Module-I

Chapter-1
Lecture-1

Introduction to Data Communication

Learning Objective:

1.1 Data & Information
1.2 Data Communication.
1.3 Data Flow

1.1 Data & Information

Data refers to the raw facts that are collected while **information** refers to processed data that enables us to take decisions.

Ex. When result of a particular test is declared it contains data of all students, when you find the marks you have scored you have the information that lets you know whether you have passed or failed.

The word ***data*** refers to any information which is presented in a form that is agreed and accepted upon by is creators and users.

1.2 Data Communication

Data Communication is a process of exchanging data or information. In case of computer networks this exchange is done between two devices over a transmission medium. This process involves a communication system which is made up of hardware and software. The hardware part involves the sender and receiver devices and the intermediate devices through which the data passes. The software part involves certain rules which specify what is to be communicated, how it is to be communicated and when. It is also called as a Protocol.

1.2.1 Characteristics of Data Communication

The effectiveness of any data communications system depends upon the following four fundamental characteristics:

1. **Delivery**: The data should be delivered to the correct destination and correct user.
2. **Accuracy**: The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.
3. **Timeliness**: Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data.
4. **Jitter**: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted.

1.2.2 Components of Data Communication

A Data Communication system has five components as shown in the diagram below:

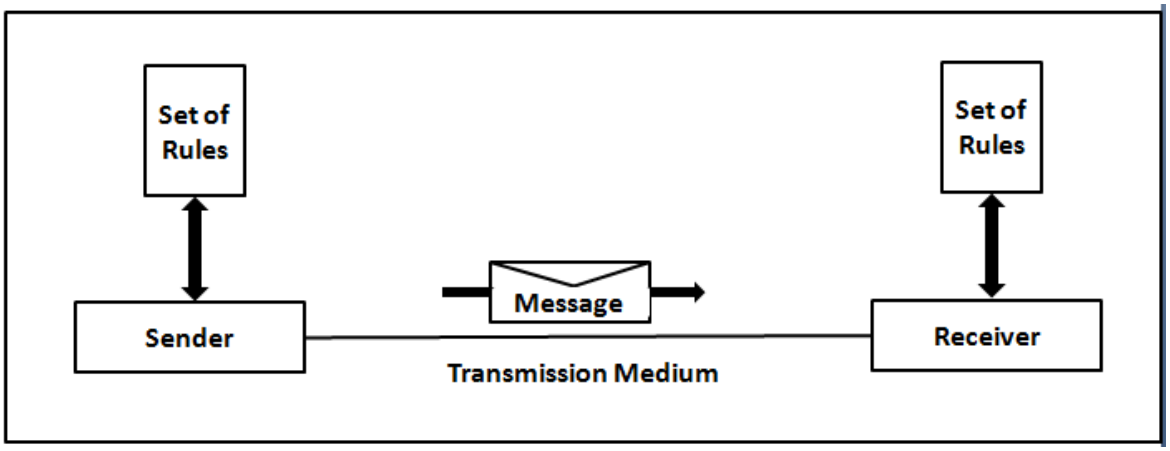


Figure 1.1. Components of a Data Communication System

- **Message**
  Message is the information to be communicated by the sender to the receiver.
- **Sender**
  The sender is any device that is capable of sending the data (message).
- **Receiver**
  The receiver is a device that the sender wants to communicate the data (message).
- **Transmission Medium**
  It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.
- **Protocol**
  It is an agreed upon set or rules used by the sender and receiver to communicate data. A protocol is a set of rules that governs data communication. A Protocol is a necessity in data communications without which the communicating entities are like two persons trying to talk to each other in a different language without know the other language.

1.2.3 Data Flow

Devices communicate with each other by sending and receiving data. The data can flow between the two devices in the following ways.

- Simplex
- Half Duplex
- Full Duplex

1.2.3.1 Simplex

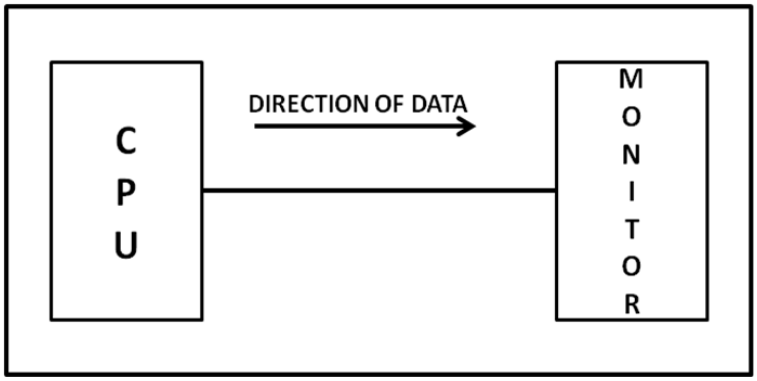


Figure: 1.2 Simplex mode of communication

In Simplex, communication is unidirectional. Only one of the devices sends the data and the other one only receives the data.

Example: in the above diagram: a cpu send data while a monitor only receives data.

1.2.3.2 Half Duplex

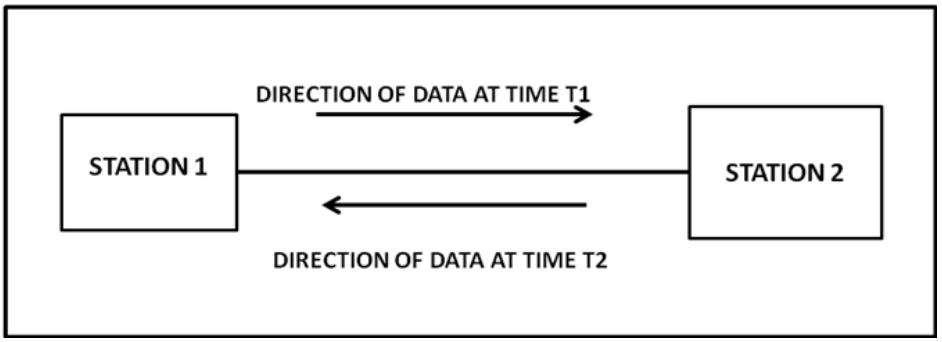


Figure: 1.3 Half Duplex Mode of Communication

In half duplex both the stations can transmit as well as receive but not at the same time. When one device is sending other can only receive and vice-versa (as shown in figure 1.3.)

Example: A walkie-talkie.

1.2.3.3 Full Duplex

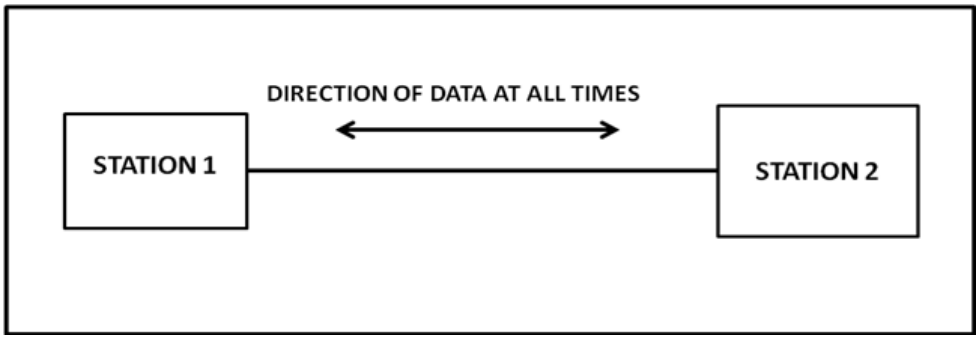


Figure: 1.4 Full Duplex Mode of Communication

In Full duplex mode, both stations can transmit and receive at the same time.
Example: mobile phones

Module-I

Chapter-1
Lecture-2

Learning Objective:

1.4 Computer Network

1.5 Physical Structures

1.6 Physical Topology

1.4 Computer Network

A computer network can be defined as a collection of nodes. A node can be any device capable of transmitting or receiving data. The communicating nodes have to be connected by communication links.

A Compute network should ensure

- **reliability** of the data communication process, is measured by the frequency of failure and recovery time
- **security** of the data
- **performance** by achieving higher throughput and smaller delay times

1.5 Physical Structures

1.5.1 Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. There are two possible types of connections: point-to-point and multipoint.

1.5.1.1 Point-to-Point

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.

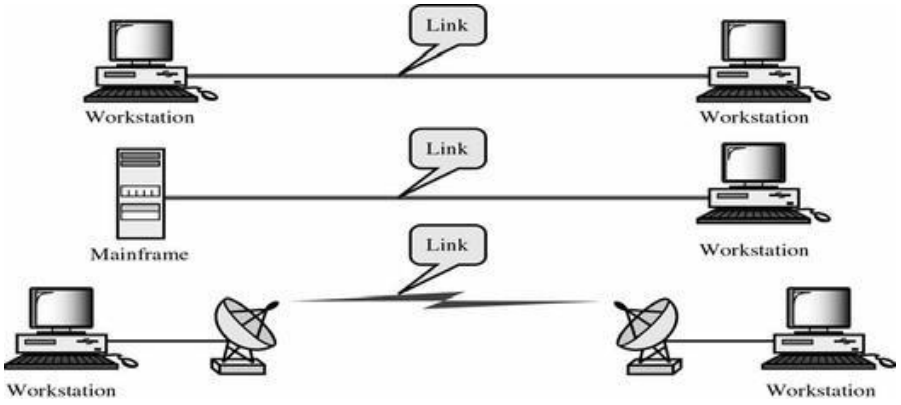


Figure: 1.5 Point to point connection

1.5.1.2 Multipoint

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure). In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

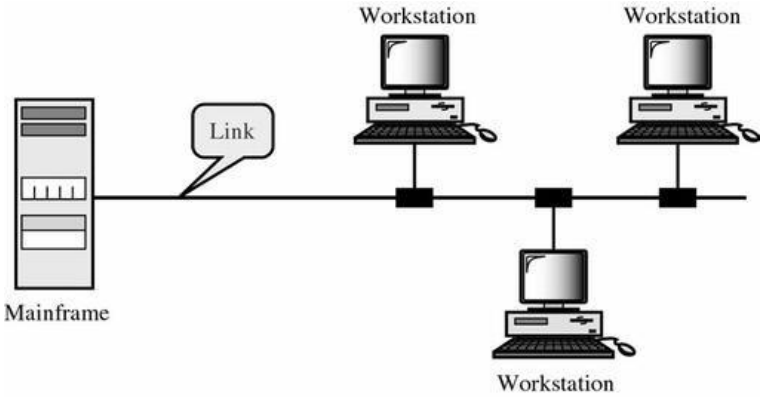


Figure: 1.6 Multi point connection

1.6 Physical Topology

The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are five basic topologies possible: mesh, star, bus, ring, Hybrid Topology.

1.6.1 Mesh Topology

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.

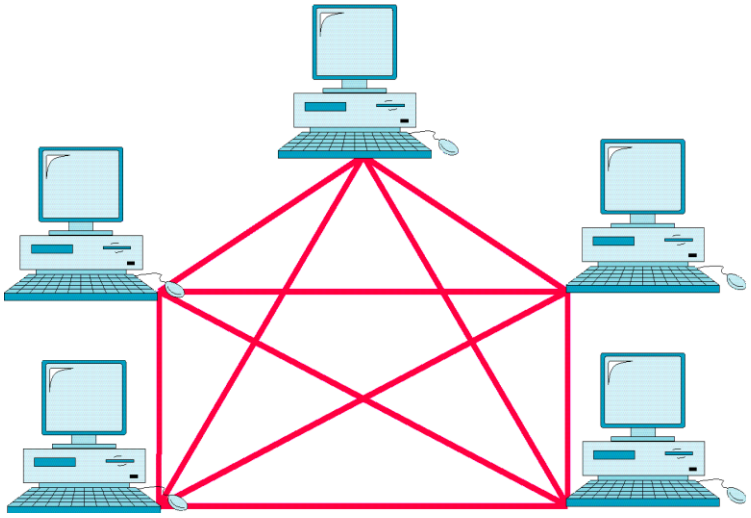


Figure: 1.7 Mesh Topology

Advantages

- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
- Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
- Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems.

Disadvantages

- The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required. First, because every device must be connected to every other device, installation and reconnection are difficult.
- Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

1.6.2 Star Topology

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. The controller acts as an exchange. If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

Advantage

- A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
- Other advantages include robustness. If one link fails, only that link is affected. All other links remain active.

Disadvantages

- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub.
- If the hub goes down, the whole system is dead.
- Often more cabling is required in a star than in some other topologies (such as ring or bus).

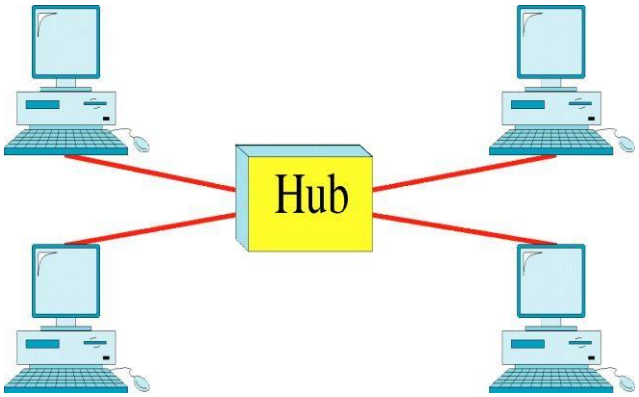


Figure: 1.8 Star Topology

1.6.3 Bus Topology

A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network. Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.

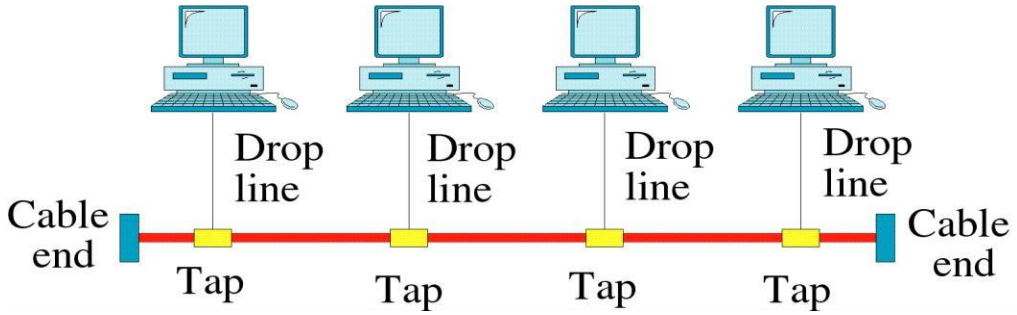


Figure: 1.9 Bus Topology

Advantages

- Ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.

Disadvantages

- Difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation.

1.6.4 Ring Topology

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

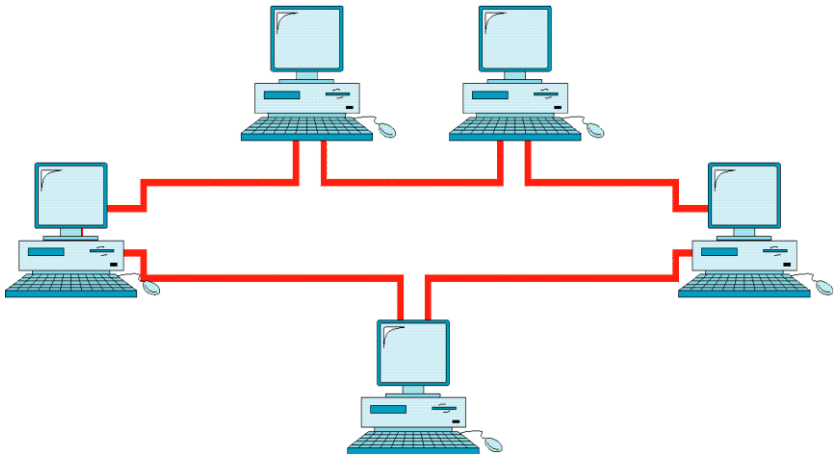


Figure: 1.10 Ring Topology

Advantages

- A ring is relatively easy to install and reconfigure.

Disadvantages

- Unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

1.6.5 Hybrid Topology

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology or star or ring Topology..

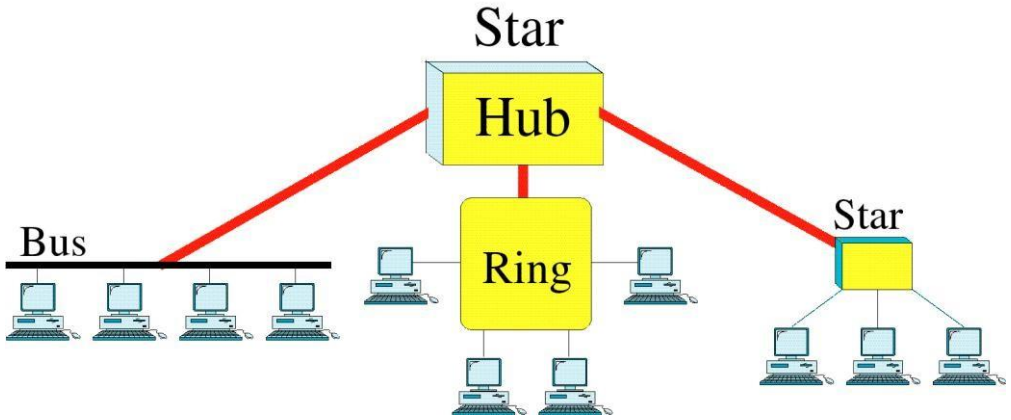
- 

Figure: 1.11 Hybrid Topology

Module-I

Chapter-1
Lecture-3

Learning Objective:

1.7 Network Protocol

1.8 Categories of Network

1.7 Network Protocol

A Protocol is defined as a set of rules that governs data communications. A protocol defines what is to be communicated, how it is to be communicated and when it is to be communicated.

Elements of a Protocol

There are three key elements of a protocol:

A. Syntax

- It means the structure or format of the data.
- It is the arrangement of data in a particular order.

B. Semantics

- It tells the meaning of each section of bits and indicates the interpretation of each section.
- It also tells what action/decision is to be taken based on the interpretation.

C. Timing

- It tells the sender about the readiness of the receiver to receive the data.
- It tells the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver.

1.8 Categories of Network

Networks are categorized on the basis of their size. The three basic categories of computer networks are:

1.8.1 Local Area Networks (LAN) is usually limited to a few kilometers of area. It may be privately owned and could be a network inside an office on one of the floor of a building or a LAN could be a network consisting of the computers in a entire building.

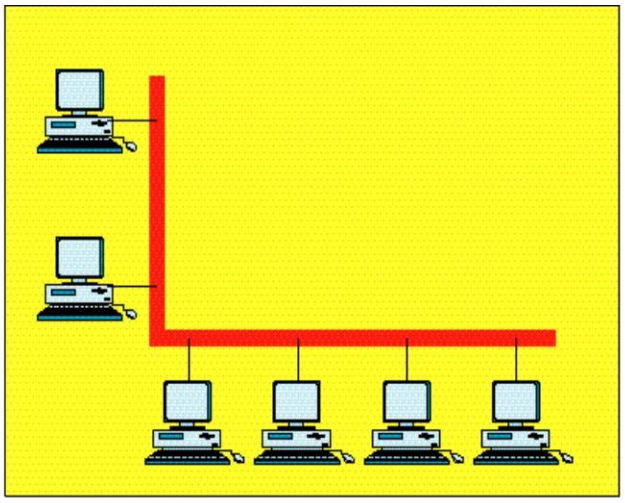


Figure: 1.12 Local Area Networks

1.8.2 Wide Area Network (WAN) is made of all the networks in a (geographically) large area. The network in the entire state of Odisha could be a WAN.

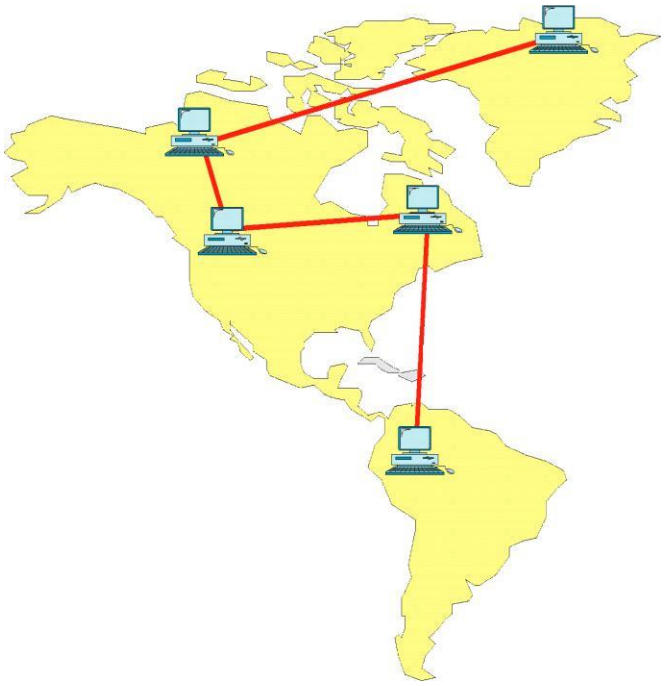


Figure: 1.13 Wide Area Networks

1.8.3 Metropolitan Area Network (MAN) is of size between LAN & WAN. It is larger than LAN but smaller than WAN. It may comprise the entire network in a city like Mumbai.

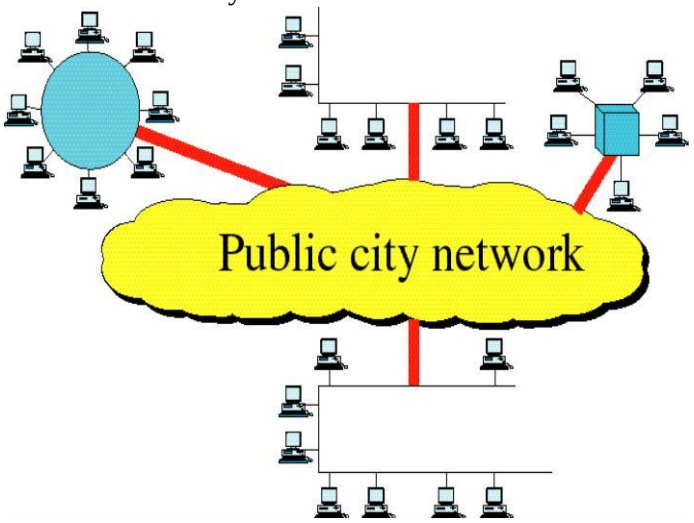


Figure: 1.14 Metropolitan Area Network

Short Questions

1. What are the objective of computer network?

Ans. –Communication between applications on different computer

- Must understand application needs/demands
- Traffic data rate
- Target.

2. What are possible ways of data exchange?

Ans. Simplex, Half duplex, Full duplex.

3. What are the components of data communication?

Ans- Message, Sender, Receiver, Transmission Medium, Protocol

4. What is the difference between half duplex and full duplex communication?

Ans -In half duplex both the stations can transmit as well as receive but not at the same time. When one device is sending other can only receive and vice-versa.

In Full duplex mode, both stations can transmit and receive at the same time.

5. What is the difference between point to point and multipoint connection?

Ans - A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.

6. What is the difference between mesh and star topology?

Ans - In a mesh topology, every device has a dedicated point-to-point link to every other device. In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. The controller acts as an exchange.

7. What is Topology?

Ans - The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.

Long Questions

1. Discuss different types of topology.
2. Differentiate between LAN, MAN and WAN.
3. What are the components of Data communication? Explain with suitable diagram.

Module-I

Chapter-2
Lecture-4

Introduction to OSI Model & its layers

Learning Objective:

2.1 OSI Model

2.1 OSI Model

The Open Systems Interconnection (OSI) Model was developed by International Organization for Standardization (ISO). ISO is the organization, OSI is the model. It was developed to allow systems with different platforms to communicate with each other. Platform could mean hardware, software or operating system. It is a network model that defines the protocols for network communications.

It is a hierarchical model that groups its processes into layers. It has 7 layers as follows:

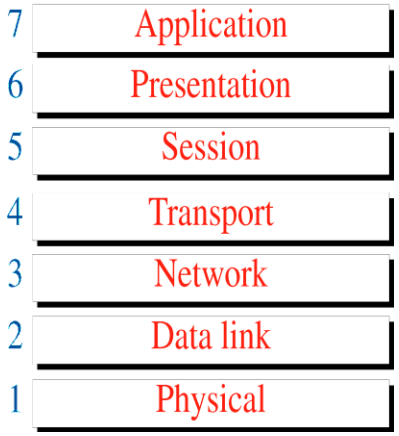


Figure: 2.1 OSI Model Layers

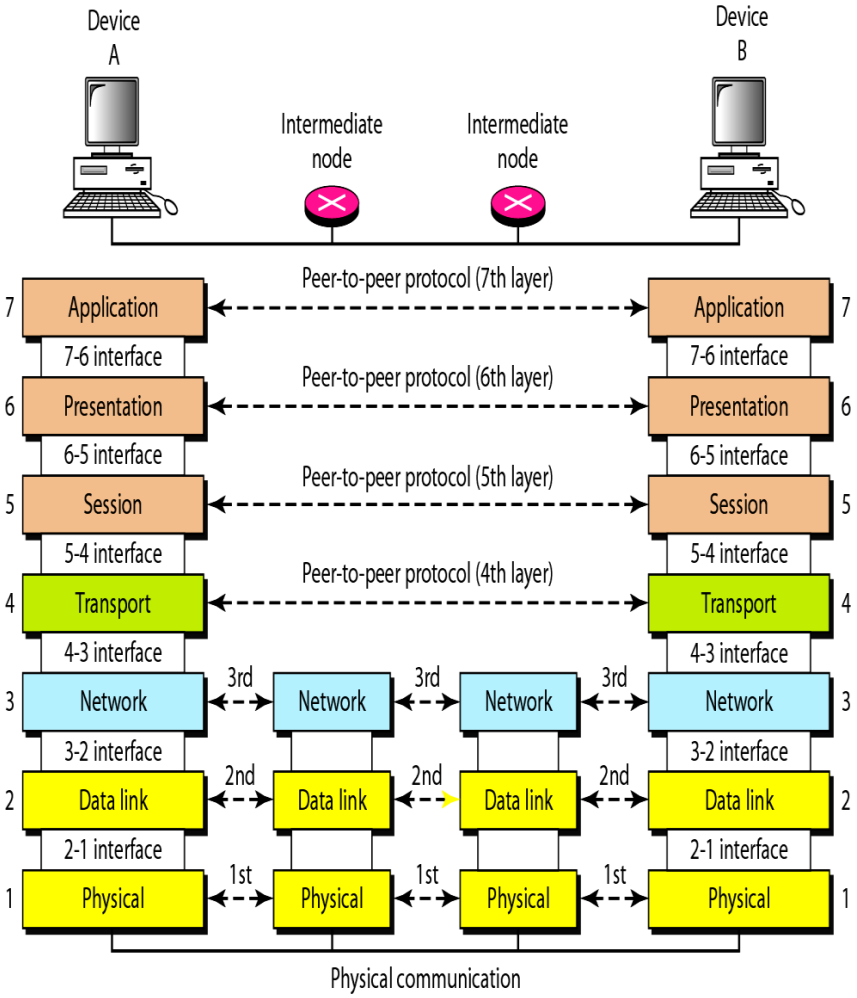


Figure: 2.2 Communication & Interfaces in the OSI model

Physical Layer

The Physical Layer provides a standardized interface to physical transmission media, including:

- Mechanical specification of electrical connectors and cables, for example maximum cable length.
- Electrical specification of transmission line
- Bit-by-bit or symbol-by-symbol delivery

Interface

The Physical Layer defines the characteristics of interfaces between the devices & transmission medium.

Representation of bits

The physical layer is concerned with transmission of signals from one device to another which involves converting data (1‘s & 0‘s) into signals and vice versa. It is not concerned with the meaning or interpretation of bits.

Data rate

The physical layer defines the data transmission rate i.e. number of bits sent per second. It is the responsibility of the physical layer to maintain the defined data rate.

Synchronization of bits

To interpret correct and accurate data the sender and receiver have to maintain the same bit rate and also have synchronized clocks.

Line configuration

The physical layer defines the nature of the connection .i.e. a point to point link, or a multi point link.

Physical Topology

The physical layer defines the type of topology in which the device is connected to the network. In a mesh topology it uses a multipoint connection and other topologies it uses a point to point connection to send data.

Transmission mode

The physical layer defines the direction of data transfer between the sender and receiver. Two devices can transfer the data in simplex, half duplex or full duplex mode.

Main responsibility of the physical layer

Transmission of bits from one hop to the next.

Data Link Layer

The Data Link layer adds reliability to the physical layer by providing error detection and correction mechanisms. The main responsibility of the data link layer is hop to hop transmission of frames.

- Framing.
- Physical Addressing
- Flow control
- Error control

Network Layer

The network layer makes sure that the data is delivered to the receiver despite multiple intermediate devices. The network layer is responsible for source to destination of delivery of data. Hence it may have to route the data through multiple networks via multiple intermediate devices. In order to achieve this the network layer relies on two things:

- Logical Addressing
- Routing

The main responsibility of Network Layer is transmission of packets from source to destination.

Transport Layer

The transport layer takes care of process to process delivery of data and makes sure that it is intact and in order. To ensure process to process delivery the transport layer makes use of **port address** to identify the data fromthe sending and receiving process. A Port Address is the name or label given to a process. It is a 16 bit address.

The Transport layer is responsible for segmentation and reassembly of the message into segments which bear sequence numbers. This numbering enables the receiving transport layer to rearrange the segments in proper order.

The transport layer also carries out flow control and error control functions.

Session Layer

Main responsibility of session layer **is** dialog control and synchronization.

Presentation Layer

The presentation layer performs translation, encryption and compression of data.

Application Layer

Main Responsibility of Application layer is to provide access to network resources. The application layer enables the user to communicate its data to the receiver by providing certain services. For ex. Email, File transfer, access and management, http, SMTP, FTP etc.

Module-I

Chapter-2
Lecture-5

Learning Objective:

2.2 TCP/IP Model

2.3 Functions of the Layers of TCP/IP model

2.2 TCP/IP Model

It is also called as the TCP/IP protocol suite. It is a collection of protocols. It existed even before the OSI model was developed. Originally had four layers (bottom to top):

- Host to Network Layer
- Internet Layer(Network Layer)
- Transport Layer
- Application Layer

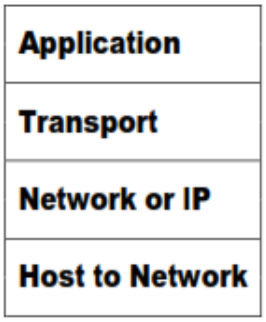


Figure: 2.3 Layers of TCP/IP Protocol Suite

The structure TCP/IP model is very similar to the structure of the OSI reference model. The OSI model has seven layers where the TCP/IP model has four layers.

- The Application layer of TCP/IP model corresponds to the Application Layer of Session, Presentation & Application Layer of OSI model.
- The Transport layer of TCP/IP model corresponds to the Transport Layer of OSI model.
- The Network layer of TCP/IP model corresponds to the Network Layer of OSI model.
- The Host to network layer of TCP/IP model corresponds to the Physical and Data link Layer of OSI model.

The diagram showing the comparison of OSI model and TCP/IP model along with the protocols is as shown below:

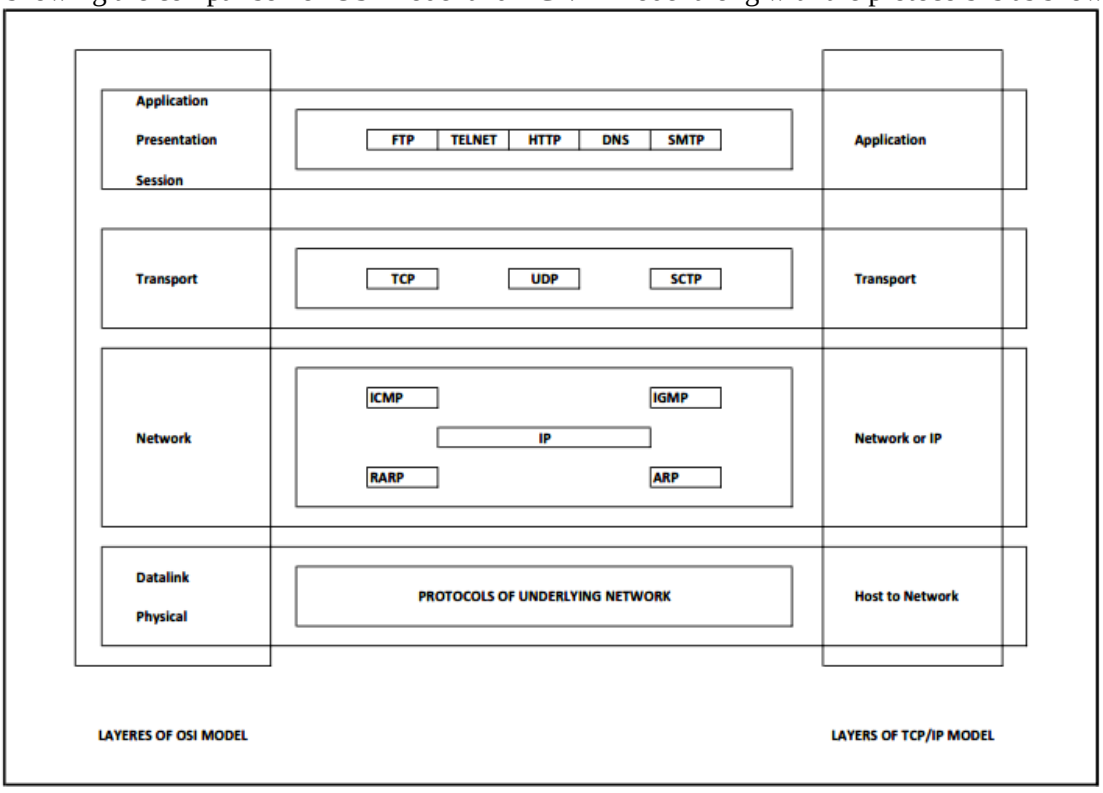


Figure: 2.4 Comparison of OSI model and TCP/IP model

2.3 Functions of the Layers of TCP/IP model

A. Host to Network Layer

This layer is a combination of protocols at the physical and data link layers. It supports all standard protocols used at these layers.

B. Network Layer or IP

Also called as the Internetwork Layer(IP). It holds the IP protocol which is a network layer protocol and is responsible for source to destination transmission of data.

- The Internetworking Protocol (IP) is an **connection-less** & **unreliable protocol.**
- It is a best effort delivery service.
- IP transports data by dividing it into **packets or datagrams** of same size. Each packet is independent of the other and can be transported across different routes and can arrive out of order at the receiver.
- The packets may get dropped during transmission along various routes. Since IP does not make any guarantee about the delivery of the data its call an **unreliable** protocol.

IP is a combination of four protocols:

1. ARP
2. RARP
3. ICMP
4. IGMP

C. Transport Layer

Transport layer protocols are responsible for transmission of data running on a process of one machine to the correct process running on another machine.

The transport layer contains three protocols:

- TCP
- UDP
- SCTP

TCP – Transmission Control Protocol

TCP is a reliable connection-oriented, reliable protocol. i.e. a connection is established between the sender and receiver before the data can be transmitted.

UDP – User Datagram Protocol

UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control.

SCTP – Stream Control Transmission Protocol

SCTP is a relatively new protocol added to the transport layer of TCP/IP protocol suite. It combines the features of TCP and UDP.

D. Application Layer

The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and define high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Module-I

Chapter-2
Lecture-6

Learning Objective:

2.4 The Internet

2.5 Standards in Networking

2.4 The Internet

The Internet is a structured, organized system.

A Brief History

A network is a group of connected communicating devices such as computers and printers. An internet (note the lowercase letter-i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks.

In the mid-1960s, mainframe computers in research organizations were stand•alone devices. Computers from different manufacturers were unable to communicate with one another. The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP). The IMPs, in turn, would be connected to one another. Each IMP had to be able to communicate with other IMPs as wellas with its own attached host.

By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided communication between the hosts.

In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting Projec1. Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internetworking Protocol (lP). IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCP/IP.

The Internet Today

The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed. Today most end users who want Internet connection use the services of Internet service providers (ISPs). There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government.

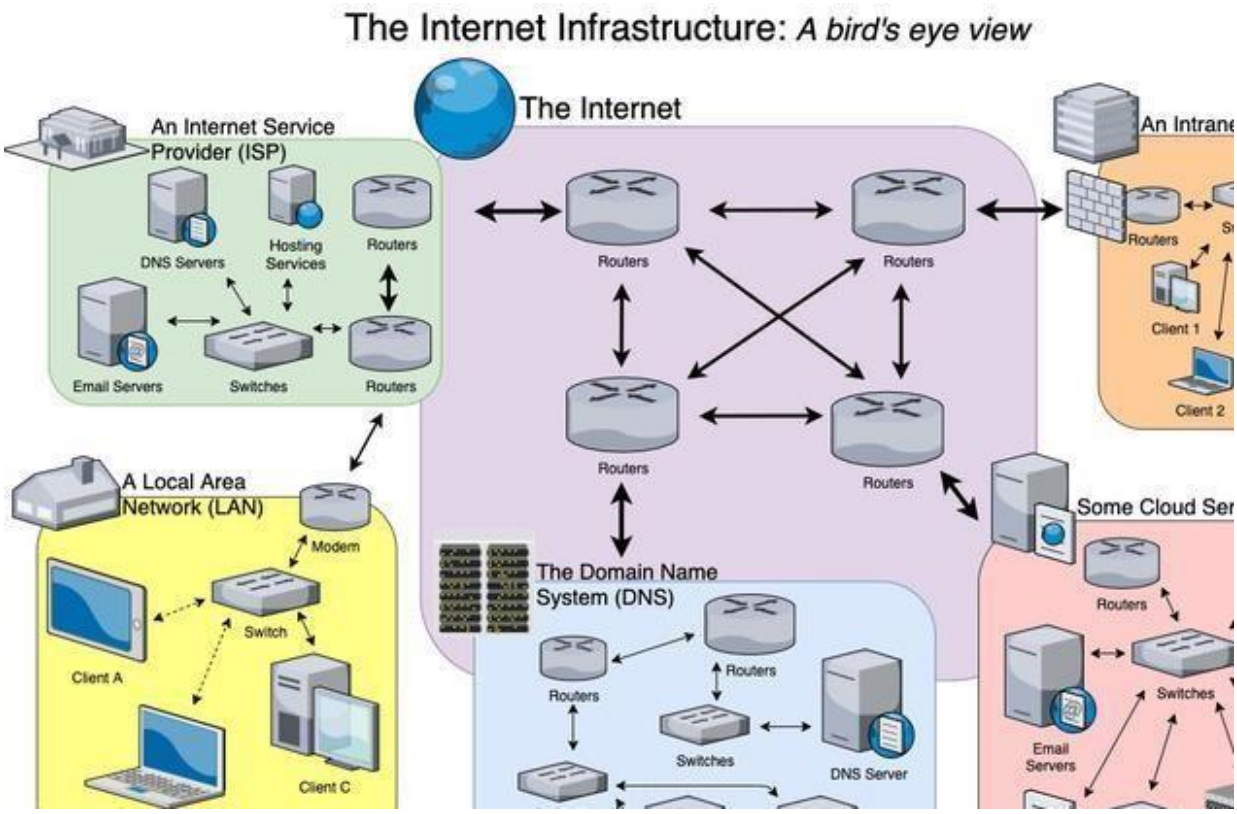


Figure: 2.5 Internet Structure

2.5 Standards in Networking

Standards are necessary in networking to ensure interconnectivity and interoperability between various networking hardware and software components. Without standards we would have proprietary products creating isolated islands of users which cannot interconnect.

Concept of Standard

Standards provide guidelines to product manufacturers and vendors to ensure national and international interconnectivity.

Data communications standards are classified into two categories:

1. De facto Standard

- These are the standards that have been traditionally used and mean by fact or by convention.
- These standards are not approved by any organized body but are adopted by widespread use.

2. De jure standard

- It means by law or by regulation.
- These standards are legislated and approved by an body that is officially recognized.

Standard Organizations in field of Networking

- Standards are created by standards creation committees, forums, and government regulatory agencies.
- Examples of Standard Creation Committees :
  1. International Organization for Standardization (ISO)
  2. International Telecommunications Union – Telecommunications Standard (ITU-T)
  3. American National Standards Institute (ANSI)
  4. Institute of Electrical & Electronics Engineers (IEEE)
  5. Electronic Industries Associates (EIA)
- Examples of Forums
  1. ATM Forum
  2. MPLS Forum
  3. Frame Relay Forum
- Examples of Regulatory Agencies:
  1. Federal Communications Committee (FCC).

Module-I

Chapter-3
Lecture-7

Physical Layer: Signals

Learning Objective:

3.1 Introduction
3.2 Data & Signals
3.3 Analog Signal

3.1 Introduction

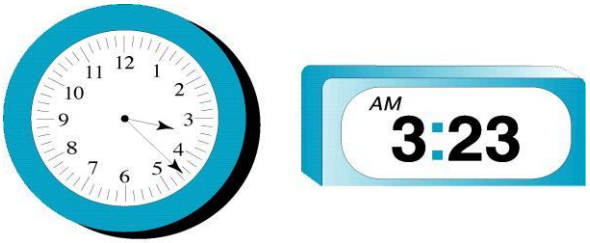
Computer networks are designed to transfer data from one point to another. During transit data is in the form of electromagnetic signals. Hence it is important to study data and signals before we move to further concepts in data communication.

3.2 Data & Signals

To be transmitted, data must be transformed to electromagnetic signals.

3.2.1. Data can be Analog or Digital.

1. Analog data refers to information that is continuous; ex. sounds made by a human voice
2. Digital data refers to information that has discrete states. Digital data take on discrete values. For example, data are stored in computer memory in the form of Os and 1s.



a. Analog b. Digital

3.2.2. Signals can be of two types:

1. Analog Signal: They have infinite values in a range.
2. Digital Signal: They have limited number of defined values

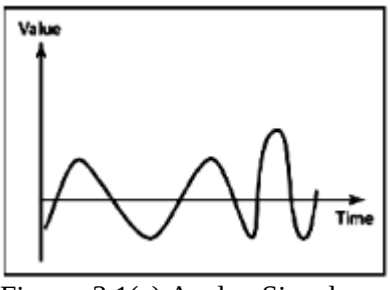


Figure: 3.1(a) Analog Signal

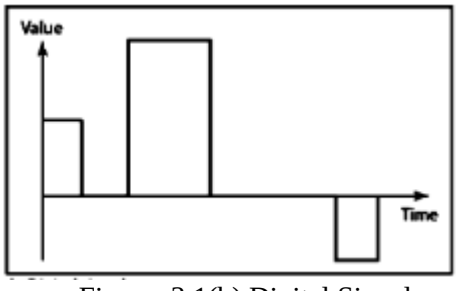


Figure: 3.1(b) Digital Signal

3.2.3 Periodic & Non Periodic Signals

- Signals which repeat itself after a fixed time period are called Periodic Signals.
- Signals which do not repeat itself after a fixed time period are called Non-Periodic Signals.
- In data communications, we commonly use **periodic analog signals and non-periodic digital signals**.

3.3 Analog Signal

- An analog signal has infinitely many levels of intensity over a period of time.
- A simple analog signal is a sine wave that cannot be further decomposed into simpler signals.

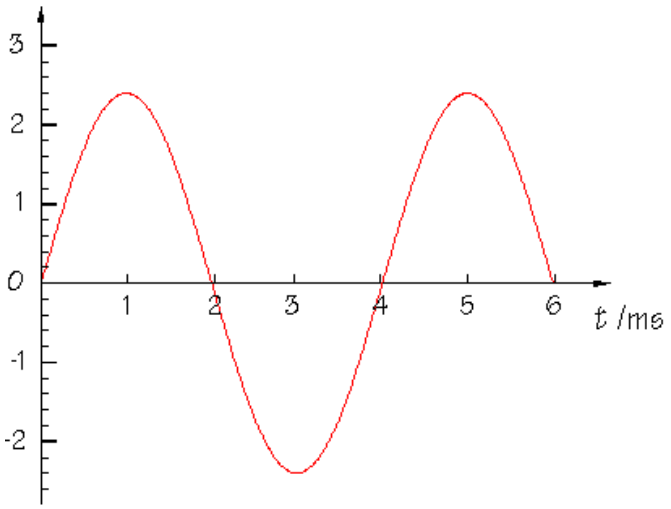


Figure: 3.2 Sine wave

A sine wave is characterized by three parameters:

1. Peak Amplitude
2. Frequency
3. Phase

3.3.1 Characteristics of an Analog Signal

3.3.1.1 Peak Amplitude

- The amplitude of a signal is the absolute value of its intensity at time t.
- The peak amplitude of a signal is the absolute value of the highest intensity.
- The amplitude of a signal is proportional to the energy carried by the signal.

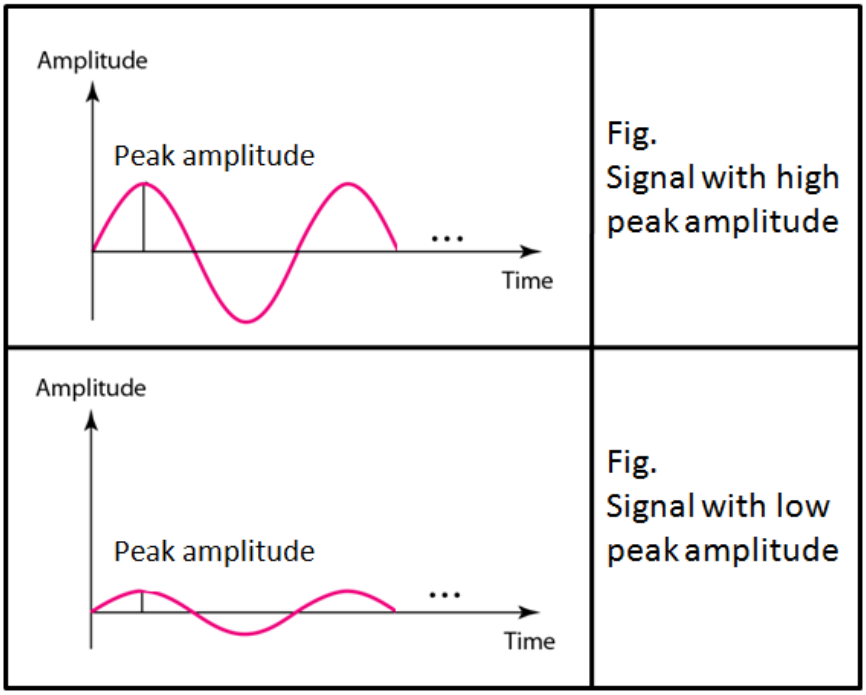


Figure: 3.3 Amplitude of a sine wave

3.3.1.2. Frequency

- Frequency refers to the number of cycles completed by the wave in one second.
- Period refers to the time taken by the wave to complete one second.

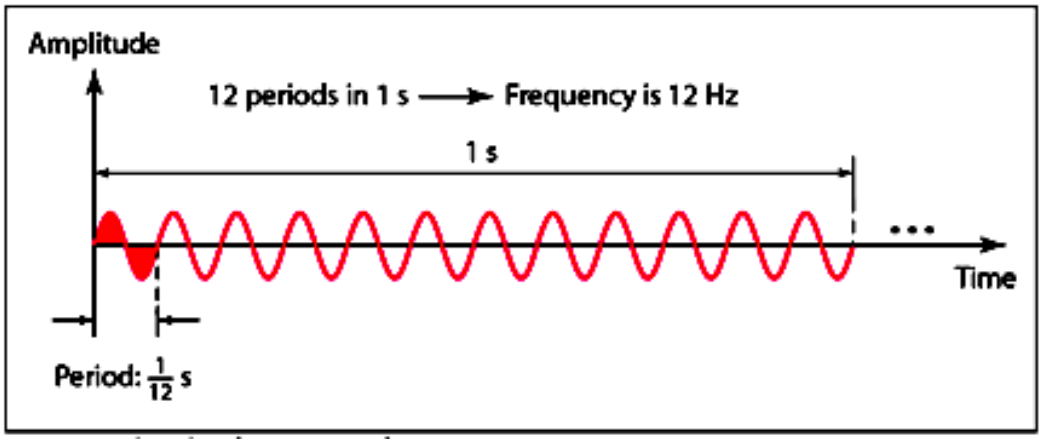


Figure: 3.4 Frequency & Period of a sine wave

3.3.1.3. Phase

- Phase describes the position of the waveform with respect to time (specifically relative to time O).

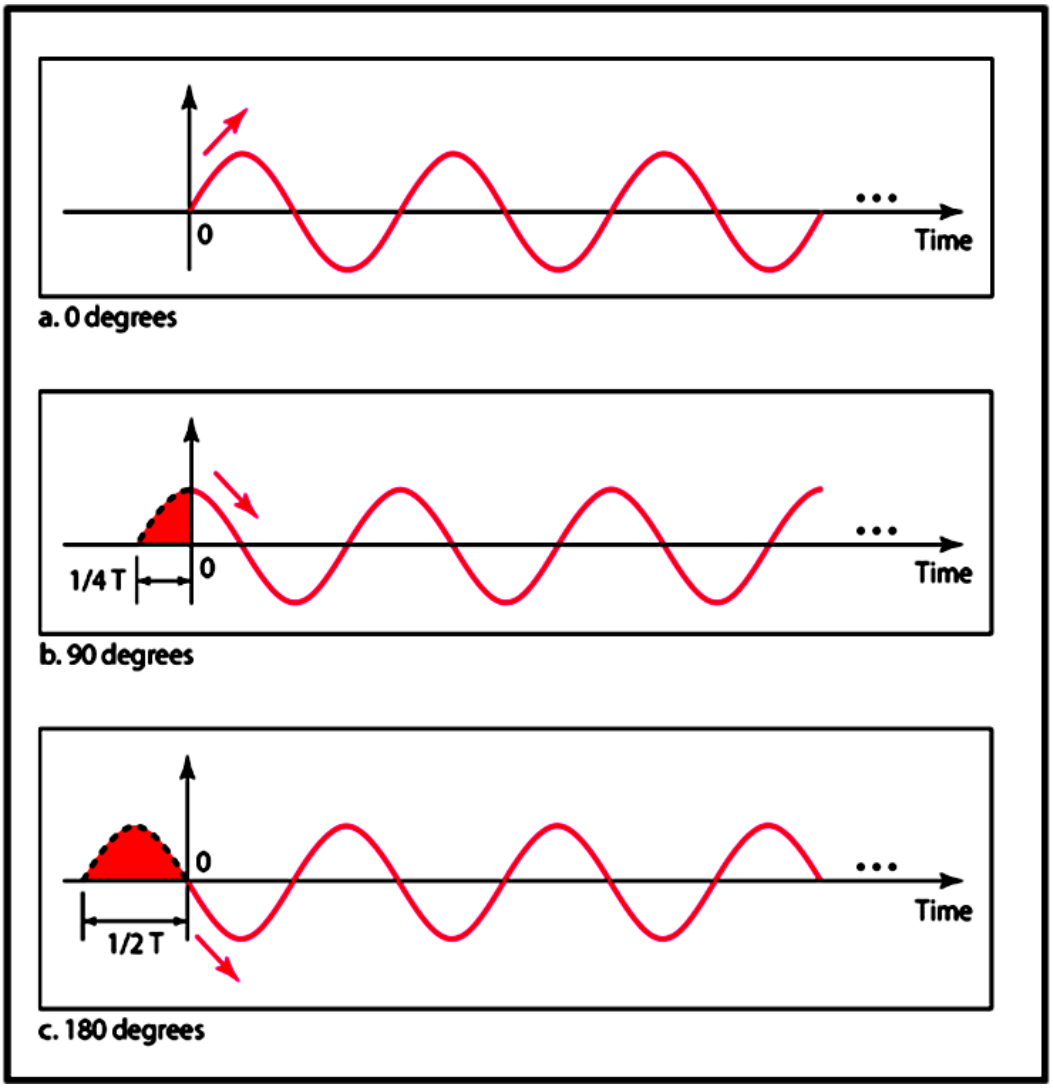


Figure: 3.5 Phase of a sine wave

- Phase indicates the forward or backward shift of the waveform from the axis.
- It is measured in degrees or radian.
- The figure above shows the sine waves with same amplitude and frequency but different phases.

3.3.2 Relation between Frequency & Period

- Frequency & Period are inverse of each other.
- It is indicated by the following formula:

$$T = 1/f$$
$$\text{Or}$$
$$f = 1/T$$

Example1. A wave has a frequency of 100hz. Its period(T) is given by

$$T = 1/f = 1/100 = 0.01 \text{ sec}$$

Example2. A wave completes its one cycle in 0.25 seconds. Its frequency is given by

$$f = 1/T = 1/0.25 = 4 \text{ Hz}$$

2.3.3 Wavelength

- The wavelength of a signal refers to the relationship between frequency (or period) and propagation speed of the wave through a medium.
- The wavelength is the distance a signal travels in one period.
- It is given by

  Wavelength = Propagation Speed X Period

  OR

  Wavelength = Propagation Speed X 1 / Frequency
- It is represented by the symbol : λ (pronounced as lamda)
- It is measured in micrometers

3.3.4. Time Domain and Frequency domain representation of signals

- A sine wave can be represented either in the time domain or frequency domain.
- The time-domain plot shows changes in signal amplitude with respect to time. It indicates time and amplitude relation of a signal.
- The frequency-domain plot shows signal frequency and peak amplitude.

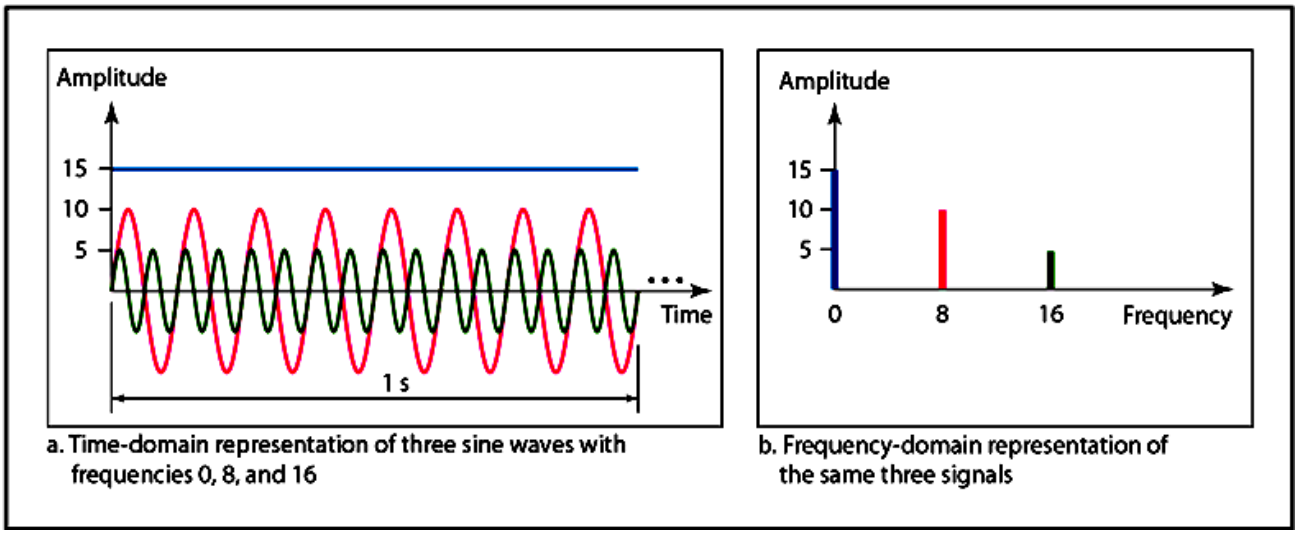


Figure: 3.6 Time domain and frequency domain plots of three sine waves

3.3.5. Composite Signal

A composite signal is a combination of two or more simple sine waves with different frequency, phase and amplitude.

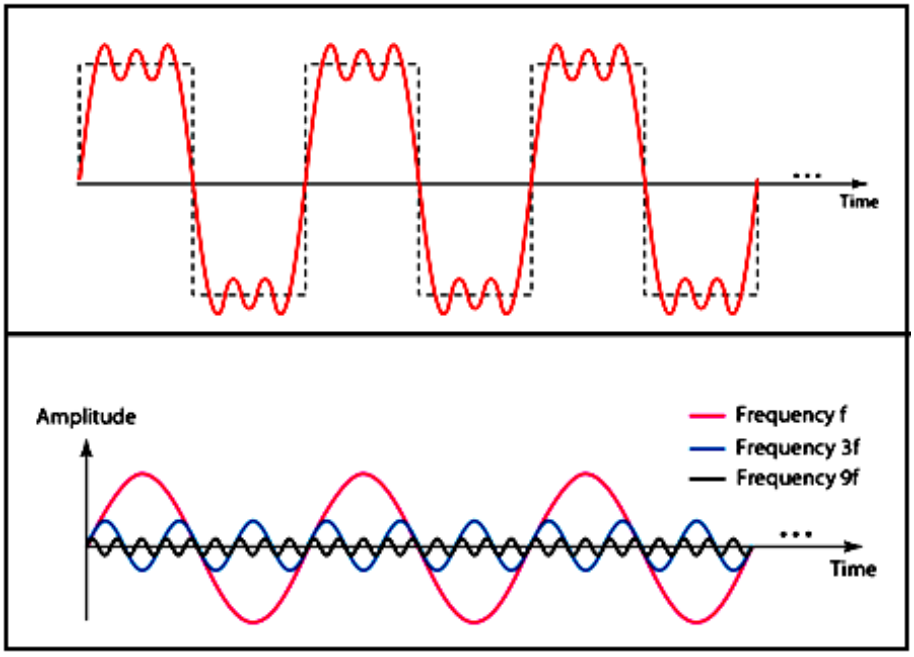


Figure: 3.7 A Composite signal with three component signals

- Composite signals can be periodic or non periodic.
- A periodic composite signal can be decomposed into a series of signals with discrete frequencies.
- A non-periodic signal when decomposed gives a combination of sine waves with continuous frequencies.

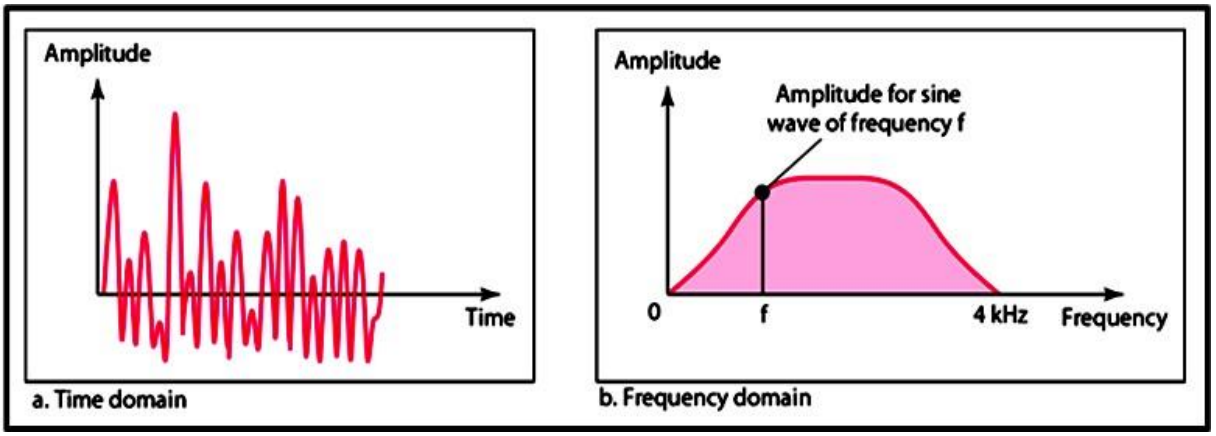


Figure: 3.8 The time and frequency domains of a non-periodic composite analog signal

Module-I

Chapter-3
Lecture-8

Learning Objective:
3.4 Digital Signal
3.5 Bandwidth
3.6 Types of Channels
3.7 Transmission of Digital signal

3.4 Digital Signal

- Information can also be explained in the form of a digital signal.
- A digital signal can be explained with the help of following points:

3.4.1 Definition:-

- A digital is a signal that has discrete values.
- The signal will have value that is not continuous.

3.4.2 LEVEL

- Information in a digital signal can be represented in the form of voltage levels.

- Ex. In the signal shown below, a '1' is represented by a positive voltage and a '0' is represented by a Zero voltage.

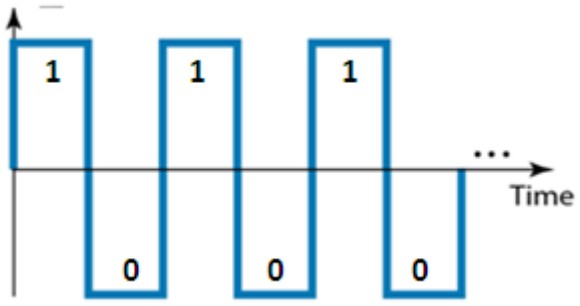


Figure:3.9 A digital signal with Two levels. „1" represented by a positive voltage and „0" represented by a negative voltage

- A Signal can have more than two levels

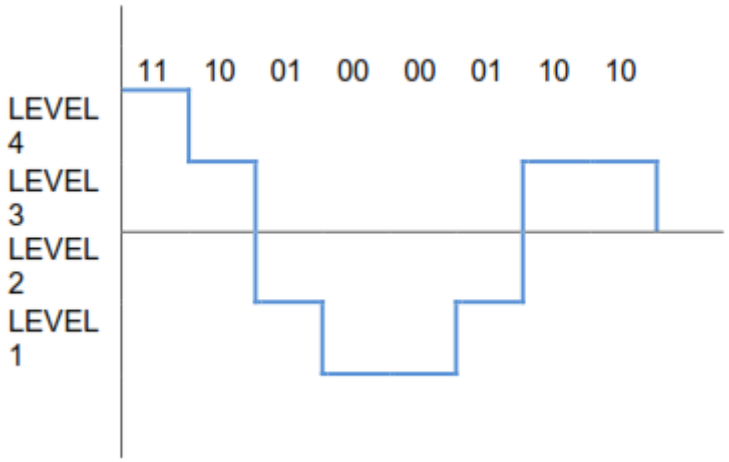


Figure: 3.10 A digital signal with four levels

In general, if a signal has L levels then, each level need Log_2L bits
Example: Consider a digital Signal with four levels, how many bits are required per level?
Answer: Number of bits per level = Log_2L
$= Log_24$
$= 2$
Hence, 2 bits are required per level for a signal with four levels.

3.4.3 Bit Length or Bit Interval (T_b)

- It is the time required to send one bit.
- It is measured in seconds.

3.4.4 Bit Rate

- It is the number of bits transmitted in one second.
- It is expressed as bits per second (bps).
- Relation between bit rate and bit interval can be as follow

  Bit rate = 1 / Bit interval

3.4.5 Baud Rate

- It is the rate of Signal Speed, i.e the rate at which the signal changes.
- A digital signal with two levels =0‘ & =1‘ will have the same baud rate and bit rate & bit rate.
- The diagram below shows three signal of period (T) 1 second
  a) Signal with a bit rate of 8 bits/ sec and baud rate of 8 baud/sec
  b) Signal with a bit rate of 16 bits/ sec and baud rate of 8 baud/sec
  c) Signal with a bit rate of 16 bits/ sec and baud rate of 4 baud/sec

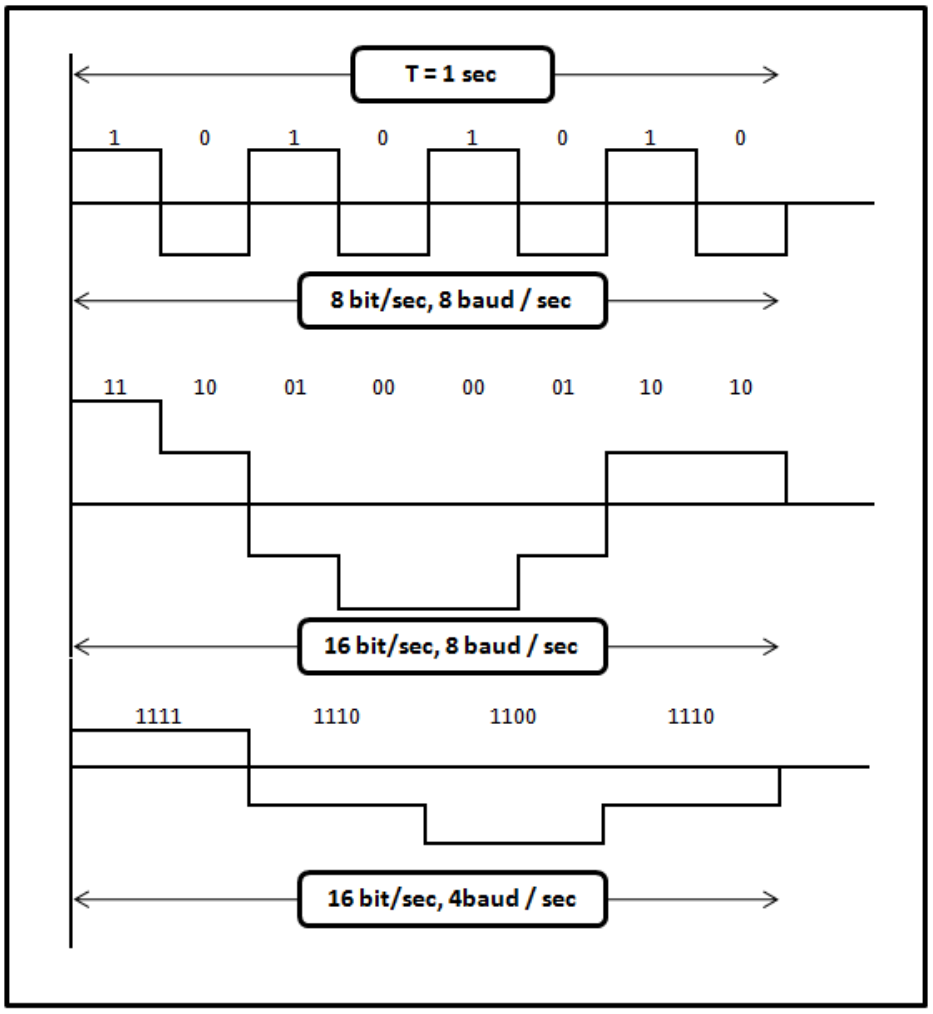


Figure: 3.11 Three signals with different bit rates and baud rates

3.5 BANDWIDTH OF A SIGNAL

- Bandwidth can be defined as the portion of the electromagnetic spectrum occupied by the signal.
- It may also be defined as the frequency range over which a signal is transmitted.
- Different types of signals have different bandwidth. Ex. Voice signal, music signal, etc

3.5.1 Bandwidth of an analog signal

- Bandwidth of an analog signal is expressed in terms of its frequencies.
- It is defined as the range of frequencies that the composite analog signal carries.
- It is calculated by the difference between the maximum frequency and the minimum frequency.
- Consider the signal shown in the diagram below:

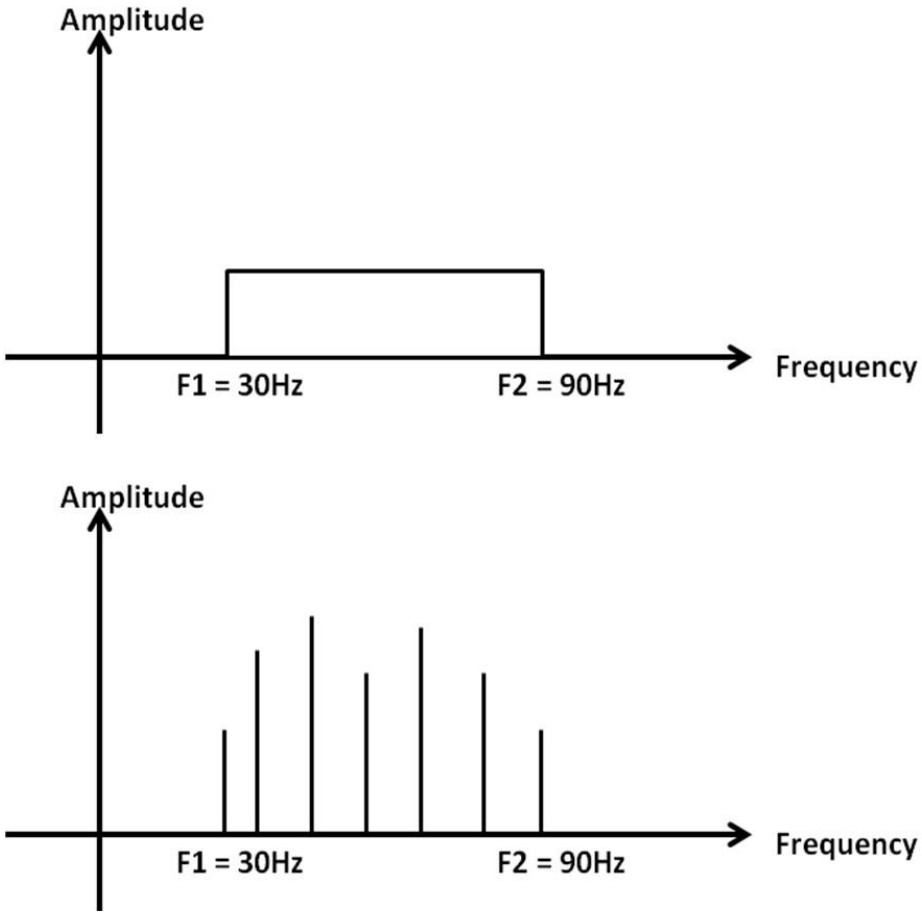


Figure: 3.12 Bandwidth of a signal in time domain and frequency domain

- The signal shown in the diagram is an composite analog signal with many component signals.
- It has a minimum frequency of F1 = 30Hz and maximum frequency of F2 = 90Hz.
- Hence the bandwidth is given by F2 – F1 = 90 – 30 = 60 Hz

3.5.2 Bandwidth of a digital signal

- It is defined as the maximum bit rate of the signal to be transmitted.
- It is measured in bits per second.

3.6 Types of Channels

Each composite signal has a lowest possible (minimum) frequency and a highest possible (maximum) frequency. From the point of view of transmission, there are two types of channels:

3.6.1 Low pass Channel

- This channel has the lowest frequency as ‘0‘ and highest frequency as some non-zero frequency ‘f1‘.
- This channel can pass all the frequencies in the range 0 to f1.

3.6.2 Band pass channel

- This channel has the lowest frequency as some non-zero frequency ‘f1’ and highest frequency as some non-zero frequency ‘f2‘.
- This channel can pass all the frequencies in the range f1 to f2.

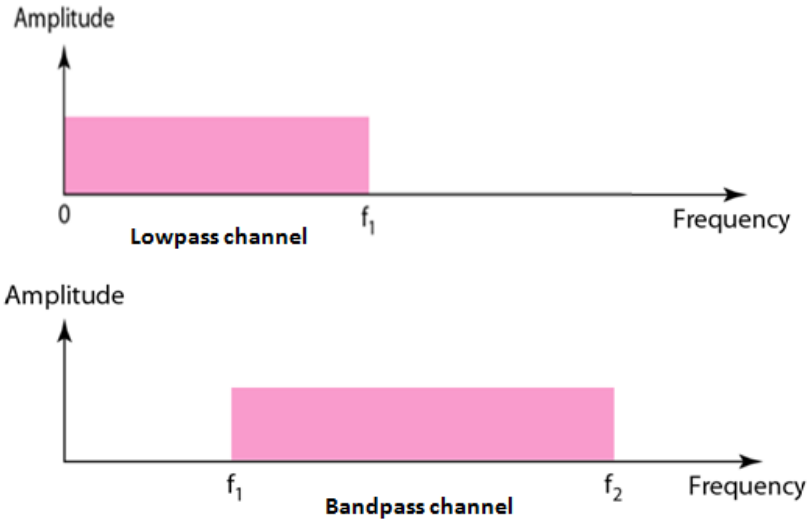


Figure: 3.13 Low-pass Channel & Band-pass Channel

3.7 Transmission of Digital signal

Digital signal can be transmitted in the following two ways:

3.7.1 Baseband Transmission

- The signal is transmitted without making any change to it (ie. Without modulation)
- In baseband transmission, the bandwidth of the signal to be transmitted has to be less than the bandwidth of the channel.

2.6.2 Broad band Transmission

- Given a bandpass channel, a digital signal cannot be transmitted directly through it
- In broadband transmission we use modulation, i.e we change the signal to analog signal before transmitting it.
- The digital signal is first converted to an analog signal, since we have a bandpass channel we cannot directly send this signal through the available channel.

Module-I

Chapter-3
Lecture-9

Learning Objective:

3.8 Data Rate Limits

3.9 Transmission Impairment

3.8 Data Rate Limits

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)

The quality of the channel indicates two types:

a) A Noiseless or Perfect Channel

- An ideal channel with no noise.
- The Nyquist Bit rate derived by Henry Nyquist gives the bit rate for a Noiseless Channel.

b) A Noisy Channel

- A realistic channel that has some noise.
- The Shannon Capacity formulated by Claude Shannon gives the bit rate for a Noisy Channel

3.8.1 Nyquist Bit Rate

The Nyquist bit rate formula defines the theoretical maximum bit rate for a noiseless channel

$$\text{Bit rate} = 2 \times \text{Bandwidth} \times \text{Log}_2 L$$

Where,

- Bitrate is the bitrate of the channel in bits per second
- Bandwidth is the bandwidth of the channel
- L is the number of signal levels.

Example

What is the maximum bit rate of a noiseless channel with a bandwidth of 5000 Hz transmitting a signal with two signal levels?

Solution:

The bit rate for a noiseless channel according to Nyquist Bit rate can be calculated as follows:

$$\text{BitRate} = 2 \times \text{Bandwidth} \times \text{Log}_2 L$$
$$= 2 \times 5000 \times \log_2 2 = \mathbf{10000\ bps}$$

3.8.2 Shannon Capacity

The Shannon Capacity defines the theoretical maximum bit rate for a noisy channel

$$\text{Capacity} = \text{bandwidth} \times \log_2 (1 + \text{SNR})$$

Where,

- Capacity is the capacity of the channel in bits per second
- Bandwidth is the bandwidth of the channel
- SNR is the Signal to Noise Ratio. $\text{SNR} = \frac{average\ \ signal\ \ power}{average\ noise\ power}$

Example:

Calculate the bit rate for a noisy channel with SNR 300 and bandwidth of 3000Hz.

Solution:

The bit rate for a noisy channel according to Shannon Capacity can be calculated as follows:

$$\text{Capacity} = \text{bandwidth} \times \log_2 (1 + \text{SNR})$$
$$= 3000 \times \log_2 (1 + 300)$$
$$= 3000 \times \log_2 (301) = 3000 \times 8.23 = \mathbf{24{,}690bps}$$

3.9 Transmission Impairment

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the 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.

3.9.1 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. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

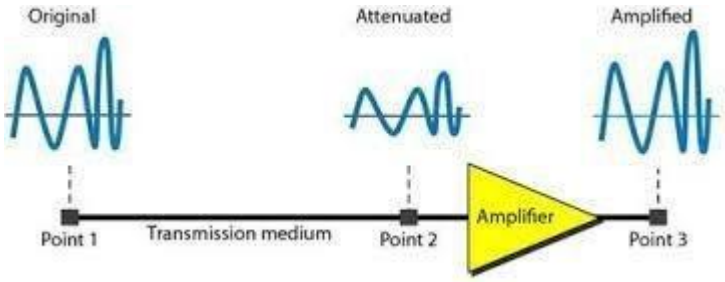


Figure: 3.14 Attenuation & Amplification

3.9.2 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. In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same.

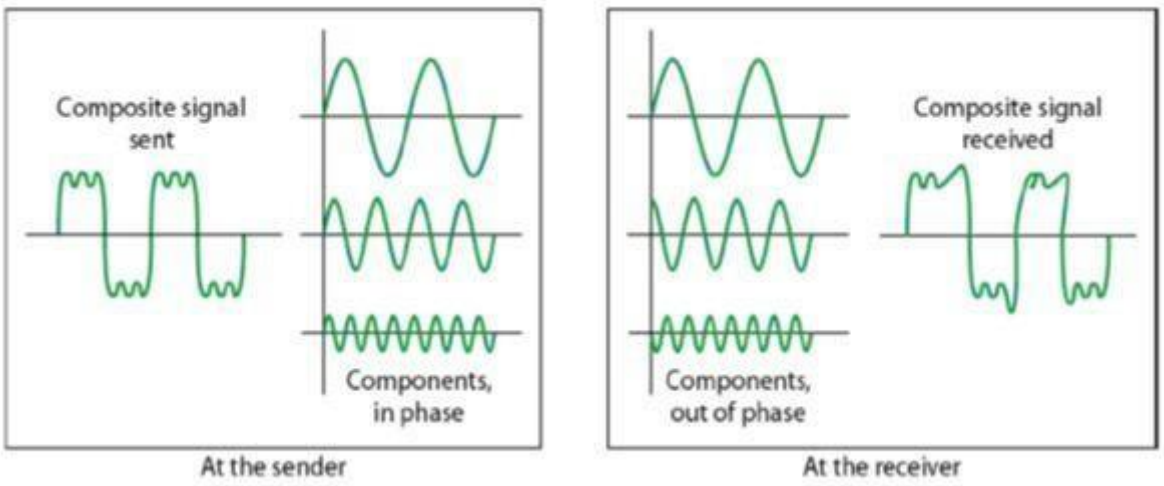


Figure: 3.15 Distortion

3.9.3 Noise

Noise is defined as an unwanted data. When some electromagnetic signal gets inserted during the transmission, it is generally called as a Noise. Due to Noise it is difficult to retrieve the original data or information.

- Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter.
- 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.
- Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.
- Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.

Short Questions

1. What is the relationship between frequency and period?

Ans - Frequency & Period are inverse of each other. It is indicated by the following formula: T=1/f or f=1/T.

2. What is wavelength?

Ans - The wavelength of a signal refers to the relationship between frequency (or period) and propagation speed of the wave through a medium.

The wavelength is the distance a signal travels in one period.

It is given by

Wavelength = Propagation Speed X Period

OR

Wavelength =Propagation Speed X 1 / Frequency

3. Define Bit rate and baud rate.

Ans - Bit rate is the number of bits transmitted in one second.

Baud rate is the rate of Signal Speed, i.e the rate at which the signal changes

4. What are the different types of channels?

Ans - Low pass Channel : This channel has the lowest frequency as '0' and highest frequency as some non-zero frequency 'f1'. This channel can pass all the frequencies in the range 0 to f1.

Band pass channel: This channel has the lowest frequency as some non-zero frequency 'f1' and highest frequency as some nonzero frequency 'f2'. This channel can pass all the frequencies in the range f1 to f2.

5. Define Nyquist Data rate.

Ans - The Nyquist bit rate formula defines the theoretical maximum bit rate for a noiseless channel

Bit rate = 2 x Bandwidth x Log_2 L.

Long Questions

1. Write a short note on Transmission Impairment.

Module-I

Chapter-4
Lecture-10

Digital Transmission

Learning Objective:

4.1 Digital to Digital Conversion

4.1.1 Line Encoding

Digital Transmission

A computer network is designed to send information from one point to another. This information needs to be converted to either a digital signal or an analog signal for transmission.

4.1 Digital to Digital Conversion

The conversion involves three techniques: line coding, block coding, and scrambling.

4.1.1 Line Encoding

- It is the process of converting Digital data into digital signal.
- In other words, it is converting of binary data(i.e. A sequence of bits) into digital signal (i.e. a sequence of discrete, discontinuous voltage pulses)

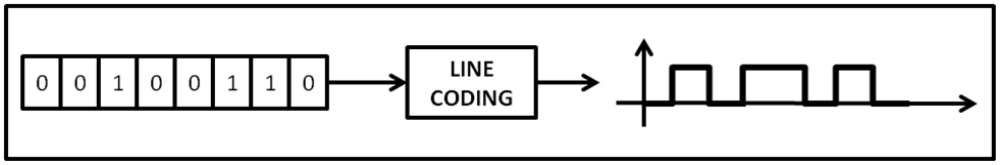


Figure: 4.1 Line Coding

Classification of Line Codes

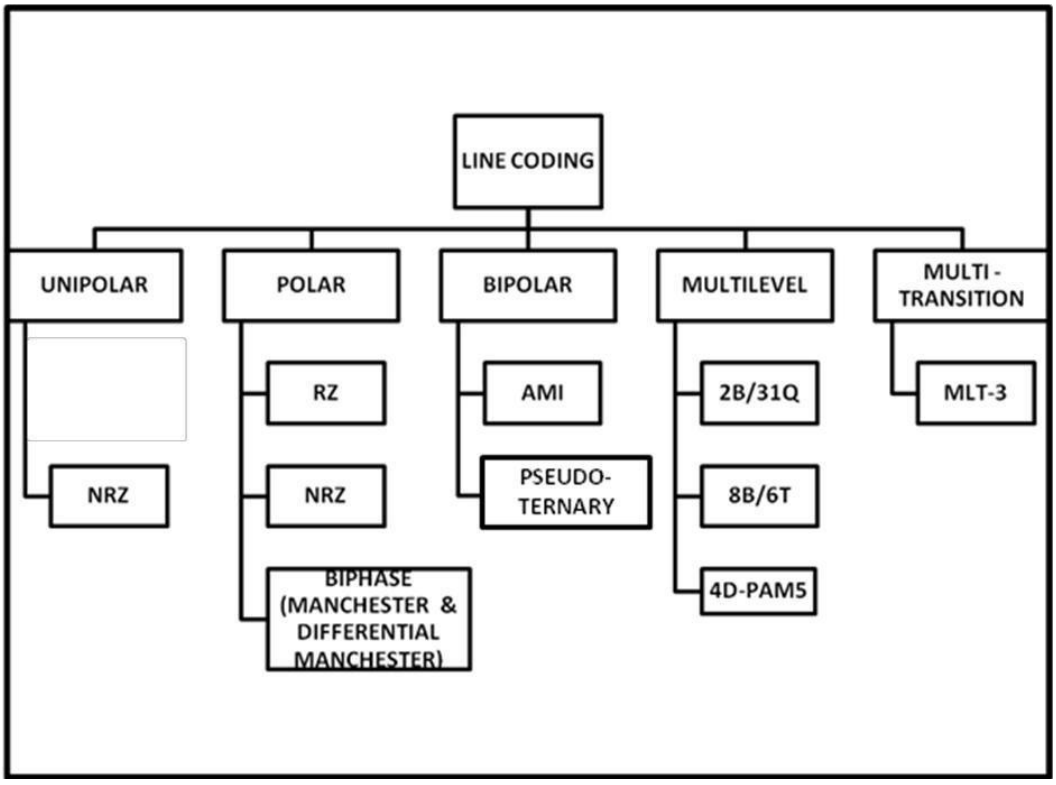


Figure: 4.2 Classification of Line Codes

4.1.1.1 Unipolar

- All signal levels are either above or below the time axis.
- NRZ - Non Return to Zero scheme is an example of this code. The signal level does not return to zero during a symbol transmission.

4.1.1.2 Polar

- **Polar NRZ**
  - **voltages** are on both sides of the time axis.

  Polar NRZ scheme can be implemented with two voltages. E.g. +V for 1 and -V for 0.

  There are two variations:
  - **NZR - Level (NRZ-L)** - positive voltage for one symbol and negative for the other
  - **NRZ - Inversion (NRZ**-I) - the change or lack of change in polarity determines the value of a symbol. E.g. a '1' symbol inverts the polarity a '0' does not.
- **Polar – RZ**
  - The Return to Zero (RZ) scheme uses three voltage values. +, 0, -.
  - Each symbol has a transition in the middle. Either from high to zero or from low to zero.
  - More complex as it uses three voltage level.

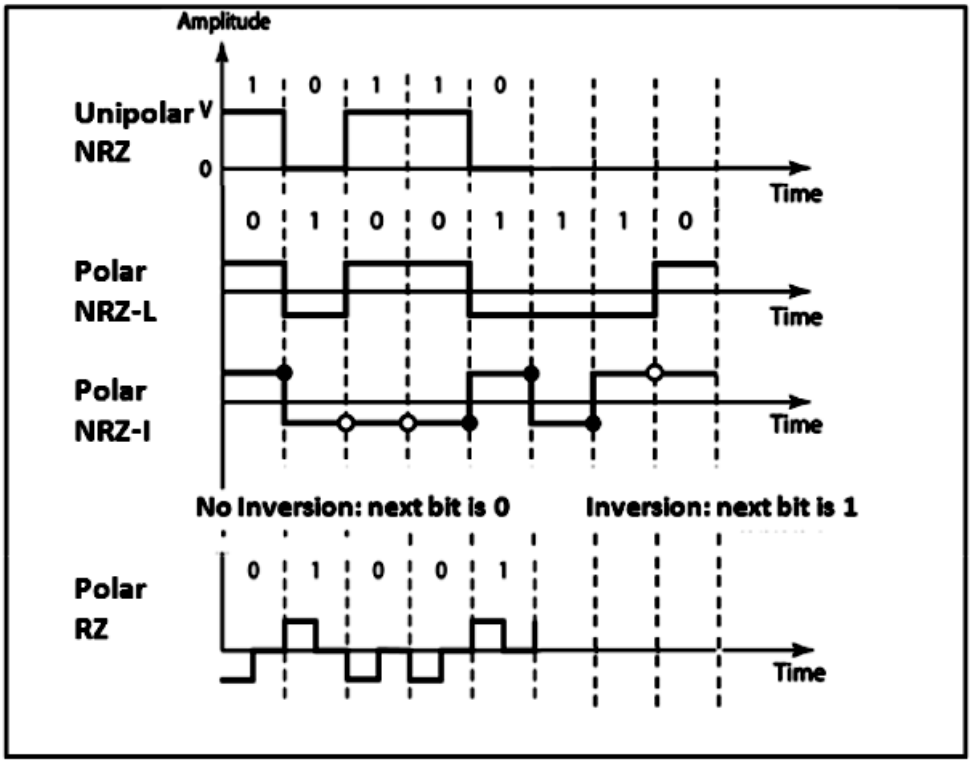


Figure: 4.3 Unipolar(NRZ) & Polar(RZ & NRZ) Encoding

- **Polar - Biphase**
  - **Manchester and Differential Manchester Manchester coding** is a combination of NRZ-L and RZ schemes. Every symbol has a level transition in the middle: from high to low or low to high. It uses only two voltage levels.
  - **Differential Manchester coding** consists of combining the NRZ-I and RZ schemes. Every symbol has a level transition in the middle. But the level at the beginning of the symbol is determined by the symbol value. One symbol causes a level change the other does not.

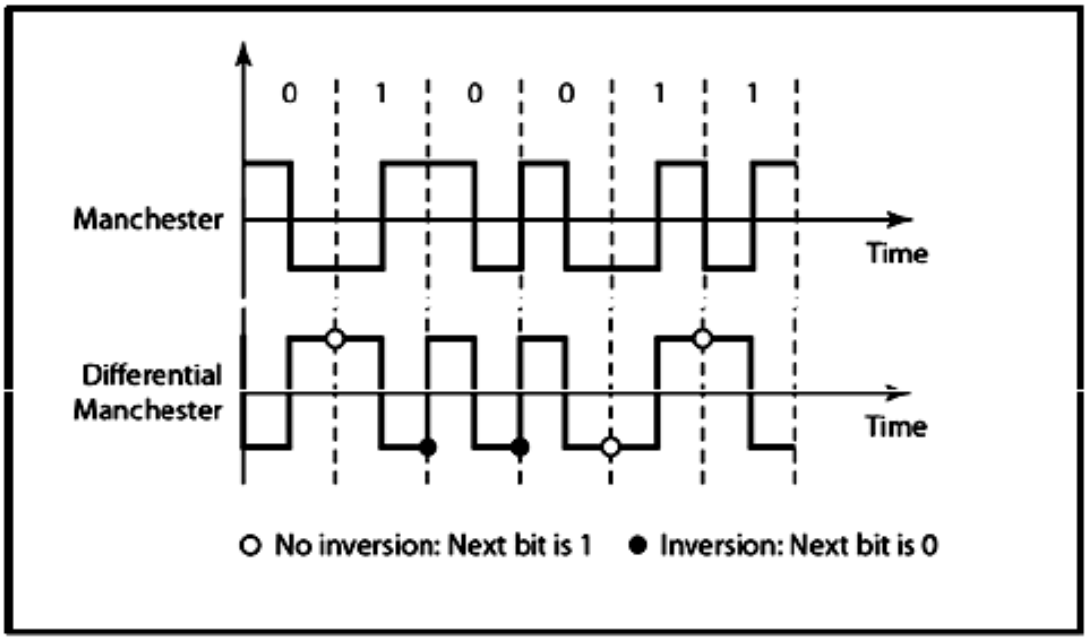


Figure: 4.4 Polar biphase: Manchester and differential Manchester coding schemes

4.1.1.3 Bipolar - AMI and Pseudoternary

- This coding scheme uses 3 voltage levels +, 0, -, to represent the symbols .
- Voltage level for one symbol is at '0' and the other alternates between + & -.
  - **Bipolar Alternate Mark Inversion (AMI)** - the '0' symbol is represented by zero voltage and the '1' symbol alternates between +V and -V.
  - **Pseudoternary** is the reverse of AMI.

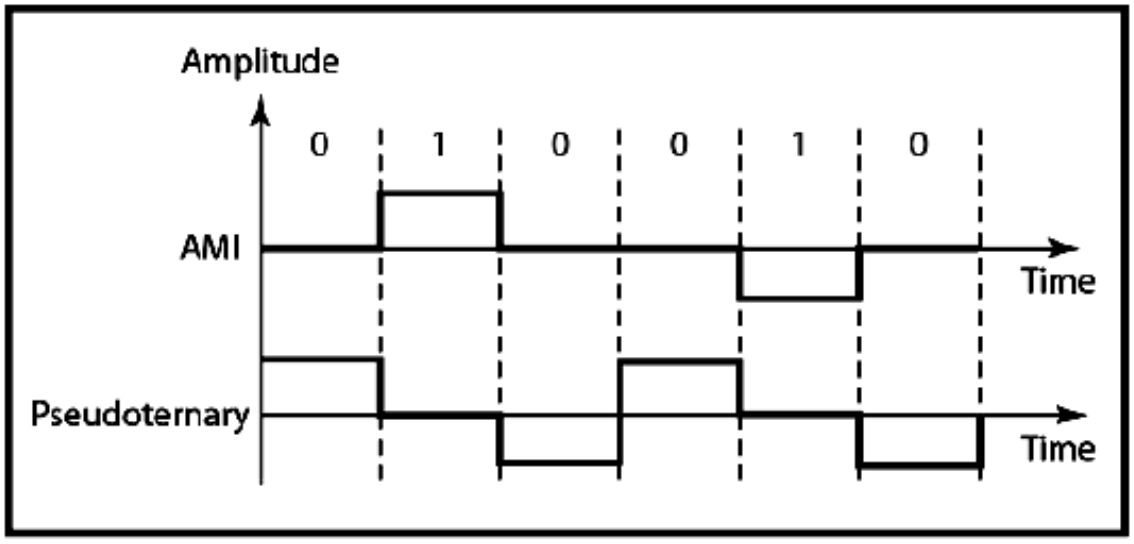


Figure: 4.5 Bipolar coding scheme - AMI and Pseudoternary

4.1.1.4 Multilevel

These types of codings are classified as **mBnL** schemes. In***mBnL*** schemes, a pattern of *m* data elements is encoded as a pattern of *n* signal elements in which $2^m < L^n$

.

- **2B1Q (**two binary, one quaternary**)**
  Here m = 2; n = 1 ; Q = 4. It uses data patterns of size 2 and encodes the 2-bit patterns as one signal element belonging to a four-level signal.

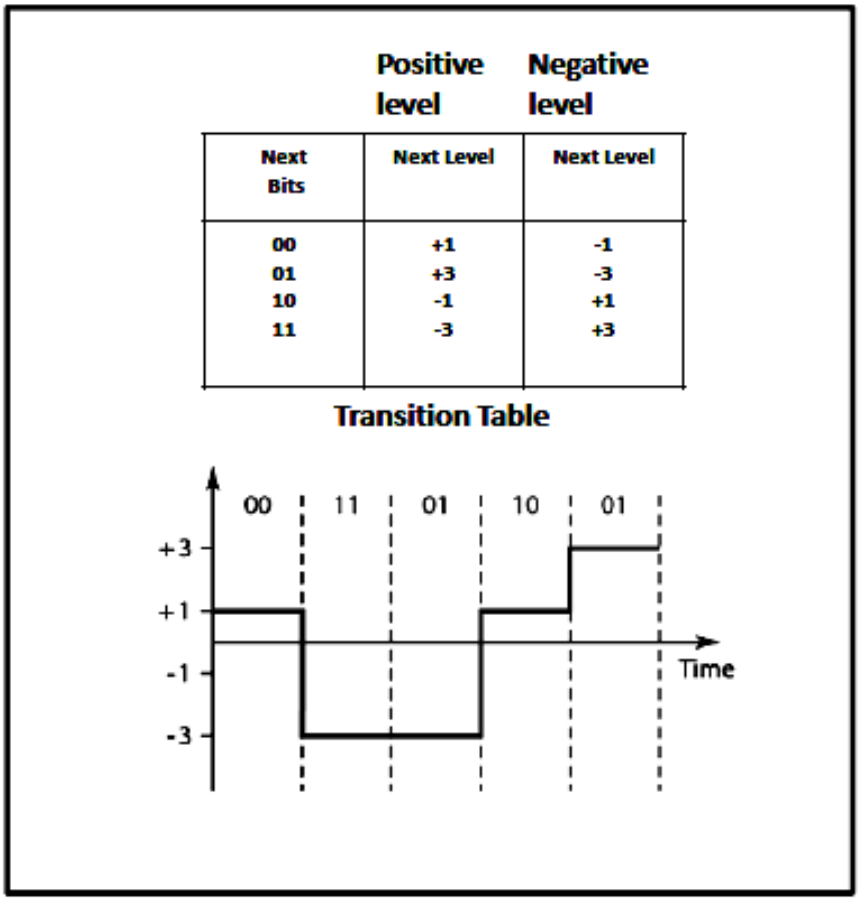


Figure: 4.6 Multilevel coding scheme : 2B1Q

- **8B6T(eight binary, six ternary)**

Here a pattern of 8 bits is encoded a pattern of 6 signal elements, where the signal has three levels
Here m = 8; n = 6 ; T = 3
So we can have 2^8 =256 different data patterns and 3^6=478 different signal patterns.

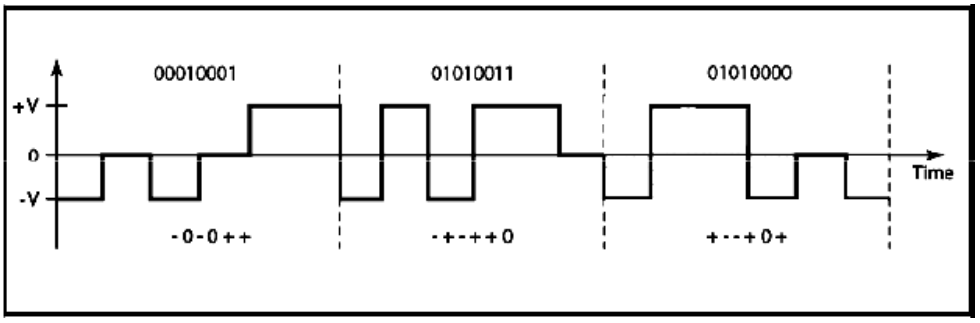


Figure: 4.7 Multilevel coding scheme : 8B6T

4.1.1.5 Multitransition

- **MLT-3**

Signal rate is same as NRZ-I

- Uses three levels (*+v,* 0, and - *V)* and three transition rules to move between the levels.
  - If the next bit is 0, there is no transition.
  - If the next bit is 1 and the current level is not 0, the next level is 0.
  - If the next bit is 1 and the current level is 0, the next level is the opposite of the last nonzero level.

Module-I

Chapter-4
Lecture-11

Learning Objective:

4.1 Digital to Digital Conversion

4.1.2 Block Coding

4.1.3 Scrambling

4.1.2 Block Coding

Block coding adds redundancy to line coding so that error detection can be implemented. Block coding changes a block of *m* bits into a block of *n* bits, where *n* is larger than *m*. Block coding is referred to as an *mB/nB* encoding technique. The additional bits added to the original -m bits‖ are called parity bits or check bits.

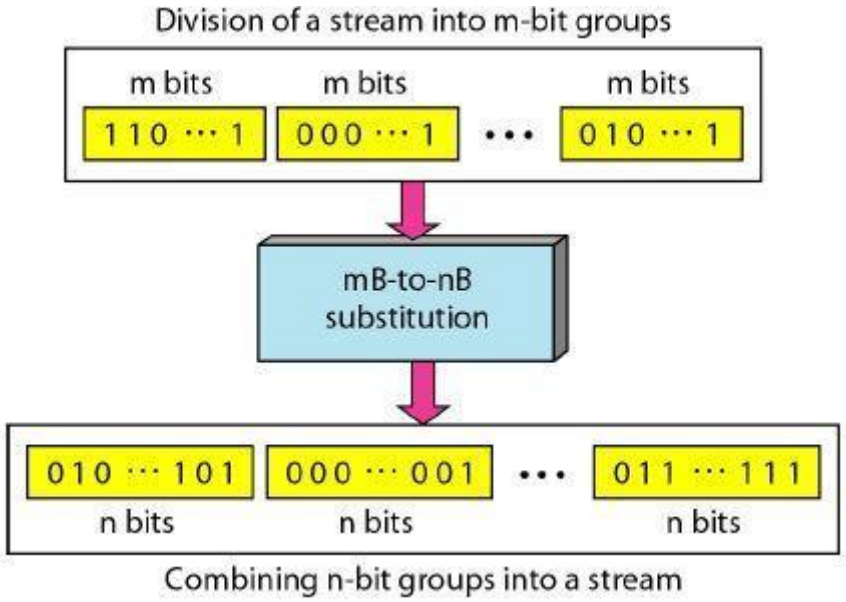


Figure: 4.8 Block Coding

Block coding normally involves three steps: division, substitution, and combination. In the division step, a sequence of bits is divided into groups of m bits. The heart of block coding is the substitution step. In this step, we substitute an m-bit group for an n-bit group. For example, in 4B/5B encoding we substitute a 4-bit code for a 5-bit group. Finally, the n-bit groups are combined together to form a stream. The new stream has more bits than the original bits.

- **4B/5B**

The four binary/five binary (4B/5B) coding scheme was designed to be used in combination with NRZ-I.

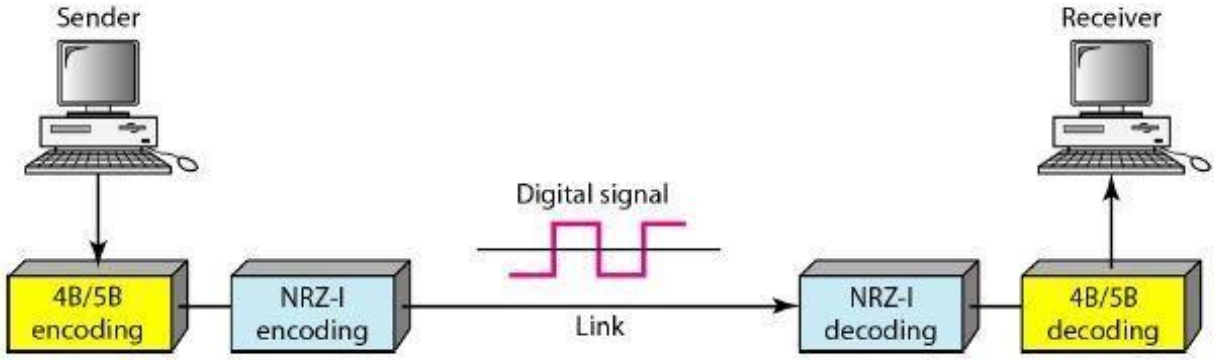


Figure: 4.9 Block coding 4B/5B with NRZ-I line coding scheme

- **8B/10B**

The eight binary/ten binary (8B/10B) encoding is similar to 4B/5B encoding except that a group of 8 bits of data is now substituted by a l0-bit code. It provides greater error detection capability than 4B/5B. The 8B/10B block coding is actually a combination of 5B/6B and 3B/4B encoding.

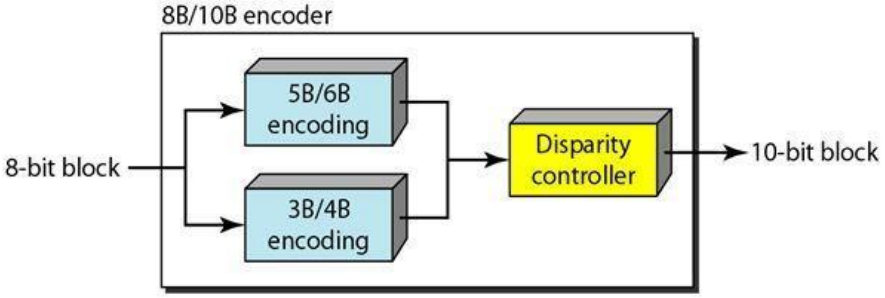


Figure: 4.10 8B/10B block encoding

4.1.3 Scrambling

Scrambling substitutes long zero-level pulses with a combination of other levels to provide synchronization. We modify part of the AMI rule to include scrambling. Two common scrambling techniques are B8ZS and HDB3.

4.1.3.1 Bipolar with 8-zero substitution (B8ZS)

In this technique, eight consecutive zero-level voltages are replaced by the sequence OOOVBOVB. The V in the sequence denotes violation; this is a nonzero voltage that breaks an AMI rule of encoding (opposite polarity from the previous). The B in the sequence denotes bipolar; which means a nonzero level voltage in accordance with the AMI rule.

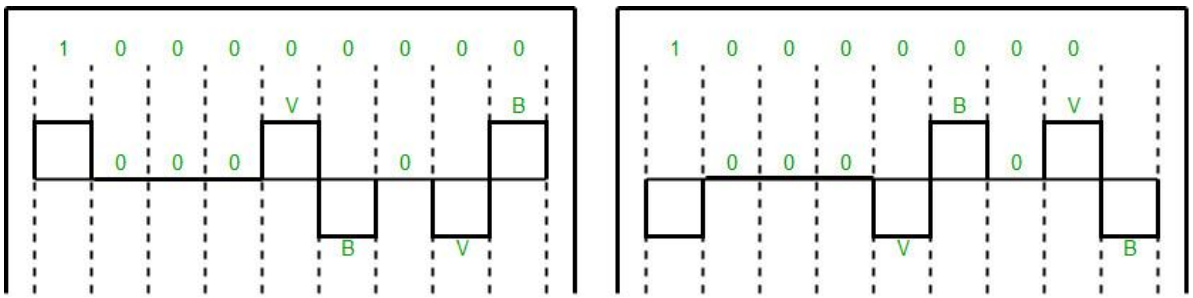


Figure: 4.11 Two cases ofB8ZS scrambling technique

4.1.3.2 High-density bipolar 3-zero (HDB3)

In this technique, four consecutive zero-level voltages are replaced with a sequence of OOOV or BOOV. The two rules can be stated as follows:

1. If the number of nonzero pulses after the last substitution is odd, the substitution pattern will be **OOOV**, which makes the total number of nonzero pulses even.

2. If the number of nonzero pulses after the last substitution is even, the substitution pattern will be **BOOV**, which makes the total number of nonzero pulses even.

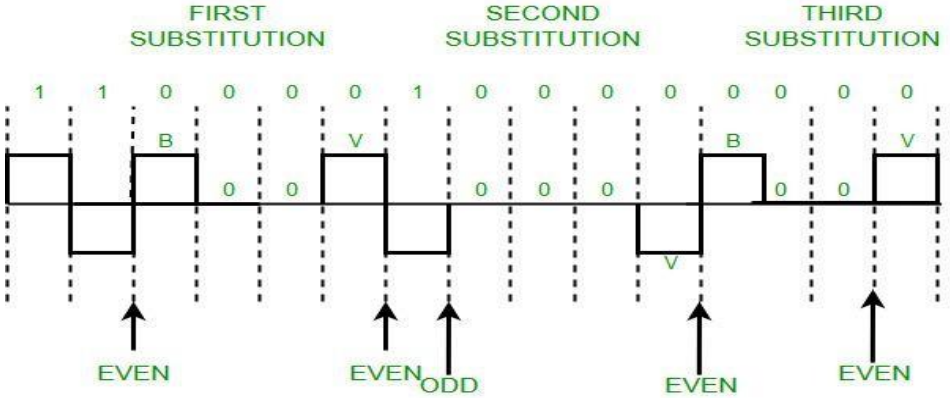


Figure: 4.12 HDB3 scrambling technique

Module-I

Chapter-4
Lecture-12

Learning Objective:

4.2 Analog to Digital Conversion

4.3 Transmission Modes

4.2 Analog to Digital Conversion

It converts analog signals to digital signals. There are two basic approaches: pulse code modulation and delta modulation.

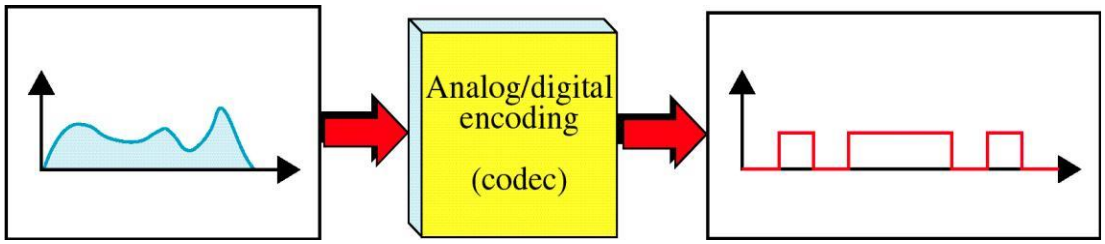


Figure: 4.13 Analog to Digital Conversion

4.2.1 Pulse Code Modulation (PCM)

Pulse Code Modulation involves the following three basic steps as shown in Figure: 4.14

1. The analog signal is sampled (PAM).
2. The sampled signal is quantized.
3. The quantized values are encoded as streams of bits.

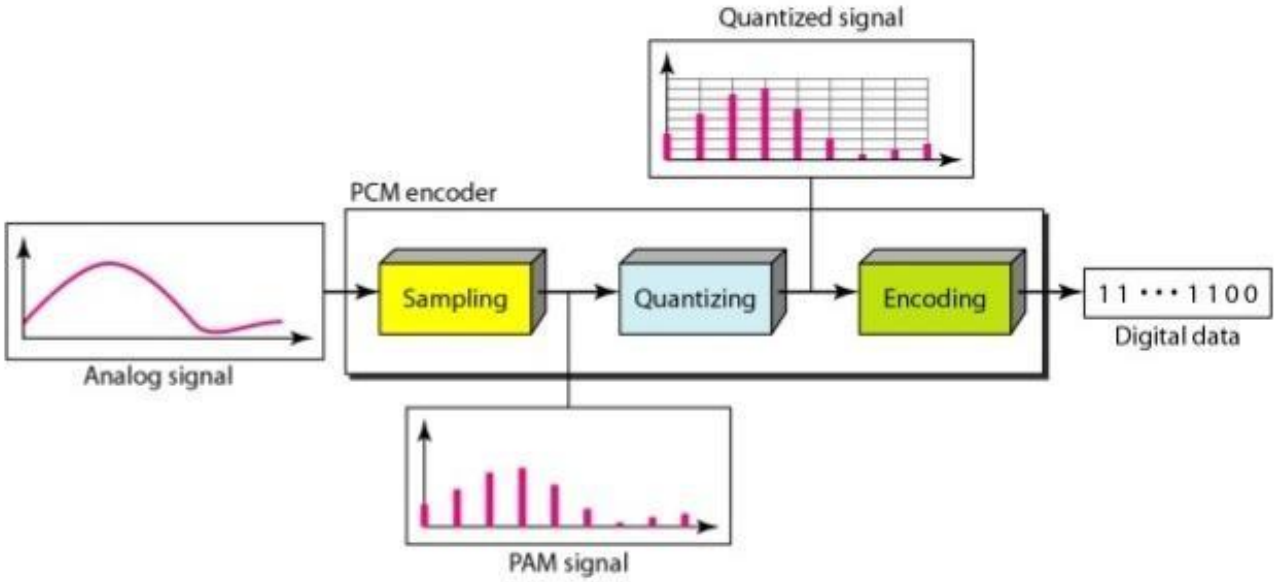


Figure: 4.14 Components of PCM

Sampling

The analog signal is sampled every T_s s, where T_s is the sample interval or the period. There are three sampling methods-ideal, natural, and flat-top. According to the Nyquist theorem, to reproduce the original analog signal, one necessary condition is that the sampling rate be at least twice the highest frequency in the original signal. The sampling process is sometimes referred to as **pulse amplitude modulation (PAM).**

Quantization

Quantization is the process in which we assign the numbers to the discrete values depending upon their amplitude values. Quantizer converts the sampled signal into an approximate quantized signal which consists of only finite number of predecided voltage levels. Each sampled value at the input of the quantizer is approximated or rounded to the nearest standard predecided voltage level (Quantization levels).

Encoding

The last step in PCM is encoding. After each sample is quantized and the number of bits per sample is decided, each sample can be changed to an n_b-bit code word. Note that the number of bits for each sample is determined from the number of quantization levels. If the number of quantization levels is L, the number of bits is $n_b = \log_2 L$..

4.2.2 Delta Modulation (DM)

Delta Modulation is a very popular alternative of PCM with much reduced complexity. Here the analog input is approximated by a staircase function, which moves up or down by one quantization level (a constant amount) at each sampling interval. Each sample delta modulation process can be represented by a single binary digit, which makes it more efficient than the PCM technique. In this modulation technique, instead of sending the entire encodingof each and every sample, we just send the change from previous sample. If the difference between analog input and the feedback signal is positive, then encoded output is 1, otherwise it is 0. So, only one bit is to be sent per sample.

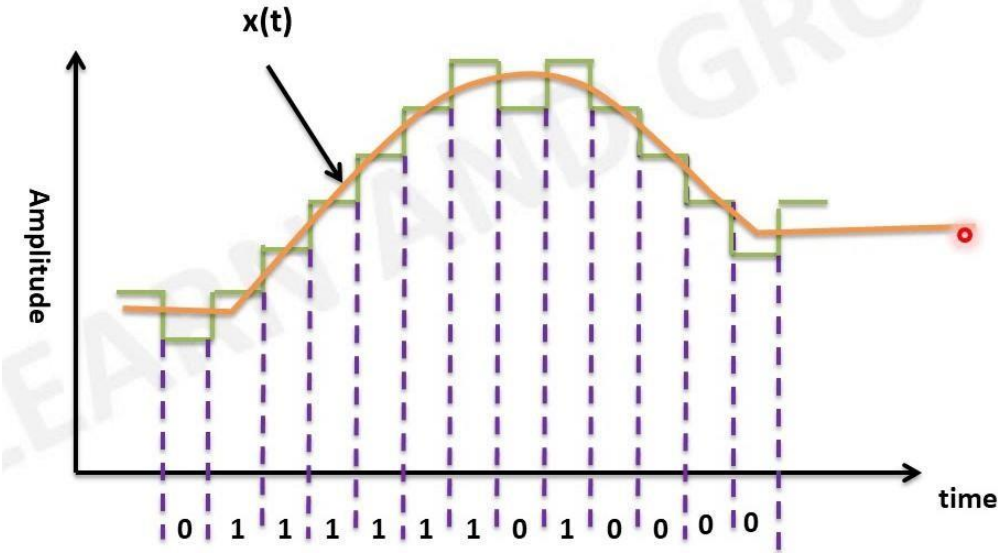


Figure: 4.15 Delta Modulation

4.3 Transmission Mode

Transmission mode refers to the mode used for transmitting the data. The transmission medium may be capable of sending only a single bit in unit time or multiple bits in unit time.

When a single bit is transmitted in unit time the transmission mode used is Serial Transmission and when multiple bits are sent in unit time the transmission mode used is called Parallel transmission.

Types of Transmission Modes:

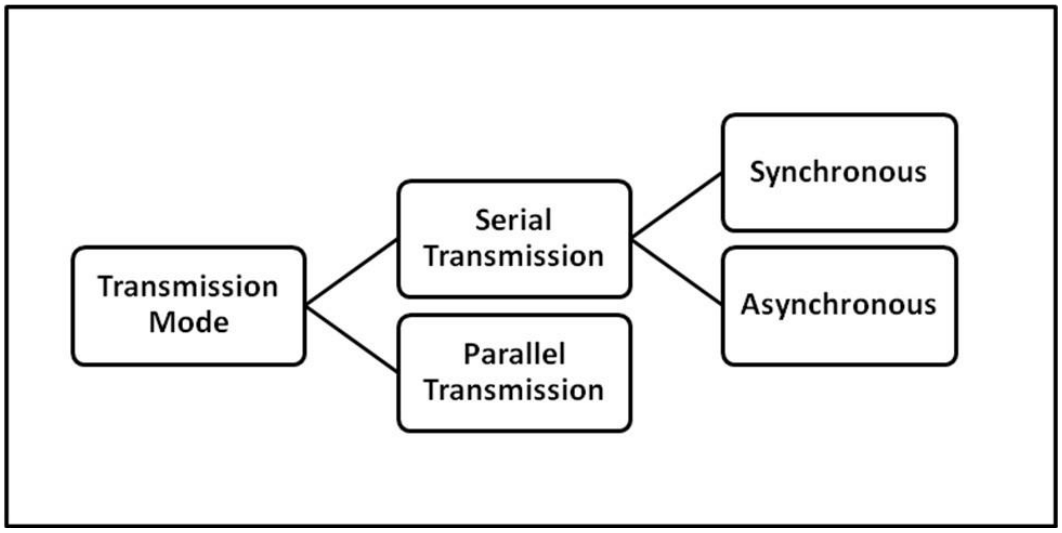


Figure: 4.16 Types of Transmission Modes

4.3.1 Parallel Transmission

- It involves simultaneous transmission of *N* bits over *N* different channels.
- Parallel Transmission increases transmission speed by a factor of *N* over serial transmission.
- Disadvantage of parallel transmission is the cost involved, N channels have to be used, hence, it can be used for short distance communication only.

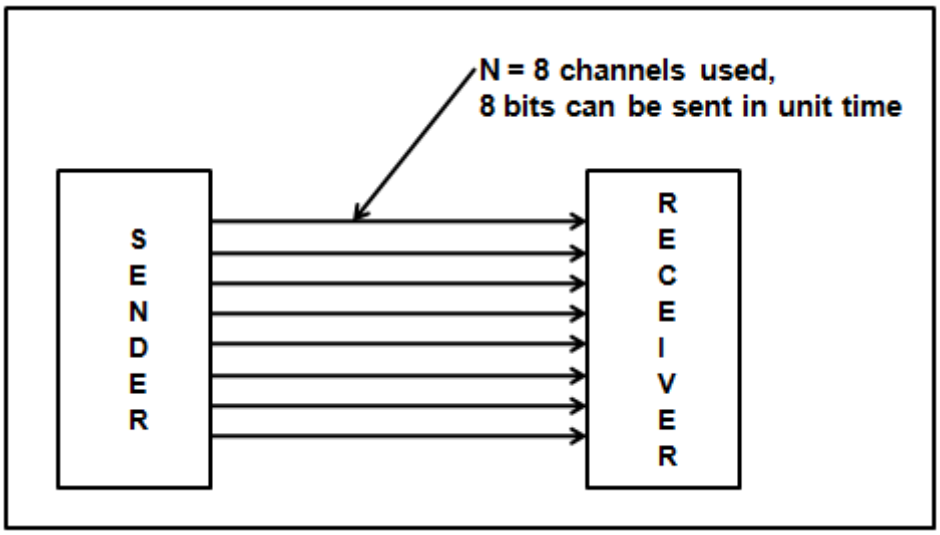


Figure: 4.17 Parallel Transmission

4.3.2 Serial Transmission

- In Serial Transmission, as the name suggests data is transmitted serially, i.e. bit by bit, one bit at a time.
- Since only one bit has to be sent in unit time only a single channel is required.

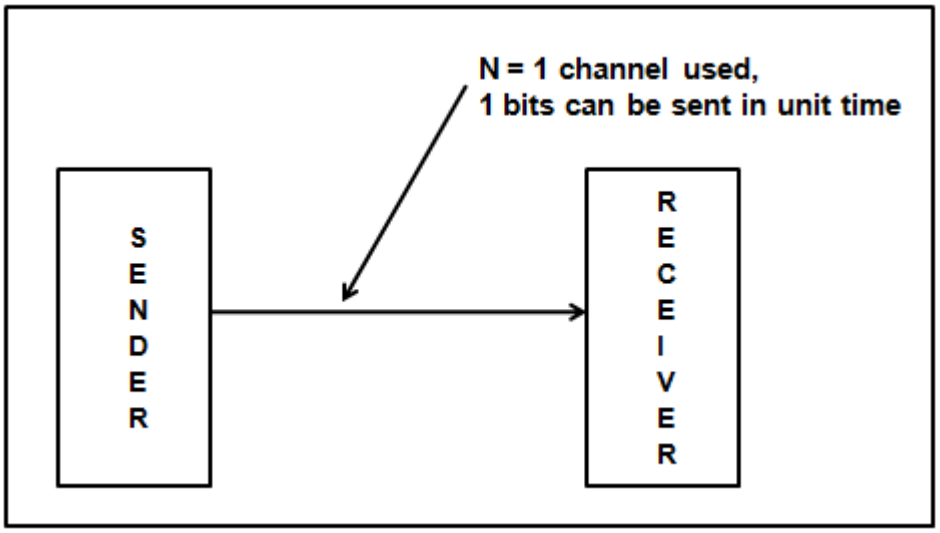


Figure: 4.18 Serial Transmission

Types of Serial Transmission:

Depending upon the timing of transmission of data there are two types of serial transmission as:

4.3.2.1 Asynchronous Transmission

- In asynchronous serial transmission the sender and receiver are not synchronized.
- The data is sent in group of 8 bits i.e. in bytes.
- The sender can start data transmission at any time instant without informing the receiver.
- To avoid confusing the receiver while receiving the data, ‘start’ and ‘stop’ bits are inserted before and after every group of 8 bits.
- The start bit is indicated by ‘0’ and stop bit is indicated by ‘1’.

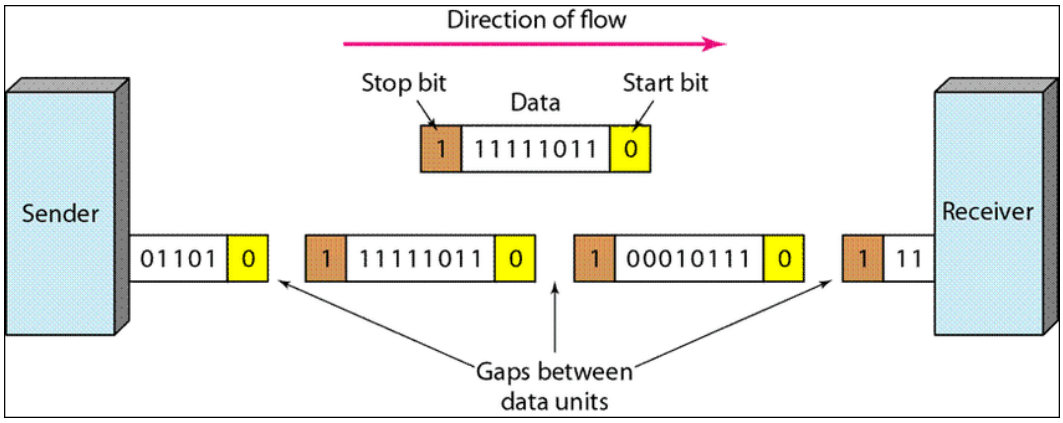


Figure: 4.19 Asynchronous Serial Transmission

4.3.2.1 Synchronous Transmission

- In Synchronous Serial Transmission, the sender and receiver are highly synchronized.
- No start, stop bits are used.
- Instead a common master clock is used for reference.
- The sender simply send stream of data bits in group of 8 bits to the receiver without any start or stop bit.
- It is the responsibility of the receiver to regroup the bits into units of 8 bits once they are received.

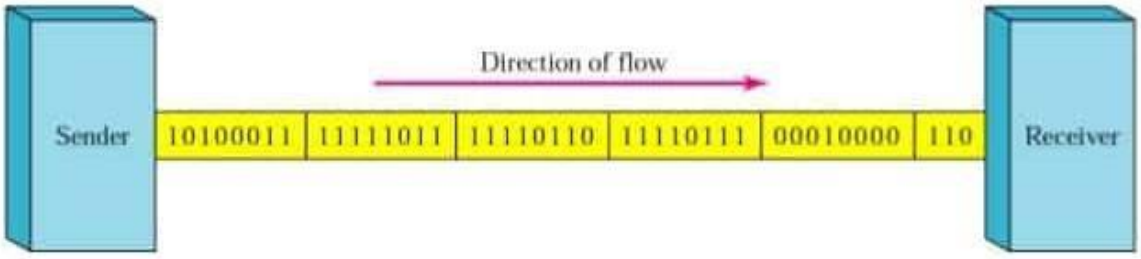


Figure: 4.20 Synchronous Serial Transmission

Short Questions

1. What is line Coding?

Ans - It is the process of converting Digital data into digital signal. It is converting of binary data(i.e. A sequence of bits) into digital signal (i.e. a sequence of discrete, discontinuous voltage pulses).

2. Differentiate between Manchester and Differential Manchester encoding.

Ans - **Manchester coding** is a combination of NRZ-L and RZ schemes. Every symbol has a level transition in the middle: from high to low or low to high. It uses only two voltage levels.

Differential Manchester coding consists of combining the NRZ-I and RZ schemes. Every symbol has a level transition in the middle. But the level at the beginning of the symbol is determined by the symbol value. One symbol causes a level change the other does not.

3. What is PAM Signal?

Ans - The analog signal is sampled every T_s s, where T_s is the sample interval or the period. According to the Nyquist theorem, to reproduce the original analog signal, one necessary condition is that the sampling rate be at least twice the highest frequency in the original signal. The sampling process is sometimes referred to as **pulse amplitude modulation (PAM).**

Long Questions

1. Write a short note on Block Coding.
2. What is PCM. Discuss.
3. Differentiate between Parallel and Serial Transmission.

Module-I

Chapter-5
Lecture-12

Analog Transmission

Learning Objective:

5.1 Digital to Analog Conversion

5.2 Analog to Analog Conversion

Analog Transmission

Converting digital data to a bandpass analog signal.is traditionally called digital•to-analog conversion. Converting a low-pass analog signal to a bandpass analog signal is traditionally called analog-to-analog conversion.

5.1 Digital to Analog Conversion

Digital-to-analog conversion is the process of changing one of the characteristics of an analog signal based on the information in digital data.

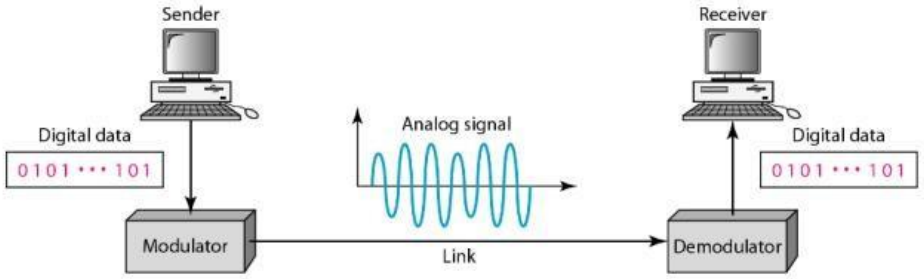
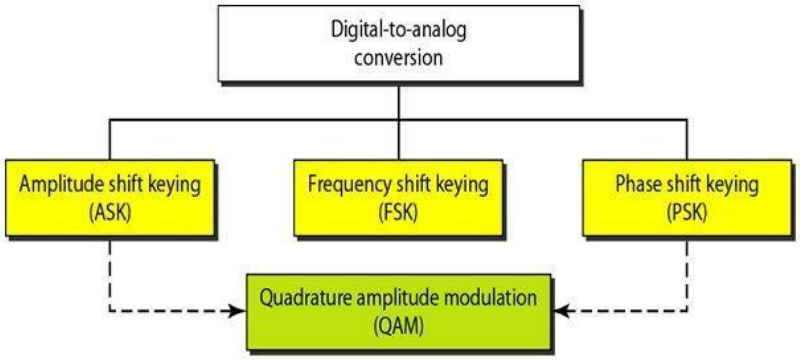


Figure: 5.1 Digital to Analog Conversion

Types of Digital-to-analog conversion



5.1.1 Amplitude Shift Keying

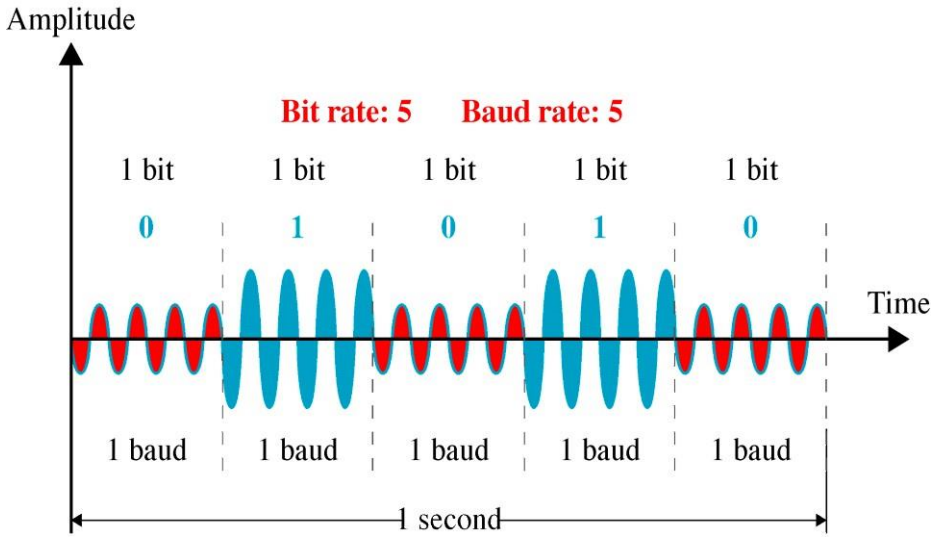


Figure: 5.2 Amplitude Shift Keying

In amplitude shift keying, the amplitude of the carrier signal is varied to create signal elements. Both frequency and phase remain constant while the amplitude changes.

5.1.2 Frequency Shift Keying

In frequency shift keying, the frequency of the carrier signal is varied to represent data. Both peak amplitude and phase remain constant for all signal elements.

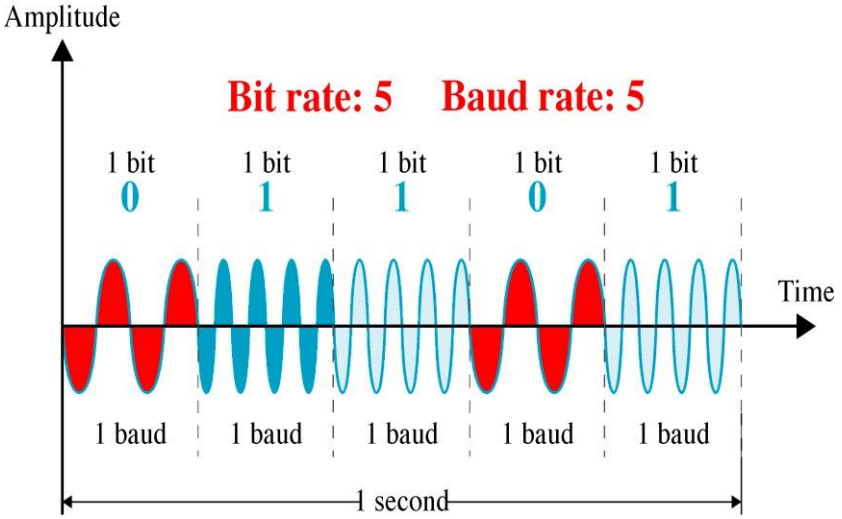


Figure: 5.3 Frequency Shift Keying

5.1.3 Phase Shift Keying

In phase shift keying, the phase of the carrier is varied to represent two or more different signal elements. Both peak amplitude and frequency remain constant as the phase changes.

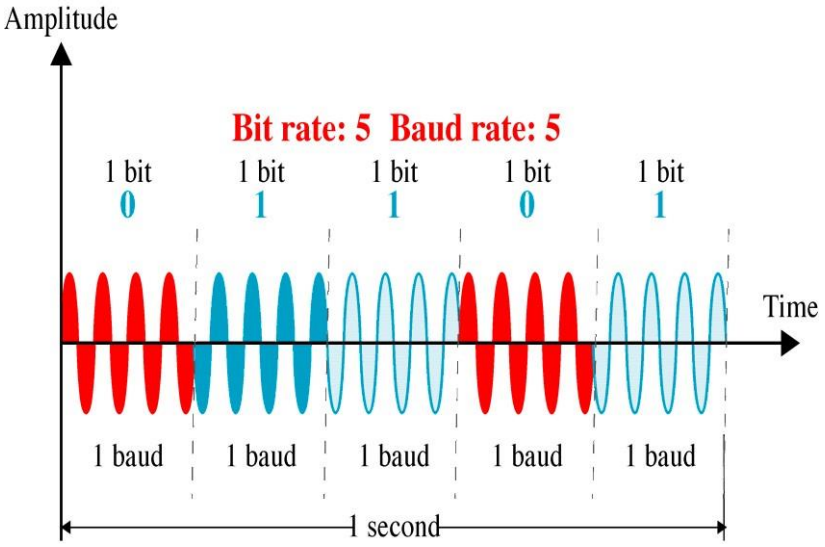


Figure: 5.4 Phase Shift Keying

- **Binary PSK (BPSK)**

  The simplest PSK is binary PSK, in which we have only two signal elements, one with a phase of 0°, and the other with a phase of 180°.

- **PSK Constellation**

Bit	Phase
0	0
1	180

Bits

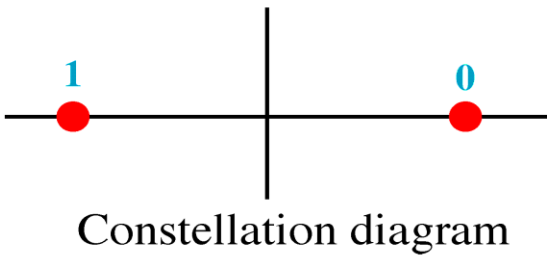


Figure: 5.5 Constellation diagram of BPSK

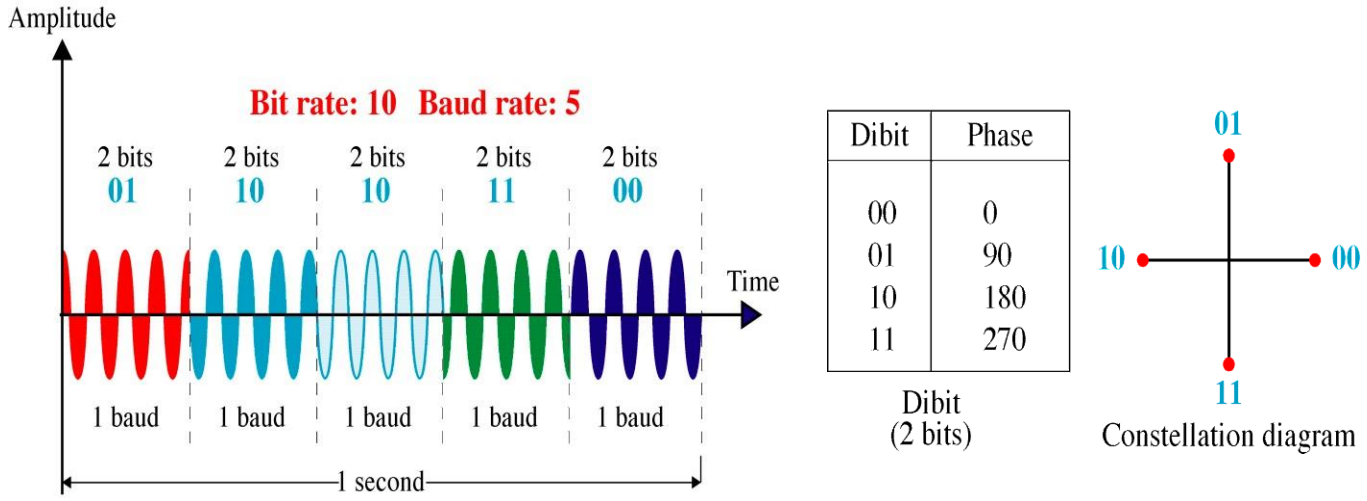


Figure: 5.6 Constellation diagram of 4-PSK

5.1.4 Quadrature Amplitude Modulation

Quadrature amplitude modulation is a combination of ASK and PSK. The idea of using two carriers, one in-phase and the other quadrature, with different amplitude levels for each carrier is the concept behind Quadrature amplitude modulation (QAM).

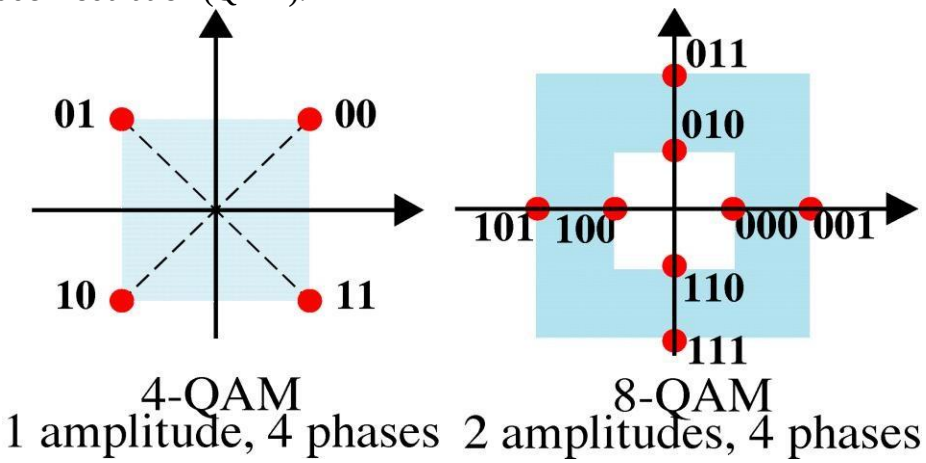


Figure: 5.7 4-QAM and 8-QAM Constellations

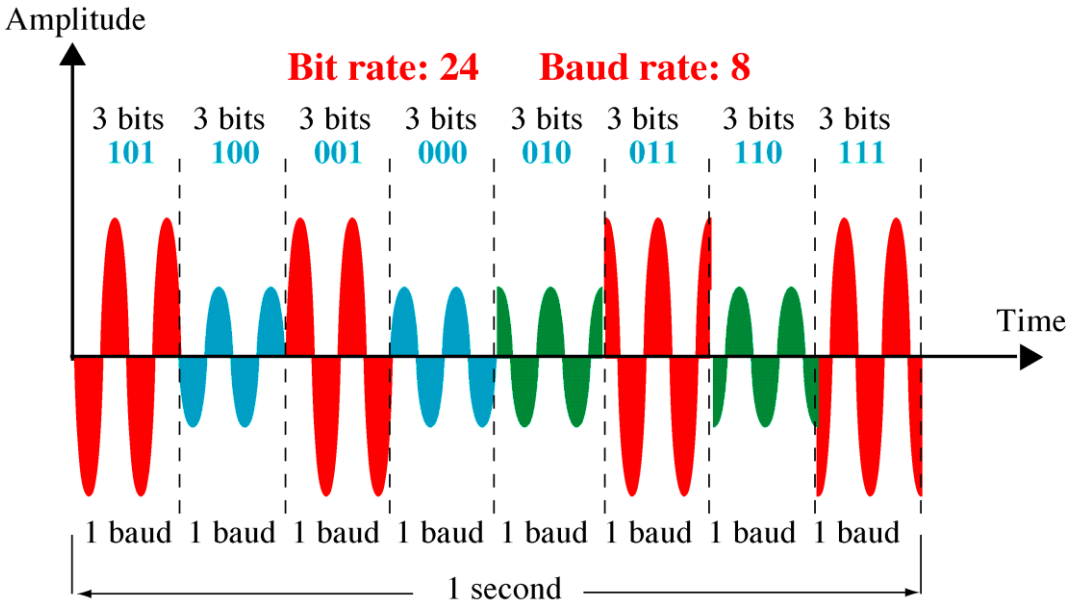


Figure: 5.7 8-QAM Signal

5.2 Analog to Analog Conversion

Analog-to-analog conversion, or analog modulation, is the representation of analog information by an analog signal.

Note: Modulation is needed if the medium is bandpass in nature or if only a bandpass channel is available to us. An example is radio. The government assigns a narrow bandwidth to each radio station. The analog signal produced by each station is a low-pass signal, all in the same range. To be able to listen to different stations, the low-pass signals need to be shifted, each to a different range.

Analog-to-analog conversion can be accomplished in three ways: amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM).

5.2.1 Amplitude Modulation

In AM transmission, the carrier signal is modulated so that its amplitude varies with the changing amplitudes of the modulating signal. The frequency and phase of the carrier remain the same; only the amplitude changes to follow variations in the information. The modulating signal is the envelope of the carrier.

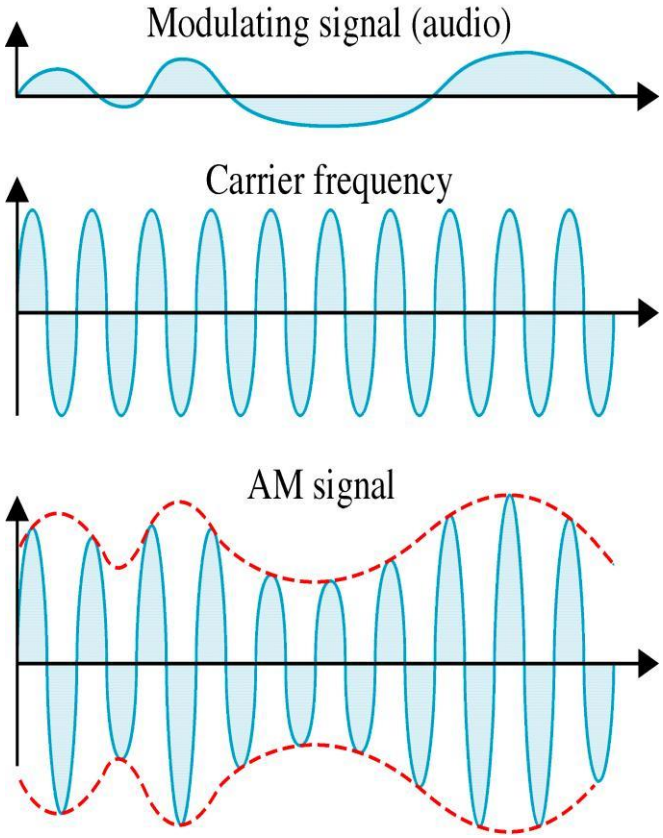


Figure: 5.8 Amplitude Modulation

5.2.2 Frequency Modulation

In FM transmission, the frequency of the carrier signal is modulated to follow the changing voltage level (amplitude) of the modulating signal. The peak amplitude and phase of the carrier signal remain constant, but as the amplitude of the information signal changes, the frequency of the carrier changes correspondingly (Figure: 5.9).

5.2.3 Phase Modulation

In PM transmission, the phase of the carrier signal is modulated to follow the changing voltage level (amplitude) of the modulating signal. The peak amplitude and frequency of the carrier signal remain constant, but as the amplitude of the information signal changes, the phase of the carrier changes correspondingly (Figure: 5.10).

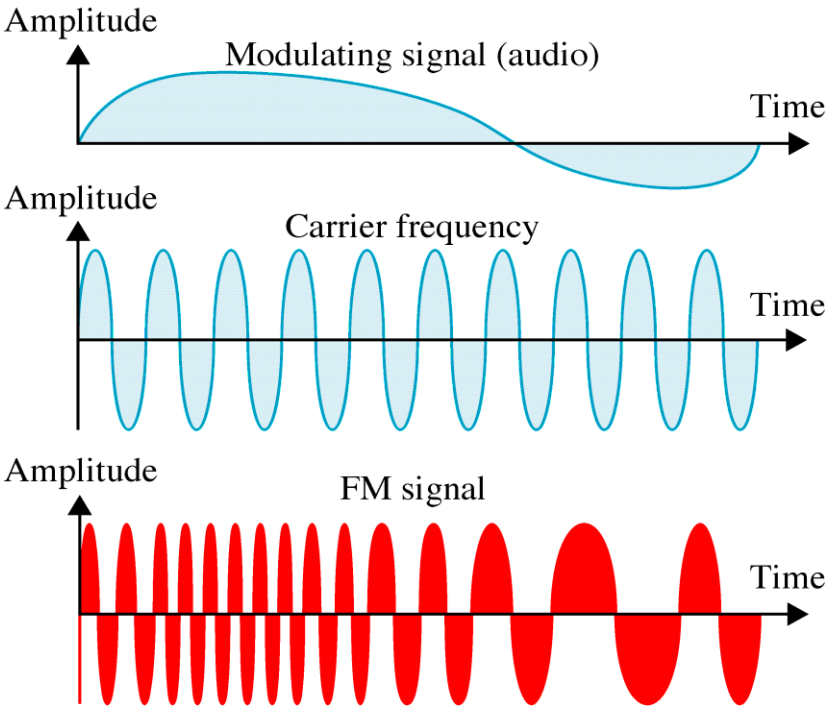


Figure: 5.9 Frequency Modulation

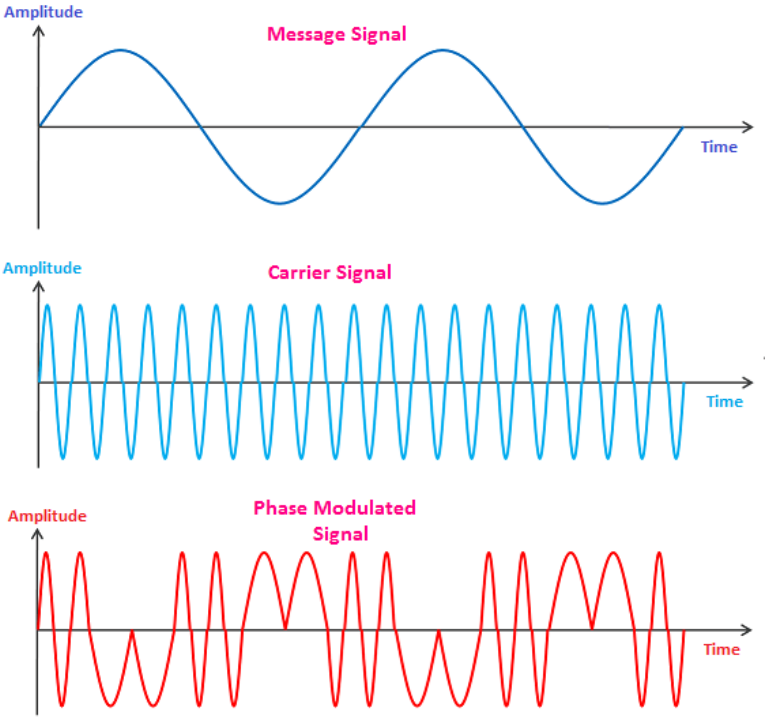


Figure: 5.10 Phase Modulation

Short Questions

1. What is QAM?

Ans - Quadrature amplitude modulation is a combination of ASK and PSK. The idea of using two carriers, one in-phase and the other quadrature, with different amplitude levels for each carrier is the concept behind Quadrature amplitude modulation (QAM).

Long Questions

1. Discuss ASK,FSK and PSK.
2. Discuss AM, FM, PM.

Module-I

Chapter-6
Lecture-14

Multiplexing & Switching Techniques

Learning Objective:

6.1 Multiplexing

6.1 Multiplexing

Multiplexing is the sharing of a medium or bandwidth. It is the process in which multiple signals coming from multiple sources are combined and transmitted over a single communication/physical line.

Figure: 6.1 Multiplexing

Types of Multiplexing

There are three types of Multiplexing :

1. Frequency Division Multiplexing (FDM)
2. Time-Division Multiplexing (TDM)
3. Wavelength Division Multiplexing (WDM)

6.1.1 Frequency Division Multiplexing

Frequency division multiplexing is defined as a type of multiplexing where the bandwidth of a single physical medium is divided into a number of smaller, independent frequency channels.

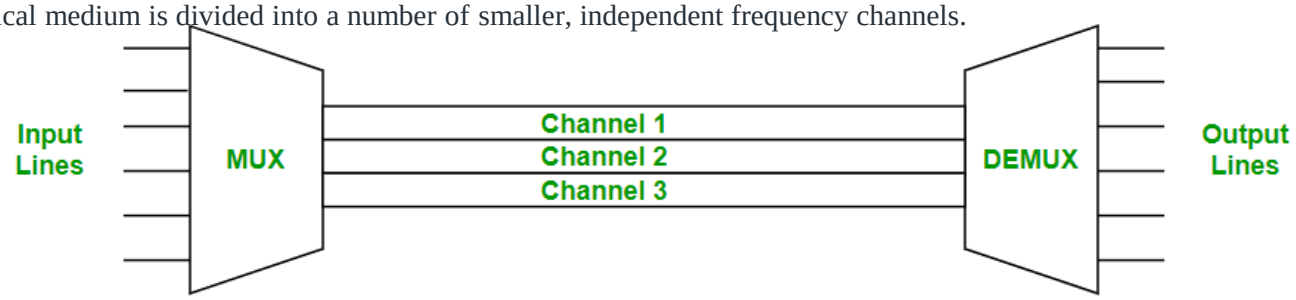


Figure: 6.2 Frequency division multiplexing

Frequency Division Multiplexing is used in radio and television transmission. In FDM, we can observe a lot of inter-channel cross-talk, due to the fact that in this type of multiplexing the bandwidth is divided into frequency channels. In order to prevent the inter-channel cross talk, unused strips of bandwidth must be placed between each channel. These unused strips between each channel are known as guard bands.

6.1.2 Time Division Multiplexing

Time-division multiplexing is defined as a type of multiplexing wherein FDM, instead of sharing a portion of the bandwidth in the form of channels, in TDM, time is shared. Each connection occupies a portion of time in the link (Figure: 6.3).

There are two types of Time Division Multiplexing :

1. Synchronous Time Division Multiplexing
2. Statistical (or Asynchronous) Time Division Multiplexing

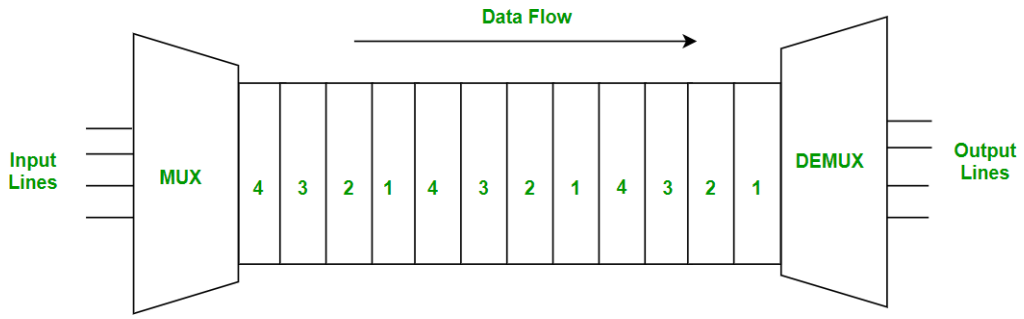


Figure: 6.3 Time division multiplexing

6.1.2.1 Synchronous TDM

Synchronous TDM is a type of Time Division Multiplexing where the input frame already has a slot in the output frame. Time slots are grouped into frames. One frame consists of one cycle of time slots. Synchronous TDM is not efficient because if the input frame has no data to send, a slot remains empty in the output frame. In synchronous TDM, we need to mention the synchronous bit at the beginning of each frame.

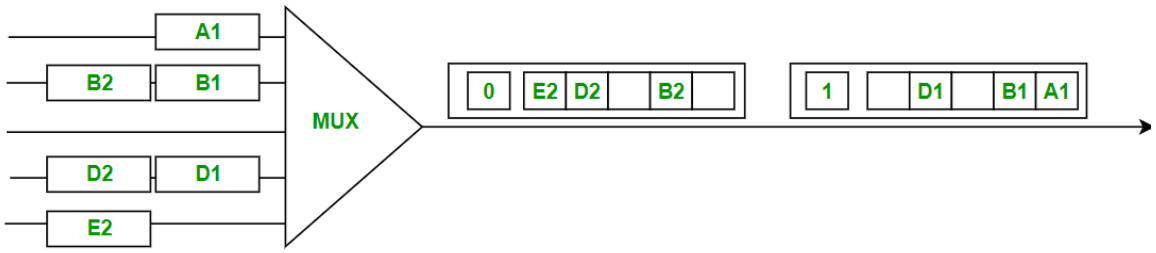


Figure: 6.4 Synchronous Time Division Multiplexing

6.1.2.2 Statistical(Asynchronous) TDM

Statistical TDM is a type of Time Division Multiplexing where the output frame collects data from the input frame till it is full, not leaving an empty slot like in Synchronous TDM. In statistical TDM, we need to include the address of each particular data in the slot that is being sent to the output frame.

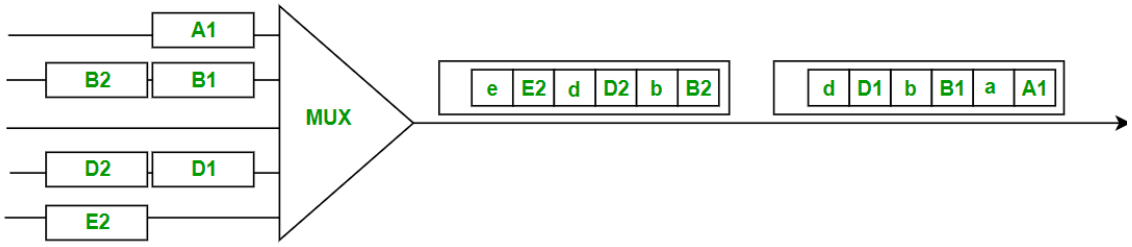


Figure: 6.5 Statistical(Asynchronous) Time Division Multiplexing

6.1.3 Wavelength Division Multiplexing :

Wavelength Division Multiplexing is used on fiber optics to increase the capacity of a single fiber. It is an analog multiplexing technique. Optical signals from the different sources are combined to form a wider band of light with the help of multiplexers. At the receiving end, the demultiplexer separates the signals to transmit them to their respective destinations.

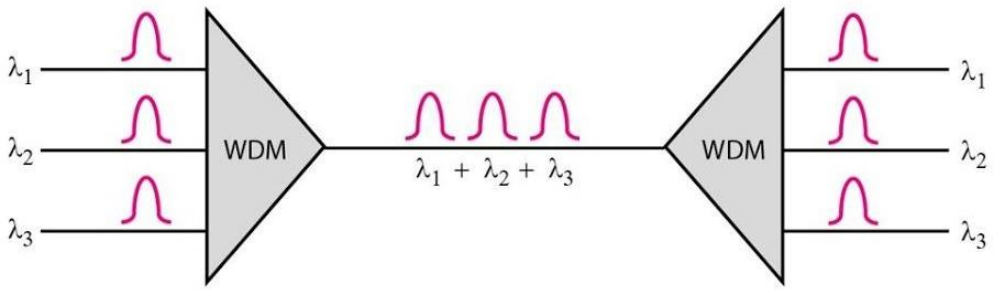


Figure: 6.6 Wavelength Division Multiplexing

Module-I

Chapter-6
Lecture-15

6.2 Switching Techniques

6.2 Switching Techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission. Switching technique is used to connect the systems for making one-to-one communication.

Classification Of Switching Techniques

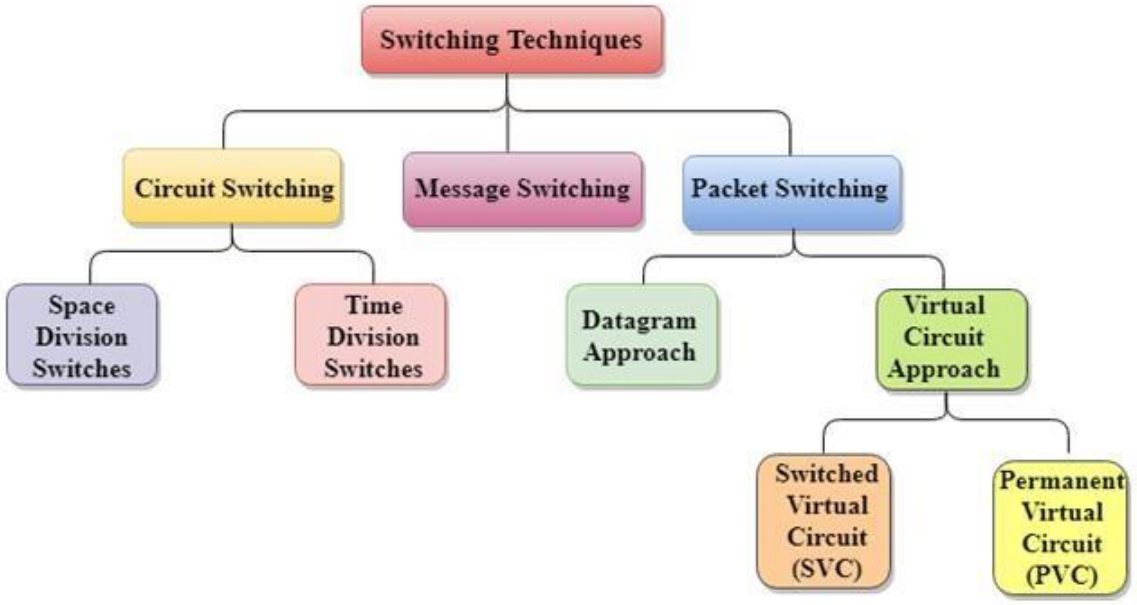


Figure: 6.7 Classification of Switching Techniques

6.2.1 Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect

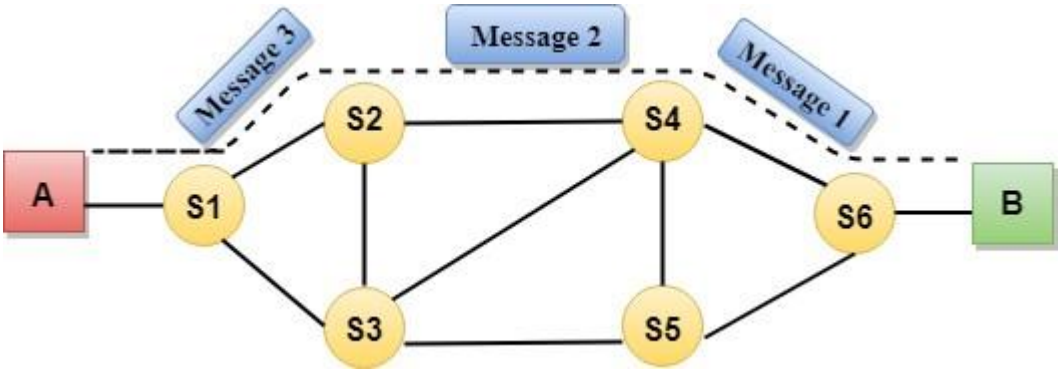


Figure: 6.8 Communication through circuit switching

Circuit Switching can use either of the two technologies:

Space Division Switches:

- Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.
- Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic crosspoint or semiconductor gate that can be enabled or disabled by a control unit.

Space Division Switches can be categorized in two ways:

- **Crossbar Switch**
- **Multistage Switch**

Crossbar Switch

- The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **crosspoints.**

  Disadvantage of Crossbar switch:

  The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

- Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- It reduces the number of crosspoints.
- If one path fails, then there will be an availability of another path.

Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.

6.2.2 Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.

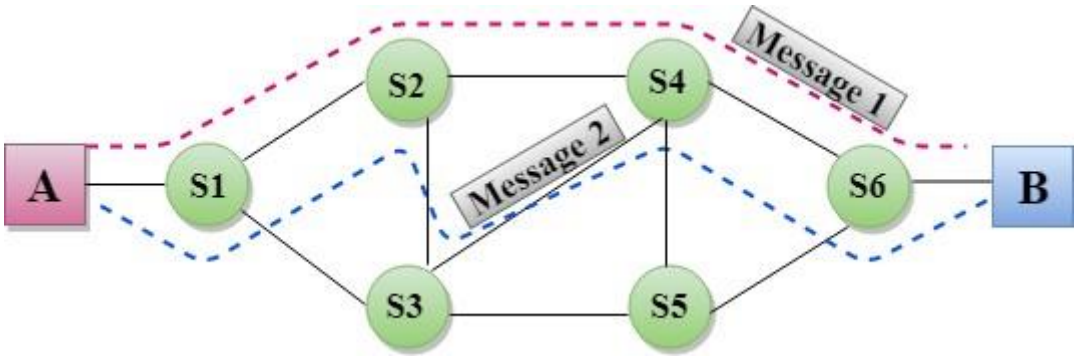


Figure: 6.9 Message Switching

Advantages Of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages Of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

6.2.3 Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.

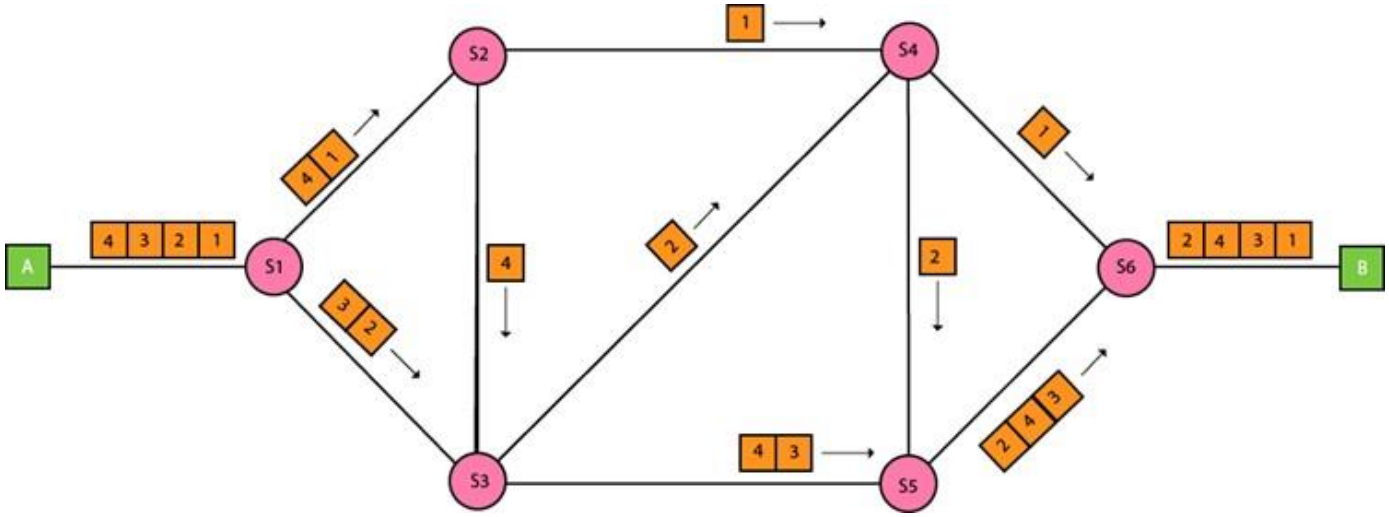


Figure: 6.10 Packet Switching

Approaches Of Packet Switching:

There are two approaches to Packet Switching:

6.2.3.1 Datagram Packet switching

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

6.2.3.2 Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Concept of virtual circuit switching through a diagram:

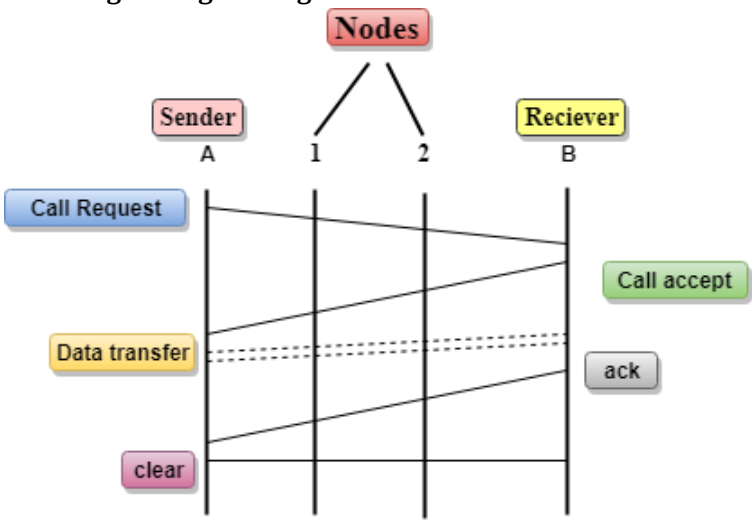


Figure: 6.11 virtual circuit switching

- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

Short Questions

1. What is Multiplexing?

Ans - Multiplexing is the sharing of a medium or bandwidth. It is the process in which multiple signals coming from multiple sources are combined and transmitted over a single communication/physical line.

2. Differentiate between FDM and TDM.

Ans - Frequency division multiplexing is defined as a type of multiplexing where the bandwidth of a single physical medium is divided into a number of smaller, independent frequency channels.

Time-division multiplexing is defined as a type of multiplexing wherein FDM, instead of sharing a portion of the bandwidth in the form of channels, in TDM, time is shared. Each connection occupies a portion of time in the link.

Long Questions

1. Differentiate between Circuit Switching, Packet Switching and Message Switching.

Module-I

Chapter-7
Lecture-16

Transmission Media

7.1 Transmission Media

7.1 Transmission Media

- Transmission media is a means by which a communication signal is carried from one system to another.
- A transmission medium can be defined as anything that can carry information from a source to a destination.
- The transmission medium is usually free space, metallic cable or fiber – optic cable.

Categories of transmission media

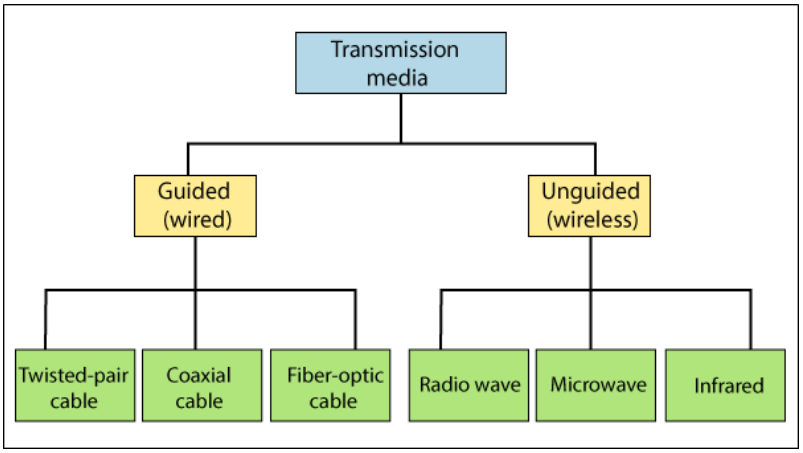


Figure: 7.1 Categories of transmission media

7.1.1 Guided Media

Guided Transmission media uses a cabling system that guides the data signals along a specific path. Guided media also known as Bounded media, which are those that provide a medium from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.

7.1.1.1 Twisted-pair cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

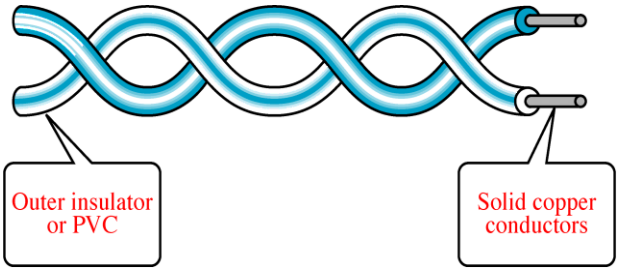


Figure: 7.2 Twisted-pair cable

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.

Unshielded Versus Shielded Twisted-Pair Cable

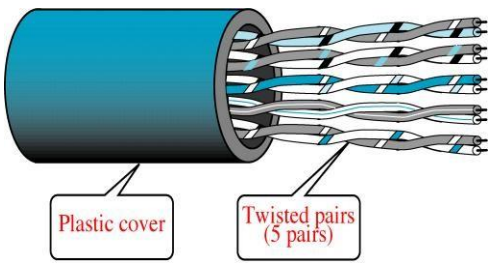


Figure: 7.3 Unshielded Twisted-Pair Cable

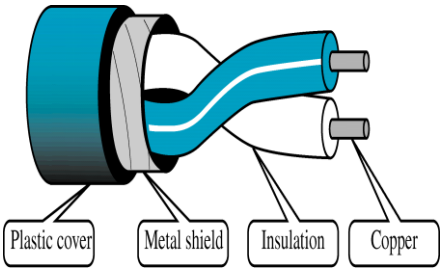


Figure: 7.4 Shielded Twisted-Pair Cable

Cables with the shield are called shielded twisted pair and commonly abbreviated STP. Cables without a shield are called unshielded twisted pair or UTP. UTP or unshielded twisted pair cable is used on Ethernet. UTP cables are used for Ethernet cabling where 4 twisted pair cables (a total of 8 wires are used).

7.1.1.2 Co-Axial Cable

Coaxial cable consists of 2 conductors. The inner conductor is contained inside the insulator with the other conductor weaves around it providing a shield. An insulating protective coating called a jacket covers the outer conductor. The outer shield protects the inner conductor from outside electrical signals.

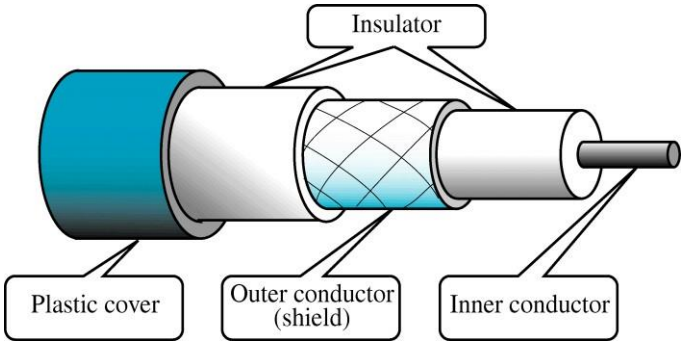


Figure: 7.5 Co-Axial Cable

Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals. Cable TV networks (see Chapter 9) also use coaxial cables.

7.1.1.3 Fiber-Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. The typical optical fiber consists of a very narrow strand of glass called the cladding. A typical core diameter is 62.5 microns. Typically cladding has a diameter of 125 minors. Coating the cladding is a protective coating consisting of plastic, it is called the jacket. The device generating the message has it in electromagnetic form (electrical signal); this has to be converted into light (i.e.optical signal) to send it on optic fiber cable. The process of converting light to electric signal is done on the receiving side.

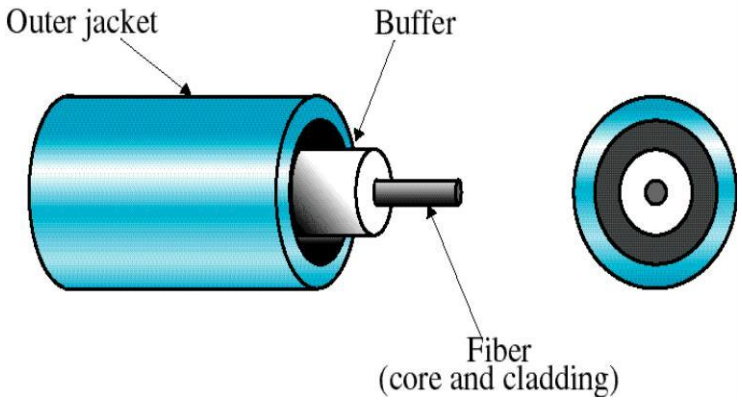


Figure: 7.6 Fiber-Optic Construction

- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

7.1.2 Unguided media

Unguided media transport data without using a physical conductor. This type of communication is often referred to as wireless communication. It uses wireless electromagnetic signals to send data.

Before understanding the different types of wireless transmission medium, let us first understand the ways in which wireless signals travel. These signals can be sent or propagated in the following three ways:

1. Ground-wave propagation
2. Sky-wave propagation
3. Line-of-sight propagation

Ground-wave propagation

- Follows contour of the earth
- Can Propagate considerable distances
- Frequencies up to 2 MHz
- Example : AM radio

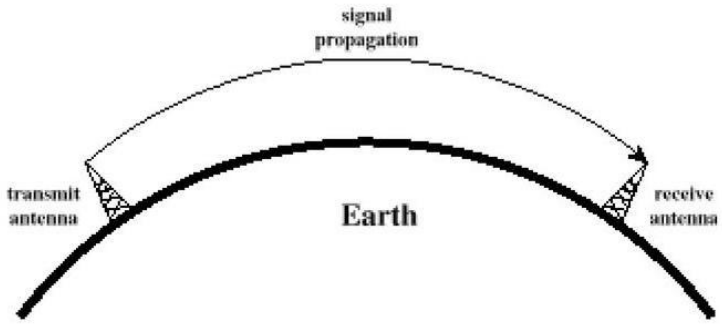


Figure: 7.7 Ground-wave propagation

Sky-wave propagation

- Signal reflected from ionized layer of atmosphere back down to earth
- Signal can travel a number of hops, back and forth between ionosphere and earth‘s surface

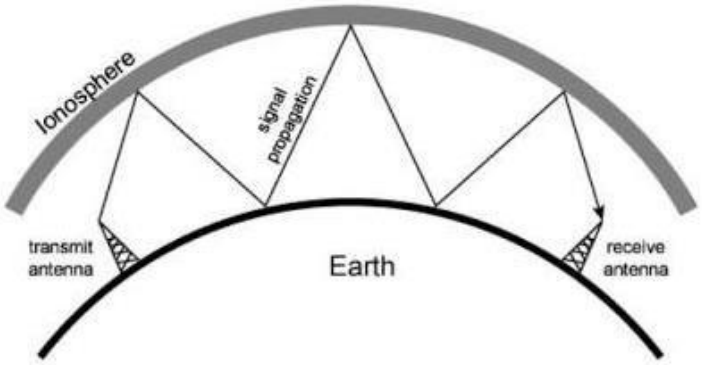


Figure: 7.8 Sky-wave propagation

Line-of-sight propagation

- Transmitting and receiving antennas must be within line of sight.

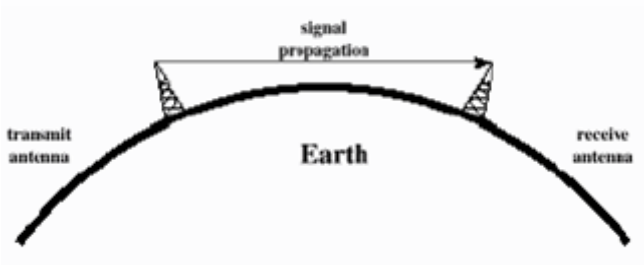


Figure: 7.9 Line-of-sight propagation

7.1.2.1 Radio Waves

- Electromagnetic wave ranging in frequencies between 3 KHz and 1GHz are normally called radio waves.
- Radio waves are omni-directional when an antenna transmits radio waves they are propagated in all directions. This means that sending and receiving antenna do not have to he aligned. A sending antenna can send waves that can be received by any receiving antenna.
- Radio waves particularly those waves that propagate in sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio.

7.1.2.2 Microwaves

- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.
- Microwaves are unidirectional; when an antenna transmits microwaves they can be narrowly focused. This means that the sending and receiving antennas need to be aligned.

- Microwaves propagation is line-of-sight.
- Parabolic dish antenna and horn antenna are used for this means of transmission.

7.1.2.3 Infrared

- Infrared signals with frequencies ranges from 300 GHz to 400 GHz can be used for short range communication.
- Infrared signals, having high frequencies, cannot penetrate walls. This helps to prevent interference between one system and another.

Long Questions

1. Write a short note on:
   a. Twisted pair cable
   b. Co-axial cable
   c. Fibre Optics.

Module-II

Chapter-8

Lecture-17

Data Link Layer: Error Detection & Correction

Learning Objective:

8.1 Types OF Errors

8.2 Error Detection

8.1 Types OF Errors

If the signal comprises of binary data there can be two types of errors which are possible during the transmission:

1. Single bit error
2. Burst Errors

8.1.1 Single-bit error

In single-bit error, a bit value of 0 changes to bit value 1 or vice versa. Single bit errors are more likely to occur in parallel transmission.

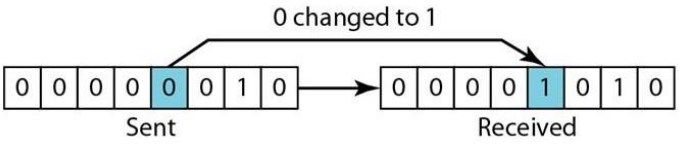


Figure: 8.1 Single-bit error

8.1.2 Burst errors

In Burst error, multiple bits of the binary value changes. Burst error can change any two or more bits in a transmission. These bits need not be adjacent bits. Burst errors are more likely to occur in serial transmission.

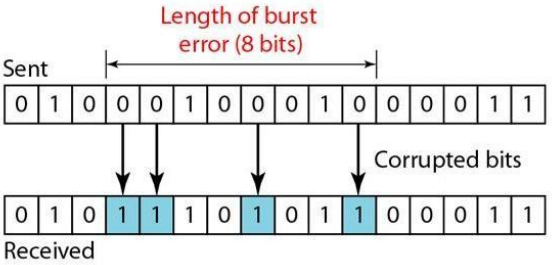


Figure: 8.2 Burst errors

8.2 Error Detection

Error detection is simpler than error correction and is the first step in the error correction process.

Redundancy

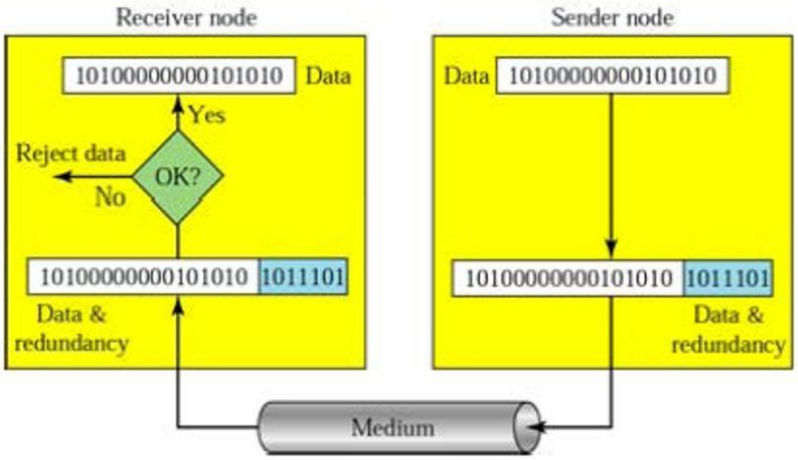


Figure: 8.3 Redundancy

In order to detect and correct the errors in the data communication we add some extra bits to the original data. These extra bits are nothing but the redundant bits which will be removed by the receiver after receiving the data.

Their presence allows the receiver to detect or correct corrupted bits. Instead of repeating the entire data stream, a short group of bits may be attached to the entire data stream. This technique is called redundancy because theextra bits are redundant to the information: they are discarded as soon as the accuracy of the transmission has been determined.

There are different techniques used for transmission error detection and correction.

8.2.1 Parity Check

Simple parity Check

In this technique, a redundant bit called a parity bit is added to every data unit so that the total number of 1‘s in the unit (including the parity bit) becomes even (or odd).

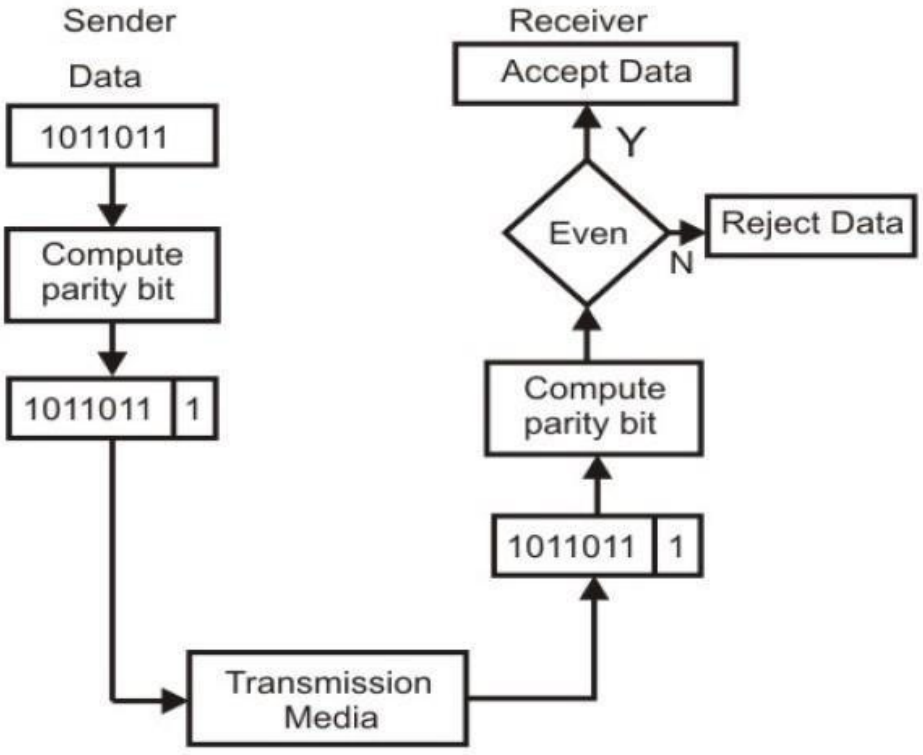


Figure: 8.4 Even parity Checking

Simple parity check can detect all single-bit errors. It can also detect burst errors as long as the total number of bits changed is odd. This method cannot detect errors where the total number of bits changed is even.

Two-Dimensional Parity Check

In this method, a block of bits is organized in a table (rows and columns). First we calculate the parity bit for each data unit. Then we organize them into a table. We then calculate the parity bit for each column and create a new row of 8 bits.

We then calculate the parity bit for each column and create a new row of 8 bits; they are the parity bits for the whole block.

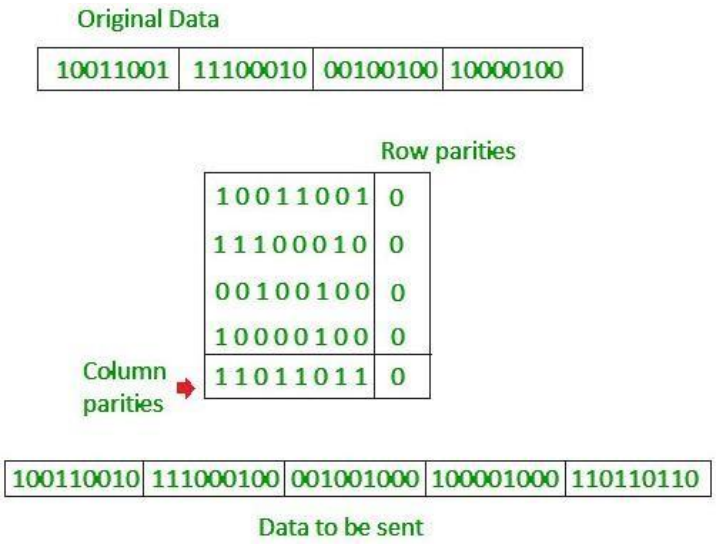


Figure: 8.5 Two-Dimensional Parity

8.2.2 Cyclic Redundancy Check (CRC)

This method is based on the binary division. In CRC, the desired sequences of redundant bits are generated and is appended to the end of data unit. It is also called as CRC reminder. So that the resulting data unit becomes exactly divisible by a predetermined binary number.

At its destination, the incoming data unit is divided by the same number. If at this step there is no remainder then the data unit is assumed to be correct and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

The redundancy bits used by CRC are derived by dividing the data unit by a predetermined divisor; the remainder is the CRC. To be valid, a CRC must have two qualities: It must have exactly one less bit than the divisor, and appending it to the end of the data string must make the resulting bit sequence exactly divisible by the divisor.

The following figure shows the process:

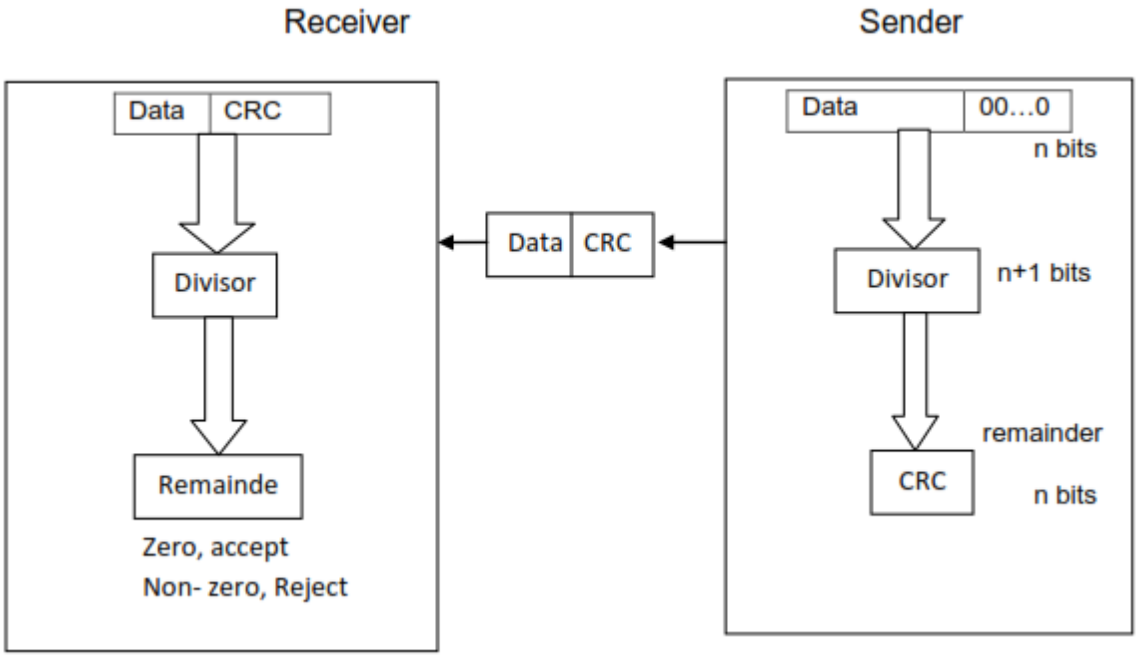


Figure: 8.6 CRC Generator and Checker

Example

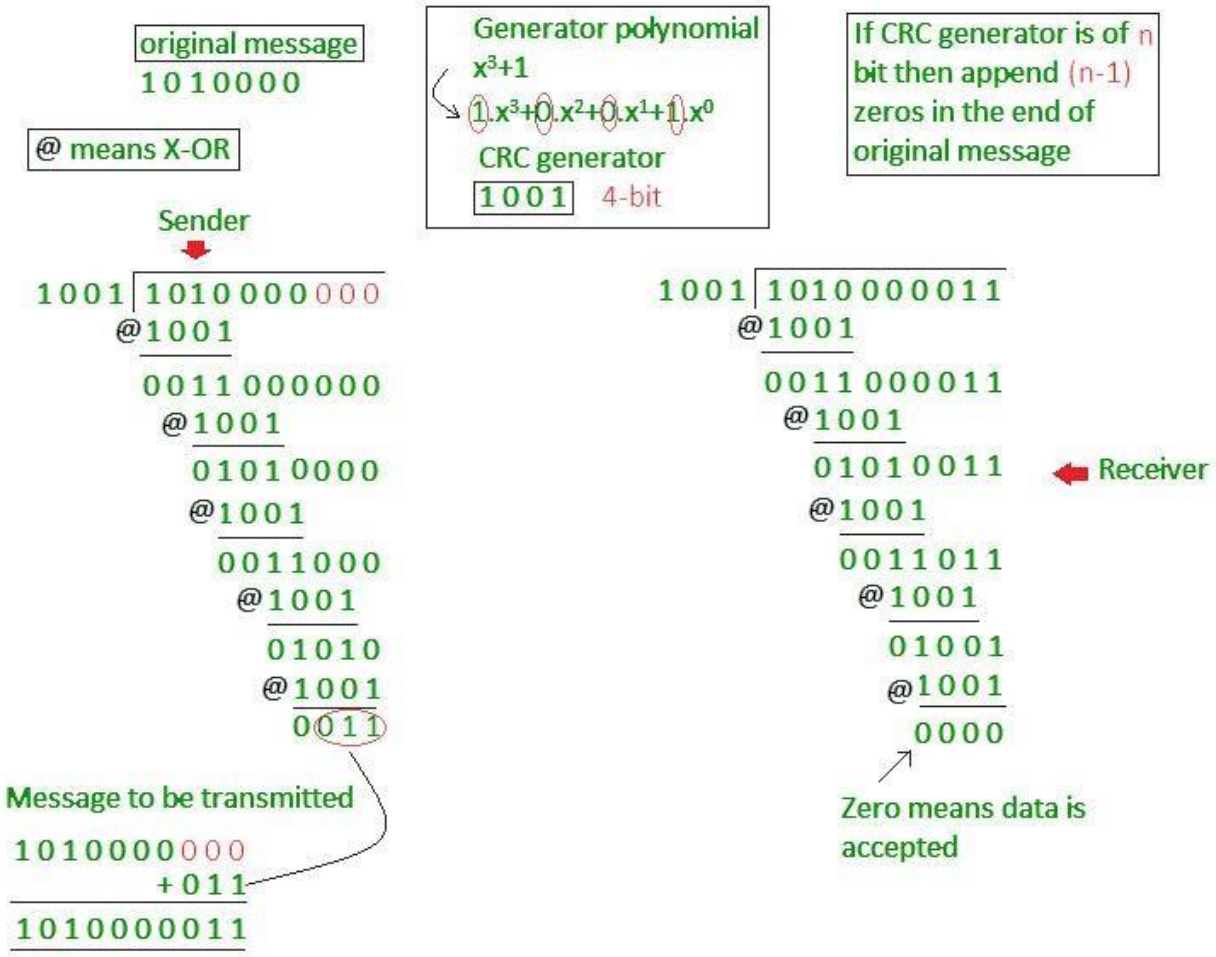


Figure: 8.7 CRC Checking

Module-II

Chapter-8
Lecture-18

Learning Objective:

8.2 Error Detection

8.2.3 Checksum

8.3 Error Correction

8.2.3 Checksum

In checksum error detection scheme, the data is divided into k segments each of m bits. In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum. The checksum segment is sent along with the data segments. At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented. If the result is zero, the received data is accepted; otherwise discarded.

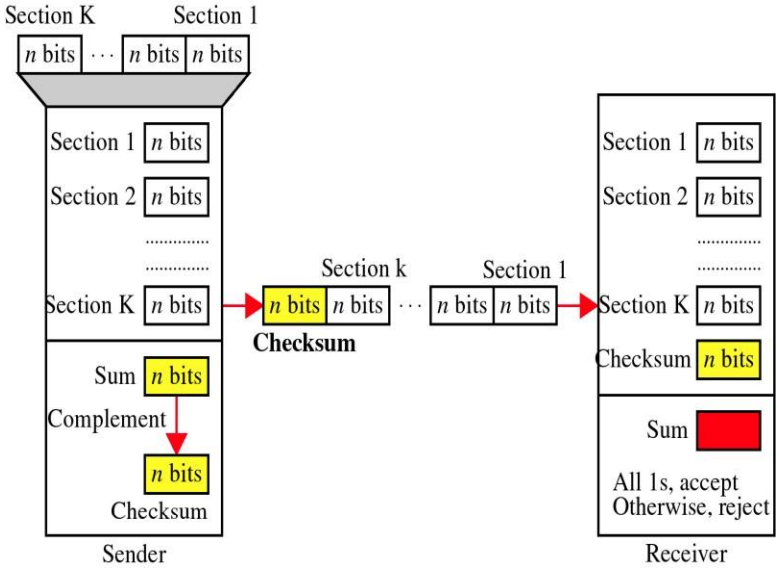


Figure: 8.8

Example

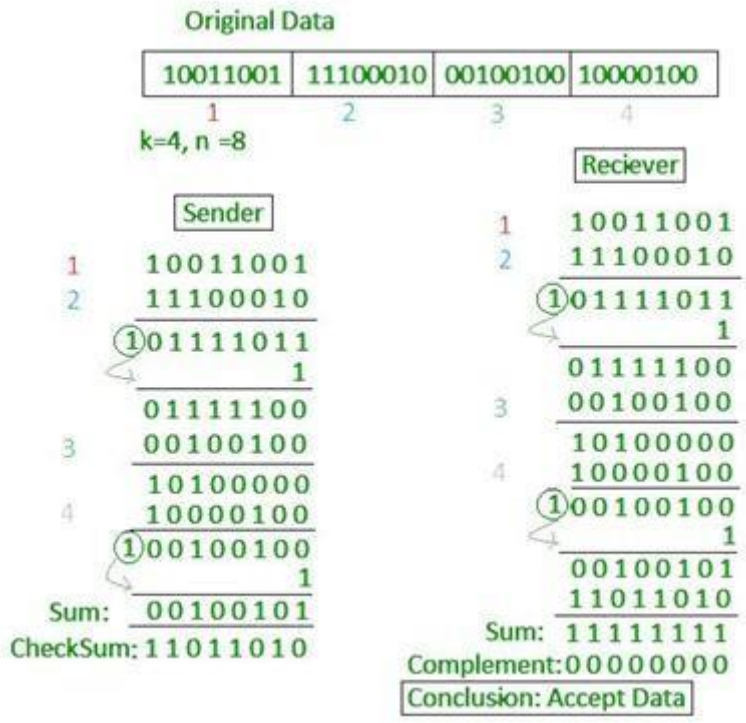


Figure: 8.9

8.3 Error Correction

Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.

Error Correction can be handled in two ways:

- **Backward error correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
- **Forward error correction:** In this case, the receiver uses the error-correcting code which automatically corrects the errors.

A single additional bit can detect the error, but cannot correct it.

For correcting the errors, one has to know the exact position of the error. For example, If we want to calculate a single-bit error, the error correction code will determine which one of seven bits is in error. To achieve this, we have to add some additional redundant bits.

Hamming Code

It is a technique developed by R.W. hamming. This can be applied to data units of any length. This code mainly uses the relationship between data and redundancy bits. The hamming code technique, which is an **error- detection and error-correction technique**, was proposed by **R.W. Hamming**. Whenever a data packet is transmitted over a network, there are possibilities that the data bits may get lost or damaged during transmission.

The **redundant bits** are some extra binary bits that are not part of the original data, but they are generated & added to the original data bit. All this is done to ensure that the data bits don't get damaged and if they do, we can recover them.Now the question arises, how do we determine the number of redundant bits to be added?

We use the formula, $2^r >= m+r+1$; where **r = redundant bit** & **m = data bit**.

For example, a 7-bit ASCII code requires 4 redundancy bits that can be added to the end of the data unit or interspersed with the original data bits. In following Figure, these bits are placed in positions 1, 2,4, and 8 (the positions in an 11-bit sequence that are powers of 2). For clarity in the examples below, we refer to these bits as r1, r2, r4, and r8.

11	10	9	8	7	6	5	4	3	2	1
d	d	d	*r8*	d	d	d	*r4*	d	*r2*	*r1*

In the Hamming code, each r bit is the parity bit for one combination of data bits, is shown below:

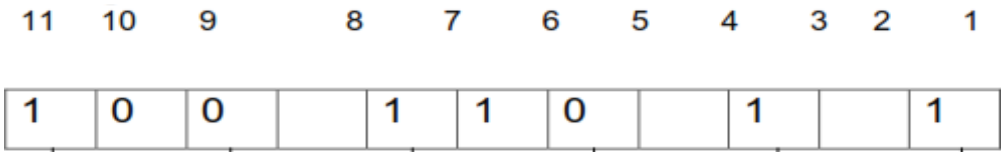
r1 : bits 1,3,5,7,9,11
r2 : bits 2,3,6,7,10,11
r3 : bits 4,5,6,7
r4 : bits 8,9,10,11

Now suppose we have 1001101 data to be sent, then the redundant bits are calculated by the following method:

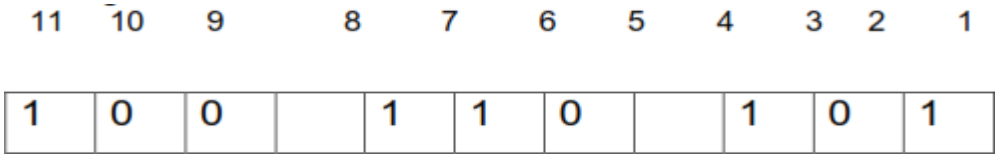
Data is: 1 0 0 1 1 0 1

11	10	9	8	7	6	5	4	3	2	1
1	0	0		1	1	0		1		

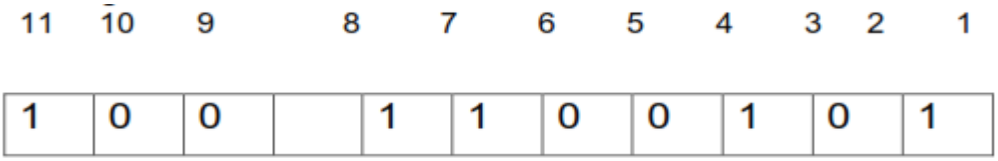
Adding r1:



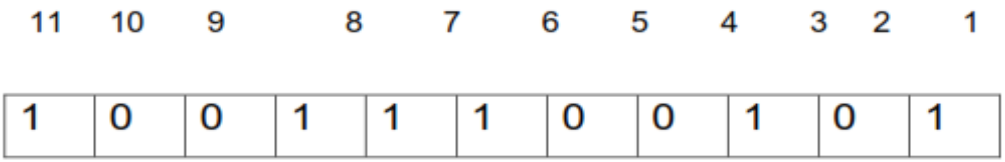
Adding r2:



Adding r4:

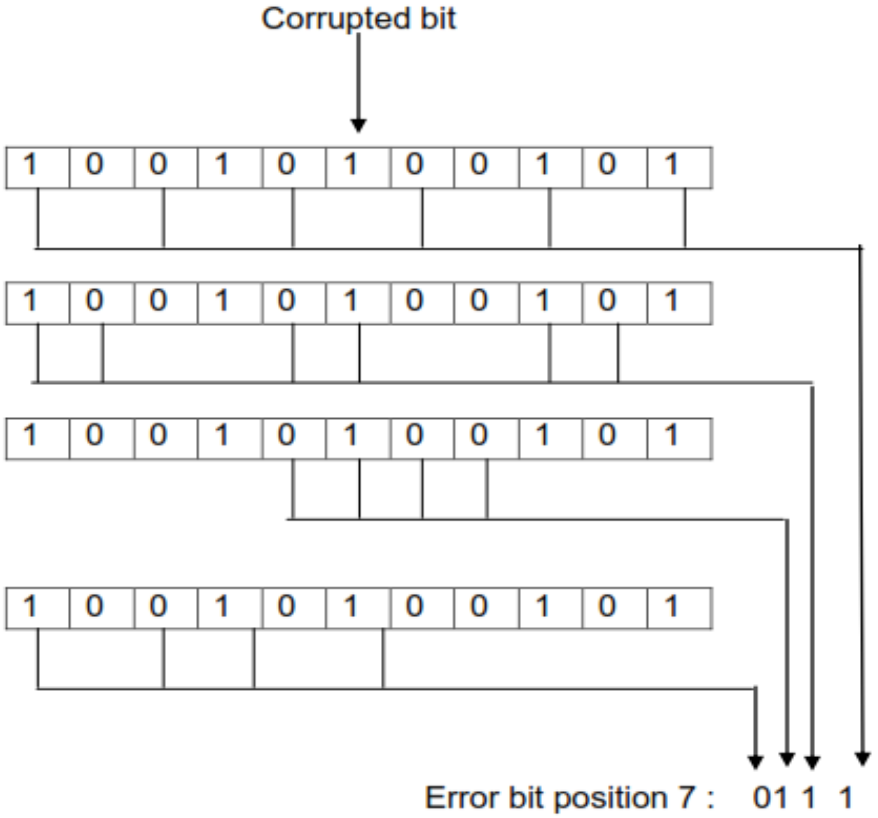


Adding r8:



Code: 10011100101

Now imagine that by the time the above transmission is received, the number **7** bit has been changed from **1** to **0.**The receiver takes the transmission and recalculates 4 new parity bits, using the same sets of bits used by the sender plus the relevant parity r bit for each set (see following Fig.). Then it assembles the new parity values into a binary number in order of r position (r8 r4, r2, r1). In our example, this step gives us the binary number 0111 (7 in decimal), which is the precise location of the bit in error.



Once the bit is identified, the receiver can reverse its value and correct the error.

Short Questions

1. What are the types of Error?

If the signal comprises of binary data there can be two types of errors which are possible during the transmission:

- Single bit error
- Burst Errors

2. What is Parity checking?

In this technique, a redundant bit called a parity bit is added to every data unit so that the total number of 1‘s in the unit (including the parity bit) becomes even (or odd).

3. What is Checksum?

In checksum error detection scheme, the data is divided into k segments each of m bits. In the sender’s end the segments are added using 1’s complement arithmetic to get the sum. The sum is complemented to get the checksum. The checksum segment is sent along with the data segments. At the receiver’s end, all received segments are added using 1’s complement arithmetic to get the sum. The sum is complemented. If the result is zero, the received data is accepted; otherwise discarded.

Long Questions

1. Explain Parity checking with suitable example.
2. Find the CRC of dataword 1010000 with polynomial divisor x^3+1 and find the dataword received at receiver is correct or not. (Verify).
3. Describe Forward Error Correction method with a example.

Module-II

Chapter-9
Lecture-19

Data Link Layer Protocols

Learning Objective:

9.1 Flow and Error Control

9.1.1 Stop-and-Wait Protocol

9.1 Flow and Error Control

Flow Control mainly coordinates with the amount of data that can be sent before receiving an acknowledgment from the receiver and it is one of the major duties of the data link layer.

- For most of the protocols, **flow control** is a set of procedures that mainly tells the sender how much data the sender can send before it must **wait for an acknowledgment** from **the receiver**.
- The data flow must not be allowed to overwhelm the receiver; because any receiving device has a very limited speed at which the device can process the incoming data and the limited amount of memory to store the incoming data.

Error Control contains both error detection and error correction. It mainly allows the receiver to inform the sender about any damaged or lost frames during the transmission and then it coordinates with the retransmission of those frames by the sender.

The term Error control in the data link layer mainly refers to the methods of error detection and retransmission. Error control is mainly implemented in a simple way and that is whenever there is an error detected during the exchange, then specified frames are retransmitted and this process is also referred to as **Automatic Repeat request(ARQ).**

Flow and Error Control Mechanisms (ARQ Protocols)

9.1.1 Stop-and-Wait Protocol

Stop and wait ARQ is also referred to as the alternating protocol is a method used in two-way communication systems to send information between two connected devices (sender and a receiver). It is referred to as stop and wait ARQ because the function of this protocol is to send **one frame at a time**.

After sending a frame or packet, the sender doesn't send any further packets until it receives an acknowledgement from the receiver. Moreover, the sender keeps a copy of the sent packet. After receiving the desired frame, the receiver sends an acknowledgement. If the acknowledgement does not reach the sender before the specified time, known as the timeout, the sender sends the same packet again. The timeout is reset after each frame transmission.

Normal Operation

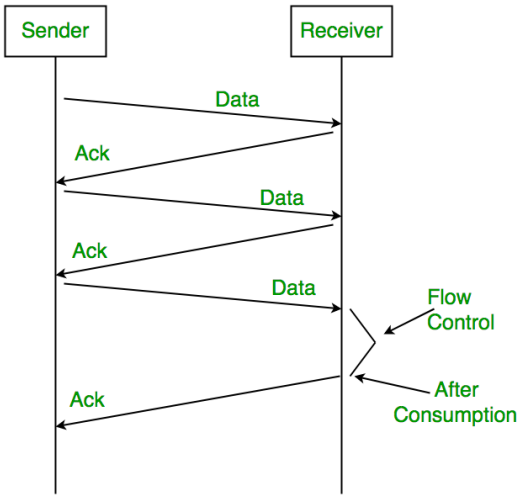


Figure: 9.1 Normal Operation of Stop-and-Wait Protocol

Lost Data

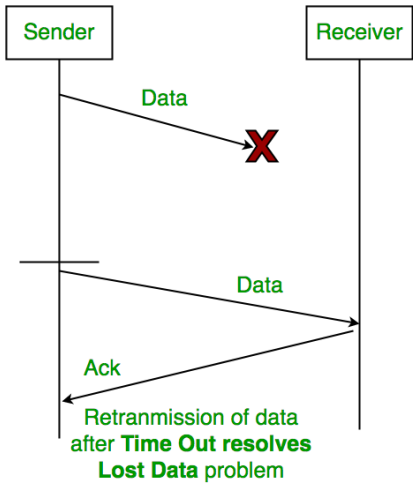


Figure: 9.2 Lost Data Operation of Stop-and-Wait Protocol

Lost Acknowledgement

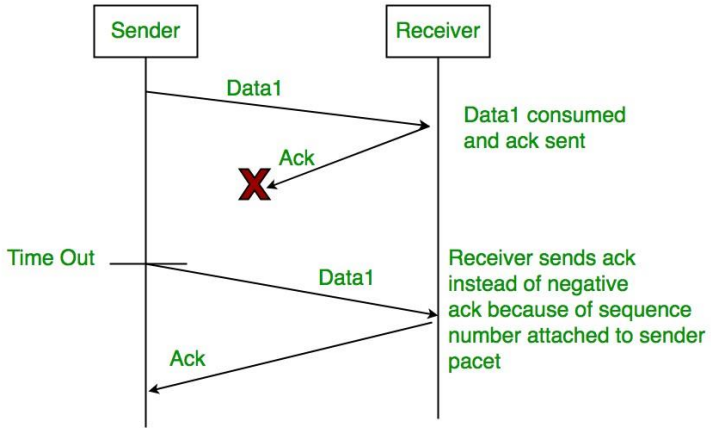


Figure: 9.3 Lost Acknowledgement Operation of Stop-and-Wait Protocol

1) Sender A sends a data frame or packet with sequence number 0.
2) Receiver B, after receiving the data frame, sends an acknowledgement with sequence number 1 (the sequence number of the next expected data frame or packet) .
There is only a one-bit sequence number that implies that both sender and receiver have a buffer for one frame or packet only.

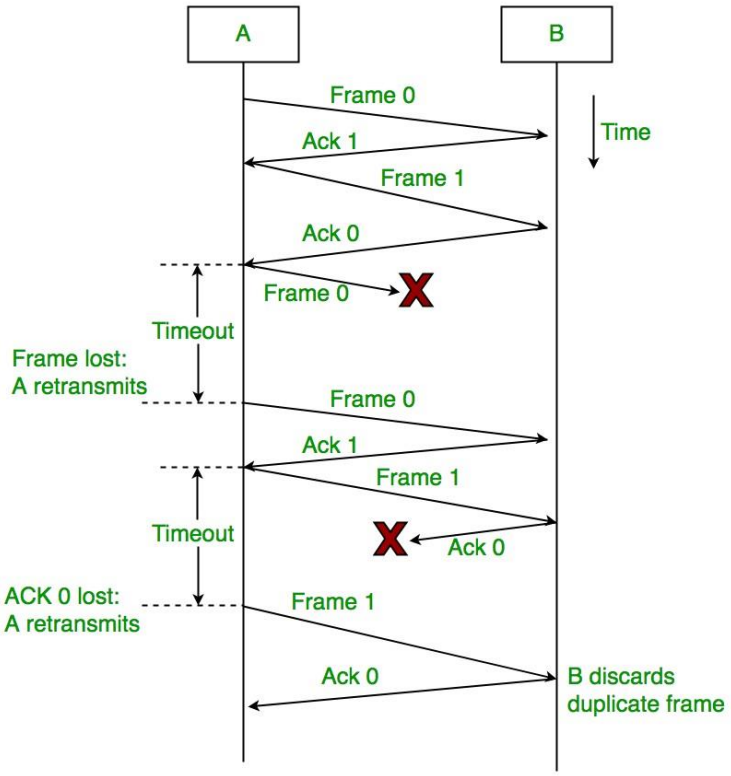


Figure: 9.4 Different Operations of Stop-and-Wait Protocol

Module-II

Chapter-9
Lecture-20

Learning Objective:

9.1 Flow and Error Control

9.1.2 Go Back-N ARQ

9.1.2 Go Back-N ARQ

Go-Back-N ARQ is a type of the ARQ protocol, in which the sending process continues to send several frames or packets even without receiving an acknowledgement packet from the receiver. The receiver process keeps track of the sequence number of the next packet it expects to receive and sends that sequence number with every acknowledgement to the sender. The receiver will remove any packet that does not have the desired sequence number it expects and will resend an acknowledgement for the last correct frame.

Once the sender has sent all of the frames in its window, it will identify that all of the frames since the first lost frame, and will go back to the sequence number of the last acknowledgement signal that it received from the receiver pr and continue the process over again. The only drawback of this type of system is that it results in sending packets multiple times: if any frame was lost or found to be corrupted, then that frame and all following frames in the send window will be re-transmitted.

Sender (sliding) window for Go-Back-N ARQ

Basically, the range which is in the concern of the sender is known as the send sliding window for the Go-Back-N ARQ. It is an imaginary box that covers the sequence numbers of the data frame which can be in transit.
The size of this imaginary box is 2^m-1 having three variables Sf(which indicates send window, the first outstanding frame), Sn(indicates the send window, the next frame to be sent), SSize.(indicates the send window, size).

- The sender can transmit N frames before receiving the ACK frame.
- The size of the send sliding window is N.
- The copy of sent data is maintained in the sent buffer of the sender until all the sent packets are acknowledged.
- If the timeout timer runs out then the sender will resend all the packets.
- Once the data get acknowledged by the receiver then that particular data will be removed from the buffer.

Whenever a valid acknowledgement arrives then the send window can slide one or more slots.

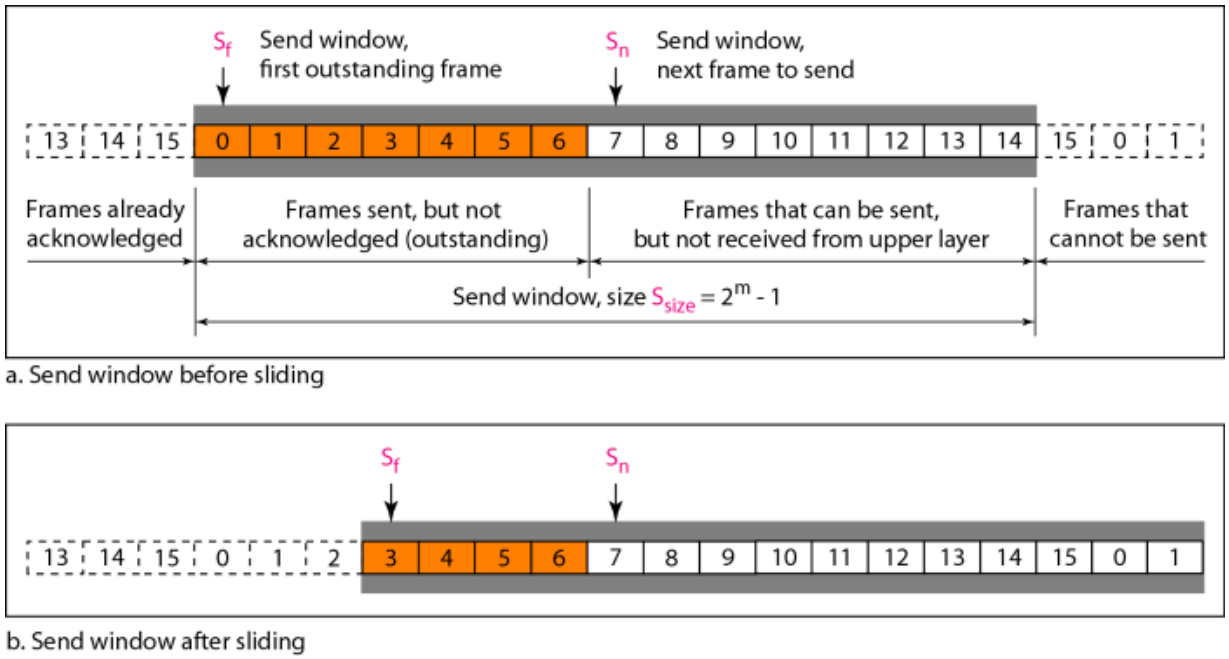


Figure: 9.5 Sender (sliding) window

Receiver (sliding) window for Go-Back-N ARQ

The range that is in the concern of the receiver is called the receiver sliding window.

- The receive window is mainly an abstract concept of defining an imaginary box whose size is 1and has a single variable Rn.
- The window slides when a correct frame arrives, the sliding occurs one slot at a time.
- The receiver always looks for a specific frame to arrive in the specific order.
- Any frame that arrives out of order at the receiver side will be discarded and thus need to be resent by the sender.
- If a frame arrives at the receiver safely and in a particular order then the receiver send ACK back to the sender.
- The silence of the receiver causes the timer of the unacknowledged frame to expire.

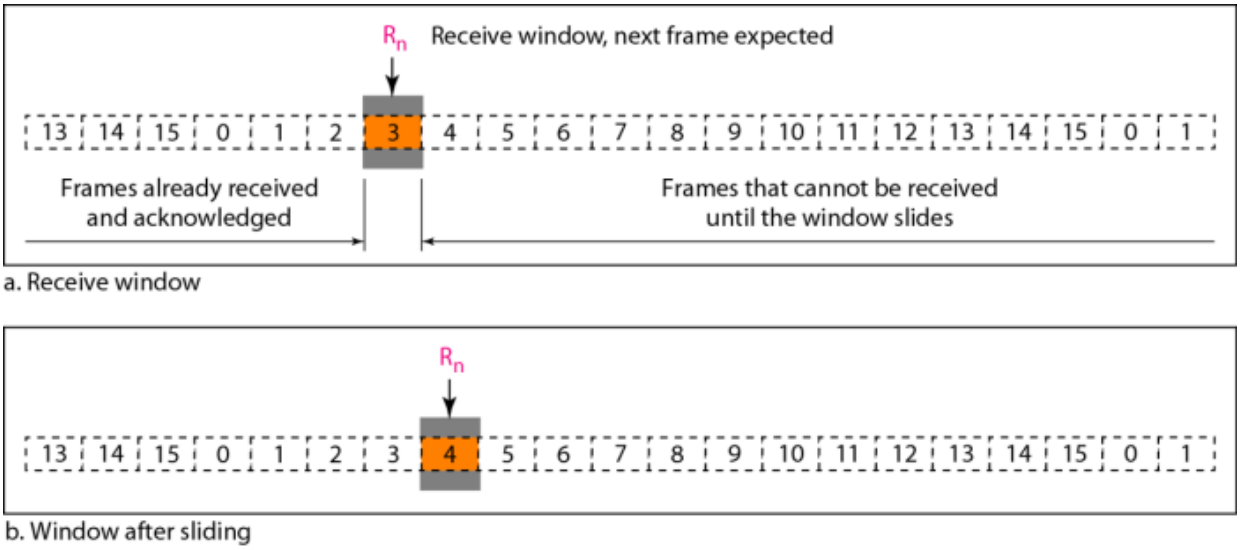


Figure: 9.6 Receiver (sliding) window

Flow Diagram

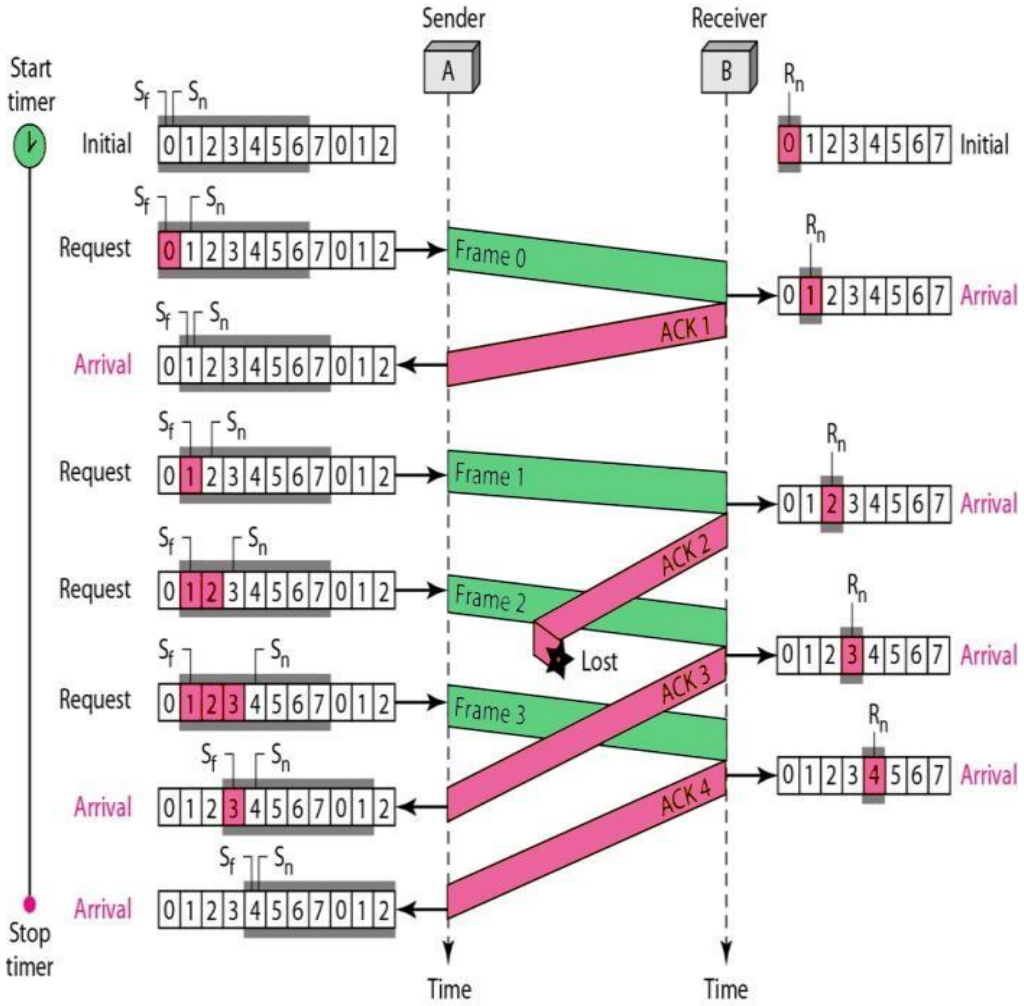


Figure: 9.7 Go-Back-N ARQ with sliding window

Module-II

Chapter-9
Lecture-21

Learning Objective:

9.1 Flow and Error Control

9.1.3 Selective Repeat ARQ

9.1.3 Selective Repeat ARQ

Selective Repeat ARQ/Selective Reject ARQ protocol mechanism is similar to the Go-Back-N protocol mechanism but in Selective Repeat ARQ the sending process continues even after a frame is found to be corrupt or lost. This is achieved: the receiver process keeps track of the sequence number of the earliest frame it has not received and sends the respective sequence number with the acknowledgement signal. If a frame is not received at the receiver end, the sender continues to send the succeeding frames until it has emptied its window. Once this error-correction process has been done, the process continues where it left off. Unlike, Go back-N protocol this does not send a packet multiple times.

Selective Repeat ARQ also requires full-duplex link. backward acknowledgements are also in progress.

- Sender's Windows size = Receiver's Windows size.
- Window size should be less than or equal to half the sequence number in SR protocol. This is to avoid packets being recognized incorrectly. If the size of the window is greater than half the sequence number space, then if an ACK is lost, the sender may send new packets that the receiver believes are retransmissions.
- Sender can transmit new packets as long as their number is with Window of all unACKed packets.
- Sender retransmits un-ACKed packets after a timeout – Or upon a NAK if NAK is employed.
- Receiver ACKs all correct packets.
- Receiver stores correct packets until they can be delivered in order to the higher layer.
- In Selective Repeat ARQ, the size of the sender and receiver window must be at most one-half of 2^m.

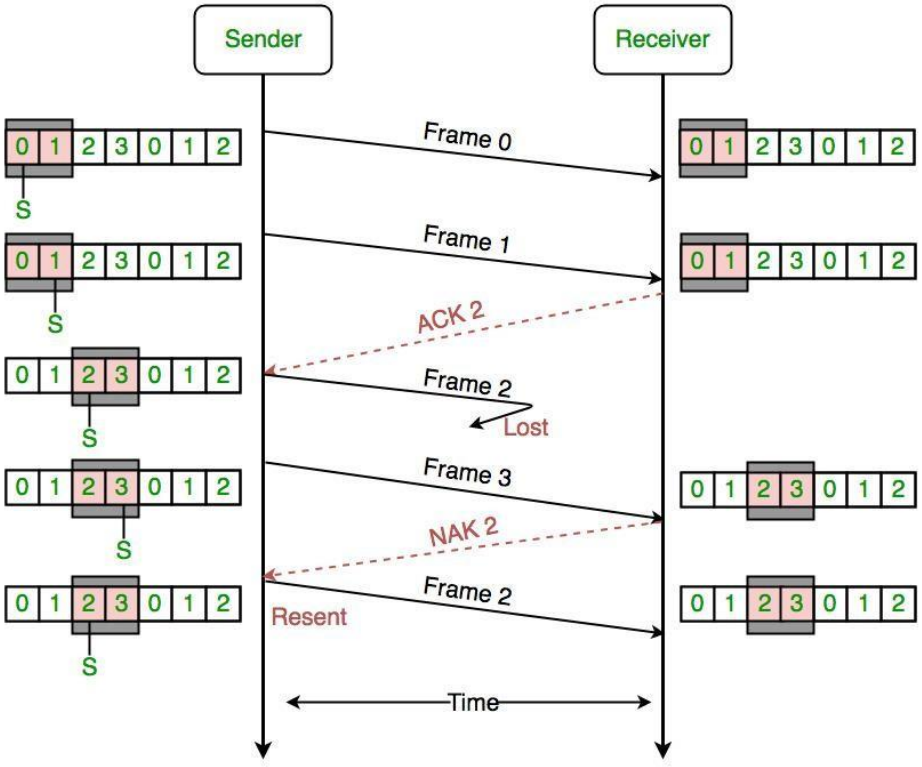


Figure: 9.8 Selective Repeat ARQ with NAK

Module-II

Chapter-9
Lecture-22

Learning Objective:

9.2 HDLC

9.3 Bit Stuffing

9.2 HDLC

HDLC (High-Level Data Link Control) is a bit-oriented protocol that is used for communication over the point-to-point and multipoint links. This protocol implements the mechanism of ARQ (Automatic Repeat Request). With the help of the HDLC protocol, full-duplex communication is possible. **HDLC** is the most widely usedprotocol and offers reliability, efficiency, and a high level of Flexibility.

In order to make the HDLC protocol applicable for various network configurations, there are three types of stations and these are as follows:

- **Primary Station** This station mainly looks after data like management. In the case of the communication between the primary and secondary station; it is the responsibility of the primary station to connect and disconnect the data link. The frames issued by the primary station are commonly known as commands.
- **Secondary Station** The secondary station operates under the control of the primary station. The Frames issued by the secondary stations are commonly known as responses.
- **Combined Station** The combined station acts as both Primary stations as well as Secondary stations. The combined station issues both commands as well as responses.

9.2.1 Transfer Modes in HDLC

The HDLC protocol offers two modes of transfer that mainly can be used in different configurations. These are as follows:

- Normal Response Mode(NRM)
- Asynchronous Balance Mode(ABM)

9.2.1.1 Normal Response Mode(NRM)

In this mode, the configuration of the station is unbalanced. There are one primary station and multiple secondary stations. Where the primary station can send the commands and the secondary station can only respond.
This mode is used for both **point-to-point** as well as **multiple-point links.**

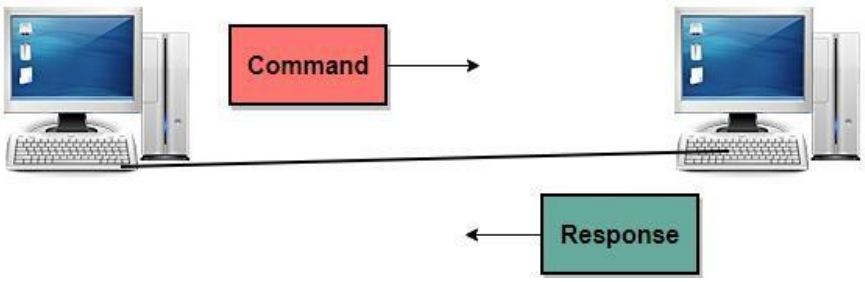


Figure: 9.9 point-to-point Normal Response Mode

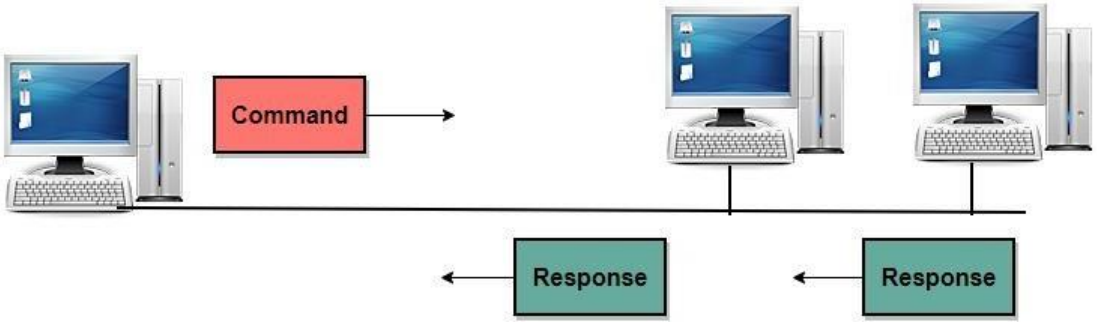


Figure: 9.10 multiple-point Normal Response Mode

9.2.1.2 Asynchronous Balance Mode(ABM)

In this mode, the configuration of the station is balanced. In this mode, the link is point-to-point, and each station can function as a primary and as secondary.

Asynchronous Balance mode(ABM) is a commonly used mode today.

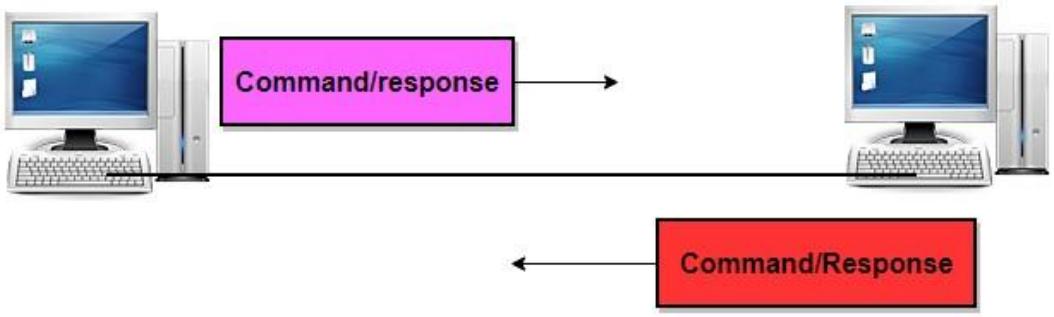


Figure: 9.11 Asynchronous Balance mode

9.2.2 HDLC Frames

In order to provide the flexibility that is necessary to support all the options possible in the modes and Configurations that are just described above. There are three types of frames defined in the HDLC:

- **Information Frames(I-frames)** These frames are used to transport the user data and the control information that is related to the user data. If the first bit of the control field is 0 then it is identified as I-frame.
- **Supervisory Frames(S-frames)** These frames are only used to transport the control information. If the first two bits of the control field are 1 and 0 then the frame is identified as S-frame
- **Unnumbered Frames(U-Frames)** These frames are mainly reserved for system management. These frames are used for exchanging control information between the communicating devices.

Each type of frame mainly serves as an envelope for the transmission of a different type of message.

9.2.3 Frame Format

There are up to six fields in each HDLC frame. There is a beginning flag field, the address field then, a control field, an information field, a frame check sequence field(FCS), and an ending field.

In the case of the multiple-frame transmission, the ending flag of the one frame acts as the beginning flag of the next frame.

Different HDLC frames:

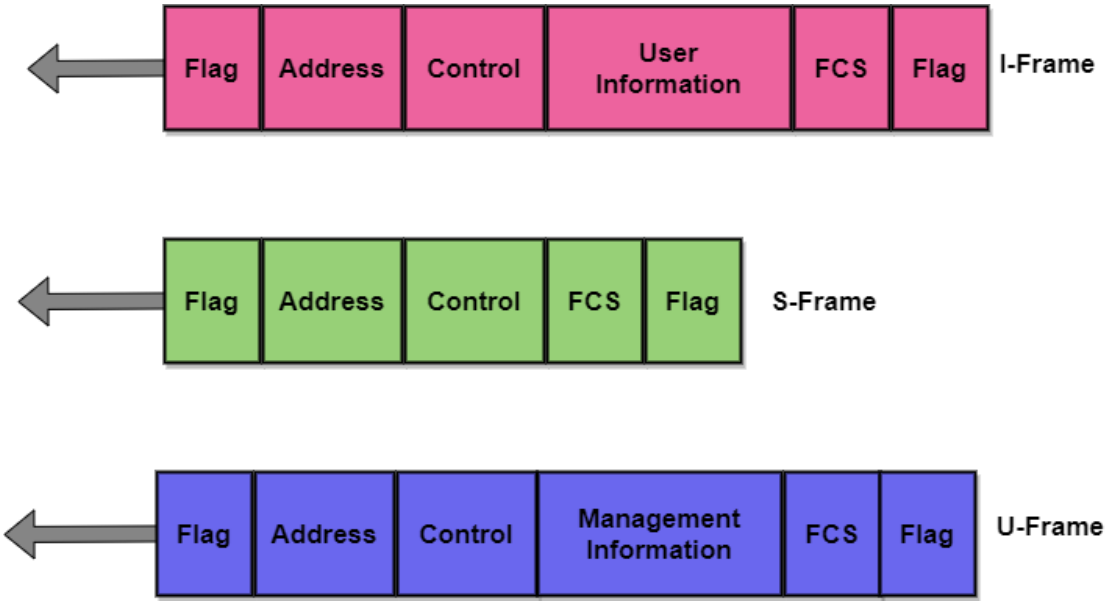


Figure: 9.12 Different HDLC frames

Now its time to discuss the fields and the use of fields in different frame types:

1. Flag Field

This field of the HDLC frame is mainly a sequence of 8-bit having the bit pattern 01111110 and it is used to identify the beginning and end of the frame. The flag field mainly serves as a synchronization pattern for the receiver.

2. Address Field

It is the second field of the HDLC frame and it mainly contains the address of the secondary station. This field can be 1 byte or several bytes long which mainly depends upon the need of the network. In case if the frame is sent by the primary station, then this field contains the address(es) of the secondary stations. If the frame is sent by the secondary station, then this field contains the address of the primary station.

3. Control Field

This is the third field of the HDLC frame and it is a 1 or 2-byte segment of the frame and is mainly used for flow control and error control. Bits interpretation in this field mainly depends upon the type of the frame.

4. Information Field

This field of the HDLC frame contains the user's data from the network layer or the management information. The length of this field varies from one network to another.

5. FCS Field

FCS means Frame check sequence and it is the error detection field in the HDLC protocol. There is a 16 bit CRC code for error detection.

9.3 Bit Stuffing

Data link layer is responsible for something called Framing, which is the division of stream of bits from network layer into manageable units (called frames). Frames could be of fixed size or variable size. In variable-size framing, we need a way to define the end of the frame and the beginning of the next frame.

Bit stuffing is the insertion of non information bits into data. Note that stuffed bits should not be confused with overhead bits. Overhead bits are non-data bits that are necessary for transmission (usually as part of headers, checksums etc.).

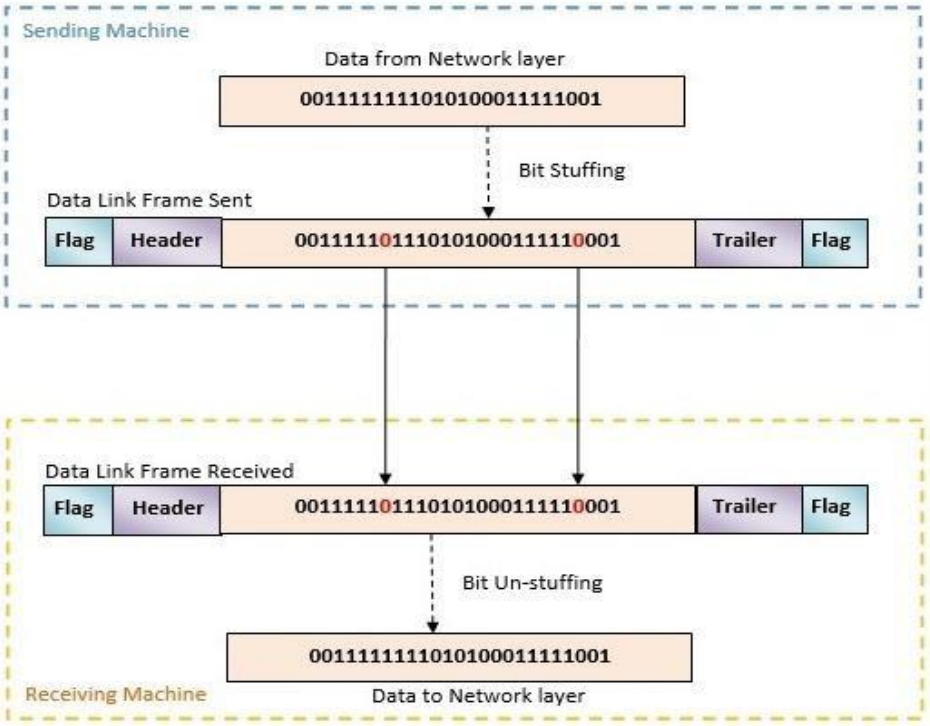


Figure: 9.13 Bit stuffing

Example of bit stuffing –

Bit sequence: 1101011111010111111010111111110 (without bit stuffing)

Bit sequence: 11010111111**0**01011111**0**1010111111**0**110 (with bit stuffing)

After 5 consecutive 1-bits, a 0-bit is stuffed.

Short Questions

1. What is Flow control and Error control?

Flow Control mainly coordinates with the amount of data that can be sent before receiving an acknowledgment from the receiver and it is one of the major duties of the data link layer.
Error Control contains both error detection and error correction. It mainly allows the receiver to inform the sender about any damaged or lost frames during the transmission and then it coordinates with the retransmission of those frames by the sender.
2. What is Stop and Wait Protocol?
Stop and wait ARQ is also referred to as the alternating protocol is a method used in two-way communication systems to send information between two connected devices (sender and a receiver). It is referred to as stop and wait ARQ because the function of this protocol is to send one frame at a time.
3. What is HDLC?
HDLC (High-Level Data Link Control) is a bit-oriented protocol that is used for communication over the point-to-point and multipoint links. This protocol implements the mechanism of ARQ (Automatic Repeat Request).
4. What is the difference NRM and ABM?
NRM : In this mode, the configuration of the station is unbalanced. There are one primary station and multiple secondary stations. Where the primary station can send the commands and the secondary station can only respond.
ABM : In this mode, the configuration of the station is balanced. In this mode, the link is point-to-point, and each station can function as a primary and as secondary.
5. What is bit stuffing?
Bit stuffing is the insertion of non information bits into data. Stuffed bits should not be confused with overhead bits. Overhead bits are non-data bits that are necessary for transmission (usually as part of headers, checksums etc.).

Long Questions

1. Describe Stop and Wait Protocol.

2. Differentiate Go back N ARQ and Selective ARQ.
3. Discuss different HDLC frame format.

Module-II

Chapter-10
Lecture-23

PPP and Multiple Access Protocols

Learning Objective:

10.1 Point-to-Point Protocol

10.1 Point-to-Point Protocol (PPP)

PPP (Point-To-Point) protocol is a protocol used in the data link layer. The **PPP** protocol is mainly used to establish a direct connection between two nodes. The Point-To-Point protocol mainly provides connections over multiple links.

- This protocol defines how two devices can authenticate with each other.
- PPP protocol also defines the format of the frames that are to be exchanged between the devices.
- This protocol also defines how the data of the network layer are encapsulated in the data link frame.
- The PPP protocol defines how the two devices can negotiate the establishment of the link and then can exchange the data.
- This protocol provides multiple services of the network layer and also supports various network-layer protocols.
- This protocol also provides connection over multiple links.

10.1.1 PPP Frame Format

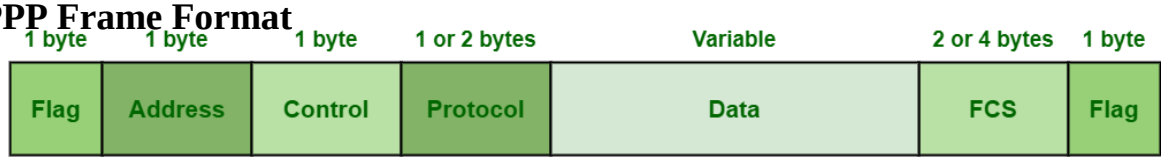


Figure: 10.1 PPP Frame format

1. Flag

The PPP frame mainly starts and ends with a 1-byte flag field that has the bit pattern: 01111110. It is important to note that this pattern is the same as the flag pattern used in HDLC. But there is a difference too and that is PPP is a byte-oriented protocol whereas the HDLC is a bit-oriented protocol.

2. Address

The value of this field in PPP protocol is constant and it is set to 11111111 which is a broadcast address. The two parties can negotiate and can omit this byte.

3. Control

The value of this field is also a constant value of 11000000. We have already told you that PPP does not provide any flow control and also error control is limited to error detection. The two parties can negotiate and can omit this byte.

4. Protocol

This field defines what is being carried in the data field. It can either be user information or other information. By default, this field is 2 bytes long.

5. Payload field

This field carries the data from the network layer. The maximum length of this field is 1500 bytes. This can also be negotiated between the endpoints of communication.

6. FCS

It is simply a 2-byte or 4-byte standard CRC (Cyclic redundancy check).

10.1.2 Transition phases of PPP protocol

- **Dead:** Dead is a transition phase which means that the link is not used or there is no active carrier at the physical layer.
- **Establish:** If one of the nodes starts working then the phase goes to the establish phase. In short, we can say that when the node starts communication or carrier is detected then it moves from the dead to the establish phase.

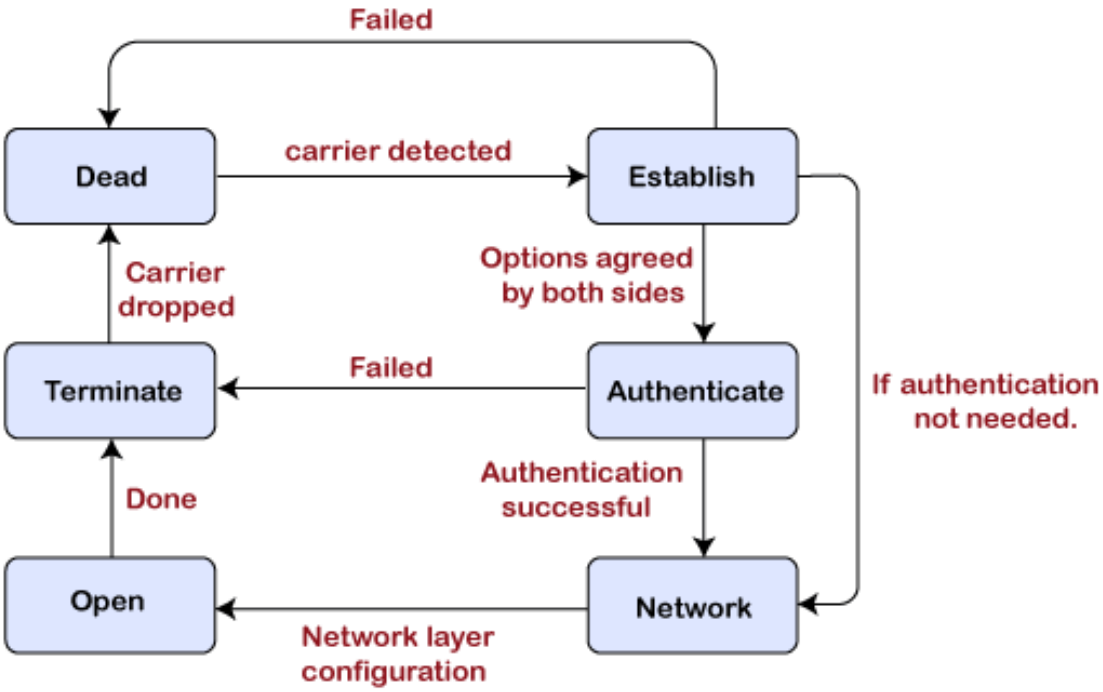


Figure: 10.2 Transition phases of PPP protocol

- **Authenticate:** It is an optional phase which means that the communication can also moves to the authenticate phase. The phase moves from the establish to the authenticate phase only when both the communicating nodes agree to make the communication authenticated.
- **Network:** Once the authentication is successful, the network is established or phase is network. In this phase, the negotiation of network layer protocols take place.
- **Open:** After the establishment of the network phase, it moves to the open phase. Here open phase means that the exchange of data takes place. Or we can say that it reaches to the open phase after the configuration of the network layer.
- **Terminate:** When all the work is done then the connection gets terminated, and it moves to the terminate phase.

10.1.3 PPP Stack

In PPP stack, there are three set of protocols:

10.1.3.1 Link Control Protocol (LCP)

The role of LCP is to establish, maintain, configure, and terminate the links. It also provides negotiation mechanism.

10.1.3.2 Authentication protocols

There are two types of authentication protocols, i.e., PAP (Password Authenticate protocols), and CHAP (Challenged Handshake Authentication Protocols).

- **PAP (Password Authentication Protocols):** The Password Authentication Protocol (PAP) is a simple authentication procedure with a two-step process (Figure: 10.3):

  1. The user who wants to access a system sends an authentication identification(usually the user name) and a password.
  2. The system checks the validity of the identification and password and either accepts or denies connection.

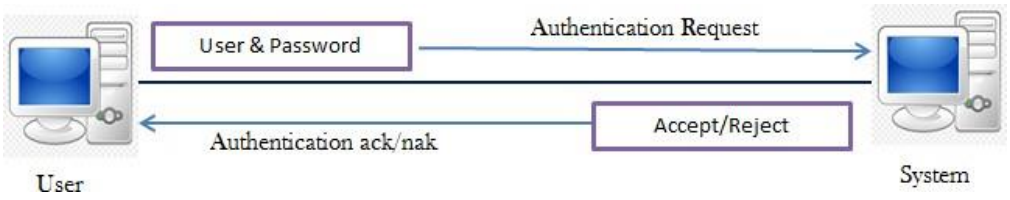


Figure: 10.3 PAP protocol

- **CHAP** (**Challenge Handshake Authentication Protocol):** The Challenge Handshake Authentication Protocol (CHAP) is a three-way hand-shaking authentication protocol that provides greater security than PAP. In this method, the password is kept secret; it is never sent online.
  1. The system sends the user a challenge packet containing a challenge value, usually a few bytes.
  2. The user applies a predefined function that takes the challenge value and the user's own password and creates a result. The user sends the result in the response packet to the system.
  3. The system does the same. It applies the same function to the password of the user (known to the system) and the challenge value to create a result. If the result created is the same as the result sent in the response packet, access is granted; otherwise, it is denied.

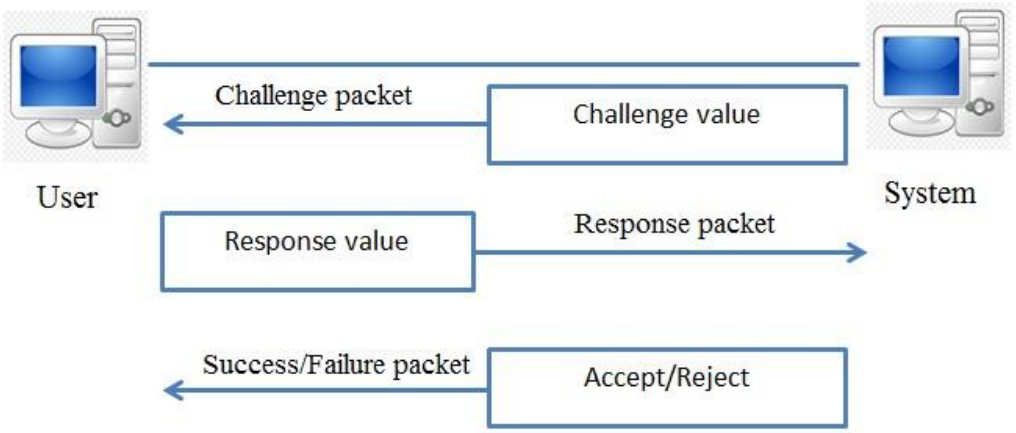


Figure: 10.3 CHAP protocol

10.1.3.3 Network Control Protocol (NCP)

After the establishment of the link and authentication, the next step is to connect to the network layer. So, PPP uses another protocol known as network control protocol (NCP). The NCP is a set of protocols that facilitates the encapsulation of data which is coming from the network layer to the PPP frames.

Module-II

Chapter-10
Lecture-24

Learning Objective:

10.2 Multiple Access

10.2.1 Random Access Protocol

10.2 Multiple Access

We can consider the data link layer as two sublayers. The upper sublayer is responsible for data link control, and the lower sublayer is responsible for resolving access to the shared media. If the channel is dedicated, we do not need the lower sublayer.

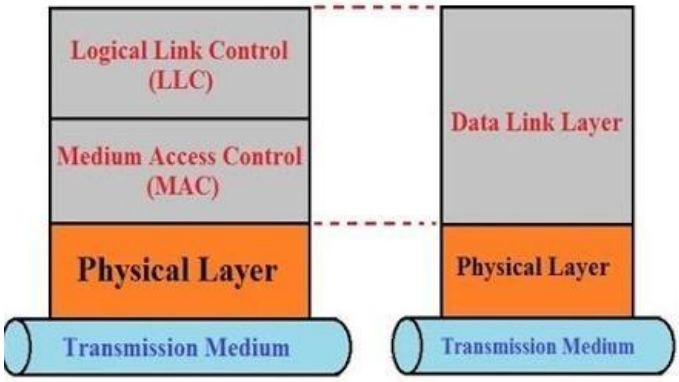


Figure: 10.4 Medium Access Control Sub layer (MAC)

The upper sublayer that is responsible for flow and error control is called the logical link control (LLC) layer; the lower sublayer that is mostly responsible for multiple•access resolution is called the media access control (MAC) layer.

When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link.

Types of Multiple Access Protocol

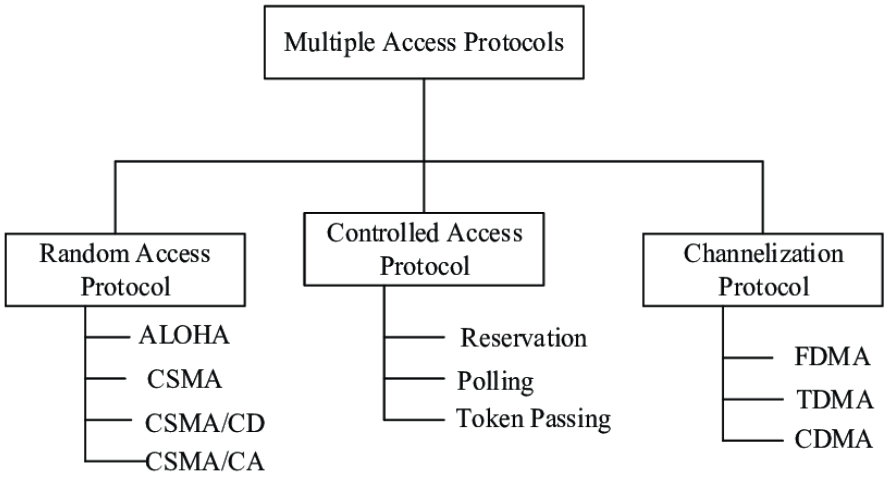


Figure: 10.5 Types of Multiple Access Protocol

10.2.1 Random Access Protocol

In a random access method, each station has the right to the medium without being controlled by any other station. However, if more than one station tries to send, there is an access conflict-collision-and the frames will be either destroyed or modified.

10.2.1.1 ALOHA (Multiple Access)

The ALOHA protocol or also known as the **ALOHA method** is a simple communication scheme in which every transmitting station or source in a network will send the data whenever a frame is available for transmission. If we succeed and the frame reaches its destination, then the next frame is lined-up for transmission. But remember, ifthe data frame is not received by the receiver (maybe due to collision) then the frame is sent again until it successfully reaches the receiver's end.

Whenever we talk about a wireless broadcast system or a half-duplex two-way link, the ALOHA method works efficiently. But as the network becomes more and more complex e.g. the ethernet. Now here in the ethernet, the system involves multiple sources and destinations which share a common data path or channel, then the conflict occursbecause data-frames collide, and the information is lost.

Following is the flow chart of **Pure ALOHA**.

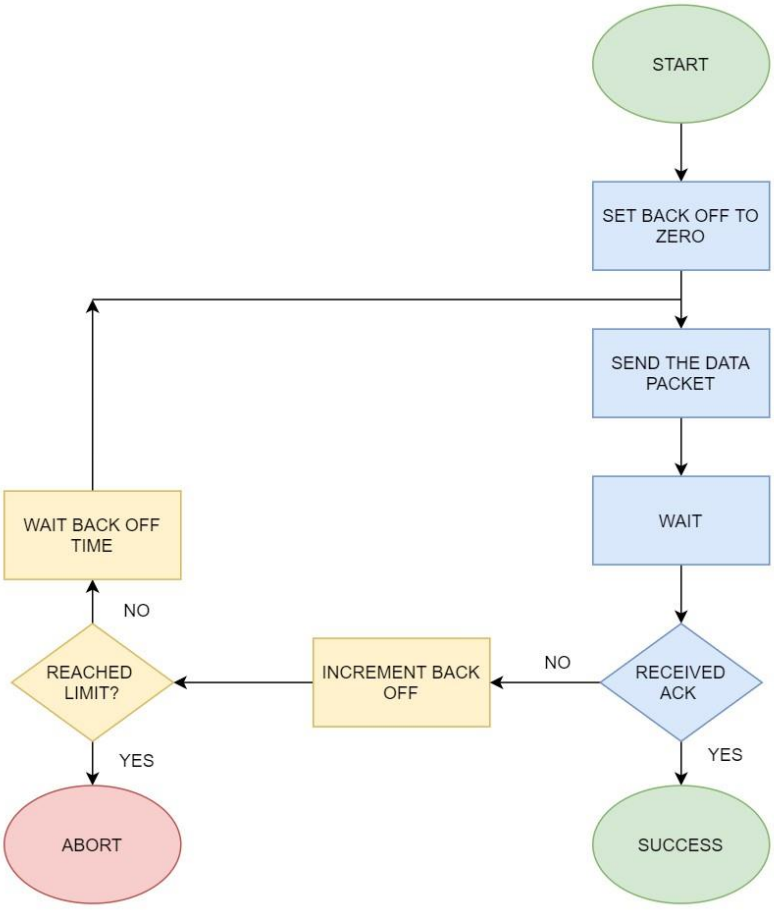


Figure: 10.6 Multiple Access (Pure Aloha)

So, to minimize these collisions and to optimize network efficiency as well as to increase the number of subscribers that can use a given network, the **slotted ALOHA** was developed. This system consists of the signals termed as beacons which are sent at precise time intervals and inform each source when the channel is clear to send theframe.

Module-II

Chapter-10
Lecture-25

Learning Objective:

10.2 Multiple Access

10.2.1 Random Access Protocol

10.2.1.2 CSMA (Carrier Sense Multiple Access)

10.2.1.2 CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

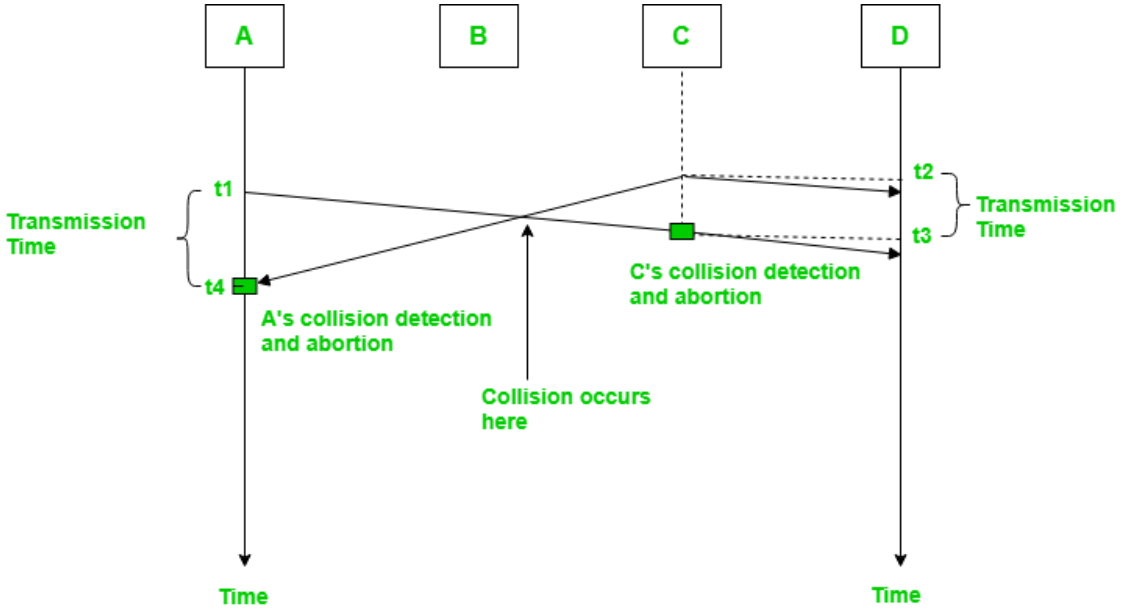


Figure: 10.7 Collision in CSMA

CSMA Access Modes

1-Persistent:

In 1-persistent CSMA, station continuously senses channel to check its state i.e. idle or busy so that it can transfer data. In case when channel is busy, station will wait for channel to become idle. When station finds an idle channel, it transmits frame to channel without any delay with probability 1. Due to probability 1, it is called 1- persistent CSMA. The problem with this method is that there is a huge chance of collision, as two or more stations can find channel in idle state and transmit frames at the same time. At the time when a collision occurs station has to wait for random time for channel to be idle and to start all again.

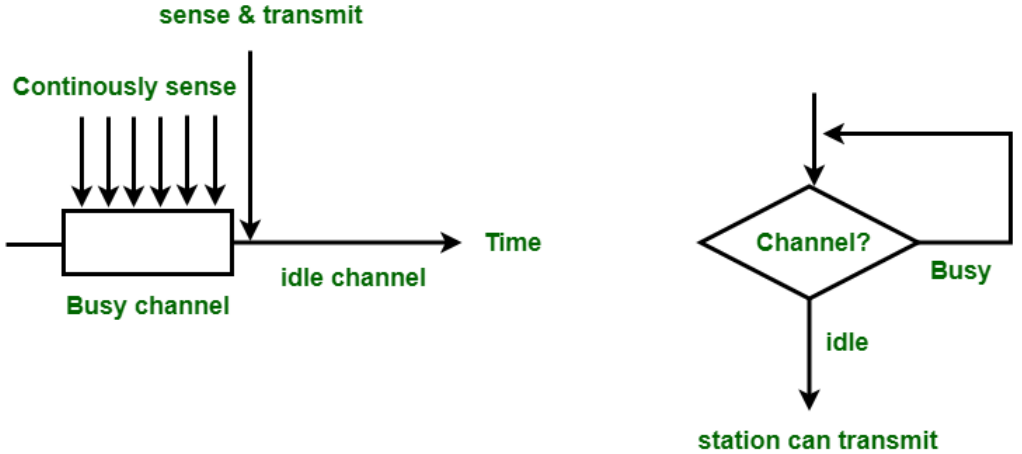
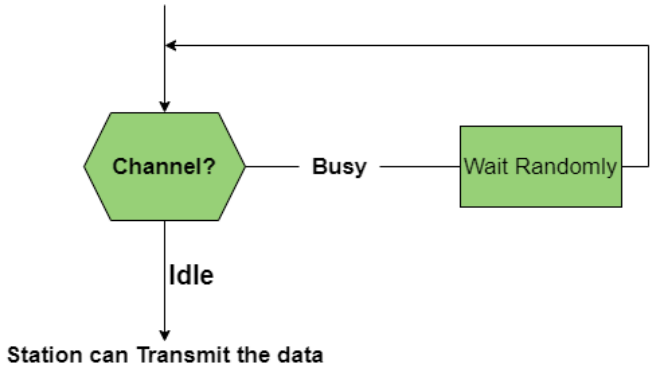


Figure: 10.8 1-persistent CSMA

Non-Persistent:

It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.



p-persistent CSMA :

p-persistent CSMA is used when a channel has time-slots and that time-slot duration is equal to or greater than maximum propagation delay time for that channel. When station is ready to send frames, it will sense channel. If channel found to be busy, station will wait for next time-slot. But if channel is found to be idle, station transmits frame immediately with a probability p. The station thus waits for left probability i.e. q which is equal to 1-p, for beginning of next time-slot. If the next time-slot is also found idle, station transmits or waits again with probabilities p and q.This process repeats until either frame gets transmitted or another station starts transmitting.

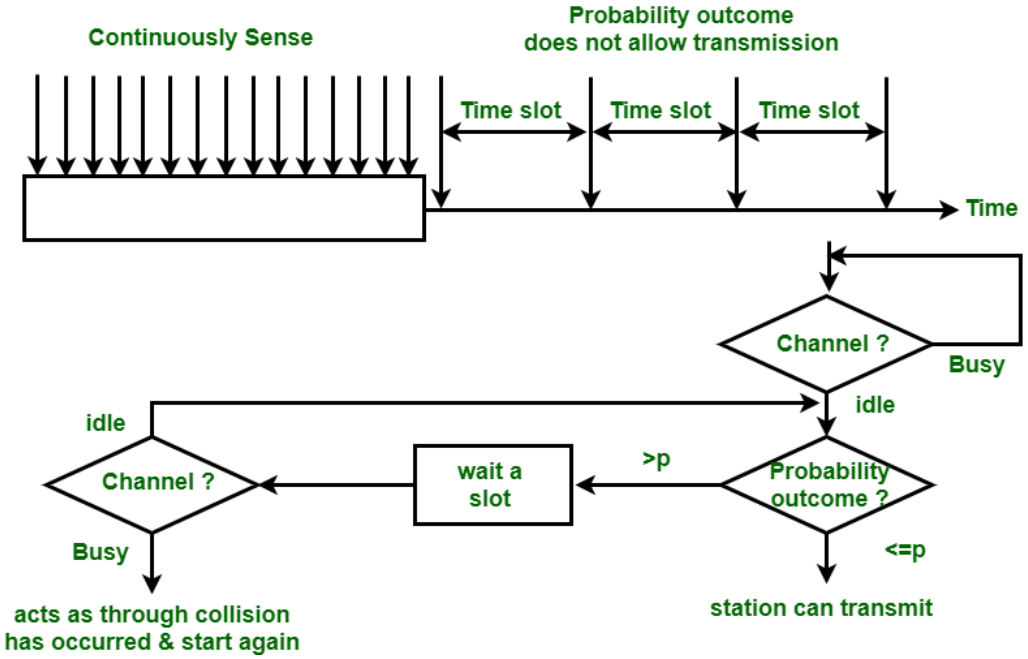


Figure: 10.9 p-persistent CSMA

Module-II

Chapter-10
Lecture-26

Learning Objective:

10.2 Multiple Access

10.2.1 Random Access Protocol

10.2.1.3 CSMA/CD

10.2.1.4 CSMA/CA

10.2.1.3 CSMA/ CD (Carrier Sense Multiple Access/ Collision Detection)

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waitsfor a random time before sending a frame to a channel.

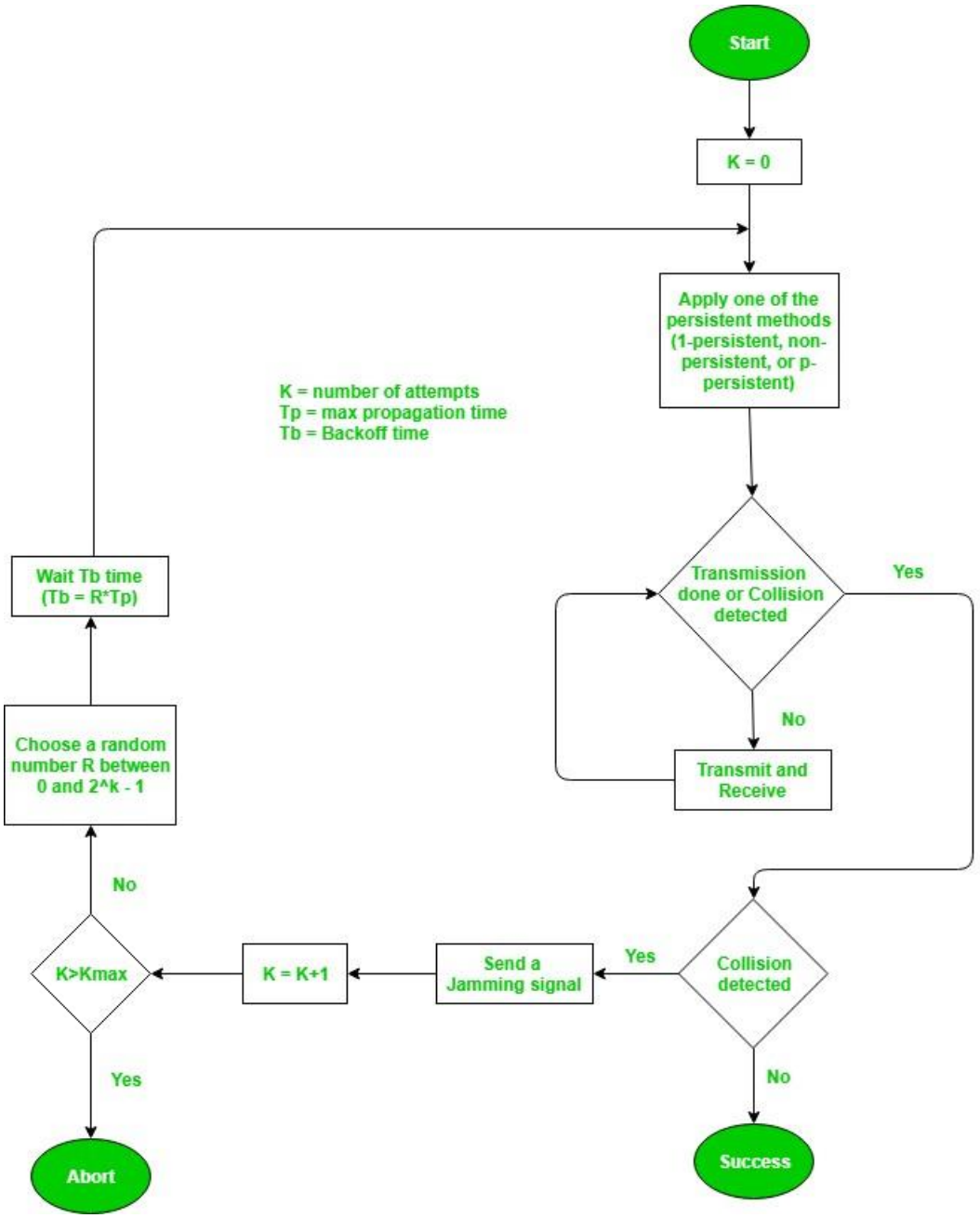


Figure: 10.10 Collision Detection Flowchart

10.2.1.4 CSMA/ CA (Carrier Sense Multiple Access/Collision Avoidance)

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the CSMA/ CA to avoid the collision:

Interframe space:

In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the Interframe space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window:

In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment:

In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

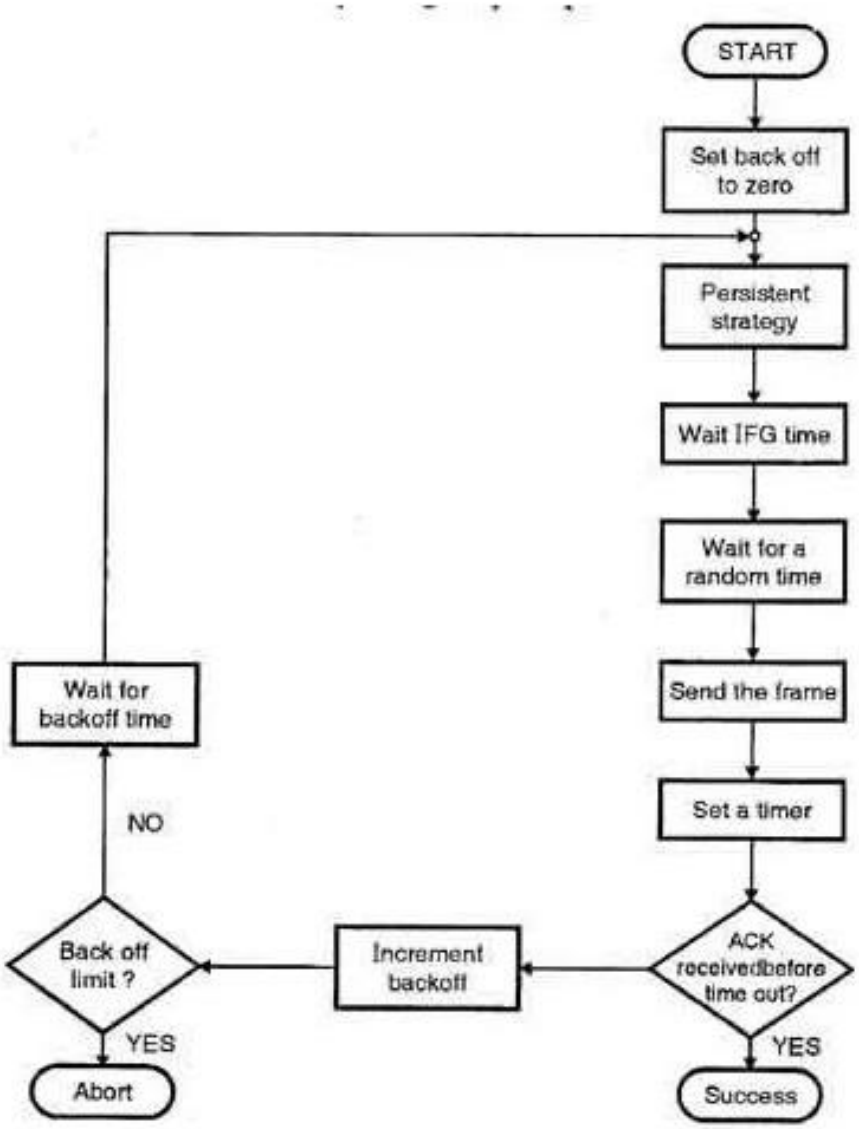


Figure: 10.11 Collision Avoidance Flowchart

Module-II

Chapter-10
Lecture-27

Learning Objective:

10.2 Multiple Access

10.2.2 Controlled Access

10.2.2 Controlled Access Protocols

In the Controlled access technique, all stations need to consult with one another in order to find out which station has the right to send the data.

- The controlled access protocols mainly grant permission to send only one node at a time; thus in order to avoid the collisions among the shared mediums.
- No station can send the data unless it has been authorized by the other stations.

The protocols lies under the category of Controlled access are as follows:

1. Reservation
2. Polling
3. Token Passing

10.2.2.1 Reservation

In this method, a station needs to make a reservation before sending the data.

- Time is mainly divided into intervals.
- Also, in each interval, a reservation frame precedes the data frame that is sent in that interval.
- Suppose if there are '**N**' stations in the system in that case there are exactly '**N**' reservation minislots in the reservation frame; where each minislot belongs to a station.
- Whenever a station needs to send the data frame, then the station makes a reservation in its own minislot.
- Then the stations that have made reservations can send their data after the reservation frame.

Example

Let us take an example of 5 stations and a 5-minislot reservation frame. In the first interval, the station 2,3 and 5 have made the reservations. While in the second interval only station 2 has made the reservations.

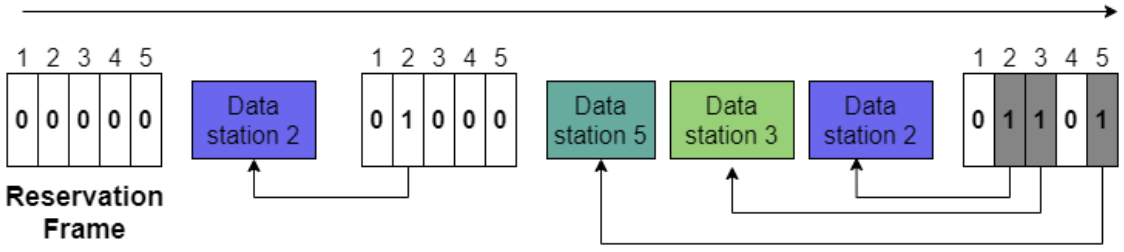


Figure: 10.12 Reservation Access Method

10.2.2.2 Polling

The polling method mainly works with those topologies where one device is designated as the primary station and the other device is designated as the secondary station.

- All the exchange of data must be made through the primary device even though the final destination is the secondary device.
- Thus to impose order on a network that is of independent users, and in order to establish one station in the network that will act as a controller and periodically polls all other stations is simply referred to as **polling**.
- The Primary device mainly controls the link while the secondary device follows the instructions of the primary device.
- The responsibility is on the primary device in order to determine which device is allowed to use the channel at a given time.

- Therefore the primary device is always an initiator of the session.

Poll Function

In case if primary devices want to receive the data, then it usually asks the secondary devices if they have anything to send. This is commonly known as **Poll Function**.

- There is a poll function that is mainly used by the primary devices in order to solicit transmissions from the secondary devices.
- When the primary device is ready to receive the data then it must ask(poll) each secondary device in turn if it has anything to send.
- If the secondary device has data to transmit then it sends the data frame, otherwise, it sends a negative acknowledgment (NAK).
- After that in case of the negative response, the primary then polls the next secondary, in the same manner until it finds the one with the data to send. When the primary device received a positive response that means (a data frame), then the primary devices reads the frame and then returns an acknowledgment (ACK)frame,

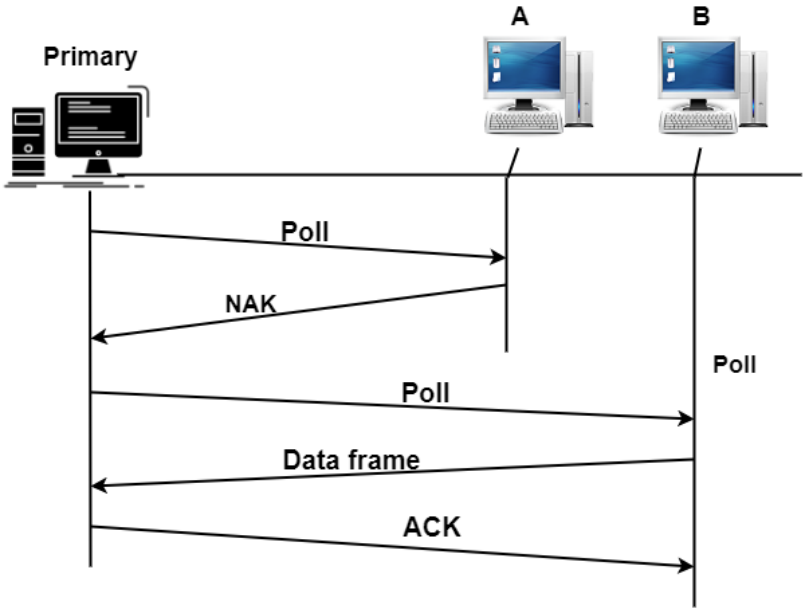


Figure: 10.13 Polling

Select Function

In case, if the primary device wants to send the data then it tells the secondary devices in order to get ready to receive the data. This is commonly known as the **Select function**.

- Thus the select function is used by the primary device when it has something to send.
- We had already told you that the primary device always controls the link.
- Before sending the data frame, a select (SEL) frame is created and transmitted by the primary device, and one field of the SEL frame includes the address of the intended secondary.
- The primary device alerts the secondary devices for the upcoming transmission and after that wait for an acknowledgment (ACK) of the secondary devices.

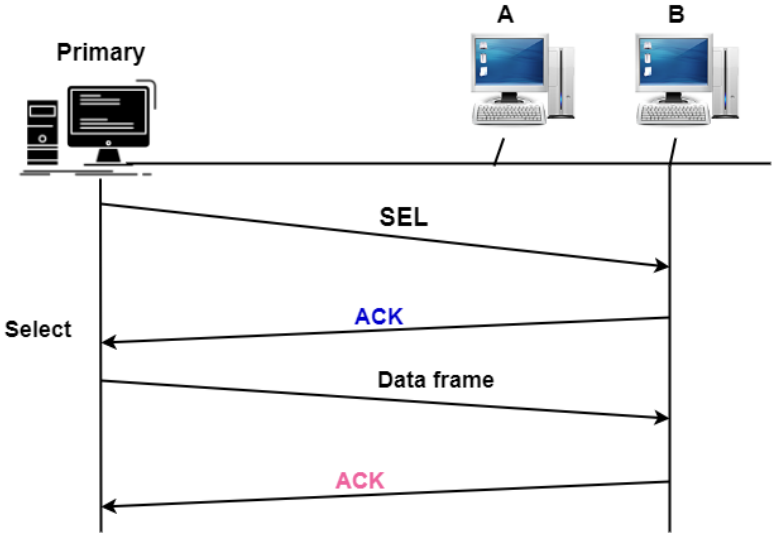


Figure: 10.14 Select

10.2.2.3 Token Passing

In the token passing methods, all the stations are organized in the form of a logical ring. We can also say that for each station there is a predecessor and a successor.

- The predecessor is the station that is logically before the station in the ring; while the successor is the station that is after the station in the ring. The station that is accessing the channel now is the **current station**.
- Basically, a special bit pattern or a small message that circulates from one station to the next station in some predefined order is commonly known as a **token**.
- Possessing the token mainly gives the station the right to access the channel and to send its data.
- When any station has some data to send, then it waits until it receives a token from its predecessor. After receiving the token, it holds it and then sends its data. When any station has no more data in order to send then it releases the token and then passes the token to the next logical station in the ring.
- Also, the station cannot send the data until it receives the token again in the next round.
- In Token passing, when a station receives the token and has no data to send then it just passes the token to the next station.

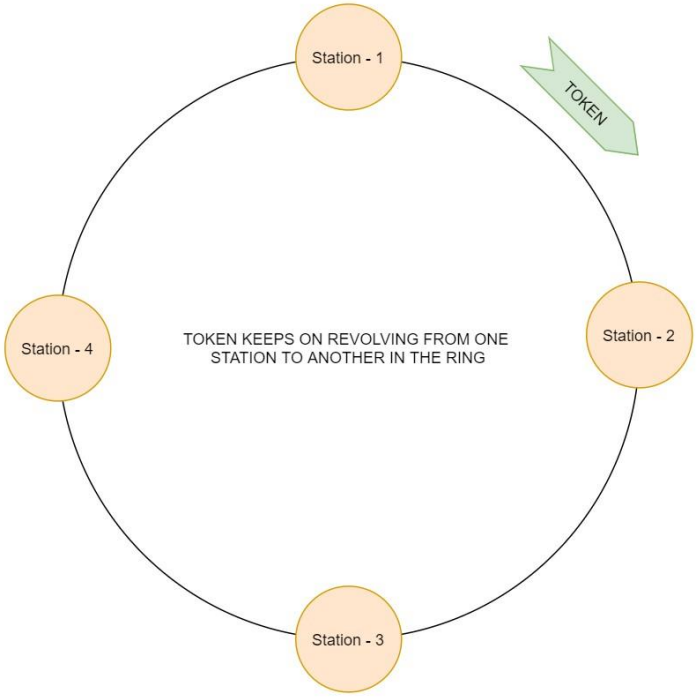


Figure: 10.15 Token Passing

Module-II

Chapter-10
Lecture-28

Learning Objective:

10.2 Multiple Access

10.2.3 Channelization

10.2.3 Channelization

Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations. The three channelization protocols are FDMA, TDMA, and CDMA.

10.2.3.1 Frequency-Division Multiple Access (FDMA)

In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data. In other words, each band is reserved for a specific station, and it belongs to the station all the time. Each station also uses a bandpass filter to confine the transmitter frequencies. To prevent station interferences, the allocated bands are separated from one another by small guard bands.

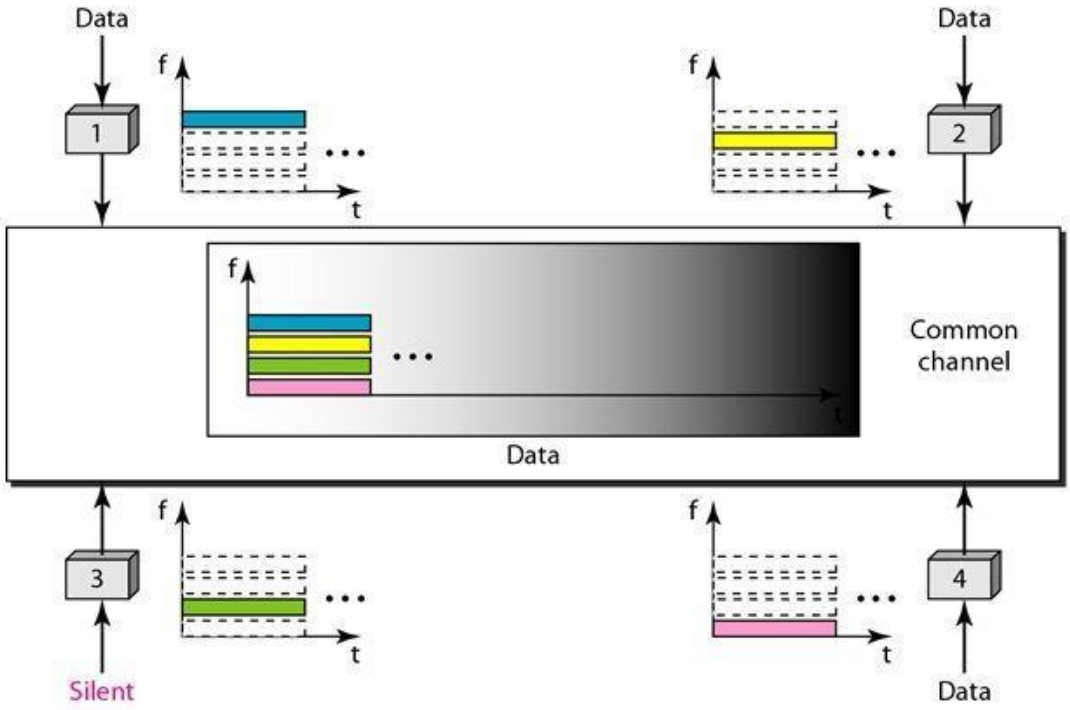


Figure: 10.16 FDMA

10.2.3.2 Time-Division Multiple Access (TDMA)

In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time. Each station is allocated a time slot during which it can send data. Each station transmits its data in is assigned time slot.

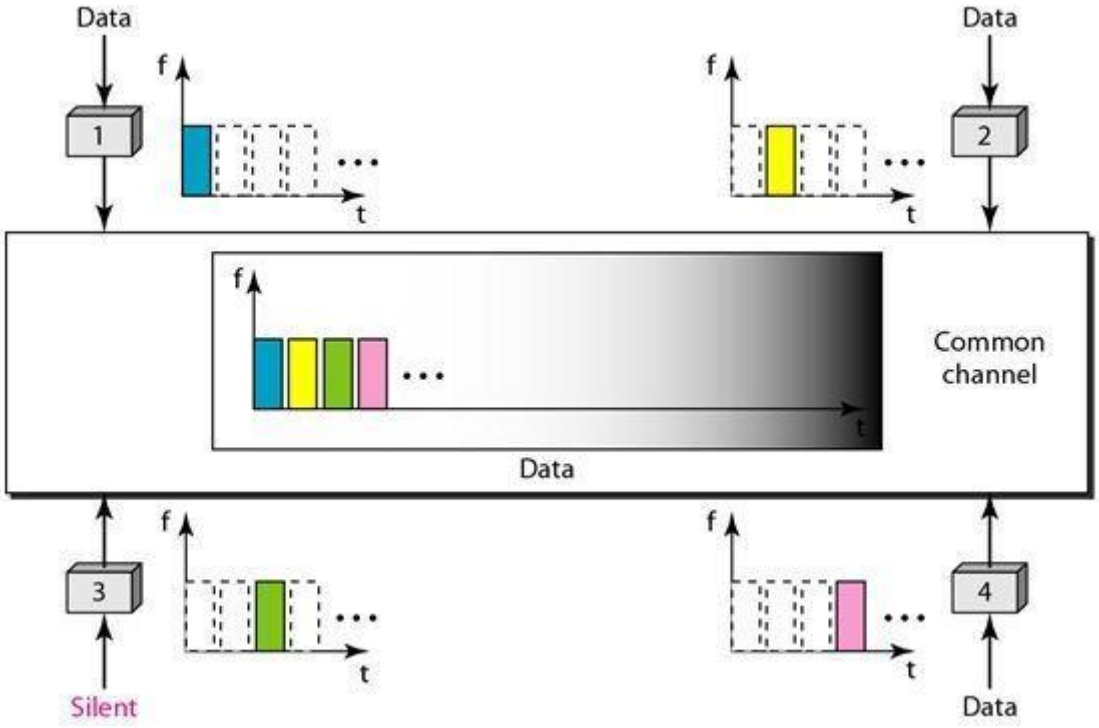


Figure: 10.17 TDMA

10.2.3.3 Code-Division Multiple Access (CDMA)

CDMA simply means communication with different codes. CDMA differs from FDMA because only one channel occupies the entire bandwidth of the link. It differs from TDMA because all stations can send data simultaneously; there is no timesharing.

Implementation:

Let us assume we have four stations 1, 2, 3, and 4 connected to the same channel. The data from station 1 are d1 , from station 2 are d2, and so on. The code assigned to the first station is c1, to the second is c2, and so on. We assume that the assigned codes have two properties.

1. If we multiply each code by another, we get 0.
2. If we multiply each code by itself, we get 4 (the number of stations).

With these two properties in mind, how the above four stations can send data using the same common channel, as shown in the following figure.

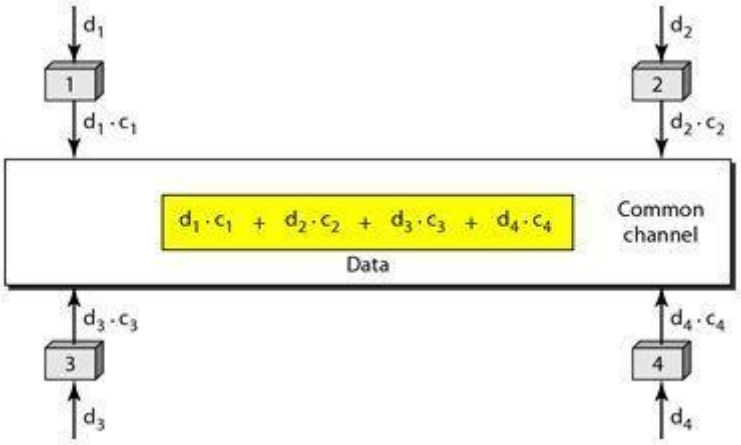


Figure: 10.18 CDMA

Station 1 multiplies (a special kind of multiplication, as we will see) its data by its code to get d1.c1. Station 2 multiplies its data by its code to get d2.c2. And so on. The data that go on the channel are the sum of all these terms, as shown in the box.

Any station that wants to receive data from one of the other three multiplies the data on the channel by the code of the sender. For example, suppose stations 1 and 2 are talking to each other. Station 2 wants to hear what station 1 is saying. It multiplies the data on the channel by c1 the code of station1.
Because (c1.c1) is 4, but (c2 . c1), (c3. c1), and (c4 .c1) are all 0s, station 2 divides the result by 4 to get the data from station1.

data =(d1.c1+d2.c2+d3.c3+d4.c4).c1

= c1. d1. c1+ c1. d2. c2+ c1. d3. c3+ c1. d4. c4= 4d1

Chips:

CDMA is based on coding theory. Each station is assigned a code, which is a sequence of numbers called chips, as shown in the following figure. The codes are for the previous example.

Figure: 10.19 Chip codes

We need to know that we did not choose the sequences randomly; they were carefully selected. They are called orthogonal sequences and have the following properties:

1. Each sequence is made of N elements, where N is the number of stations.

2. If we multiply a sequence by a number, every element in the sequence is multiplied by that element. This is called multiplication of a sequence by a scalar. For example,

2. [+1 +1-1-1] = [+2+2-2-2]

3. If we multiply two equal sequences, element by element, and add the results, we get N, where N is the number of elements in the each sequence. This is called the inner product of two equal sequences. For example,

[+1 +1-1 -1]. [+1 +1 -1 -1] = 1 + 1 + 1 + 1 = 4

4. If we multiply two different sequences, element by element, and add the results, we get 0. This is called inner product of two different sequences. For example,

[+1 +1 -1-1] • [+1 +1 +1 +1] = 1 + 1 - 1 - 1 = 0

5. Adding two sequences means adding the corresponding elements. The result is another sequence. For example,

[+1+1-1-1]+[+1+1+1+1]=[+2+2 +0 +0]

Data Representation:

We follow the following rules for encoding: If a station needs to send a 0 bit, it encodes it as -1, if it needs to send a 1 bit, it encodes it as +1. When a station is idle, it sends no signal, which is interpreted as a 0.

Encoding and Decoding:

As a simple example, we show how four stations share the link during a 1-bit interval. The procedure can easily be repeated for additional intervals. We assume that stations 1 and 2 are sending a 0 bit and channel 4 is sending a 1 bit. Station 3 is silent.

The data at the sender site are translated to -1, -1, 0, and +1. Each station multiplies the corresponding number by its chip (its orthogonal sequence), which is unique for each station. The result is a new sequence which is sent to the channel. For simplicity, we assume that all stations send the resulting sequences at the same time. The sequence on the channel is the sum of all four sequences as defined before. The following figure shows the situation.

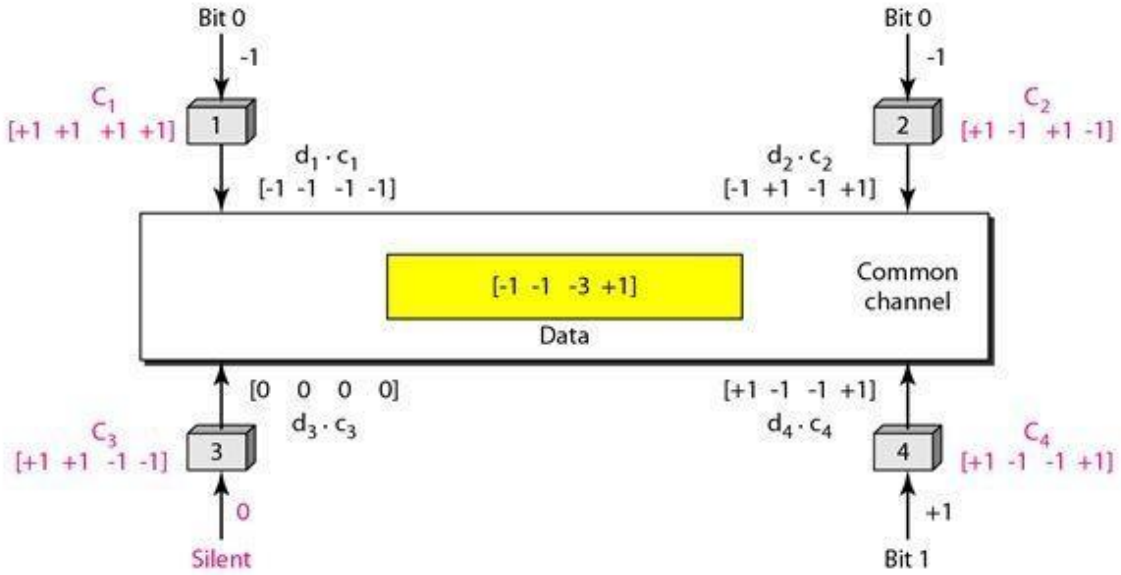


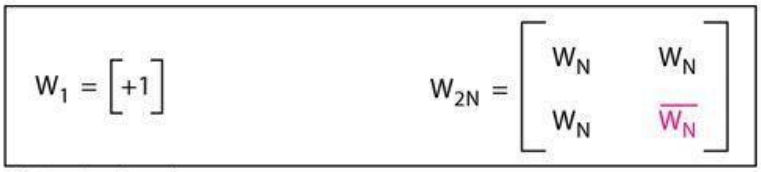
Figure: 10.20 CDMA

Now imagine station 3, which we said is silent, is listening to station 2. Station 3 multiplies the total data on the channel by the code for station 2, which is [+1 -1 +1-1],
to get

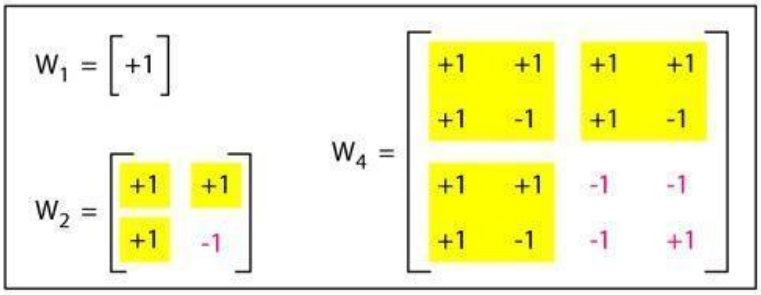
[-1-1-3 +1]• [+1-1 +1-1] =-4/4 =-1 -------> bit 1

Sequence Generation:

To generate chip sequences, we use a Walsh table, which is a two-dimensional table with an equal number of rows and columns, as shown in the following figure.



a. Two basic rules



b. Generation of W_1, W_2, and W_4

Figure: 10.21 Walsh Table

In the Walsh table, each row is a sequence of chips. W1 for a one-chip sequence has one row and one column. We can choose –1 or +1 for the chip for this trivial table (we chose +1).

According to Walsh, if we know the table for N sequences WN we can create the table for 2N sequences W2N, as shown in Figure. The WN with the overbar WN stands for the complement of WN where each +1 is changed to -1 and vice versa.

Short Questions

1. What are the transition phases of PPP protocol?

Dead, Establish, Authenticate, Network, Open and Terminate

2. What is PAP (Password Authentication Protocols)?

The Password Authentication Protocol (PAP) is a simple authentication procedure with a two-step

a. The user who wants to access a system sends an authentication identification(usually the user name) and a password.

b. The system checks the validity of the identification and password and either accepts or denies connection.

3. Draw the PPP Frame Format.

4. Differentiate between Pure ALOHA and slotted ALOHA.

Key	Pure Aloha	Slotted Aloha
Time Slot	In Pure Aloha, any station can transmit data at any time.	In Slotted Aloha, any station can transmit data only at the beginning of a time slot.
Time	In Pure Aloha, time is continuous and is not globally synchronized.	In Slotted Aloha, time is discrete and is globally synchronized.

5. Differentiate between CSMA/CD and CSMA/CA.

S.NO	CSMA/CD	CSMA/CA
a.	CSMA / CD is effective after a collision.	Whereas CSMA / CA is effective before a collision.
b.	CSMA / CD is used in wired networks.	Whereas CSMA / CA is commonly used in wireless networks.
c.	It only reduces the recovery time.	Whereas CSMA/ CA minimizes the possibility of collision.
d.	CSMA / CD resends the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
e.	CSMA / CD is used in 802.3 standard.	While CSMA / CA is used in 802.11 standard.

6. What is token passing method?

Token passing is a channel access method where a packet called a token is passed between nodes to authorize that node to communicate.

7. What is Reservation method?

In this method, a station needs to make a reservation before sending the data.

- Time is mainly divided into intervals.
- Also, in each interval, a reservation frame precedes the data frame that is sent in that interval.
- Suppose if there are '**N**' stations in the system in that case there are exactly '**N**' reservation minislots in the reservation frame; where each minislot belongs to a station.

- Whenever a station needs to send the data frame, then the station makes a reservation in its own minislot.
- Then the stations that have made reservations can send their data after the reservation frame.

Long Questions

1. What are the difference between PAP and CHAP?
2. Describe CSMA/CD and CSMA/CA.
3. Differentiate between Poll and select Function.
4. Describe Channelization Methods.

Module-II

Chapter-11
Lecture-29

LAN and Wireless LAN

Learning Objective:

11.1 LAN: Ethernet

11.1 LAN: Ethernet

Ethernet is the technology that is commonly used in wired local area networks (LANs). Ethernet isa network protocol that controls how data is transmitted over a LAN and is referred to as the IEEE 802.3 protocol. The protocol has evolved and improved over time to transfer data at the speed of more than a gigabit per second.

Ethernet is the most popular physical layer LAN technology in use today. It defines the number of conductors that are required for a connection, the performance thresholds that can be expected, and provides the framework for data transmission. A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps).

Ethernet was developed over several years in the early 1970s by group researchers within the company Xerox Palo Alto Research Center (**Xerox PARC**) including, in particular, Robert Metcalfe (who founded later 3Com company). The goal the research project was to connect networked computers and laser printers.

Types of Ethernet network

The maximum data rate of the original Ethernet technology is 10 megabits per second (Mbps), but a second generation fast ethernet carries 100 Mbps, and the latest version called gigabit ethernet works at 1000 Mbps. Ethernet network can be classified into 3 types:

11.1.1 Fast Ethernet

This type of Ethernet can transfer data at a rate of 100 Mbps. Fast Ethernet makes use of twisted pair cable or fiber optic cable for communication.

There are three types of fast Ethernet, which are as follows:

- 100BASE-TX
- 100BASE-FX
- 100BASE-T4

11.1.2 Gigabit Ethernet

This type of Ethernet network can transfer data at a rate of 1000 Mbps. Gigabit Ethernet also makes use of twisted pair cable or fiber optic cable. 48 bits used for addressing in Gigabit Ethernet. Nowadays gigabit Ethernet is very popular. The latest Gigabit Ethernet is a 10 Gigabit Ethernet, which can transfer data at a rate of 10 Gbps. Gigabit Ethernet was developed so that it can meet the needs of the user like faster communication network, faster transfer of data etc.

11.1.3 Switch Ethernet

Switched Ethernet involves adding switches so that each workstation can have its own dedicated 10 Mbps connection rather than sharing the medium, which can improve network throughput – it has the advantage over rival switched technologies such as asynchronous transfer mode that it employs the same low-level protocols, cheap cabling, and network interface cards as ordinary Ethernet.

When we use a switch in a network, then we use a regular network cable rather than using a crossover cable. The crossover cable is made up of a transmission pair at one end and a receiving pair at the other end. The main task of the switch in a network is to transfer the data from one device to another device in the same network without affecting the other devices. It supports different data transfer rates like 10Mbps to 100Mbps for fast Ethernet and 1000Mbps to

10 Gbps for the latest Ethernet. This type of Ethernet makes use of star topology.

Features of Ethernet

The features of Ethernet are as follows:

• Through Ethernet network, data can be sent and received at very high speed.

• Ethernet network is less expensive.

• With the help of Ethernet networking, your data is secured as it protected your data. Suppose that someone is attempting on your network, and then all of the devices in your network stop processing instantly and wait until the user attempts to transmit it again.

• Ethernet facilitates us to share our data and resources like printers, scanners, computers etc.

• Ethernet network quickly transmits the data. That's why, nowadays most of the universities and college campuses make use of Ethernet technology, which is based upon the Gigabit Ethernet.

Module-II

Chapter-11
Lecture-30

Learning Objective:
11.2 Wireless LAN

11.2 Wireless LAN (IEEE 802.11)

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

11.2.1 Architecture

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).

The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.

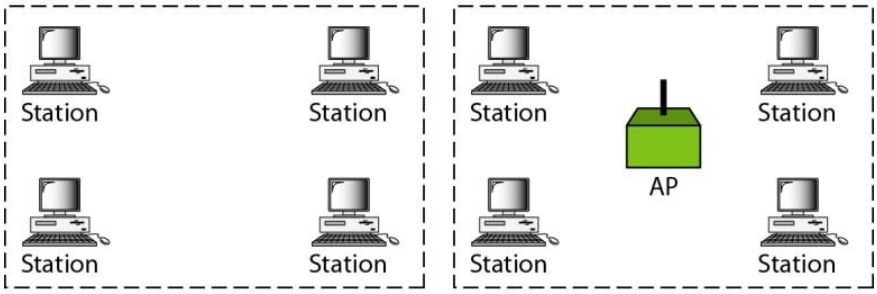


Figure: 11.1 BSS without AP and BSS with AP

Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is usually a wired LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. The extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. Thestationary stations are AP stations that are part of a wired LAN. Figure 11.2 shows an ESS.

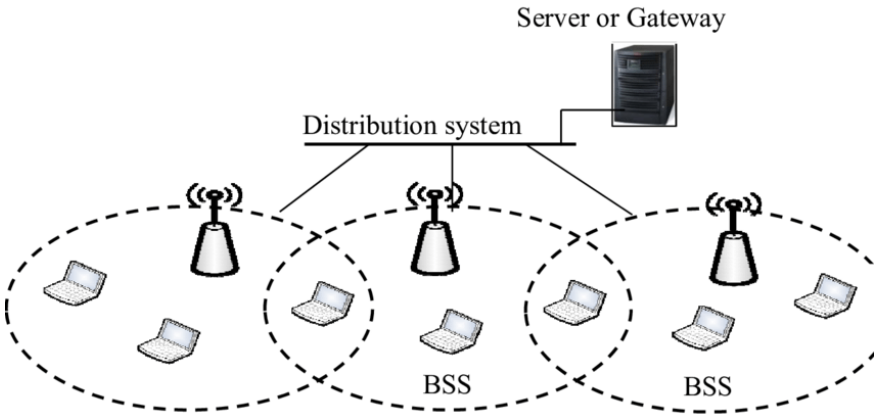


Figure: 11.2 Extended Service Set

11.2.2 MAC Sublayer

IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF).

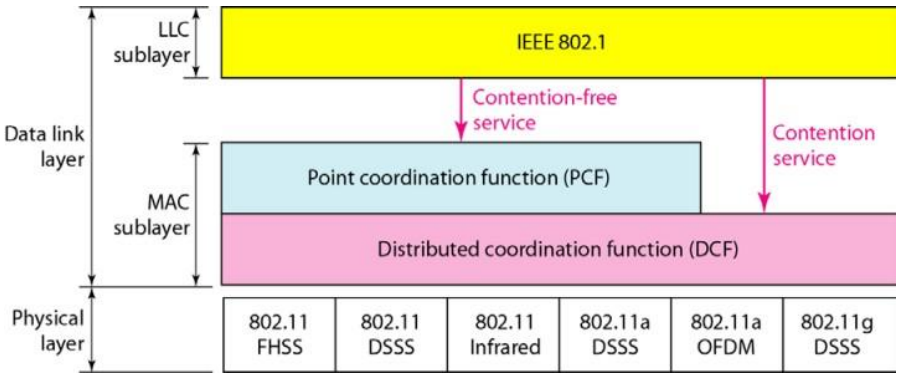


Figure: 11.3 MAC Sublayer

11.2.2.1 Distributed Coordination Function

It must be included in any station for Ad-hoc capability.

•A basic "contention" medium access method based on the CSMA/CA.

•Why not CSMA/CD? Because of the following reasons:

1. For collision detection a station must be able to send data and receive collision signals at the same time. This can mean costly stations and increased bandwidth requirements.

2. Collision may not be detected because of the hidden station problem.

3. The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

Process Flowchart & Frame Exchange Time Line

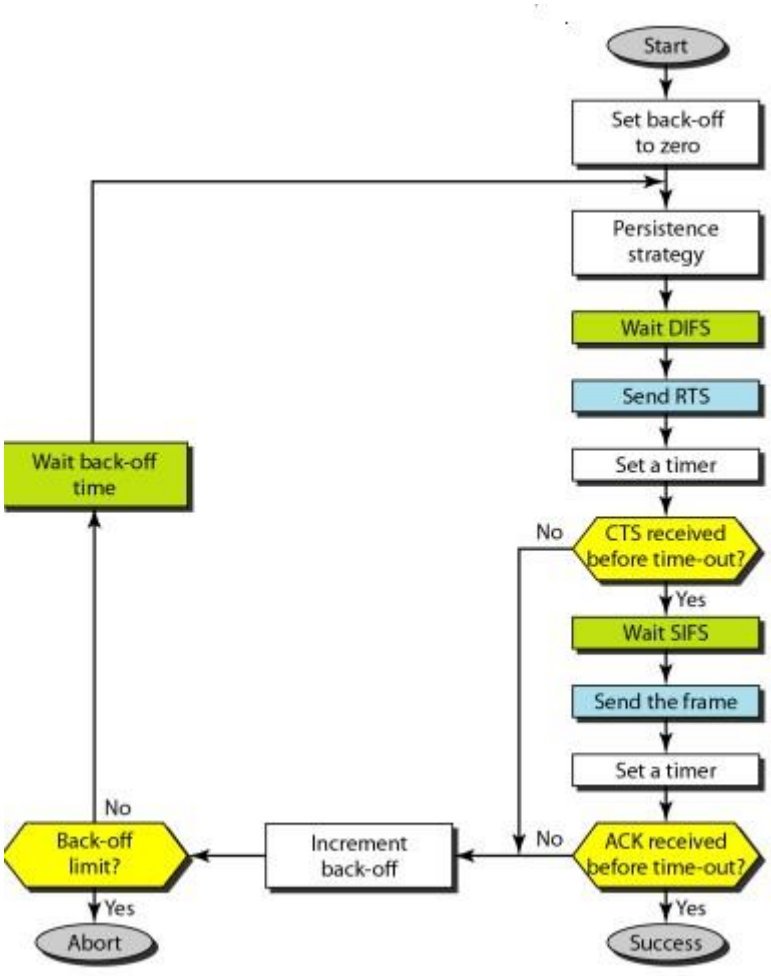


Figure: 11.4 IEEE802.11 CSMA/CA protocol (CSMA + MACA-virtual sense) Process Flowchart

- Only when the channel is idle, applying persistence strategy, the station waits for a period of Distributed Inter-Frame Space (DIFS), then sends a "Request To Send" (RTS) control frame.
- After the receiver gets the RTS, it waits for Short Inter-Frame Space (SIFS) then sends a "Clear To Send" (CTS) control frame, indicating readiness to receive data, back to the sender.

- The sender after getting the CTS, waits for SIFS period before sending data.
- The receiver, after getting the data, waits for ISFS, then send the data ACK.

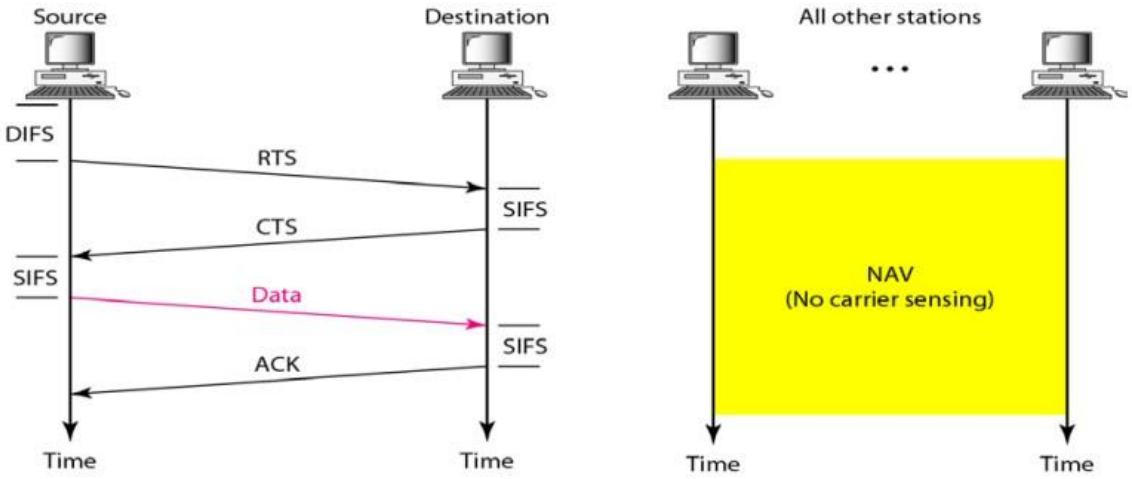


Figure: 11.5 Exchange of data and control frames in time.

When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a **network allocation vector (NAV)** that shows how much time must pass before these stations are allowed to check the channel for idleness. Each time a station accesses the system and sends an RTS frame, other stations start their NAV. In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired.

Collision During Handshaking

Two or more stations may try to send RTS frames at the same time. These control frames may collide. However, because there is no mechanism for collision detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver. The back-off strategy is employed, and the sender tries again.

11.2.2.2 Point Coordination Function (PCF)

It is implemented on top of the DCF and is used mostly for time-sensitive transmission. PCF has a centralized, contention-free polling access method. The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium. To prevent this, a repetition interval has been designed to cover both contention-free (PCF) and contention-based (DCF) traffic. The repetition interval, which is repeated continuously, starts with a special control frame, called a beacon frame. When the stations hear the beacon frame, they start their NAV for the duration of the Contention-free period of the repetition interval.

Fragmentation:

It is more efficient in such wireless noisy medium NOT to transmit large frames; hence divide each frame into smaller frames (fragments).

11.2.3 Frame Format

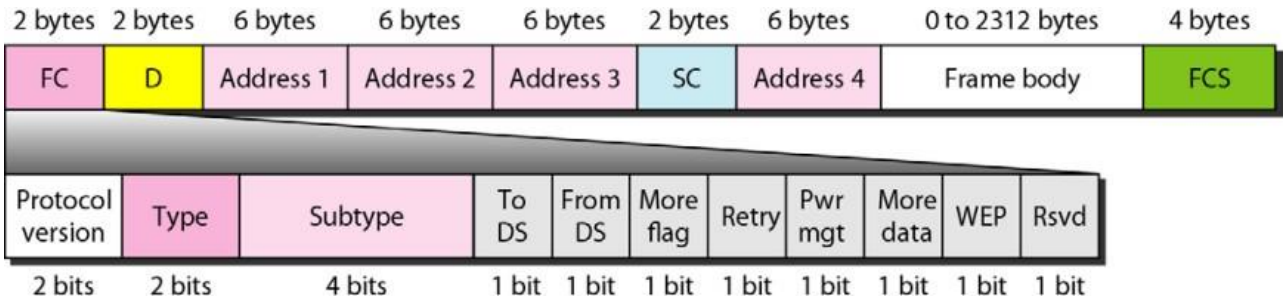


Figure: 11.6 Frame format of IEEE 802.11

Module-II

Chapter-11
Lecture-31

Learning Objective:
11.3 Bluetooth

11.3 Bluetooth

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet.

Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. Blaatand translates to Bluetooth in English.
Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

11.3.1 Architecture

Bluetooth defines two types of networks: piconet and scatternet.

11.3.1.1 Piconets

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; and the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary. A piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many.

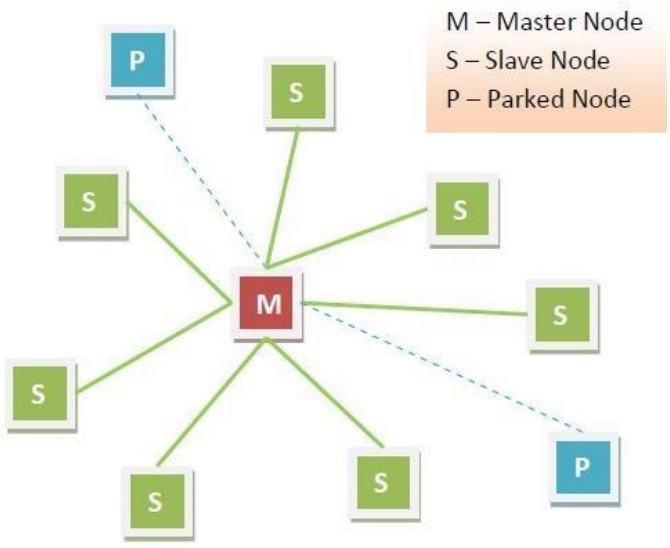


Figure: 11.7 Piconet

11.3.1.2 Scatternet

Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.

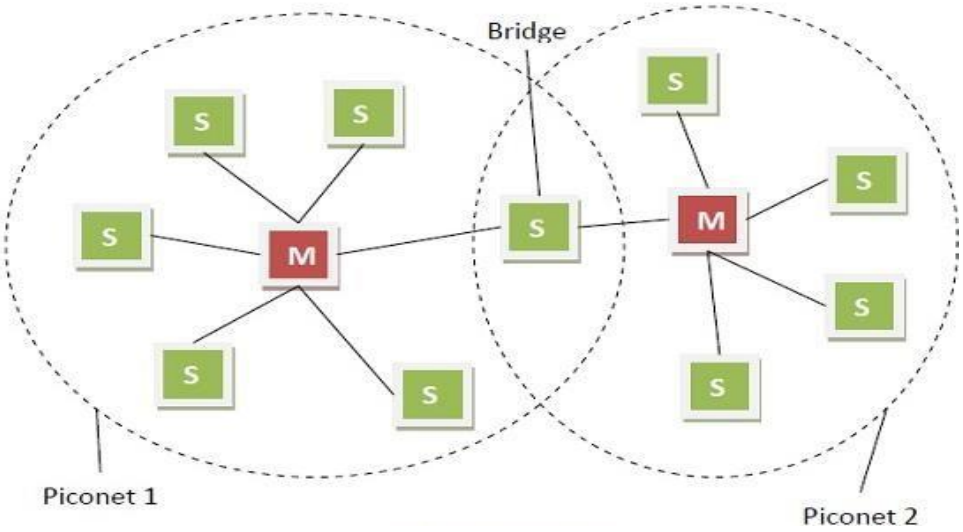


Figure: 11.8 Scatternet

11.3.2 Bluetooth Devices

A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs.

11.3.3 Bluetooth Layers

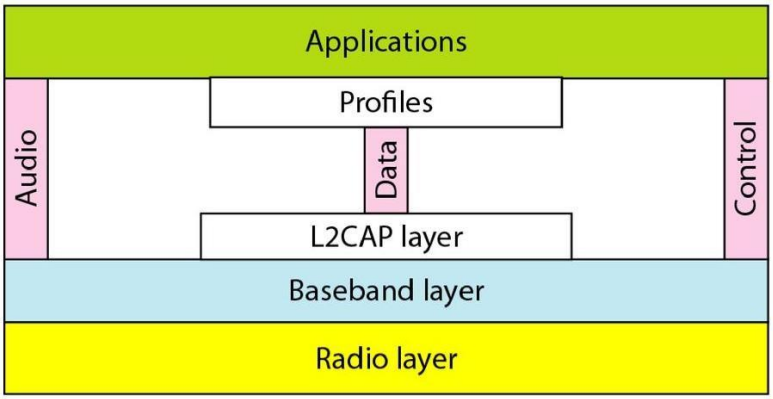


Figure: 11.9 Bluetooth layers

Radio Layer

- The radio layer is roughly equivalent to the physical layer ofthe Internet model. Bluetooth devices are low-power and have a range of 10 m.
- Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.
- Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks.
- Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering).

Baseband Layer

- The baseband layer is roughly equivalent to the MAC sublayer in LANs.
- Bluetooth uses a form of TDMA that is called TDD-TDMA (time• division duplex TDMA).

L2CAP

- The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs.
- It is used for data exchange on an ACL link; SCQ channels do not use L2CAP.
- The L2CAP has specific duties: multiplexing, segmentation and reassembly, quality of service (QoS), and group management.

Short Questions

1. What is Ethernet? What are different types of Ethernet Network?

Ethernet is the traditional technology for connecting devices in a wired local area network (LAN) or wide area network (WAN). It enables devices to communicate with each other via a protocol, which is a set of rules or common network language.

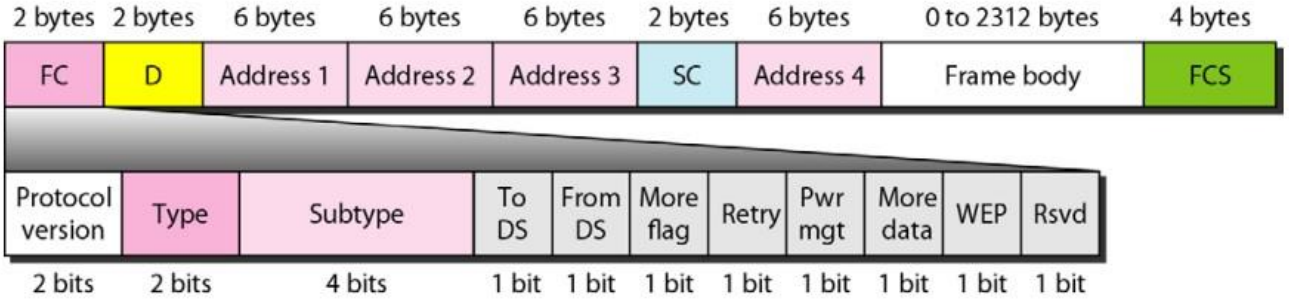
Types:

Name	IEEE Standard	Data Rate
Ethernet	802.3	10 Mbps
Fast Ethernet/ 100Base-T	802.3u	100 Mbps
Gigabit Ethernet/ GigE	802.3z	1000 Mbps
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps

2. What is network allocation vector (NAV)?

When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a **network allocation vector (NAV).**

3. Draw the frame format of Wireless LAN.



4. What is Ad-hoc Network/

The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture.

5. What is Bluetooth?

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on.

6. What is piconet?

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; and the rest are called secondaries.

Long Questions

1. Write short notes on:
    a. Wireless LAN
    b. Bluetooth