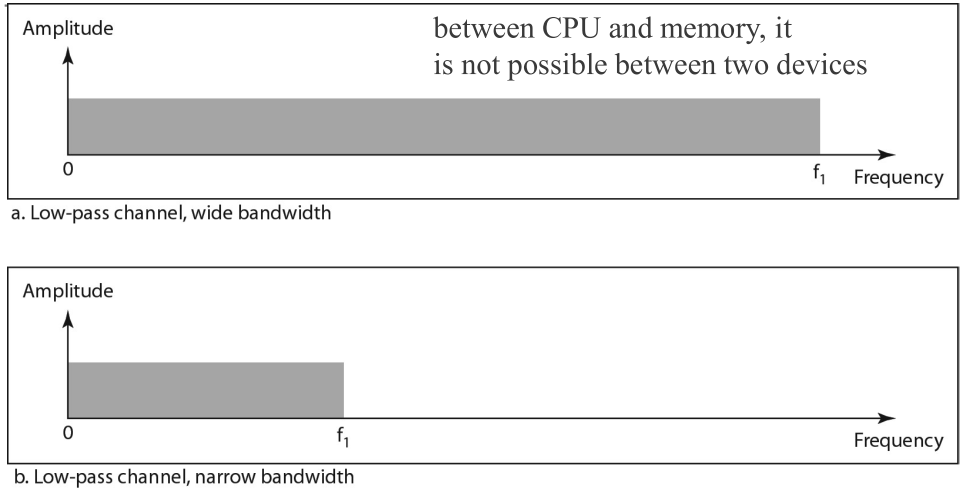
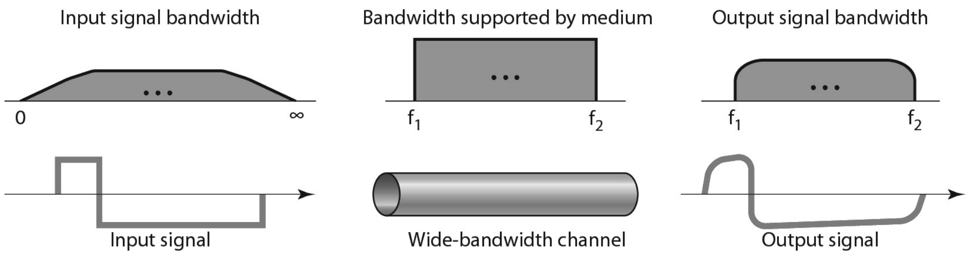


Figure 3.20 *Baseband transmission using a dedicated medium*



full bandwidth
Radio, TV, cell phones must use modulations like AM, FM or QAM, since they share the air medium with many other transmitters, and each one must fit in a thin slice of the bandwidth.

Example 3.21

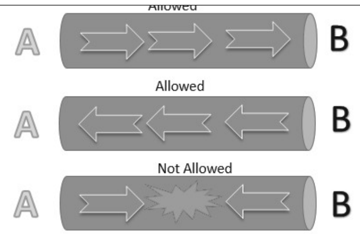
- *An example of a dedicated channel where the entire bandwidth of the medium is used as one single channel is a LAN.*
- *Almost every wired LAN today uses a dedicated channel for two stations communicating with each other.*
- *In a bus topology LAN with multipoint connections, only two stations can communicate with each other at each moment in time (timesharing);*
- *the other stations need to refrain from sending data.*
- *In a star topology LAN, the entire channel between each station and the hub is used for communication between these two entities.*

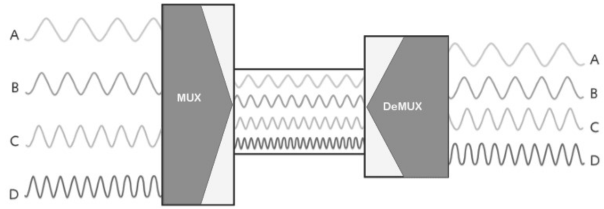
Note

In baseband transmission, the required bandwidth is proportional to the bit rate; if we need to send bits faster, we need more bandwidth.

Note

If the available channel is a bandpass channel, we cannot send the digital signal directly to the channel; we need to convert the digital signal to an analog signal before transmission.





Frequency Division Multiplexing.
FDM (Frequency Division Multiplexing) divides the channel (medium or path) into several sub-channels and assigns a sub-channel to each node.
Each sub-channel can carry a separate carrier wave.

Example 3.24

- *An example of broadband transmission using modulation is the sending of computer data through a telephone subscriber line, the line connecting a resident to the central telephone office.*
- *These lines are designed to carry voice with a limited bandwidth.*
- *The channel is considered a bandpass channel.*
- *We convert the digital signal from the computer to an analog signal, and send the analog signal.*
- *We can install two converters to change the digital signal to analog and vice versa at the receiving end. The converter, in this case, is called a modem*

Example 3.25

- *A second example is the digital cellular telephone.*
- *For better reception, digital cellular phones convert the analog voice signal to a digital signal*
- *Although the bandwidth allocated to a company providing digital cellular phone service is very wide, we still cannot send the digital signal without conversion. The reason is that we only have a bandpass channel available between caller and callee.*
- *We need to convert the digitized voice to a composite analog signal before sending.*

Fundamentals
of
Computer Networks

Course Code: CSE3003

Dr. Shubhra dwivedi

Assistant Professor

School - SCOPE

VIT-AP Amaravati

Shubhra.d@vitap.ac.in

Reasons for Choosing Encoding Techniques

• Digital data, digital signal
– Equipment less complex and expensive than digital-to-analog modulation equipment
• Analog data, digital signal
– Permits use of modern digital transmission and switching equipment
• Digital data, analog signal
– Some transmission media will only propagate analog signals
– E.g., optical fiber and unguided media
• Analog data, analog signal
– Analog data in electrical form can be transmitted easily and cheaply
– Done with voice transmission over voice-grade lines

Factors Used to Compare Encoding Schemes

• **Signal spectrum**
– With lack of high-frequency components
=> less bandwidth required
– With no dc (direct current) component
=> ac coupling via transformer possible (electrical isolation)
– Transfer function of a channel is worse near band edges
=> concentrate transmitted power in the middle
• **Clocking**
– Ease of determining beginning and end of each bit position
• **Signal interference and noise immunity**
– Performance in the presence of noise
• **Cost and complexity**
– The higher the signal rate to achieve a given data rate, the greater the cost

Encoding

Encoding is the process of converting the data or a given sequence of characters, symbols, alphabets etc., into a specified format, for the secured transmission of data. Decoding is the reverse process of encoding which is to extract the information from the converted format.

Data Encoding
Encoding is the process of using various patterns of voltage or current levels to represent 1s and 0s of the digital signals on the transmission link.

The common types of line encoding are Unipolar, Polar, Bipolar, and Manchester.

Encoding Techniques

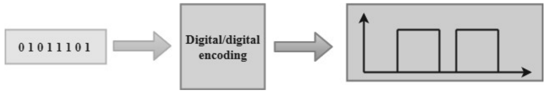
The data encoding technique is divided into the following types, depending upon the type of data conversion.

Analog data to Analog signals – The modulation techniques such as Amplitude Modulation, Frequency Modulation and Phase Modulation of analog signals, fall under this category.

Analog data to Digital signals – This process can be termed as digitization, which is done by Pulse Code Modulation PCM. Hence, it is nothing but digital modulation. As we have already discussed, sampling and quantization are the important factors in this. Delta Modulation gives a better output than PCM.

Digital data to Analog signals – The modulation techniques such as Amplitude Shift Keying ASK, Frequency Shift Keying FSK, Phase Shift Keying PSK, etc., fall under this category. These will be discussed in subsequent chapters.

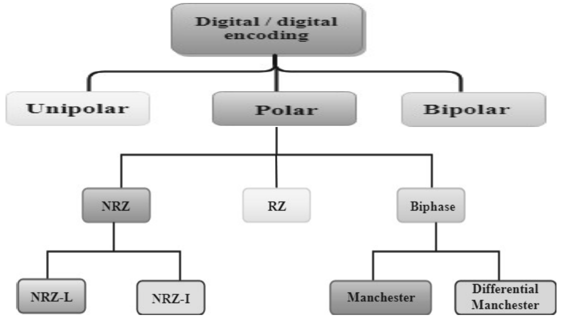
Digital data to Digital signals – It is the representation of digital information by a digital signal. When binary 1s and 0s generated by the computer are translated into a sequence of voltage pulses that can be propagated over a wire, this process is known as digital-to-digital encoding.



Digital-to-digital encoding is divided into three categories:

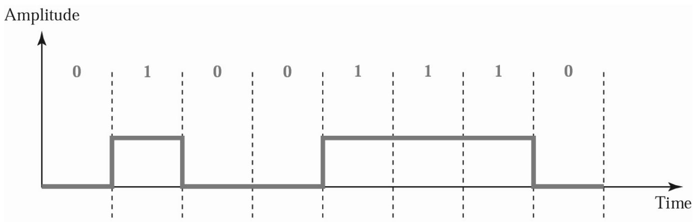
- Unipolar Encoding
- Polar Encoding
- Bipolar Encoding

Encoding Schemes



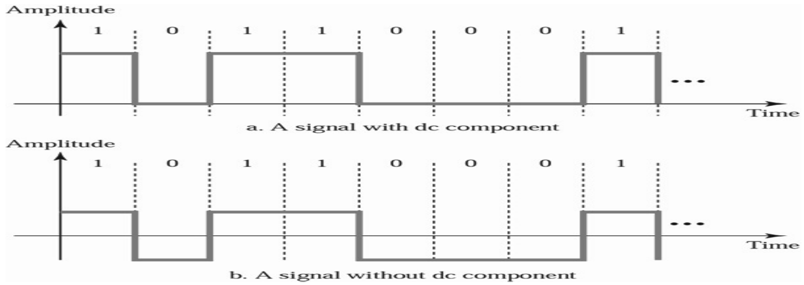
Unipolar

- Digital transmission system sends the voltage pulses over the medium link such as wire or cable.
- In most types of encoding, one voltage level represents 0, and another voltage level represents 1.
- The polarity of each pulse determines whether it is positive or negative.
- This type of encoding is known as Unipolar encoding as it uses only one polarity.
- In Unipolar encoding, the polarity is assigned to the 1 binary state.
- In this, 1s are represented as a positive value and 0s are represented as a zero value.
- In Unipolar Encoding, '1' is considered as a high voltage and '0' is considered as a zero voltage.
- Unipolar encoding is simpler and inexpensive to implement.



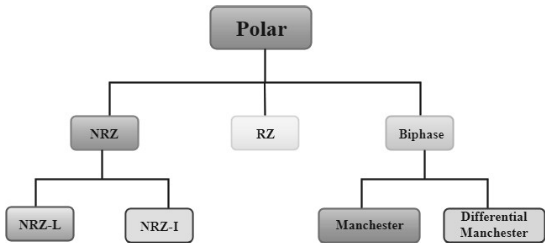
Unipolar encoding has two problems that make this scheme less desirable:

- DC Component
- Synchronization



Polar Encoding

- Polar encoding is an encoding scheme that uses two voltage levels: one is positive, and another is negative.
- By using two voltage levels, an average voltage level is reduced, and the DC component problem of unipolar encoding scheme is alleviated.



Non Return to Zero

NRZ

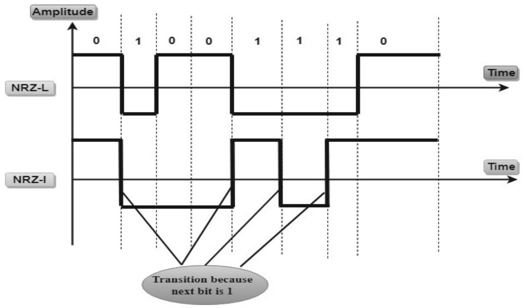
- Non-return to Zero (NRZ) -- signal is always positive or negative.
- Two main types of NRZ: NRZ-L and NRZ-I

NRZ-L

- In NRZ-L encoding, the level of the signal depends on the type of the bit that it represents.
- If a bit is 0 or 1, then their voltages will be positive and negative respectively. Therefore, we can say that the level of the signal is dependent on the state of the bit.
- Good for short and well- shielded transmission paths.

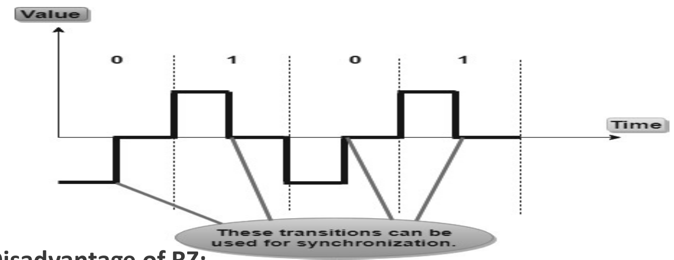
NRZ-I:

- NRZ-I is an inversion of the voltage level that represents 1 bit.
- In the NRZ-I encoding scheme, a transition occurs between the positive and negative voltage that represents 1 bit.
- In this scheme, 0 bit represents no change and 1 bit represents a change in voltage level.
- Provides more synchronization than NRZ-L because there is a transition for each 1 bit.



RZ

- RZ stands for Return to zero.
- There must be a signal change for each bit to achieve synchronization. However, to change with every bit, we need to have three values: positive, negative and zero.
- RZ is an encoding scheme that provides three values, positive voltage represents 1, the negative voltage represents 0, and zero voltage represents none.
- In the RZ scheme, halfway through each interval, the signal returns to zero.
- In RZ scheme, 1 bit is represented by positive-to-zero and 0 bit is represented by negative-to-zero.



Disadvantage of RZ:

It performs two signal changes to encode one bit that acquires more bandwidth.

Biphase

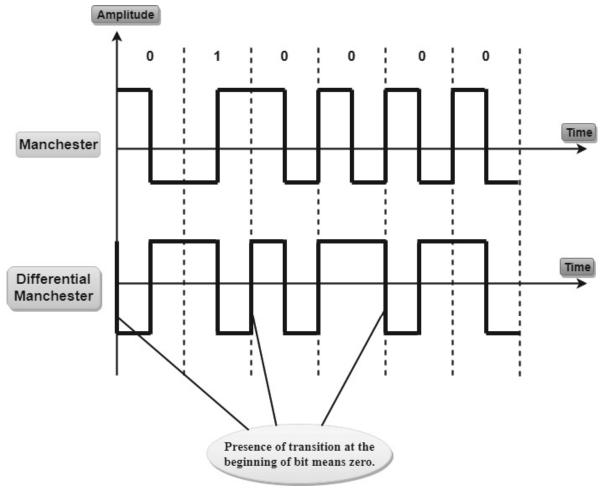
- Biphase is an encoding scheme in which signal changes at the middle of the bit interval but does not return to zero.
- Biphase encoding is implemented in two different ways:

Manchester

- It changes the signal at the middle of the bit interval but does not return to zero for synchronization.
- In Manchester encoding, a negative-to-positive transition represents binary 1, and positive-to-negative transition represents 0.
- Manchester has the same level of synchronization as RZ scheme except that it has two levels of amplitude.

Differential Manchester

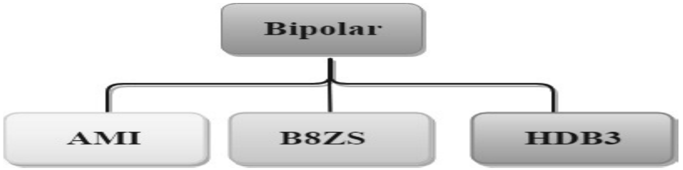
- It changes the signal at the middle of the bit interval for synchronization, but the presence or absence of the transition at the beginning of the interval determines the bit. A transition means binary 0 and no transition means binary 1.
- In Manchester Encoding scheme, two signal changes represent 0 and one signal change represent 1.



Bipolar

- In bipolar encoding (sometimes called *multilevel binary),* there are three voltage levels: positive, negative, and zero.
- In Bipolar encoding scheme, zero level represents binary 0, and binary 1 is represented by alternating positive and negative voltages.
- If the first 1 bit is represented by positive amplitude, then the second 1 bit is represented by negative voltage, third 1 bit is represented by the positive amplitude and so on. This alternation can also occur even when the 1bits are not consecutive.

Bipolar can be classified as:



AMI

- AMI stands for alternate mark inversion where mark work comes from telegraphy which means 1. So, it can be redefined as alternate 1 inversion.
- In Bipolar AMI encoding scheme, 0 bit is represented by zero level and 1 bit is represented by alternating positive and negative voltages.

Advantage:

- DC component is zero.
- Sequence of 1s bits are synchronized.

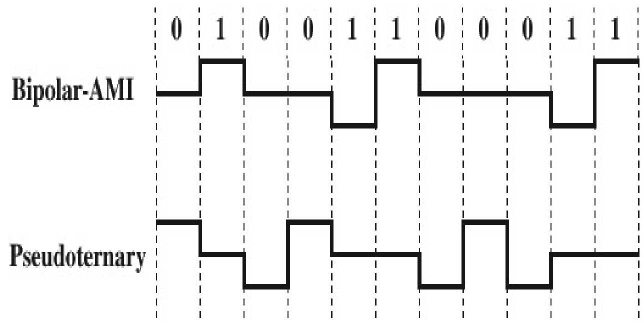
Disadvantage:

- This encoding scheme does not ensure the synchronization of a long string of 0s bits.

Pseudoternary

- A variation of AMI encoding is called pseudoternary.
- In this, the 1 bit is encoded as a zero voltage and the 0 bit is encoded as alternating positive and negative. Example: Data = 010010.

Bipolar-AMI and Pseudoternary



Trade Off for Multilevel Binary

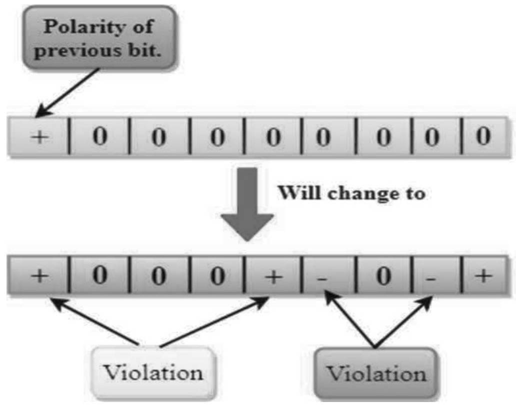
- Not as efficient as NRZ
  - Each signal element only represents one bit
  - In a 3 level system could represent $\log_2 3 = 1.58$ bits
  - Receiver must distinguish between three levels (+A, -A, 0)
  - Requires approx. 3dB more signal power for same probability of bit error

Scrambling

- does not increase the number of bits and does provide synchronization
- continuous sequence of zero's create synchronization problems one solution to this is Scrambling.
- There are two common scrambling techniques:
  - B8ZS(Bipolar with 8-zero substitution)
  - HDB3(High-density bipolar3)
- **Scrambling** is widely used in satellite, radio relay **communications** and PSTN modems

B8ZS

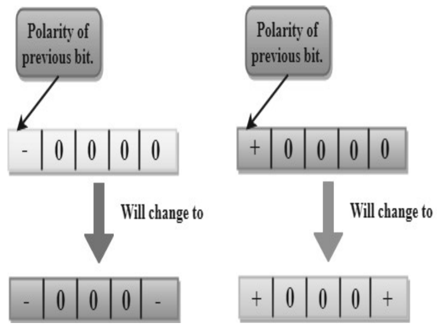
- B8ZS stands for Bipolar 8-Zero Substitution.
- This technique is adopted in North America to provide synchronization of a long sequence of 0s bits.
- In most of the cases, the functionality of B8ZS is similar to the bipolar AMI, but the only difference is that it provides the synchronization when a long sequence of 0s bits occur.
- B8ZS ensures synchronization of a long string of 0s by providing force artificial signal changes called violations, within 0 string pattern.
- When eight 0 occurs, then B8ZS implements some changes in 0s string pattern based on the polarity of the previous 1 bit.
- If the polarity of the previous 1 bit is positive, the eight 0s will be encoded as zero, zero, zero, positive, negative, zero, negative, positive.
- If the polarity of previous 1 bit is negative, then the eight 0s will be encoded as zero, zero, zero, negative, positive, zero, positive, negative.



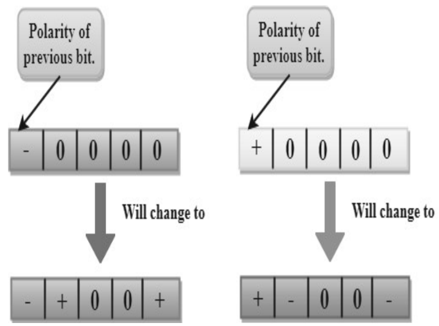
HDB3

- HDB3 stands for High-Density Bipolar 3.
- HDB3 technique was first adopted in Europe and Japan.
- HDB3 technique is designed to provide the synchronization of a long sequence of 0s bits.
- In the HDB3 technique, the pattern of violation is based on the polarity of the previous bit.
- When four 0s occur, HDB3 looks at the number of 1s bits occurred since the last substitution.
- If the number of 1s bits is odd, then the violation is made on the fourth consecutive of 0. If the polarity of the previous bit is positive, then the violation is positive. If the polarity of the previous bit is negative, then the violation is negative.
- If the number of 1s bits is even, then the violation is made on the place of the first and fourth consecutive 0s. If the polarity of the previous bit is positive, then violations are negative, and if the polarity of the previous bit is negative, then violations are positive.

If the number of 1s bits since the last substitution is odd.

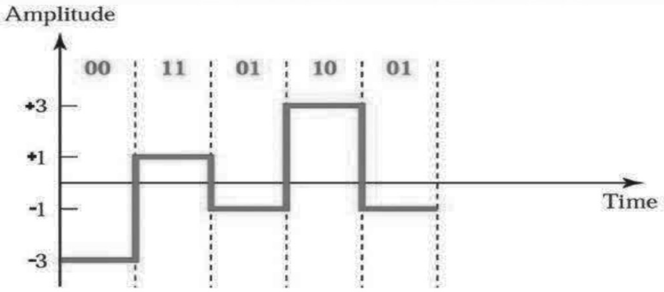


If the number of 1s bits since the last substitution is even.



2B1Q Multilevel Encoding

- The first mBnL scheme, two binary, one quaternary (2B1Q), uses data patterns of size 2 and encodes the 2-bit patterns as one signal element belonging to a four-level signal.
- In this type of encoding m =2, n =1, and L =4 (quaternary).
- Figure below shows an example of a 2B1Q signal.

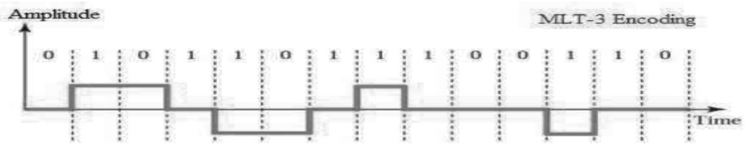


Multiline Transmission: MLT-3

NRZ-I and differential Manchester are classified as differential encoding but use two transition rules to encode binary data (no inversion, inversion). If we have a signal with more than two levels, we can design a differential encoding scheme with more than two transition rules. MLT-3 is one of them.

MLT-3 encoding uses three levels (+V, 0, -V) and three transition rules to move between levels. It is similar to NRZ-I. Following rules are applied to encode bit pattern in the example below.

• If the next bit is zero ('0'), there is no transition.
• If the next bit is one ('1) and current level is not zero '0', the next level is 0.
• If the next bit is one ('1) and current level is zero ('0'), the next level is the opposite of the last nonzero level.



Benefits or advantages of MLT-3 encoding

Following are the benefits or advantages of MLT-3 encoding:
➡It has signal rate which is (1/4)th of the bit rate.
➡Due to its signal shape, it reduces required bandwidth.

Drawbacks or disadvantages of MLT-3 encoding

Following are the drawbacks or disadvantages of MLT-3 encoding:
➡It does not support self-synchronization for long string of zeros ('0').
➡It is more complex than NRZ-I due to use of three levels and complex transition rules.

Digital-to-Digital Encoding Schemes

- 3 Broad Categories: Unipolar, Polar, and Bipolar

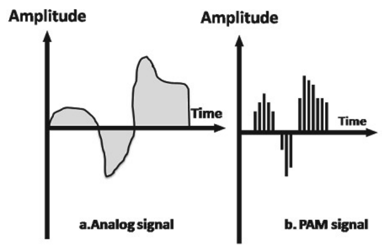
-Nonreturn to Zero-Level (NRZ-L) } Magnetic Recording
-Nonreturn to Zero Inverted (NRZI)
-Manchester } LAN
-Differential Manchester
-Bipolar -AMI } WAN
-B8ZS
-HDB3

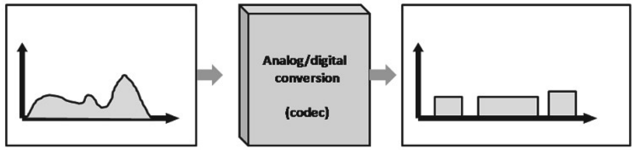
ANALOG-TO-DIGITAL CONVERSION

- When an analog signal is digitalized, this is called an analog-to-digital conversion.
- Suppose human sends a voice in the form of an analog signal, we need to digitalize the analog signal which is less prone to noise. It requires a reduction in the number of values in an analog message so that they can be represented in the digital stream.
- In analog-to-digital conversion, the information contained in a continuous wave form is converted in digital pulses.
- Techniques for Analog-To-Digital Conversion

PAM

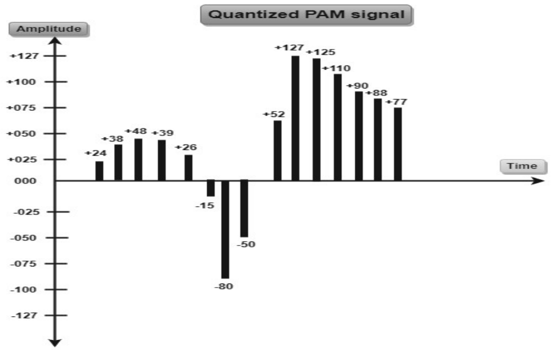
- PAM stands for pulse amplitude modulation.
- PAM is a technique used in analog-to-digital conversion.
- PAM technique takes an analog signal, samples it, and generates a series of digital pulses based on the result of sampling where sampling means measuring the amplitude of a signal at equal intervals.
- PAM technique is not useful in data communication as it translates the original wave form into pulses, but these pulses are not digital. To make them digital, PAM technique is modified to PCM technique.



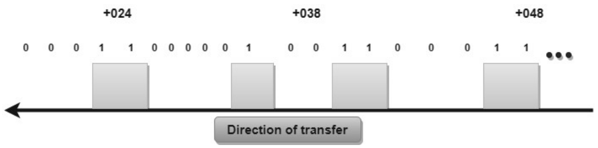


PCM

- PCM stands for Pulse Code Modulation.
- PCM technique is used to modify the pulses created by PAM to form a digital signal. To achieve this, PCM quantizes PAM pulses. Quantization is a process of assigning integral values in a specific range to sampled instances.
- PCM is made of four separate processes: PAM, quantization, binary encoding, and digital-to-digital encoding.



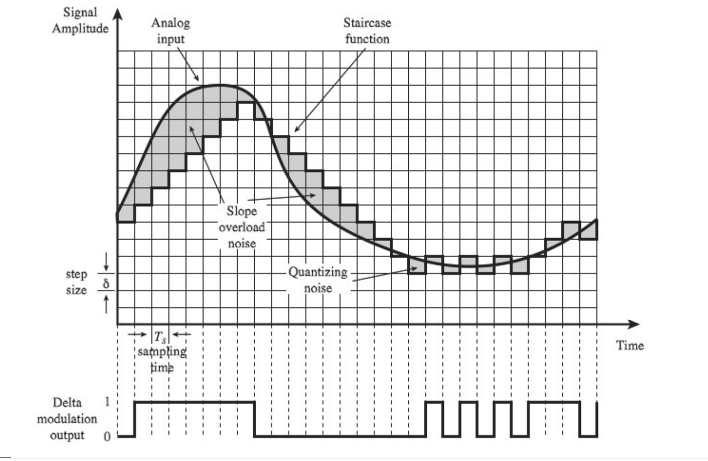
PCM



Delta Modulation

- Analog input is approximated by a staircase function
- Move up or down one level (δ) at each sample interval
- Binary behavior
  - Function moves up or down at each sample interval
  - Moving up: generating 1
  - Moving down: generating 0
- DM versus PCM
  - DM: simpler implementation
  - PCM: better SNR at the same data rate

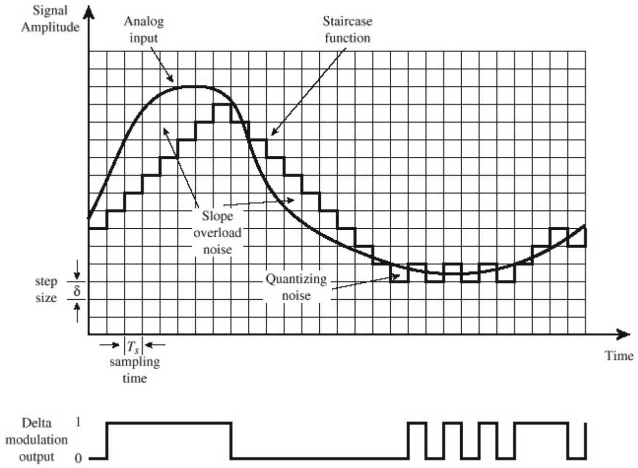
Delta Modulation Example



- At each sampling time, the analog input is compared to the most recent value of the approximating staircase function.
- If the value of the sampled waveform exceeds that of the staircase function, a 1 is generated; otherwise, a 0 is generated.
- Thus, the staircase is always changed in the direction of the input signal.
- The output of the DM process is therefore a binary sequence that can be used at the receiver to reconstruct the staircase function
- The size of the step assigned to each binary digit, and the sampling rate.

- The basic idea in *delta modulation* is to approximate the derivative of analog signal rather than its amplitude.
- The analog data is approximated by a staircase function that moves up or down by one quantization level at each sampling time. ➔ output of DM is a single bit.
- PCM preferred because of better SNR characteristics.

Delta Modulation



Digital-to-Analog signals

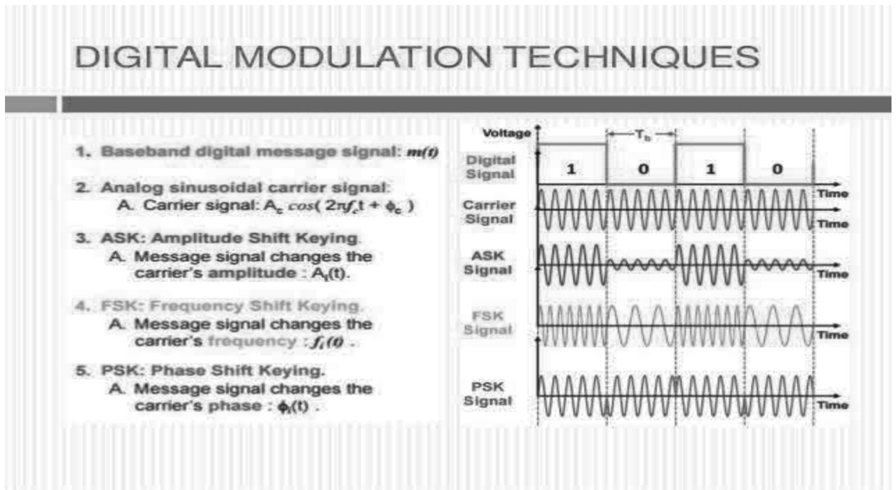
Digital Modulation provides more information capacity, high data security, quicker system availability with great quality communication. Hence, digital modulation techniques have a greater demand, for their capacity to convey larger amounts of data than analog modulation techniques.

There are many types of digital modulation techniques and also their combinations, depending upon the need. Of them all, we will discuss the prominent ones.

ASK – Amplitude Shift Keying
The amplitude of the resultant output depends upon the input data whether it should be a zero level or a variation of positive and negative, depending upon the carrier frequency.

FSK – Frequency Shift Keying
The frequency of the output signal will be either high or low, depending upon the input data applied.

PSK – Phase Shift Keying
The phase of the output signal gets shifted depending upon the input. These are mainly of two types, namely Binary Phase Shift Keying BPSK and Quadrature Phase Shift Keying QPSK, according to the number of phase shifts. The other one is Differential Phase Shift Keying DPSK which changes the phase according to the previous value.



Fundamentals of Computer Networks

Course Code: CSE3003

Ms. Shubhra dwivedi

Assistant Professor

School - SCOPE

VIT-AP Amaravati

Shubhra.d@vitap.ac.in

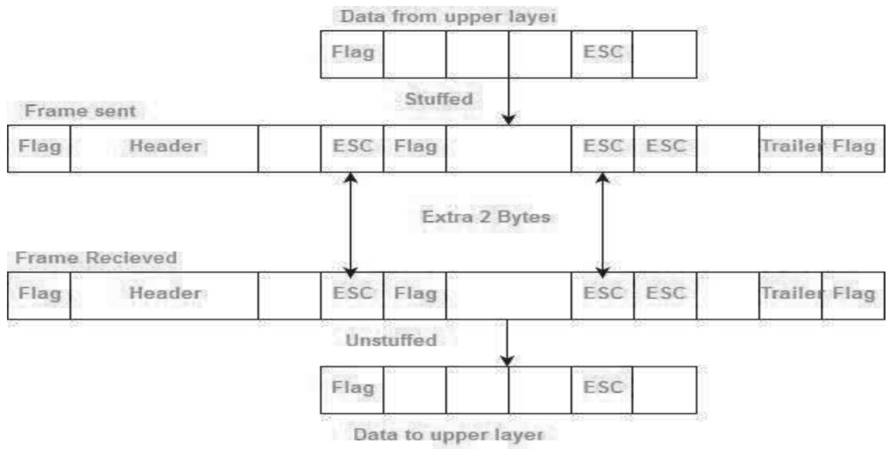
- Data link layer is responsible for something called Framing, which is the division of stream of bits from the network layer into manageable units (called frames).
- Each frame consists of the sender's address and a destination address. The destination address defines where the packet is to go and the sender's address helps the recipient acknowledge the receipt.
- Frames could be of fixed size or variable size. In fixed-size framing, there is no need for defining the boundaries of the frames as the size itself can be used to define the end of the frame and the beginning of the next frame.
- But, in variable-size framing, we need a way to define the end of the frame and the beginning of the next frame.
- To separate one frame from the next, an 8-bit (or 1-byte) flag is added at the beginning and the end of a frame. But the problem with that is, any pattern used for the flag could also be part of the information. So, there are two ways to overcome this problem:

1. Using Byte stuffing (or character stuffing)
2. Using Bit stuffing

Byte stuffing –
A byte (usually escape character(ESC)), which has a predefined bit pattern is added to the data section of the frame when there is a character with the same pattern as the flag. Whenever the receiver encounters the ESC character, it removes from the data section and treats the next character as data, not a flag.

But the problem arises when the text contains one or more escape characters followed by a flag. To solve this problem, the escape characters that are part of the text are marked by another escape character i.e., if the escape character is part of the text, an extra one is added to show that the second one is part of the text.
Example:

Note – Point-to-Point Protocol (PPP) is a byte-oriented protocol.



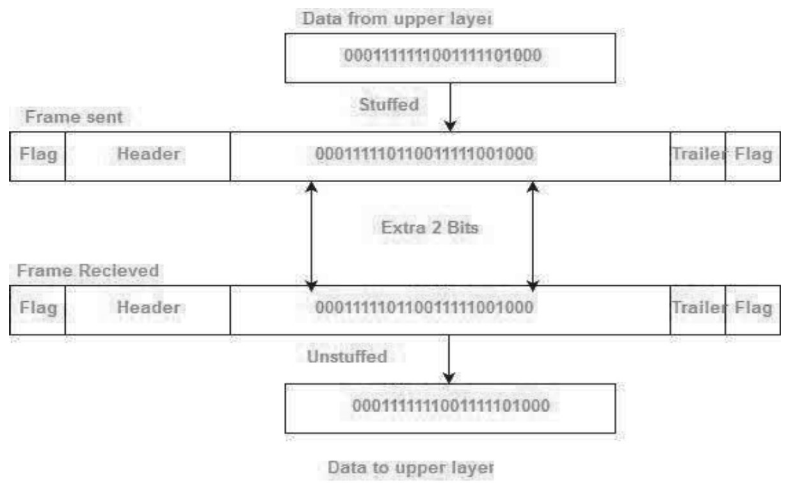
Bit stuffing –

Mostly flag is a special 8-bit pattern “01111110” used to define the beginning and the end of the frame.

Problem with the flag is the same as that was in case of byte stuffing. So, in this protocol what we do is, if we encounter 0 and five consecutive 1 bits, an extra 0 is added after these bits. This extra stuffed bit is removed from the data by the receiver.

The extra bit is added after one 0 followed by five 1 bits regardless of the value of the next bit. Also, as the sender side always knows which sequence is data and which is flag it will only add this extra bit in the data sequence, not in the flag sequence.

Example:



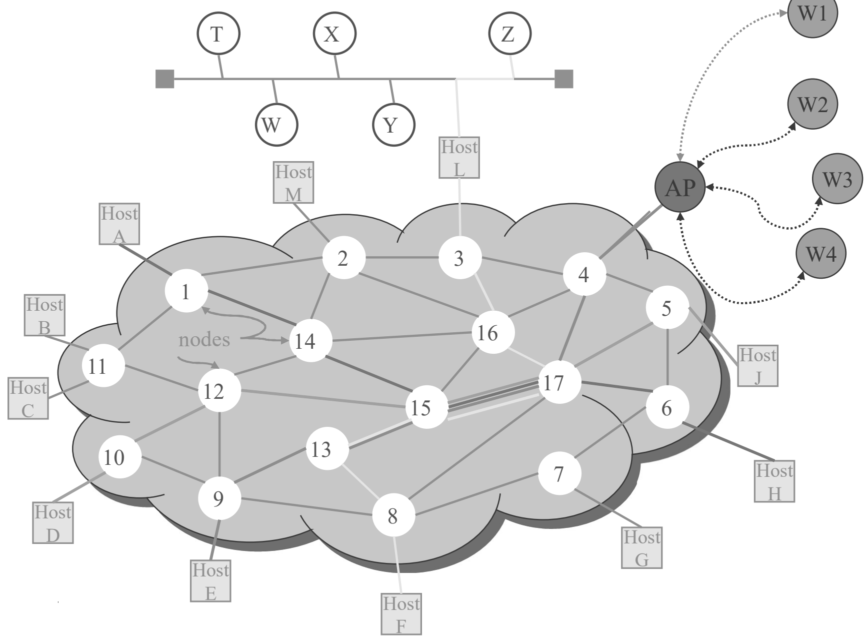
Note – High-Level Data Link Control(HDLC) is a bit-oriented protocol.

Fundamentals
of
Computer Networks
Course Code: CSE3003

Network Performance Problems

Dr. Shubhra dwivedi
Assistant Professor
School - SCOPE

VIT-AP Amaravati



Networks: Sample Performance Problems

1. What is the end-to-end packet latency in this store-and-forward subnet from router 1 to router 6 ?

Assume: All links: 2.5 km; C = 100Mbps; propagation speed = 200m/microsec.
queuing delay = processing delay =0; packet size = 1000 bytes
Solution:
end-to-end packet delay = 4 (equal hops) x link delay
link delay = PROC +QD + TRANS + PROP = 0 + 0 + transmission time + propagation delay

$$\text{transmission time} = \frac{1000 \text{ bytes}}{100 \text{ Mbps}} = \frac{8 \times 10^3 \text{ bits}}{10^8 \text{ bps}} = 8 \times 10^{-5} = 80 \text{ microseconds.}$$

$$\text{prop delay} = \frac{2500 \text{ m}}{200 \text{ m/ microsec}} = 12.5 \text{ microseconds}$$

link delay = 92.5 microseconds
end-to-end subnet delay = 4 x 92.5 = 370 microseconds

2. What is the end-to-end packet delay in this store-and-forward subnet from router 1 to router 6 under the scenario that when a packet from router 1 arrives at router 15 there are three packets enqueued for the link to router 17?

Assume: All links: 2.5 km; C = 100Mbps; propagation speed = 200m/microsec.
processing delay =0; all packet sizes = 1000 bytes
Implied Assumption: queues at 1, 14, and 17 are <u>empty</u> when the packet arrives at node 15.
Required Insight: there will be no queuing delay at 17 even if all three queued packets are going to 6.
Solution:
end-to-end packet delay = 4 (equal hops) x link delay + queuing delay at node 15.
link delay = PROC +QD + TRANS + PROP = 0 + 0 + transmission time + propagation delay

$$\text{transmission time} = \frac{1000 \text{ bytes}}{100 \text{ Mbps}} = \frac{8 \times 10^3 \text{ bits}}{10^8 \text{ bps}} = 8 \times 10^{-5} = 80 \text{ microseconds.}$$

$$\text{prop delay} = \frac{2500 \text{ m}}{200 \text{ m/ microsec}} = 12.5 \text{ microseconds}$$

link delay = 92.5 microseconds
queueing delay at node 15 = 3 packets * transmission time = 3* 80 microseconds = 240 microseconds
end-to-end subnet delay = 4 x 92.5 + 240 = 610 microseconds

What is the end-to-end packet delay in this store-and-forward subnet from router 1 to router 6 under the scenario that when a packet from router 1 arrives at router 15 there are three packets enqueued for the link to router 17?

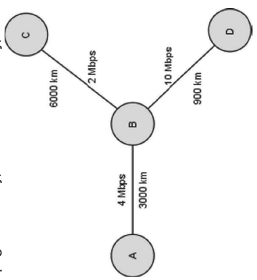
3.a **Assume Now** All links: 2.5 km; **C = 10Mbps**;
propagation speed 200m/microsec.
processing delay = 0; all packet sizes = 1000 bytes

3.b **Assume Now** All links: **25 km;** C = 100 Mbps;
propagation speed 200m/microsec.
processing delay = 0; all packet sizes = 1000 bytes

4.a **Assume Now** All links: 2.5 km; C = 100Mbps;
propagation speed 200m/microsec.
processing delay = **10 microsecs;** all packet sizes = 1000 bytes

4.B **Assume Now** All links: 2.5 km; C = 100Mbps;
propagation speed 200m/microsec.
processing delay = **10 microsecs;** all packet sizes = **3000 bytes**

Propagation Delay, Transmission Delay, Queuing Delay etc...



Assume data travels through the links at the speed of light.

<u>Problem 1</u>

(a) What is the transmission delay if
- A sends a 500 byte packet to B
- B sends a 125 byte packet to D

Transmission Delay = Size of Transfer / Link Bandwidth
A → B: Transmission Delay = (500/ ((4/8) x 10^6)) = 1ms
B → D: Transmission Delay = (125/ (10/8) x 10^6) = 100μs (or 0.1ms)

(b) What is the propagation delay between
- A to B
- B to D

Propagation Delay = Distance of link / Speed of light
A → B: Propagation Delay = 3000 / (3 x 10^5) = 10ms
B → D: Propagation Delay = 900 / (3 x 10^5) = 3ms

(c) A wants to send a 500 byte packet to D through B. B is supposed to follow the store-and-forward model, that is, B will receive the whole packet from A and then start transmitting the packet to D. What is the end-to-end delay seen by the packet?

End to end delay between A→ D = (Delay between A→B) + (Delay between B→D)

Delay on a link = Transmission Delay + Propagation Delay
Therefore, Delay between A→→→→B = 1 + 10 = 11ms, and Delay between B→→→→D = 0.4 + 3 = 3.4ms

→→→→ End to end delay between A→→→→D = 11ms + 3.4ms = 14.4ms

(d) Now, A wants to send a 5 MB file to D in chunks of 500 byte packets. To prevent any packet loss, when A sends a 500 byte packet to D (same way as explained in (c)), D responds with a 50 byte packet to A (through B) acknowledging that it has successfully received the packet. Only after receiving the acknowledgement does A send the next 500 byte packet. Assuming no losses, how long will it take A to send the file to D?

End to end delay between A→→→→D for a 500 byte packet = 14.4ms
End to end delay between A→→→→D for a 50 byte ACK = (0.1 + 10) + (0.04 + 3) = 13.14ms
Total delay for a packet and ACK = 14.4 + 13.14 = 27.54ms
#packets in a 5MB transfer = (5 x 10^6) / 500 = 10,000

Therefore, total time for transfer = 10000 x 27.54ms = 275.4 sec

<u>Problem 2</u>

A has finished transmitting everything to D. If D starts sending 500 byte packets back-to-back to B, then how many packets will D have transmitted before B starts receiving the first packet sent by D? What does this value have to do with the term "bandwidth-delay product"?

This is similar to computing the volume of a pipe. The amount of data that will be "in flight" on a network link is the product of its bandwidth and the propagation delay.

For D→B, the propagation delay is 3 x 10^{-3}, and the bandwidth is 10Mbps.
Therefore, the Bandwidth-Delay product is (10/8 x 10^6) x (3 x 10^{-3}) = 3750 bytes
This translates to 3750/500 = 7.5 packets

Problem 3
Now suppose A sends two 500 byte packets back-to-back to C. What is the end-to-end delay experienced by each packet? Is it different for the two packets?
[Notice that the bandwidth of the A-B link is more than that of the B-C link. So B cannot send packets to C as fast as it may receive from A.]

Delay for packet #1 = (Delay in A→B) + (Delay in B→C) = (1 + 10) + (2 + 20) = 33ms
Delay for packet #2 = (Delay in A→B) + (Queuing Delay in B) + (Delay in B→C)
Queuing Delay at B =
(1 – (Bandwidth of B→C/Bandwidth of A→B)) x Transmission Delay of B→C
(*Use intuition from the discussion slides on Queuing Delay)*

Therefore, delay for packet #2 = (1 + 10) + (1-2/4) x 2 + (2 + 20) = 34ms

Useful Terms and Information

Latency/Delay	
Transmission delay	Amount of time transmitting data. Measured from when the first bit of data is pushed on the wire to the when last bit of data is pushed on the wire.
Propagation delay	Time a single bit spends traversing the link. Measured as how long it takes to travel the distance of the wire at approximately the speed of light.
Queueing delay	Time spent waiting in a buffer / queue of a switch / router.
End-to-end delay	Time difference between when the sender starts transmitting the packet, and the time when the receiver receives the complete packet
Round-Trip Time (RTT)	Total time for a packet to reach destination and a response to return to the sender
Bandwidth (capacity)	Amount of data sent (or received) per unit time. Measured in bits/time.
Bandwidth-delay product	Amount of data that can be "in flight" at any time. Propagation delay × bits/time = total bits in line

Units, Constants	
Byte	8 bits
Mbps	10^6 bits per second
ms	1 x 10^{-3} seconds
Speed of Light (c)	3 x 10^5 km/second