# **1. Data communication [1 Hr]**

## **1.1 Introduction**

Data communications refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.

## **1.2 Data communication model**

The purpose of the communication system is the exchange of data between two parties.



**The key elements of the model are as follows:**

* **Source** - It generates the data to be transmitted.
* **Transmitter** - The data generated by the source system are not transmitted directly in the form in which they were generated. Rather, a transmitter transforms and encodes the information in such a way as to produce electromagnetic signals that can be transmitted across some sort of the transmission system.
* **Transmission system** - This can be a single transmission line or a complex network connecting source and destination.
* **Receiver** - The receiver accepts the signal from the transmission system and converts it into a form that can be handled by the destination device.
* **Destination** - Takes the incoming data from the receiver.



**Communication Tasks:**

| Transmission system utilization | It refers to the need to make efficient use of transmission facilities that are typically shared among a number of users.  Various techniques such as multiplexing can be used to allocate the total capacity of transmission medium among a number of users  Congestion control may be required to ensure that the system runs smoothly and not be overwhelmed by excessive demand for transmission services. |
| --- | --- |
| Interfacing | It refers to the communication between transmission devices. |
| Signal generation | It refers to the generation of signal such that it meets the following requirement   1. Capable of being transferred through the transmission system. 2. Interpretable as data at the receiver. |
| Synchronization | It refers to a sync between transmitter and receiver such that the receiver will know when a signal has begun to arrive and when it ends. |
| Exchange management | It refers to the exchange of data in both directions. For it to happen both parties must cooperate with each other. |
| Error detection and correction | It refers to finding the distortion in the signal and fixing it. |
| Flow control | It refers to the requirement to assure that the source does not overwhelm the destination by sending data faster than they can be processed and absorbed. |
| Addressing | It refers to the identity of the intended destination. |
| Routing | It refers to the specific path through which data can be transmitted to the destination. (network path/route) |
| Recovery | It refers to a condition at which the database transaction or file transfer is interrupted due to a fault somewhere in the system.  Main objective is to either resume activity at the point of interruption or at least to restore the state of the systems involved to the condition prior to the beginning of the exchange. |
| Message formatting | It refers to the agreement between two parties to the form of data to be exchanged or transmitted. |
| Security | It refers to the security and privacy of the data in which only the intended receiver is allowed to see the content. |
| Network management | It refers to the capabilities needed to configure the system, monitor its status, react to failures and overloads, and p  lan intelligently for future growth |

## **1.3 Standards related to data communication**

## 

**Network standards**

Networking standards define the rules for data communications that are needed for interoperability of networking technologies and processes. Standards help in creating and maintaining open markets and allow different vendors to compete on the basis of the quality of their products while being compatible with existing market products.

During data communication, a number of standards may be used simultaneously at the different layers. The commonly used standards at each layer are −

* **Application layer −** HTTP, HTML, POP, H.323, IMAP
* **Transport layer −** TCP, SPX
* **Network layer −**IP, IPX
* **Data link layer −** Ethernet IEEE 802.3, X.25, Frame Relay
* **Physical layer −**RS-232C (cable), V.92 (modem)

**Types of standards**

* **De facto** − These are the standards that are followed without any formal plan or approval by any organization. They have come into existence due to traditions or facts. For example, the HTTP had started as a de facto standard.
* **De jure** − These standards are the ones which have been adopted through legislation by any officially recognized standards organization. Most of the communication standards that are used today are de jure standards.

**Standards organizations**

Some of the noted standards organizations are

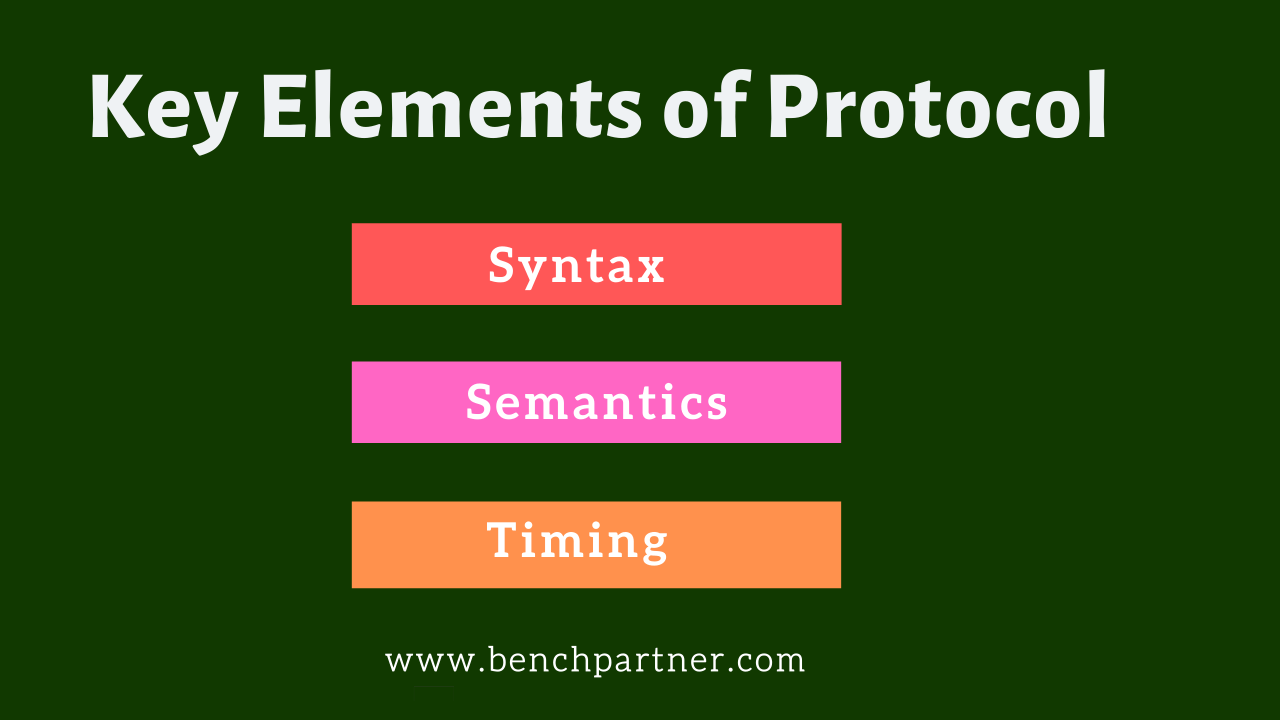
* International Standards Organization (ISO)
* International Telecommunication Union (ITU)
* Institute of Electronics and Electrical Engineers (IEEE)
* American National Standards Institute (ANSI)
* Internet Research Task Force (IETF)
* Electronic Industries Association (EIA)

## **1.4 Key element of protocol**

**Proctol -** A protocol is a set of rules that govern data communications. It defines what is communicated, how it is communicated, and when it is communicated.

**Key Elements of Protocol are as follows:**

* **Syntax**
* **Semantics**
* **Timing**



### 

### **1. Syntax**

The term syntax refers to the structure or format of the data, meaning the order in which they are presented.

For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

### **2. Semantics**

The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?

For example, does an address identify the route to be taken or the final destination of the message?

### **3. Timing**

The term timing refers to two characteristics: when data should be sent and how fast they can be sent.

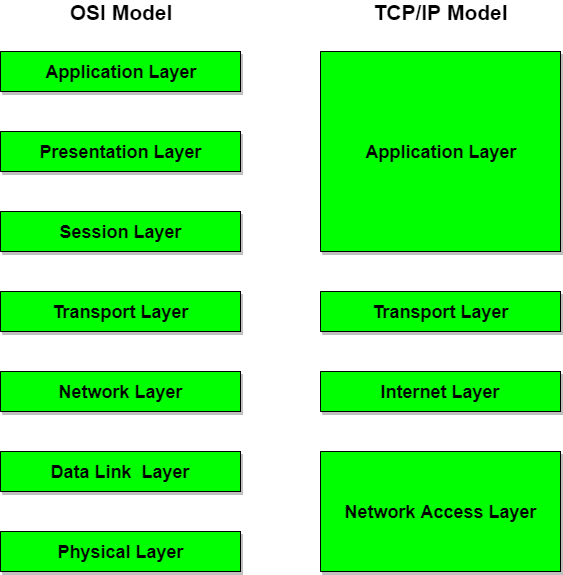
For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

**Types of protocols:**

| Transmission Control Protocol (TCP) | It divides any message into a series of packets that are sent from source to destination and there it gets reassembled at the destination. |
| --- | --- |
| Internet Protocol (IP) | IP is designed explicitly as addressing protocol.  The IP addresses in packets help in routing them through different nodes in a network until it reaches the destination system. |
| Simple mail transport Protocol (SMTP) | SMTP is designed to send and distribute outgoing email. |
| File Transfer Protocol (FTP) | FTP allows users to transfer files from one machine to another.  Types of files may include program files, multimedia files, text files, and documents, etc. |
| HyperText Transfer Protocol (HTTP) | HTTP is designed for transferring a hypertext among two or more systems.  HTTP is designed on Client-server principles which allow a client system for establishing a connection with the server machine for making a request. |
| HyperText Transfer Protocol Secure (HTTPS) | HTTPS is abbreviated as HyperText Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from web server. |
| Telnet | Telnet is a set of rules designed for connecting one system with another. The connecting process here is termed as remote login. The system which requests for connection is the local computer, and the system which accepts the connection is the remote computer. |
| Gopher | Gopher is a collection of rules implemented for searching, retrieving as well as displaying documents from isolated sites. |
| Post office Protocol (POP) | POP3 is designed for receiving incoming emails. |
| User Datagram Protocol (UDP) | primarily for creating loss-tolerating and low-latency linking between different applications. |

## **1.5 TCP/IP protocol architecture**

The TCP/IP reference model is based on a suite of protocols in which each protocol solves a particular network communications problem. The TCP/IP model can be used in a heterogeneous environment that has equipment from many different vendors.There are four layers on the TCP/IP reference model.



**Layer 1: Network Layer**

The network access layer is responsible for exchanging data between a host and the network and for delivering data between two devices on the same network. Node physical addresses are used to accomplish delivery on the local network. Functions performed at this level include encapsulation of IP datagrams(i.e. the packet format defined by Internet Protocol.) into the frames transmitted by the network, and the mapping of IP addresses into the physical addresses used by the network. The TCP/IP Network Access Layer can encompass the function of all three lower layers of the OSI reference model (Network Layer, Data Link Layer, and Physical Layer.)

**Layer 2 : Internet Layer**

The internet layer is responsible for sending source packets from any network on the internetwork and have them arrive at their destination regardless of the path they took. The Internet Protocol (IP) is used in this layer and it provides the packet delivery service on which the TCP/IP is based. The IP protocol implements a system of logical host addresses called IP addresses. The IP addresses are used by the internet and higher layers to identify devices and to perform internetwork routing.

**Layer 3: Transport Layer**

The transport layer is responsible for the reliability, flow control, and error correction of data being sent across the network.Its main protocol is called the transmission control protocol (TCP). TCP provides reliable data delivery service with end-to-end error detection and correction.User Datagram Protocol (UDP) is another protocol used which provides slow-overhead, connectionless datagram delivery service.UDP is unreliable but enhances network throughput when error correction is not required at the host-to-host-layer. Both protocols deliver data between the Application Layer and the Internet Layer. The users may choose either best suited to their means.

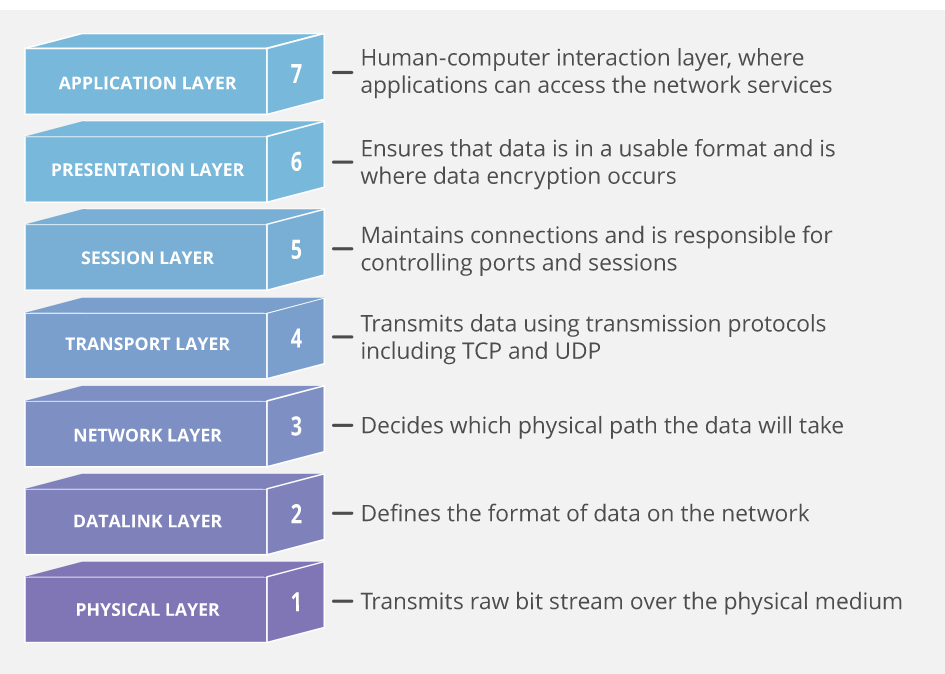
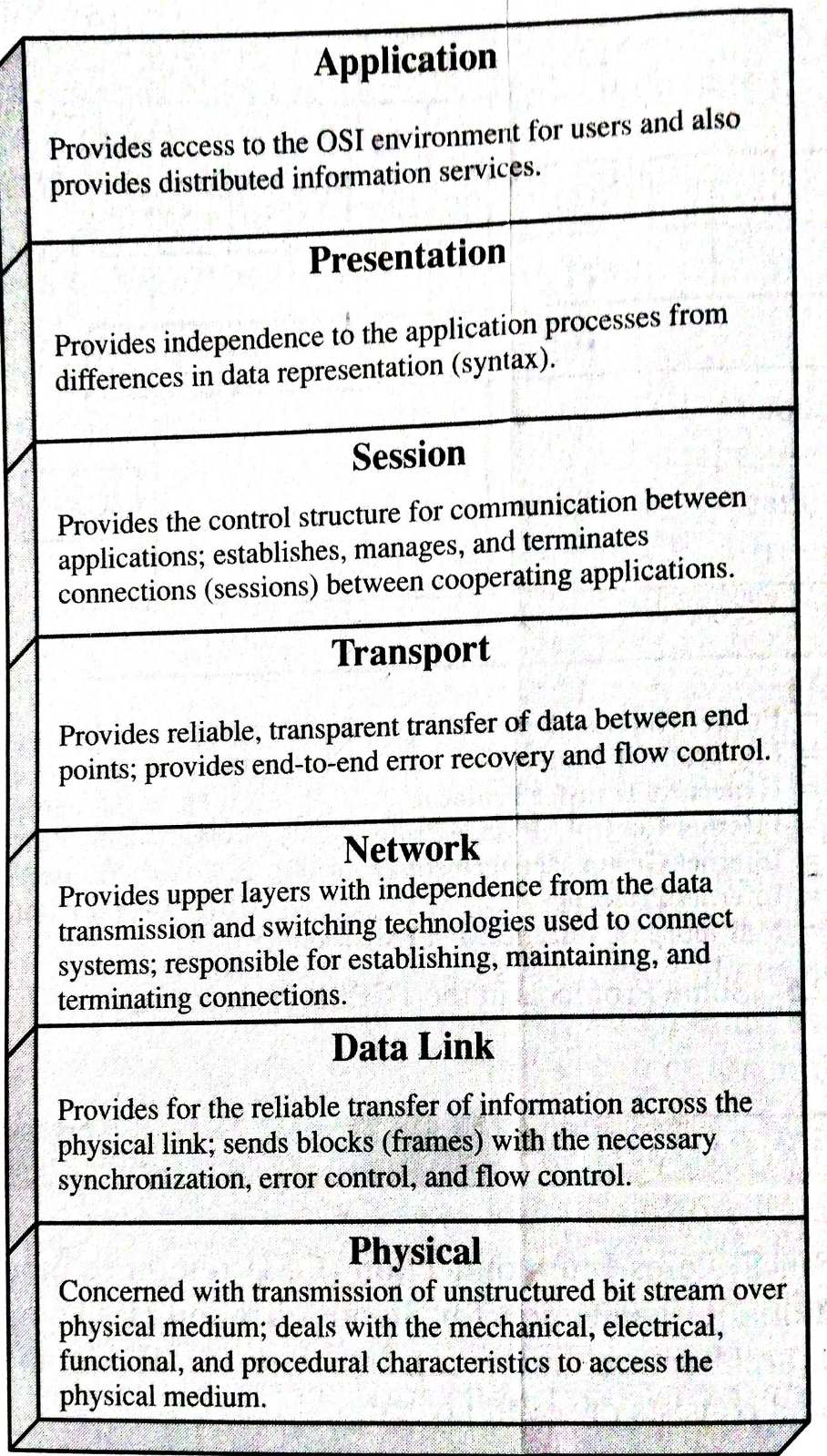
**Layer 4 : Application Layer**

The application layer is responsible for handling high-level protocols, issues of representation, encoding and dialog control. This layer is broadly equivalent to the application, presentation and session layers of the OSI model. It gives an application access to the communication environment. Examples of protocols found at this layer are Telnet, FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), HTTP (HyperText Transfer Protocol) and SMTP (Simple Mail Transfer Protocol).

## **1.6 OSI model**

In the OSI reference model, there are seven numbered layers. The purpose off each of the

seven layers in the model is to carry out part of the communication process in a well-defined way. This is achieved in a hierarchical fashion; i.e. the higher layers request the services of the lower layers to carry out their functions. Data travels across the network and is passed from layer to layer until the lowest layer is reached. Actual physical communication takes place at the lowest layer and is passed up through the layers to the highest layer and from there to the user.



**Layer 1: Physical Layer**

The physical layer is mainly concerned with the transmission of data over a communications link, i.e. a telephone cable or LAN cable. The function of the Physical Layer is to provide ''mechanical, electrical, functional, and procedural means to activate a physical connection for bit transmission'' (ISO/IEC 7498: 1984). Basically, this means that the typical role of the physical layer is to Transform bits in a computer system into electromagnetic (or equivalent) signals for a particular transmission medium (wire, fiber, ether, etc.). Repeaters operate at this level.

**Layer 2 : The Data Link Layer**

This layer attempts to make the physical layer reliable for the transmission of data. It provides synchronization and error Detection control, which allows the upper layers to assume error-free transmission over the link. Data received from the Network Layer is formatted into frames and sent to the Physical Layer for transmission. Bridges and switches operate at this level and use the machine's MAC address to filter traffic.

**Layer 3 : The Network Layer**

The network layer relieves the higher layers of the routing, switching and signaling functions required to establish the necessary physical network links .It accepts data from layer 4 and selects the best route to transfer it between end systems. The computer communicates with the network at this layer to specify the destination address and to request network facilities such as priority. The IP protocol is used at this level for packet forwarding routing. Routers are used at this level. They use packet addresses to choose the optimum route across the network.

**Layer 4 : The Transport Layer**

The transport layer ensures reliable, cost effective, end to end transfer of data. Like the data link layer, the transport layer has error control functions. Whereas the data link layer was concerned with the traffic across physical links, the transport layer is concerned with traffic between the layers. This layer provides a data transfer service, which shields the upper layers from any concern with the detailed way in which data is transferred.

**Layer 5 : The Session Layer**

The Session Layer permits two parties to hold ongoing communications called a session across a network. It provides dialogue control, which is the setting up and monitoring of connections. If the lower four layers of the model are unreliable, the session layer will attempt to correct the faults and maintain the connection with the higher layers becoming aware of any problem. Thus the applications on either end of the session can exchange data or send packets to another for as long as the session lasts. The Session layer handles session setup, data or message exchanges, and teardown when the session ends. It also monitors session identification so only designated parties can participate and security services to control access to session information.

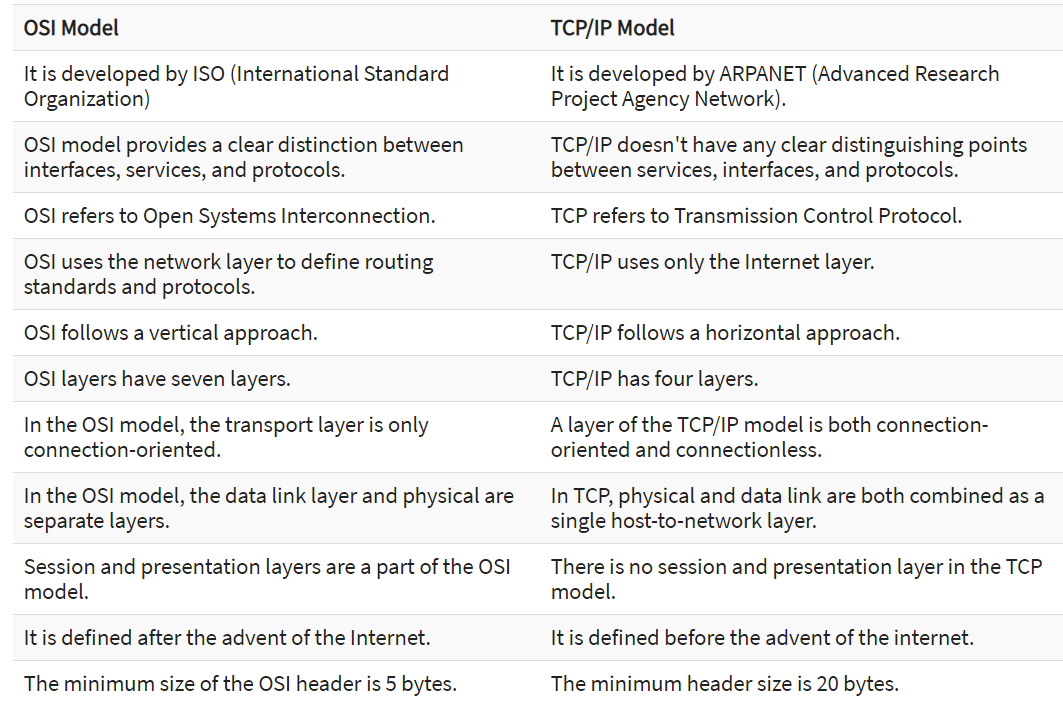
**Layer 6 : The Presentation Layer**

The presentation layer defines the format and representation of the data exchanged between users. Video displays and printers may use different data formats. Without this layering these different formats would require individual treatment. Data Encryption and compression, and Code and format conversions are some of the facilities offered by this layer. For outgoing messages, it converts data into a generic format that can survive the rigors of network transmission; for incoming messages, it converts data from its generic networked representation into a format that will make sense to the receiving application.

**Layer 7 : The Application Layer**

The Application Layer is the top layer of the reference model. It provides a set of interfaces

to allow equipment and application programs to exchange information in the OSI environment. It is the source of all data to be transferred including services such as networked file transfer, message handling, and database query processing. Gateways work at this level.



**Advantages of the OSI Model**

Here are the major benefits/pros of using the OSI model:

* It helps you to standardize router, switch, motherboard, and other hardware
* Reduces complexity and standardizes interfaces
* Facilitates modular engineering
* Helps you to ensure interoperable technology
* Helps you to accelerate the evolution
* Protocols can be replaced by new protocols when technology changes.
* Provide support for connection-oriented services as well as connectionless service.
* It is a standard model in computer networking.
* Supports connectionless and connection-oriented services.
* It offers flexibility to adapt to various types of protocols.

**Advantages of TCP/IP**

Here, are pros/benefits of using the TCP/IP model:

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

**Disadvantages of OSI Model**

Here are some cons/ drawbacks of using OSI Model:

* Fitting of protocols is a tedious task.
* You can only use it as a reference model.
* It doesn't define any specific protocol.
* In the OSI network layer model, some services are duplicated in many layers such as the transport and data link layers
* Layers can't work in parallel as each layer needs to wait to obtain data from the previous layer.

**Disadvantages of TCP/IP**

Here, are few drawbacks of using the TCP/IP model:

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

# **2. Data transmission [2 Hrs]**

## **2.1 Concept and terminology**

Data transmission occurs between transmitter and receiver over some transmission medium. Transmission medium may be classified as guided and unguided medium. In both cases, communication is in the form of electromagnetic waves.

The term direct link is used to refer to the transmission path between two devices in which signals propagate directly from transmitter to receiver with no intermediate devices, other than amplifier or repeater to increase the signal strength. Note: the term can be applied to both guided and unguided media.

A transmission may be simplex, half duplex or full duplex, in simplex transmission, signals are transmitted only one direction; one station is transmission and other is receiver. In half-duplex both stations can transmit but only one at a time. In full duplex operation, both stations can transmit simultaneously .

## **2.2 Analog and digital transmission**

## 

An **Analog signal** is any continuous signal for which the time varying feature (variable) of the signal is a representation of some other time varying quantity, i.e., analogous to another time varying signal. It differs from a digital signal in terms of small fluctuations in the signal which are meaningful.

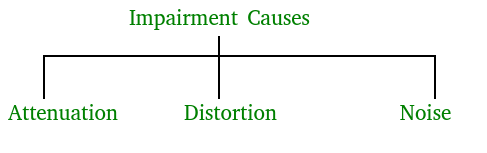
A **digital signal** uses discrete (discontinuous) values. By contrast, non-digital (or analog) systems use a continuous range of values to represent information. Although digital representations are discrete, the information represented can be either discrete, such as numbers or letters, or continuous, such as sounds, images, and other measurements of continuous systems.

|  | **Analog** | **Digital** |
| --- | --- | --- |
| **Signal** | Analog signal is a continuous signal which represents physical measurements. | Digital signals are discrete time signals generated by digital modulation. |
| **Waves** | Denoted by sine waves | Denoted by square waves |
| **Representation** | Uses continuous range of values to represent information | Uses discrete or discontinuous values to represent information |
| **Example** | Human voice in air, analog electronic devices. | Computers, CDs, DVDs, and other digital electronic devices. |
| **Technology** | Analog technology records waveforms as they are. | Samples analog waveforms into a limited set of numbers and records them. |
| **Data transmissions** | Subjected to deterioration by noise during transmission and write/read cycle. | Can be noise-immune without deterioration during transmission and write/read cycle. |
| **Response to Noise** | More likely to get affected reducing accuracy | Less affected since noise response are analog in nature |
| **Flexibility** | Analog hardware is not flexible. | Digital hardware is flexible in implementation. |
| **Uses** | Can be used in analog devices only. Best suited for audio and video transmission. | Best suited for Computing and digital electronics. |
| **Applications** | Thermometer | PCs, PDAs |
| **Bandwidth** | Analog signal processing can be done in real time and consumes less bandwidth. | There is no guarantee that digital signal processing can be done in real time and consumes more bandwidth to carry out the same information. |
| **Memory** | Stored in the form of wave signal | Stored in the form of binary bit |
| **Power** | Analog instrument draws large power | Digital instrument drawS only negligible power |
| **Cost** | Low cost and portable | Cost is high and not easily portable |
| **Impedance** | Low | High order of 100 megaohm |
| **Errors** | Analog instruments usually have a scale which is cramped at the lower end and give considerable observational errors. | Digital instruments are free from observational errors like parallax and approximation errors. |

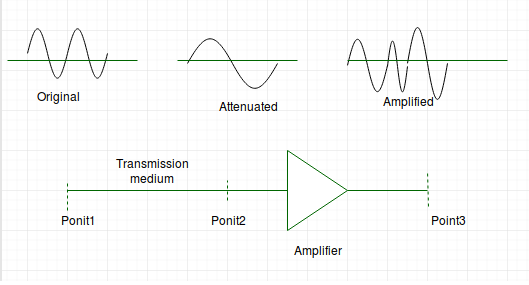
## **2.3 Transmission impairment**

In the communication system, analog signals travel through transmission media, which tends to deteriorate the quality of analog signal. This imperfection causes signal impairment. This means that the received signal is not the same as the signal that was sent.

**Causes of impairment**



**Attenuation –** It means loss of energy. The strength of the signal decreases with increasing distance which causes loss of energy in overcoming resistance of the medium. This is also known as attenuated signal. Amplifiers are used to amplify the attenuated signal which gives the original signal back.



Attenuation is measured in **decibels(dB)**. It measures the relative strengths of two signals or one signal at two different points.

Attenuation(dB) = 10log10(P2/P1)

P1 is power at sending end and P2 is power at receiving end.

* **Distortion –** It means change in the shape of a signal. This is generally seen in composite signals with different frequencies. Each frequency component has its own propagation speed travelling through a medium. Every component arrives at a different time which leads to delay distortion. Therefore, they have different phases at the receiver end from what they had at the senders end.
* **Noise –** The random or unwanted signal that mixes up with the original signal is called noise. There are several types of noise such as induced noise, crosstalk noise, thermal noise and impulse noise which may corrupt the signal.  
  **Induced** noise comes from sources such as motors and appliances. These devices act as sending antenna and transmission medium act as receiving antenna. **Thermal** noise is movement of electrons in wire which creates an extra signal. **Crosstalk** noise is when one wire affects the other wire. **Impulse** noise is a signal with high energy that comes from lightning or power lines  
   SNR = AVERAGE SIGNAL POWER / AVERAGE NOISE POWER

## **2.4 Wireless propagation**

Antenna and Wave propagation plays a vital role in wireless communication networks. An antenna is an electrical conductor or a system of conductors that radiates/collects (transmits or receives) electromagnetic energy into/from space. An idealized isotropic antenna radiates equally in all directions.

Propagation Mechanisms

Wireless transmissions propagate in three modes. They are −

* + Ground-wave propagation
  + Sky-wave propagation
  + Line-of-sight propagation

**Ground wave propagation** follows the contour of the earth, while **sky wave propagation** uses reflection by both earth and ionosphere.

**Line of sight propagation** requires the transmitting and receiving antennas to be within the line of sight of each other. Depending upon the frequency of the underlying signal, the particular mode of propagation is followed.

Examples of ground wave and sky wave communication are AM radio and international broadcasts such as BBC. Above 30 MHz, neither ground wave nor sky wave propagation operates and the communication is through line of sight.

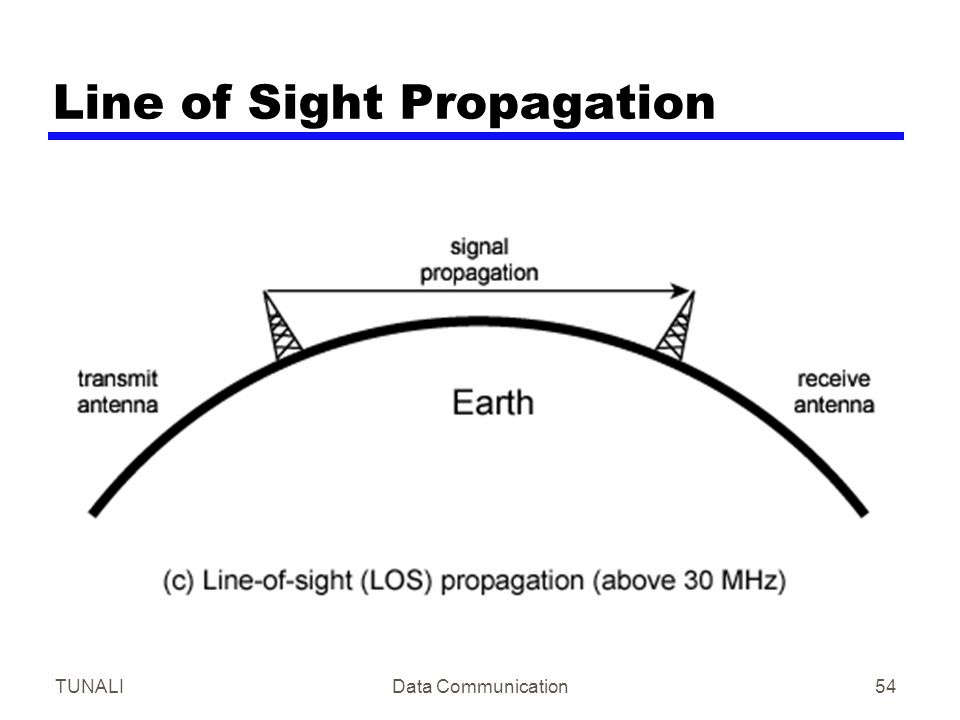
## **2.5 Line of sight transmission**

**Line of sight (LoS)** is a type of propagation that can transmit and receive data only where transmit and receive stations are in view of each other without any sort of an obstacle between them. FM radio, microwave and satellite transmission are examples of line-of-sight communication.

**Techopedia explains Line of Sight (LoS)**

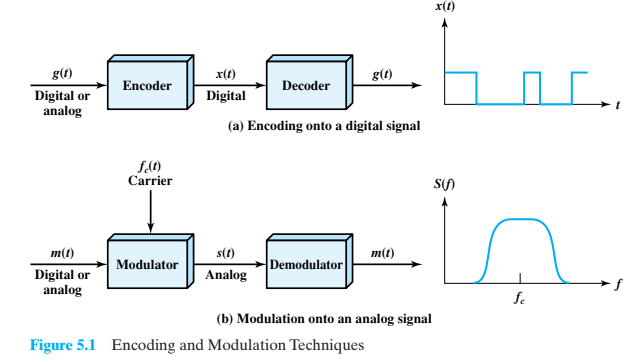
Long-distance data communication is more effective through wireless networks but geographical obstacles and the curvature of the earth bring limitations to line-of-sight transmission. However, these issues can generally be mitigated through planning, calculations and the use of additional technologies.

For example, mobile phones use a modified line-of-sight transmission, which is made possible through a combination of effects like diffraction, multipath reflection, local repeaters and rapid handoff.



# **3. Signal encoding techniques [4 Hrs]**

Modulation - It is the process of encoding source data onto a carrier signal with frequency fc



The input signal m(t) may be analog or digital and is called the modulating signal or baseband signal.The result of modulating the carrier signal is called the modulated signal s(t).

## **3.1 Digital data, digital signal**

The simplest form of digital encoding of digital data is to assign one voltage level to binary one and another to binary zero. More complex encoding schemes are used to improve performance, by altering the spectrum of the signal and providing synchronization capability.

## **3.2 Digital data, analog signal**

A modem converts digital data to an analog signal so that it can be transmitted over an analog line. The basic techniques are amplitude shift keying (ASK), frequency shift keying (FSK), and phase shift keying (PSK). All involve altering one or more characteristics of a carrier frequency to represent binary data.

## **3.3 Analog data, digital signal**

Analog data, such as voice and video, are often digitized to be able to use digital transmission facilities. The simplest technique is pulse code modulation(PCM), which involves sampling the analog data periodically and quantizing the samples.

## **3.4 Analog data, analog signal**

Analog data are modulated by a carrier frequency to produce an analog signal in a different frequency band, which can be utilized on an analog transmission system. The basic techniques are amplitude modulation(Am), frequency modulation (FM), and phase modulation(PM).

# **4. Digital data communication techniques [3 Hrs]**

For two devices linked by a transmission medium to exchange data, a high degree of cooperation is required. Typically, data is transmitted one bit at a time over the medium. The timing (rate, duration, spacing) of these bits must be the same for transmitter and receiver. In order for the receiver to sample the incoming bits properly, it must know the arrival time and duration of each bit that it receives. If the receiver times its samples based on its own clock, then there will be a problem if the transmitter and receiver clocks are not precisely aligned. And in practice the sender and receiver are not perfectly aligned and the timing synchronization drifts further and further as more and more data is sent.

## **4.1 Asynchronous and synchronous transmission**

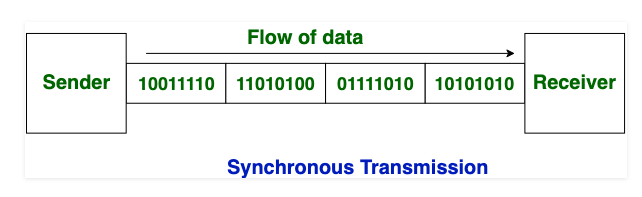
**Asynchronous transmission**

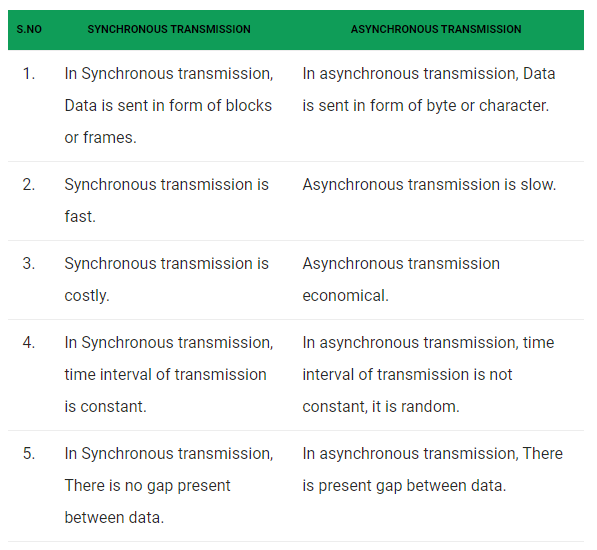
In Asynchronous Transmission, data is sent in form of byte or character. This transmission is the half duplex type transmission. In this transmission start bits and stop bits are added with data. It does not require synchronization.



**Synchronous Transmission**

In Synchronous Transmission, data is sent in the form of blocks or frames. This transmission is the full duplex type. Between sender and receiver the synchronization is compulsory. In Synchronous transmission, There is no gap present between data. It is more efficient and more reliable than asynchronous transmission to transfer the large amount of data.





## **4.2 Types of error**

These interferences can change the timing and shape of the signal. If the signal is carrying binary encoded data, such changes can alter the meaning of the data.

These errors can be divided into two types :

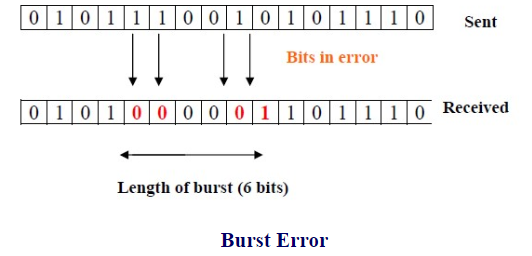
**1. Single-bit error**

The term single-bit error means that only one bit of a given data unit (such as a byte, character, or data unit) is changed from 1 to 0 or from 0 to 1. Single bit errors are the least likely type of errors in serial data transmission. However, a single-bit error can happen if we are having a parallel data transmission.



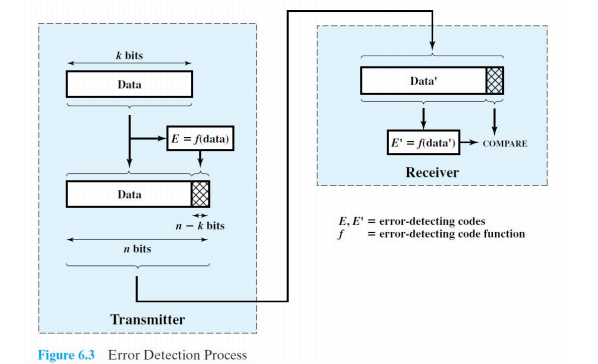
**2. Burst error.**

The term burst error means that two or more bits in the data unit have changed from 0 to 1 or vice-versa. Note that burst error doesn’t necessarily mean that error occurs in consecutive bits. The length of the burst error is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not be corrupted. Burst errors are mostly likely to happen in serial transmission.



## **4.3 Error detection and correction method**

For a given frame of bits, additional bits that constitute an error-detecting code are added by the transmitter. This code is calculated as a function of the other transmitted bits. The types of error detection are:



**Parity Check**

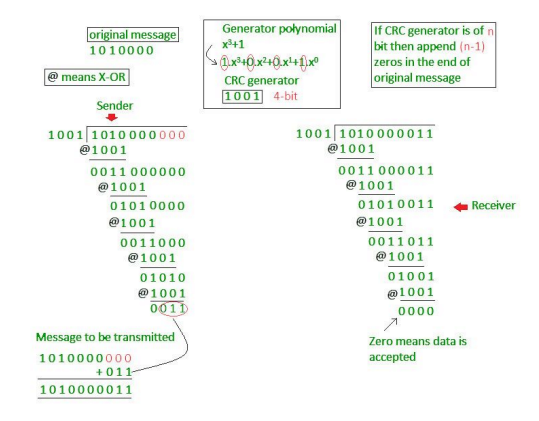
The simplest error-detecting scheme is to append a parity bit to the end of a block of data. In the Parity Check error detection scheme, a parity bit is added to the end of a block of data. The value of the bit is selected so that the character has an even number of 1s (even parity) or an odd number of 1s (odd parity). For odd parity check, the receiver examines the received character and if the total number of 1s is odd, then it assumes that no error has occurred. If any one bit (or any odd number of bits) is erroneously inverted during transmission, then the receiver will detect an error.

However,if two (or any even number) of bits are inverted due to error, an undetected error occurs. Typically, even parity is used for synchronous transmission and odd parity for asynchronous transmission. The use of the parity bit is not foolproof, as noise impulses are often long enough to destroy more than one bit, particularly at high data rates.

**Cyclic Redundancy Check (CRC)**

One of the most common, and one of the most powerful, error-detecting codes is the cyclic redundancy check (CRC).

Given a k-bit block of bits, or message, the transmitter generates a sequence, known as a frame check sequence (FCS), such that the resulting frame, consisting of n bits,n is exactly divisible by some predetermined number. The receiver then divides the incoming frame by that number and, if there is no remainder, assumes there was no error.



**Checksum**

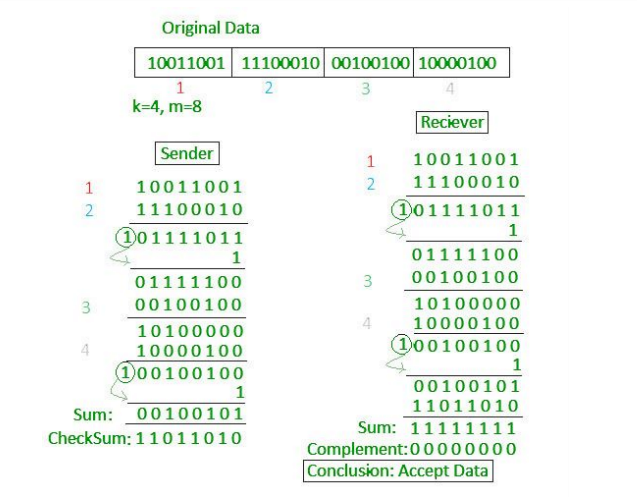
● In the checksum error detection scheme, the data is divided into k segments each of m bits.

● 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.



**Error Correction**

The techniques that we have discussed so far can detect errors, but do not correct them. Error Correction can be handled in two ways. One is when an error is discovered; the receiver can have the sender retransmit the entire data unit. This is known as **backward error correction**. In the other, the receiver can use an error-correcting code, which automatically corrects certain errors. This is known as **forward error correction**. In theory it is possible to correct any number of errors atomically. Error-correcting codes are more sophisticated than error detecting codes and require more redundant bits. The number of bits required to correct multiple-bit or burst error is so high that in most of the cases it is inefficient to do so. For this reason, most error correction is limited to one, two or at the most three-bit errors.

One of the most widely used single bit error correction codes is the hamming code.

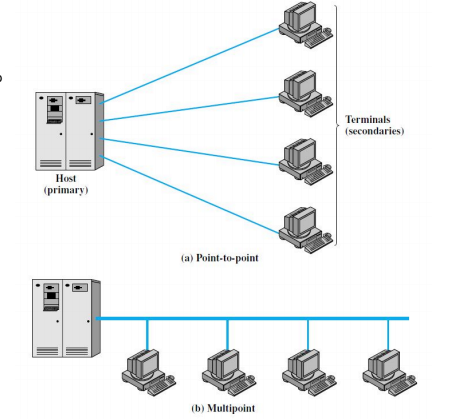
Steps:

1. Find no of parity bits(p) to use using formula

2^p >= m + p +1 Where m = no message bits.

## **4.4 Line configuration**

Two characteristics that distinguish various data link configurations are topology and whether the link is half duplex or full duplex.



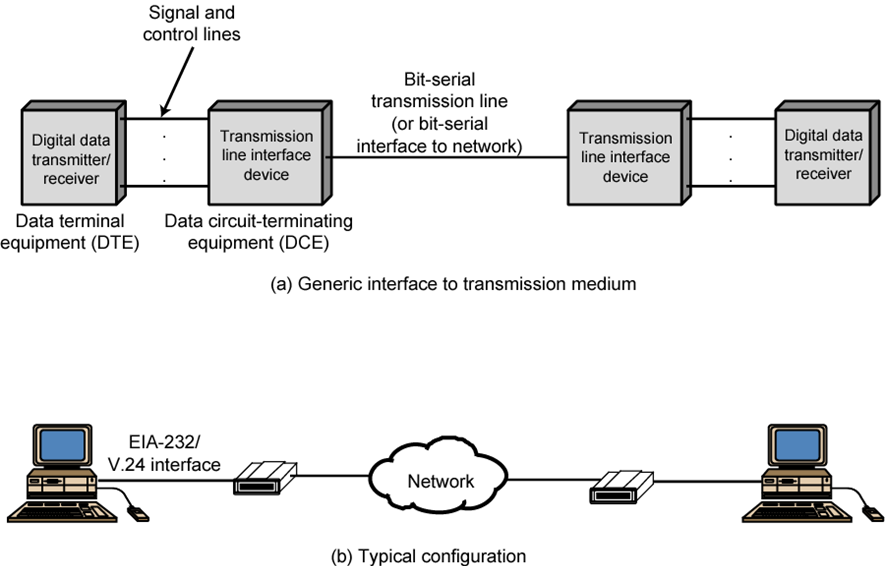
**Topology**

The topology of a data link refers to the physical arrangement of stations on a transmission medium. If there are only two stations (e.g., a terminal and a computer or two computers), the link is point to point. If there are more than two stations, then it is a multipoint topology. Traditionally, a multipoint link has been used in the case of a computer (primary station) and a set of terminals (secondary stations). In today’s environment, multipoint topology is found in local area networks. Traditional multipoint topologies are made possible when the terminals are only transmitting a fraction of the time. Figure 6.9 illustrates the advantages of the multipoint configuration. If each terminal has a point-to-point link to its computer, then the computer must have one I/O port for each terminal. Also there is a separate transmission line from the computer to each terminal. In a multipoint configuration, the computer needs only a single I/O port and a single transmission line, which saves costs.

Data exchanges over a transmission line can be classified as full duplex or half duplex.With **half-duplex transmission**, only one of two stations on a point-to-point link may transmit at a time. This mode is also referred to as two-way alternate, suggestive of the fact that two stations must alternate in transmitting or receiving. For **full-duplex transmission**, two stations can simultaneously send and receive data from each other.Thus, this mode is known as two-way simultaneous and may be compared to a two-lane, two-way bridge. For computer-to-computer data exchange, this form of transmission is more efficient than half-duplex transmission.

## **4.5 Interfacing**

Data processing devices or data terminal equipment (DTE) do not usually include data transmission facilities. So it needs an interface called data circuit terminating (DCE) like modem, NIC. DCE transmits bits on medium. DCE communicated data and control info with DTE.



# **5. Data link control [3 hrs]**

## **5.1 Flow control**

Flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from over running a slow receiver. Flow control is the management of data flow between computers or devices or between nodes in a network so that the data can be handled at an efficient pace. Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be retransmitted.

## **5.2 Error control**

Error control refers to mechanisms to detect and correct errors that occur in the transmission of frames. Two types of errors:

**Lost frame:** A frame fails to arrive at the other side. For example, a noise burst may damage a frame to the extent that the receiver is not aware that a frame has been transmitted.

**Damaged frame:** A recognizable frame does arrive, but some of the bits are in error (have been altered during transmission).

**The most common techniques for error control are:**

• **Error detection:**Error detection can be done through Parity bit, CheckSum, Cyclic Redundancy Check(CRC)

• **Positive acknowledgment:** The destination returns a positive **acknowledgment (ACK)** to successfully received, error-free frames.

• **Retransmission after timeout:**The source retransmits a frame that has not been acknowledged after a predetermined amount of time.

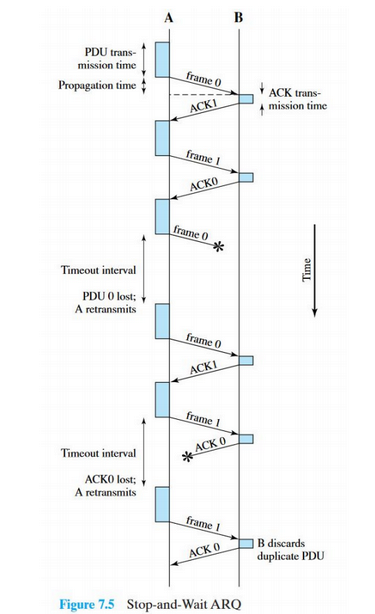
• **Negative acknowledgment and retransmission:** The destination returns a **negative acknowledgment (NACK)** to frames in which an error is detected. The source retransmits such frames.

**Collectively, these mechanisms are all referred to as automatic repeat requests (ARQ); the effect of ARQ is to turn an unreliable data link into a reliable one.**

Three versions of ARQ have been standardized:

**Stop-and-Wait ARQ**

The simplest form of flow control, known as stop-and-wait flow control, works as follows. A source entity transmits a frame. After the destination entity receives the frame, it indicates its willingness to accept another frame by sending back an acknowledgment to the frame just received. The source must wait until it receives the acknowledgment before sending the next frame. The destination can thus stop the flow of data simply by withholding acknowledgment.



**Sliding Windows Protocols**

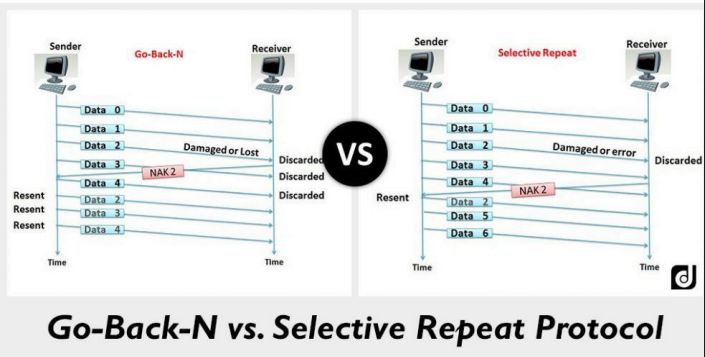
**Go back N (GBN)**

Let us take an example where the source is sending some packets to the destination as shown in figure. Here the receiver receives packet no 0 and pkt 1. But the packet no 2 is lost during transmission. The sender keeps sending other packets (packet no 3 and 4), but since the

receiver did not receive the packet no 2 it sends an NACK2 (negative ack) indicating that it didn’t receive the packet no 2. The receiver will discard packet 3 and packet 4 even though it received them just fine. The sender upon receiving the NACK2, will again start sending packet from pkt 2 as shown in figure.

**Selective Repeat (SR)**

The problem with GBN is that even though valid packets 3 and 4 were received they get discarded because the previous packet 2 was not received. The SR packet solves this by storing the received packet 3 and 4 in its buffer and sending NACK2 to request only the lost packet 2. When packet 2 is received the sender resumes sending packet from pkt 5.



## 5.3 HDLC (High-Level Data Link Control)

The most important data link control protocol is HDLC. Not only is HDLC widely used, but it is the basis for many other important data link control protocols, which use the same or similar formats and the same mechanisms as employed in HDLC.

A high-level data link control defines rules for transmitting data between network points. Data in an HDLC is organized into units called frames and is sent across networks to specified destinations. HDLC also manages the pace at which data is transmitted. HDLC is commonly used in the open systems interconnection (OSI) model's layer 2.

HDLC frames are transmitted over synchronous links or asynchronous links. This is done using a frame delimiter or flag, which contains a unique sequence of bits that are not visible inside a frame. HDLC provides both connection-oriented and connectionless service.

**There are three types of stations:**

**1. Primary station**

Sends command and accepts responses (the controlling node).

**2. Secondary station**

Accepts commands and sends responses (the controlled node).

**3. Combined station**

Sends or accepts commands and responses (this type appears in what is called balanced configurations, such as LAPB).

**The two link configurations are:**

**1. Unbalanced configuration:**

Consists of one primary and one or more secondary stations and supports both full-duplex and half-duplex transmission.

**2. Balanced configuration:**

Consists of two combined stations and supports both full-duplex and half-duplex transmission

The **three data transfer modes** are:

**1. Normal response mode (NRM):**

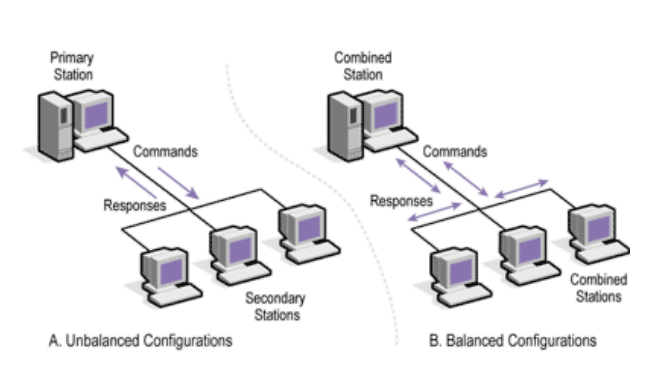
Used with an unbalanced configuration. The primary may initiate data transfer to a secondary, but a secondary may only transmit data in response to a command from the primary.

**2. Asynchronous balanced mode (ABM):**

Used with a balanced configuration.Either combined station may initiate transmission without receiving permission from the other combined station.

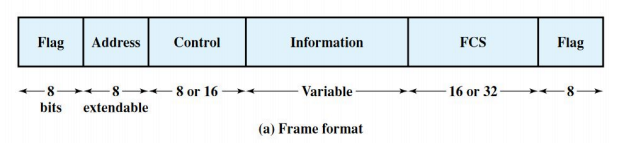
**3. Asynchronous response mode (ARM):**

Used with an unbalanced configuration. The secondary may initiate transmission without explicit permission of the primary. The primary still retains responsibility for the line, including initialization, error recovery, and logical disconnection.



**Frame Structure**

Figure 7.7 depicts the structure of the HDLC frame. The flag, address, and control fields that precede the information field are known as a header. The FCS andflag fields following the data field are referred to as a trailer.



**● Flag Fields:** Flag fields delimit the frame at both ends with the unique pattern 01111110.

**● Address Field:** The address field identifies the secondary station that transmitted or is to receive the frame.

**● Control Field:** Used to identify the type of data contained in the frame. (eg. Ack)

**● Information Field:** Contains data

**● Frame Check Sequence Field:** The frame check sequence (FCS) is an error-detecting code

# 6. Multiplexing [3 Hrs]

**Multiple Access Protocols**

Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.

Communication is possible over the air (radio frequency), using a physical media (cable) and light (optical fiber). All mediums are capable of multiplexing. When more than one sender tries to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium and identifies each and sends it to different receivers.

## **6.1 FDM, TDM, STDM, ADSL**

**Frequency Division Multiplexing (FDM)**

When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel.

Each user can use the channel frequency independently and has exclusive access to it. All channels are divided such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.

**Advantages OF FDM**

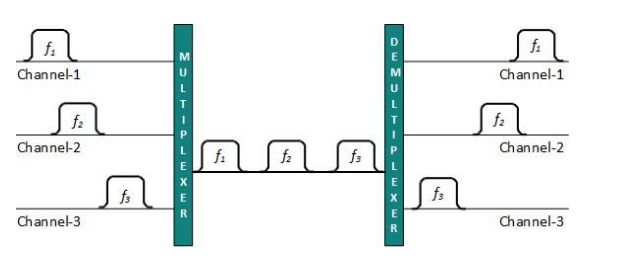
1. Simple
2. Inexpensive
3. Popular with Radio, TV, Cable TV
4. It is not sensitive to propagation delays.
5. It allows maximum transmission link usage.

**Disadvantages OF FDM**

In FDM there is a need for filters, which are very expensive and complicated to construct and design.

Analog signal only has limited frequency range.

Sometimes, it is necessary to use more complex linear amplifiers in FDM systems.

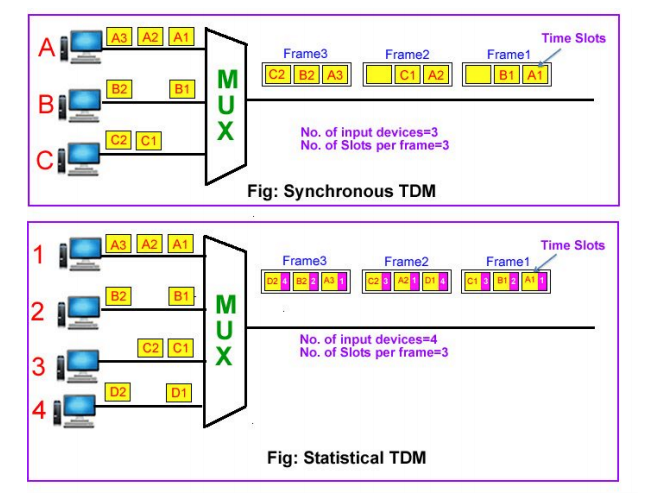


**Time Division Multiplexing**

Time-division multiplexing (TDM) is a mechanism that allows multiple logical calls or streams to share the same physical circuit, providing an equal amount of time for each conversation. Instead of sharing a portion of the bandwidth as in FDM, here in TDM time is shared. Example: telephone system

**Asynchronous/ Statistical Time Division Multiplexing (STDM)**

In SDTM, the time slots are dynamically allocated to the slots according to demand. The multiplexer checks each input stream in a round – robin manner and allocates a slot to an input line only if data is present there, otherwise, it skips to the next stream and checks it.



**Asymmetric Digital Subscriber Line (ADSL)** is a type of broadband communications technology that transmits digital data at a high bandwidth over existing phone lines to homes and businesses.

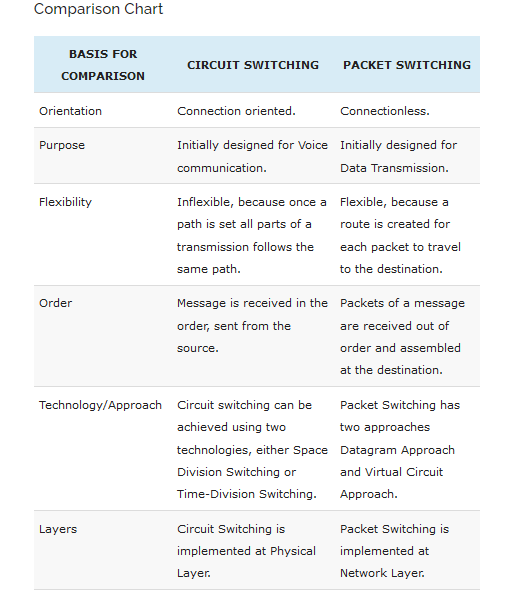
In order to access ADSL, a Digital Subscriber Line modem (DSL modem) is installed at the client side. The DSL modem sends data bits over the local loop of the telephone network. The local loop is a two – wire connection between the subscriber’s house and the end office of the telephone company. The data bits are accepted at the end office by a device called Digital Subscriber Line Access Multiplexer (DSLAM).

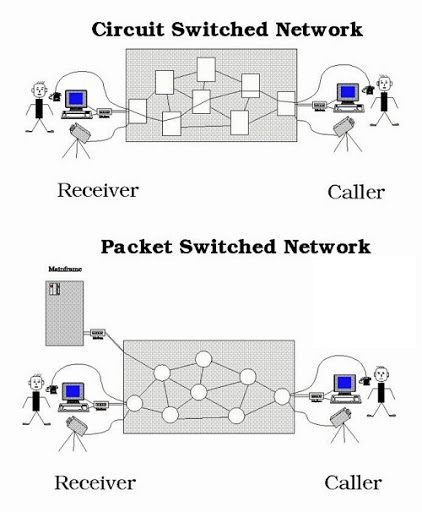
Features of ADSL

* ADSL is one among the DSL family of technologies.
* ADSL is used in the local loop of the telephone network, i.e. the part of the telephone network that connects the customer premises with the end office of the telephone company.
* The telephone company uses a Digital Subscriber Line Access Multiplexer (DSLAM) at its end office so that multiple ADSL users can be connected to the high-speed backbone network.
* Most ADSL communications are full-duplex communication. It is achieved by any of the following technologies −
  + frequency-division duplex (FDD)
  + echo-cancelling duplex (ECD)
  + time-division duplex (TDD)
* The most common technology uses FDD. Here two separate bands are used for upstream and downstream communications.
* ADSL uses frequency bands 26.075 kHz to 137.825 kHz for upstream communication and 138–1104 kHz is downstream communication. Voice transmission occurs at less than 4 KHz. So, data transmission occurs simultaneously with voice transmission.
* ADSL filters are used on customer premises with non-DSL connections.
* ADSL uses analog sinusoidal carrier waves for data transmission. The waves are modulated and demodulated at the customer premises with ADSL modems.

# 7. Switching [3 Hrs]

## **7.1 Circuit-switching and packet-switching**





## **7.2 Switched communication network**

A switched communications network transfers data from source to destination through a series of network nodes. Switching can be done in one of two ways. In a circuit-switched network, a dedicated physical path is established through the network and is held for as long as communication is necessary. An example of this type of network is the traditional (analog) telephone system. A packet-switched network, on the other hand, routes digital data in small pieces called packets, each of which proceeds independently through the network. In a process called store-and-forward, each packet is temporarily stored at each intermediate node, then forwarded when the next link becomes available. In a connection-oriented transmission scheme, each packet takes the same route through the network, and thus all packets usually arrive at the destination in the order in which they were sent. Conversely, each packet may take a different path through the network in a connectionless or datagram scheme. Since datagrams may not arrive at the destination in the order in which they were sent, they are numbered so that they can be properly reassembled. The latter is the method that is used for transmitting data through the Internet.

## **7.3 Circuit switching concept**

Switch establishes a dedicated path between any two devices that wish to communicate. The dotted lines inside the switch symbolize the connections that are currently active. The function of the digital switch is to provide a transparent signal path between any pair of attached devices. The path is transparent in that it appears to the attached pair of devices that there is a direct connection between them. Typically, the connection must allow full-duplex transmission.

The **network interface** element represents hardware needed to connect digital devices, such as data processing devices and digital telephones, to the network. Analog telephones can also be attached if the network interface contains the logic for converting to digital signals.

**The Control unit performs three general tasks.**

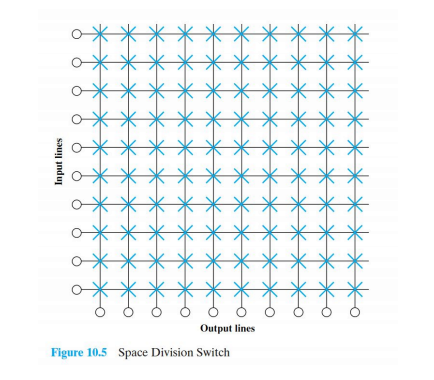
**First, it establishes connections.**To estab-lish the connection, the control unit must handle and acknowledge the request, deter- mine if the intended destination is free, and construct a path through the switch.

**Second, the control unit must maintain the connection**. Because the digital switch uses time division principles, this may require ongoing manipulation of the switching ele- ments. However, the bits of the communication are transferred transparently (from the point of view of the attached devices).

**Third, the control unit must tear down the connection**, either in response to a request from one of the parties or for its own reasons

**Space Division Switching**

Space division switching was originally developed for the analog environment and has been carried over into the digital realm. Each connection requires the establishment of a physical path through the switch that is dedicated solely to the transfer of signals between the two endpoints. The basic building block of the switch is a metallic crosspoint or semi- conductor gate that can be enabled and disabled by a control unit. Figure 10.5 shows a simple crossbar matrix with 10 full-duplex I/O lines. The matrix has 10 inputs and 10 outputs; each station attaches to the matrix via one input and one output line. Interconnection is possible between any two lines by enabling the appropriate crosspoint. Note that a total of 100 crosspoints is required.



**The crossbar switch has a number of limitations:**

1. The number of crosspoints grows with the square of the number of attached stations. This is costly for a large switch.

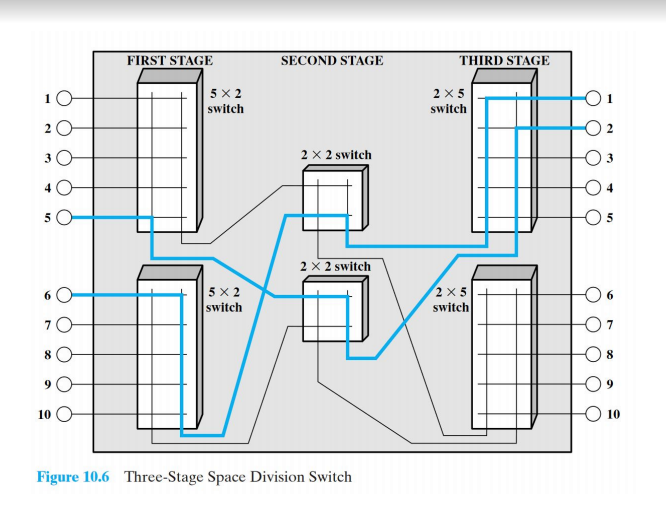
2. The loss of a crosspoint prevents connection between the two devices whose lines intersect at that crosspoint.

3. The crosspoints are inefficiently utilized; even when all of the attached devices are active, only a small fraction of the crosspoints are engaged.

To overcome these limitations, multiple-stage switches are employed. Figure 10.6 is an example of a three-stage switch. This type of arrangement has two advan- tages over a single-stage crossbar matrix:

1. The number of crosspoints is reduced, increasing crossbar utilization. In this example, the total number of crosspoints for 10 stations is reduced from 100 to 48.
2. There is more than one path through the network to connect two endpoints, increasing reliability.

A multistage network requires a more complex control scheme. A consideration with a multistage space division switch is that it may be blocking. The heavier lines indicate the lines that are already in use. In this state, input line 10, for example, cannot be connected to output line 3, 4, or 5, even though all of these output lines are available.



## **7.4 Packet switching principles and technique**

Invented to overcome the drawbacks of Circuit Switching. Here, data are divided into small chunks called packets and routed independently of others so different packets may take different paths.

**It has the following benefits**

1. Full use of available bandwidth.

2. Devices of different speeds can communicate over the same link.

3. High Availability: No waiting time for connection establishment.

4. Redundancy: Packets can be routed via alternate router even if a link fails.

**The main drawbacks are:**

1. Possible data loss or corruption due to congestion.

2. Extra protocols are needed for reliable transfer.

3. Long delay in case of high load.

**Packet switching are divided into two types**

**Virtual Circuit Method**

● In this method first a connection is established to reserver resource (bandwidth)

between the source, the intermediate paths and destination.

● Similar to circuit switching after the connection is established.

● All packets are then sent through this fixed path.

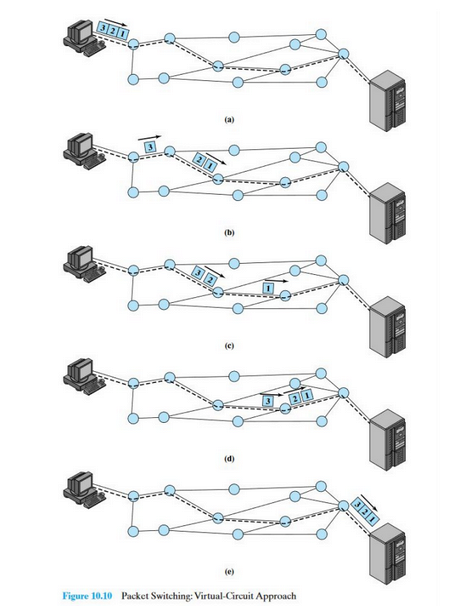
● Since all packets take the same path, packets arrive in order.

**Datagram Method**

● Here the individual packets are sent independently to each other.

● Packets may take different path and hence can arrive out of order

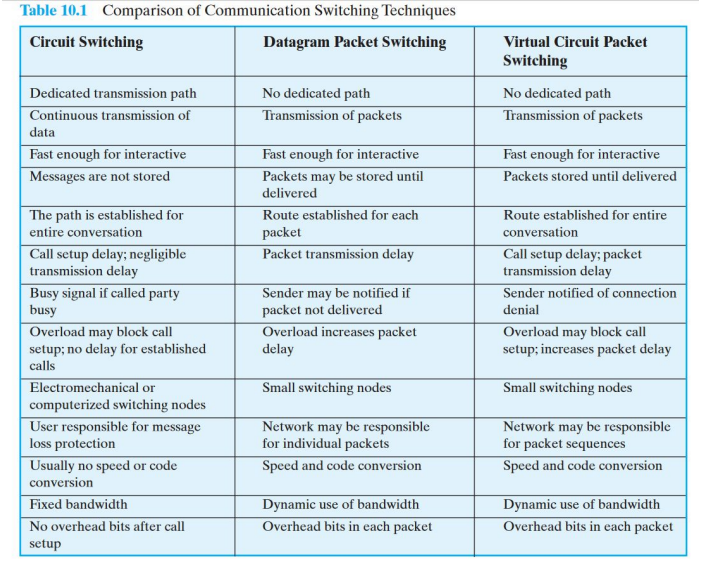
****

****

**Propagation delay:** The time it takes a signal to propagate from one node to the next. This time is generally negligible. The speed of electromagnetic signals through a wire medium, for example, is typically

• **Transmission time:**The time it takes for a transmitter to send out a block of data. For example, it takes 1 s to transmit a 10,000-bit block of data onto a 10-kbps line.

• **Node delay:**The time it takes for a node to perform the necessary processing as it switches data.

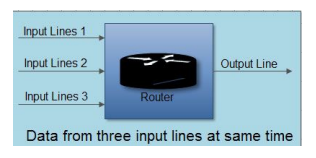


# **8. Congestion [2 Hrs]**

## **8.1 Congestion control in data network**

When the no. of packets being transmitted through a link becomes high (generally 80% of capacity), then the performance of the n/w decreases, hence increasing congestion.

**Common causes**

****

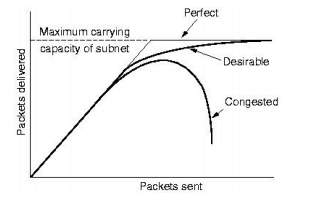
● In a packet switched network each intermediate device takes traffic in its i/p port, buffers it before transmitting out of the o/p port. If the density of incoming traffic is high there may not be enough buffer space to store the incoming traffic leading to packet drops.

● Even a large buffer space cannot solve the problem since it introduces delay, leading to timeout and retransmission.

● The slow processing of the intermediate devices.

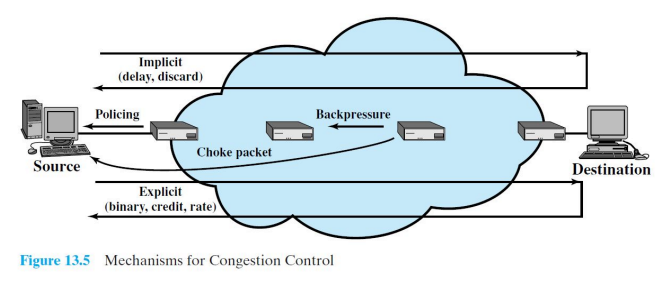
● Low network line bandwidth leading to bottleneck.

## **8.2 Effect of congestion**



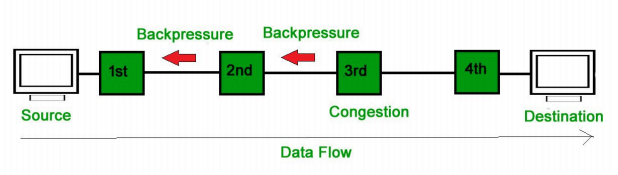
Ideally the n/w should be able to send data at the full capacity, giving 100% throughput as shown by the ideal curve in fig. 1.But practically, the congestion causes the throughput to decline sharply when the n/w is 80% saturated as shown by the uncontrolled curve. The use of congestion control algorithms can prevent this sharp decline in performances and send data efficiently at close to 80% of the n/w capacity as shown by the controlled curve.

## **8.3 Congestion control in packet switched network**



**1. Backpressure**

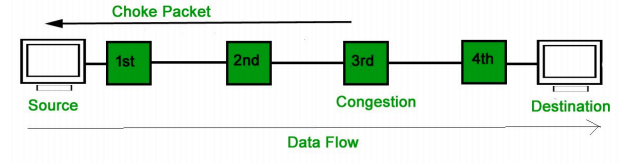
Backpressure is a technique in which a congested node stops receiving packets from upstream nodes. This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagates in the opposite direction of data flow.



In the above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may get congested due to slowing down of the output data flow. Similarly the 1st node may get congested and informs the source to slow down.

**2. Choke Packet Technique :**

A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resources and the utilization at each of its output lines. Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it feedback to reduce the traffic. The intermediate nodes through which the packets have traveled are not warned about congestion.



**3. Implicit Signaling :**

In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when the sender sends several packets and there is no acknowledgement for a while, one assumption is that there is a congestion.

**4. Explicit Signaling :**

In explicit signaling, if a node experiences congestion it can explicitly send a packet to the source or destination to inform about congestion. The **difference between choke packet** and explicit signaling is that the **signal is included in the packets that carry data rather than creating different packets** as in case of choke packet technique.

Explicit signaling can occur in either forward or backward direction.

1. **Forward Signaling :**

In forward signaling signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopts policies to prevent further congestion.

1. **Backward Signaling :**

A backward signaling signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

**Leaky Bucket Algorithm**

It is used to shape bursty rate traffic into fixed rate traffic. Its working can be compared with a tap with a bursty flow of water. If the water is collected in a bucket with a hole at the bottom for a continuous drainage of water.

Its working as follows as illustrated in the figure below:

1. A host sent data of bursty nature.

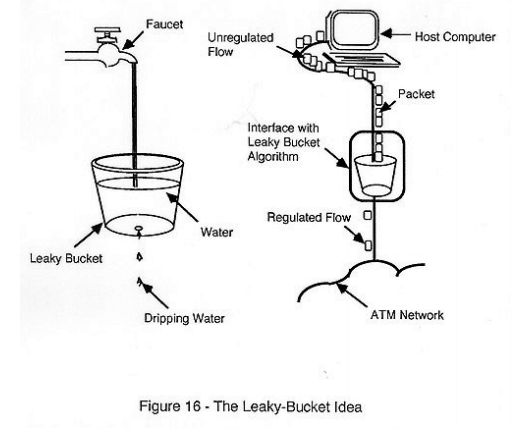
2. This data is kept in a storage buffer by the OS or the NIC.

3. This stored data is then sent out to n/w at a uniform rate.

But it has two major disadvantages

1. Traffic is lost when the bucket is full.

2. The o/p rate is fixed even if there is no congestion.



**Token Bucket Algorithm**

Token buckets were introduced to address the two major drawbacks of leaky buckets i.e. loss of traffic when the bucket is full and fixed o/p rate even in case of no congestion.

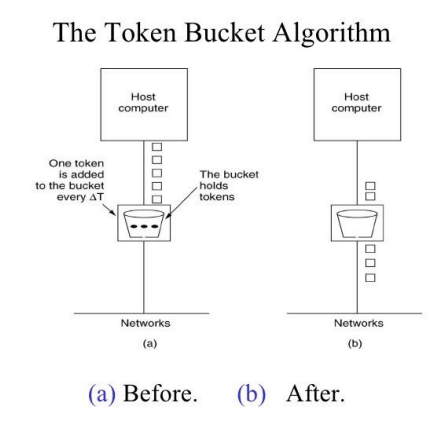
This algorithm works as follow

1. At every tick (or time interval) a token is added in the bucket.

2. Let us say there are 3 tokens at the bucket at a given time when the host sends a bursty data containing 5 packets as shown in figure 1. below.

3. Since the bucket has 3 tokens it can send 3 packets immediately as shown in figure 2 below.

4. The rest of the data are sent at subsequent ticks.



**Congestion Control In Packet-switching Networks**

A number of control mechanisms for congestion control in packet-switching networks have been suggested and tried.The following are examples:

1. Send a control packet from a congested node to some or all source nodes. This choke packet will have the effect of stopping or slowing the rate of transmission from sources and hence limit the total number of packets in the network. This approach requires additional traffic on the network during a period of congestion.

2. Rely on routing information. Routing algorithms provide link delay information to other nodes, which influences routing decisions. This information could also be used to influence the rate at which new packets are produced.

3. Make use of an end-to-end probe packet. Such a packet could be time stamped to measure the delay between two particular endpoints. This has the disadvantage of adding overhead to the network.

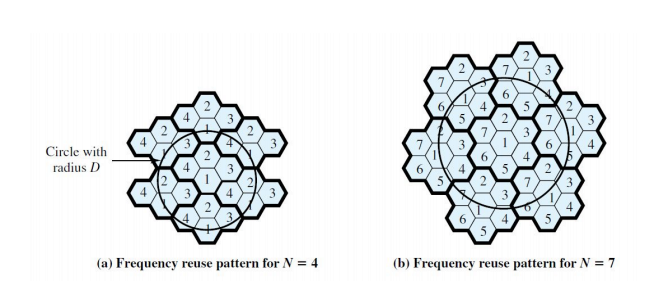
4. Allow packet-switching nodes to add congestion information to packets as they go by.

# **9. Cellular wireless network [2 Hrs]**

Cellular network is an underlying technology for mobile phones, personal communication systems, wireless networking etc. The technology is developed for mobile radio telephone to replace high power transmitter/receiver systems. Cellular networks use lower power, shorter range and more transmitters for data transmission.

## **9.1 Principle of cellular network**

Cellular network is an underlying technology for mobile phones, personal communication systems, wireless networking etc. The technology is developed for mobile radio telephone to replace high power transmitter/receiver systems. Cellular networks use lower power, shorter range and more transmitters for data transmission.

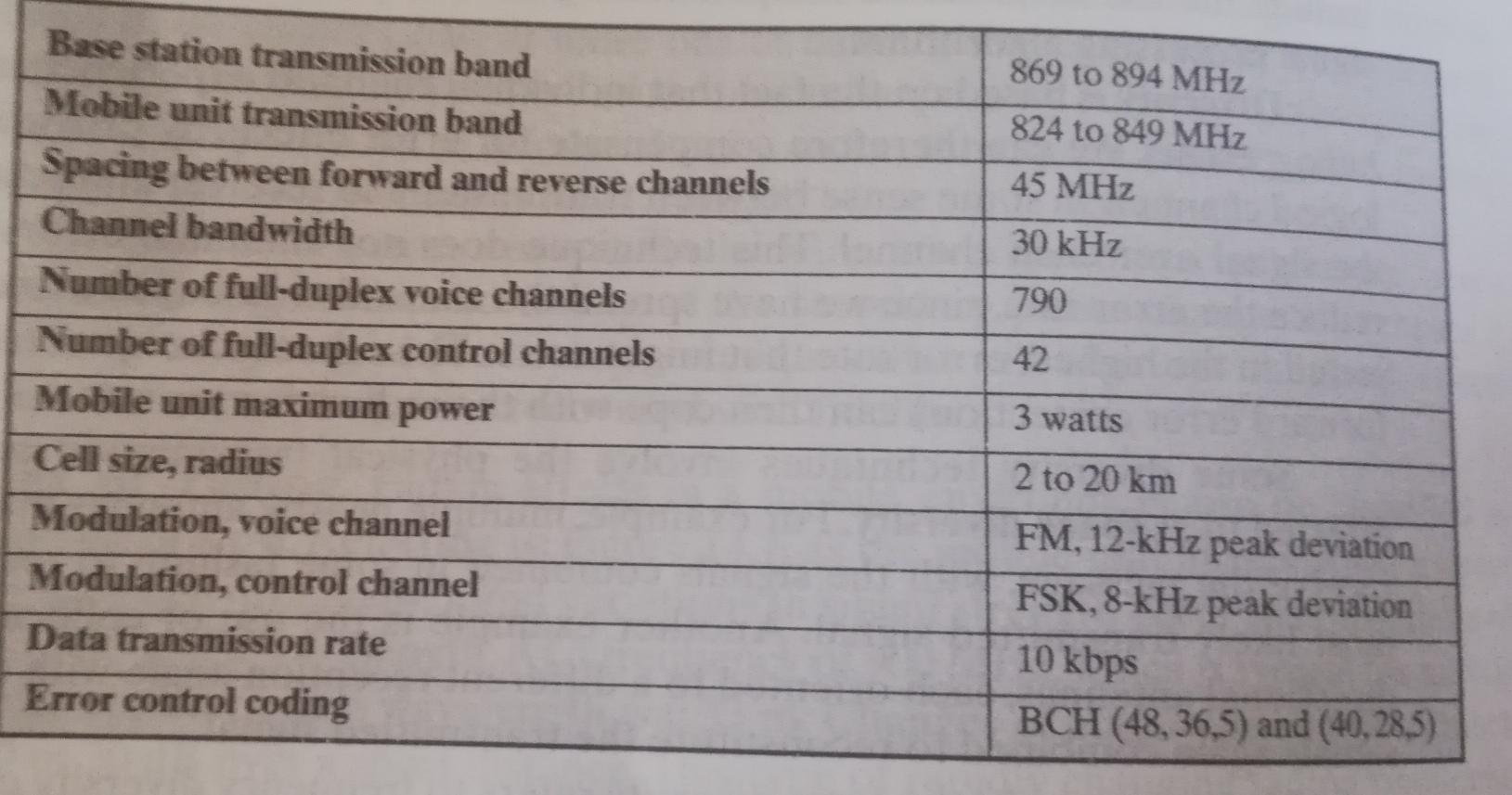


## **9.2 First generation analog**

the original cellular telephone networks provided analog traffic channels; these are now referred to as first-generation systems. Since the early 1980’s the most common first-generation system in North America has been the Advanced Mobile Phone Service (AMPS) developed by AT&T. Although gradually being replaced by second-generation systems, AMPS is still in common use.

### **Spectral Allocation( Frequency Allocation)**

Two 25-MHz bands are allocated to AMPS, one for transmission from base station to the mobile unit(869MHz - 894MHz), the other for transmission from mobile to the base station (824MHz - 849MHz). Each of these bands are split into two to encourage competition in the market. An operator is allocated only 12.5MHz in each direction for its system. The channels stretch 30kHz apart, which allows a total of 416 channels per operator. 21 channels are allocated for control, leaving 395 to carry calls. The control channels are data channels operating at 10 kbps. The conversation channels carry the conversation in analog using frequency modulation. Control information is also sent in the conversation channels in bursts as data.



### **Operation**

Each AMPS-capable cellular telephone includes a Numeric Assignment Module (NAM) in read-only memory. The NAM contains the telephone number of the phone, which is assigned by the service provider, and the serial number of the phone, which is assigned by the manufacturer. When the phone is turned on, it transmits its serial number and phone number to the MTSO; the MTSO maintains the database with information about mobile units that have been reported stolen and uses serial number lock out stolen units. The MTSO uses the phone number for billing purposes.

When a called is placed, the following sequence of event is occurred:

1. The subscriber initiates a call by keying in the telephone number of the called party and presses the send key.
2. The MTSO verified that the telephone number is valid and the user is authorised to place the call.
3. MTSO issues a message to the user's cell phone indicating which traffic channels to use for sending and receiving.
4. The MTSO sends out a ringing signal to the call party. All of these operations occur within 10 seconds of initiating a call.
5. When the called party answers, the MTSO establishes a circuit between the two parties and initiates billing information.
6. When one party hangs up, the MTSO releases the circuit, frees the radio channels and completes the billing information.

### **AMPS control channel:**

Each AMPS service includes 21 full duplex 30-KHz control channels, consisting of 21 reverse control channels (RCCs) from subscriber to base station, and 21 forward channels from base station to subscribers. These channels transmit digital data using FSK. in both channels are transmitted in frames.

## **9.3 Second generation CDMA**

### **First- and Second-Generation cellular system**

Second generation systems have been developed to provide higher quality signals, higher data rates for support of the digital services and greater capacity. Some of the following key difference between two generations are:

* **Digital traffic channels:**

The most notable difference between first and second generation is that the first generation system almost purely uses analog systems whereas second generation systems are digital. First generation systems are designed to support voice channels using FM; digital traffic is supported only by using modem.second generation systems readily support digital data; voice traffic is first encoded in digital form before transmitting.

* **Encryption**

Because all the use traffic and control traffic is digital in the second generation; it is relatively easier to encrypt all the traffic to prevent eavesdropping. All second generation systems provide this capability, whereas the first generation system sends user traffic in the clear, providing no security.

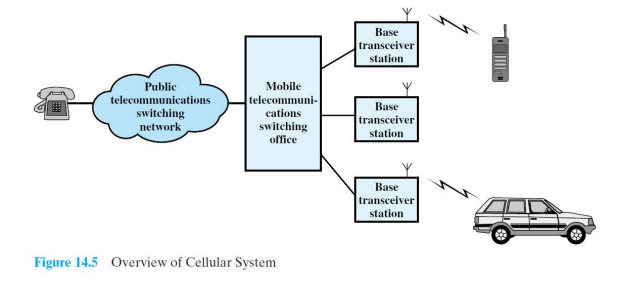
* **Error detection and correction**

The digital traffic stream of second generation systems also lends itself to the use of error detection and correction techniques. The results can be very clear voice reception.

* **Channel access:**

In the first generation system, each cell supports a number of channels. At any given time a channel is allocated to the only one user. Second generation system also provides multiple channels per cell, but each channel is dynamically shared by a number of users using time division multiple access (TDMA) or code division multiple access (CDMA).

**Operation of Cellular Systems**



**Code-division multiple access (CDMA)** is a channel access method used by various radio communication technologies.

CDMA is an example of multiple accesses, where several transmitters can send information simultaneously over a single communication channel.

• CDMA means communication with different codes.

• If codes are multiply with each other, then the answer is “0”,

• If codes are multiplied by itself, then we get “1”.

For Example, there are four stations: S1,S2,S3,S4

• Suppose C1, C2, C3, and C4 are unique code generated by each station s1, s2, s3 and s4.

• Then, data of each station is multiplied with its unique code.,i.e.:

◦ Station 1=D1\* C1

◦ Station 2=D2\* C2

◦ Station 3=D3\* C3

◦ Station 4=D4\* C4

• Then after, all these signals are transmitted through the same channel simultaneously. i.e

**(C1\*D1)+ (C2\*D2)+(C3\*D3)+ (C4\*D4)**

If station 1 want to hear what station 2 says, it multiplies the message by code of station 1 ie C2;

[D1\* C1+ D2\* C2+ D3\* C3+ D4\* C4]\*C2 =D1C2C1+C2D2C2+C2C3D3+D4C2C4 =0+D2+0+0 =D2 i.e. data sent by station 2.

# **10. LAN overview [3 Hrs]**

## **10.1 LAN protocol architecture**

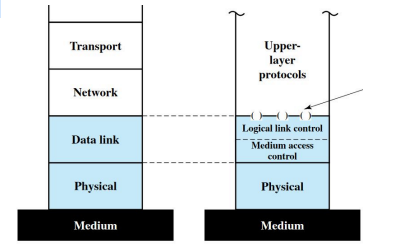
The LAN protocol is identified with IEEE 802. The DataLink Layer is uniquely positioned in that it acts as a mediator between the hardware and the software layer, hence it is divided into two sublayers:

**Logical Link Control (802.2):**

Mostly concerned with talking and providing support for multiple upper layer protocols, such as connectionless and connection oriented protocols.

**Media Access Control(MAC)**

Mostly concerned with providing the physical (MAC) address to access the shared Medium.



## **10.2 Bridges**

There is a need to expand beyond the confines of a single LAN,to provide interconnection to other LANs and to wide area networks. Two general approaches are used for this purpose: bridges and routers. The bridge is the simpler of the two devices and provides a means of interconnecting similar LANs. Therouter is a more general-purpose device, capable of interconnecting a variety ofLANs and WANs.

The bridge is designed for use between local area networks (LANs) that use identical protocols. Because the devices all use the same protocols, the amount of processing required at the bridge is minimal. More sophisticated bridges are capable of map-ping from one MAC format to another (e.g., to interconnect an Ethernet and a token ring LAN).

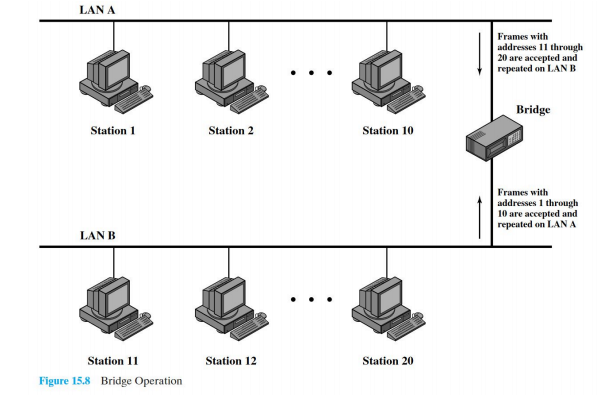
There are several reasons for the use of multiple LANs con-nected by bridges:

**•Reliability:**The danger in connecting all data processing devices in an organi-zation to one network is that a fault on the network may disable communica-tion for all devices. By using bridges, the network can be partitioned into self-contained units.

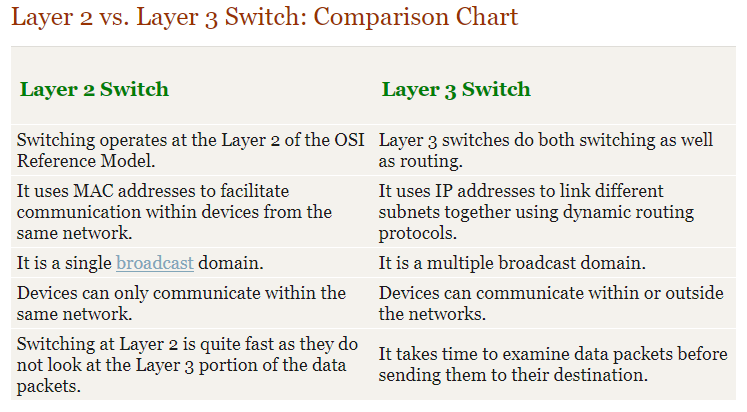
**•Performance**:In general, performance on a LAN declines with an increase in the number of devices or the length of the wire. A number of smaller LANs will often give improved performance.

**•Security:**The establishment of multiple LANs may improve security of com-munications. It is desirable to keep different types of traffic (e.g., accounting, personnel, strategic planning) that have different security needs on physically separate media.

**•Geography:**Clearly, two separate LANs are needed to support devices in two geographically distant locations.



## **10.3 Layer 2 and layer 3 switch**

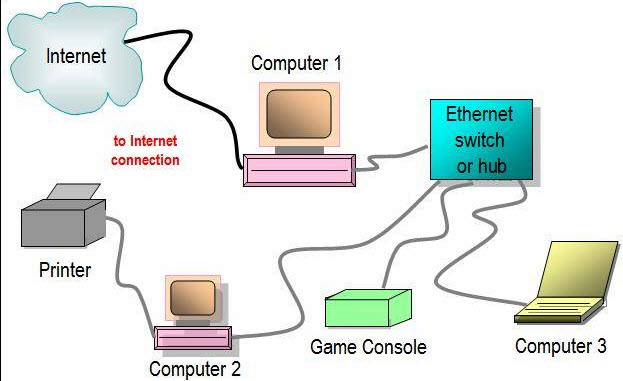


## **10.4 Ethernet**

Ethernet is a standard communication protocol embedded in software and hardware devices. It is used for building a local area network. The local area network is a computer network that interconnects a group of computers and shares the information through cables or wires.

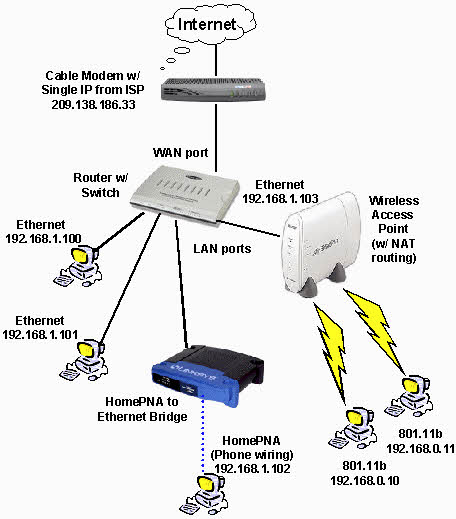
**Wired Ethernet Network**

The Ethernet technology mainly works with the fiber optic cables that connect devices within a distance of 10 km. The Ethernet supports 10 Mbps.



A computer network interface card (NIC) is installed in each computer, and is assigned to a unique address. An Ethernet cable runs from each NIC to the central switch or hub. The switch and hub act as a relay though they have significant differences in the manner in which they handle network traffic – receiving and directing packets of data across the LAN. Thus, Ethernet networking creates a communications system that allows sharing of data and resources including printers, fax machines and scanners.

**Wireless Ethernet**



Ethernet networks can also be wireless. Rather than using Ethernet cable to connect the computers, wireless NICs use radio waves for two-way communication with a wireless switch or hub. It consists of Ethernet ports, wireless NICs, switches and hubs. Wireless network technology can be more flexible to use, but also require extra care in configuring security.

**Types of Ethernet**

**1. Fast Ethernet**

The fast Ethernet is a type of Ethernet network that can transfer data at a rate of 100 Mbps using a twisted-pair cable or a fiber-optic cable. Fast Ethernet is based on the proven CSMA/CD Media Access Control (MAC) protocol, and uses existing 10BaseT cabling. Data can move from 10 Mbps to 100 Mbps without any protocol translation or changes to the application and networking software.

What is Ethernet Port Speed?

When compared to a 10 mb port, a 100 Mb port is theoretically 10 times faster than the standard port. Therefore, with a 100 Mb port more information can stream to and from your server. This will be of great help to you if you really need to explore very high speed, but not if you are under DDOS attack because you will find yourself running out of traffic allocation very fast.

**2. Gigabit Ethernet**

The Gigabit Ethernet is a type of Ethernet network capable of transferring data at a rate of 1000 Mbps based on a twisted-pair or fiber optic cable, and it is very popular. The type of twisted-pair cables that support Gigabit Ethernet is Cat 5e cable, where all the four pairs of twisted wires of the cable are used to achieve high data transfer rates. The 10 Gigabit Ethernet is a latest generation Ethernet capable of transferring data at a rate of 10 Gbps using twisted-pair or fiber optic cable.

**3. Switch Ethernet**

Multiple network devices in a LAN requires network equipment such as a network switch or hub. When using a network switch, a regular network cable is used instead of a crossover cable. The crossover cable consists of a transmission pair at one end and a receiving pair at the other end.

The main function of a network switch is to forward data from one device to another device on the same network. Thus a network switch performs this task efficiently as the data is transferred from one device to another without affecting other devices on the same network.

The network switch normally supports different data transfer rates. The most common data transfer rates include 10 Mbps – 100 Mbps for fast Ethernet, and 1000 Mbps – 10 Gbps for the latest Ethernet.

Switch Ethernet uses star topology, which is organized around a switch. The switch in a network uses a filtering and switching mechanism similar to the one used by the gateways, in which these techniques have been in use for a long time.

## **10.5 Fiber channel**

A fiber channel (FC) is a computer networking technology that is used to transfer data between one or more computers at very high speeds. It was initially designed for supercomputers but is now commonly implemented in storage networking server environments as a replacement to small computer system interface (SCSI) and other serial storage technologies.

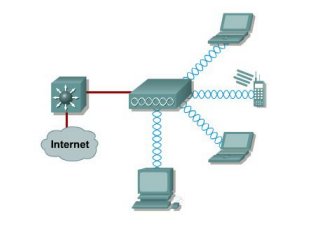
FC is used in a server environment to transfer bulk data between interconnected storage servers or clusters at very high data transfer rates (DTR). It can transfer data in excess of 1 Gbps and reach speed up to 4 Gbps.

FC-based data transfer is usually achieved by using a FC port on a computer or server and a FC-specific switch, which is known as the fabric. The port and switch can be connected using standard coaxial cables or through fiber optic cables.

The signals transmitted from a FC port can be propagated to substantial distances, reaching several kilometers in length with high-speed mediums.

## **10.6 Wireless LAN technology**

Wireless LANs (WLAN) are similar to Ethernet networks in many ways. A WLAN is a shared network. The access point is a shared device and functions like a shared Ethernet hub. In the wireless cell, only one station can transmit at any time; all other stations listen. A station that wants to transmit must wait until the wireless media is not in use by another station. This transmission setup is similar to that of a coaxial cable or half-duplex Ethernet and an Ethernet hub. The average data rate per station is total bandwidth divided by the number of stations. The actual data throughput experienced by the wireless clients is even less because of wireless-specific issues. In WLANs, data is transmitted over radio waves. WLAN signals use the same frequency for transmitting and receiving (half-duplex); therefore, a station cannot receive while it is transmitting. This is similar to coaxial cable Ethernet.



## **10.7 IEEE 802.11**

The 802.11 standard is divided into

● **802.11a** — an extension to 802.11 that applies to wireless LANs and provides up to

54-Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division

multiplexing encoding scheme rather than FHSS or DSSS.

● **802.11b** (also referred to as 802.11 High Rate or Wi-Fi) — an extension to 802.11

that applies to wireless LANS and provides 11 Mbps transmission in the 2.4 GHz

band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original

802.11 standard, allowing wireless functionality comparable to Ethernet.

● **802.11g** — applies to wireless LANs and is used for transmission over short

distances at up to 54-Mbps in the 2.4 GHz bands.

# **11. Inter network protocol [2 Hrs]**

## **11.1 Internet protocol, ipv4 and ipv6**

**Internet Protocol**

The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place. Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.

Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP. The most common transport protocols are TCP and UDP.

**IPV4**

IPv4 is the most widely used Internet protocol across the internet today. Internet protocols are mostly responsible for addressing and forwarding of data on the Internet.

The network layer packet, also referred to as datagram, plays a central role in communication across the internet. The basic format of the IPv4 datagram is shown below :

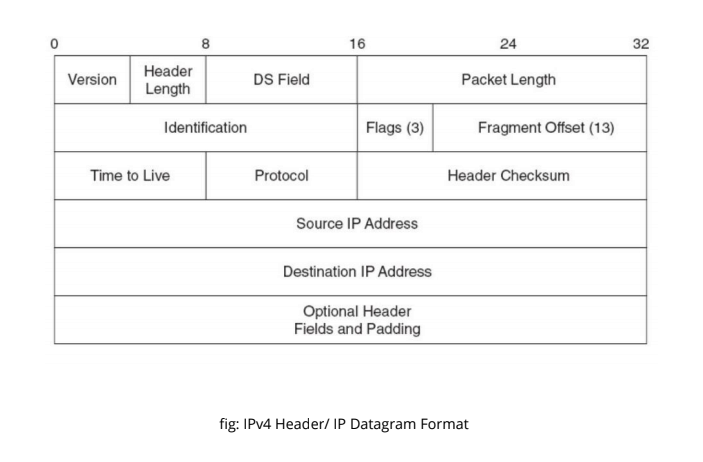


fig: IPv4 Header/ IP Datagram Format

**IPv4 Fields**

**Version**:- The first header field in an IP packet is the four-bit version field. The Version field indicates the format of the internet header. Version identifies the IP version to which the packet belongs. This four-bit field is set to binary 0100 to indicate version 4 (IPv4) or binary 0110 to indicate version 6 (IPv6).

**Header length or Internet Header Length (IHL) :-** The second field (4 bits) is the Internet Header Length (IHL), this field specifies the size of the header.

**Type of Service(ToS):-** now known as **Differentiated Services Code Point (DSCP).** The TOS field is used to carry information to provide quality of service features. An example is Voice over IP (VoIP) that is used for interactive data voice exchange.

**Total Length:-** This 16-bit field defines the entire datagram size, including header and data, in bytes.

**Identification, Flags, Fragment Offset:-** These three fields are used to fragment and reassemble large IP datagram.

**Time To Live (TTL):-**It is of 8 bit field. This field specifies the maximum no of hops (Routers) the packet can travel before it is dropped.

**Protocol:-**This field defines the protocol used in the data portion of the IP datagram. Eg. TCP, UDP etc.

**Header Checksum:-** The 16-bit checksum field is used for error-checking of the header. At each hop, the checksum of the header must be compared to the value of this field. If a header checksum is found to be mismatched, then the packet is discarded.

**Source address:-** Sets the source IP address.

**Destination address:-** An IPv4 address indicating the receiver of the packet.

**Options and Padding :-** Used to specify additional header fields if needed. They must be multiple of 32 bits.

**IPV6**

The exhaustion of the IPv4 address space has forced the technology world to look for newer solutions to the addressing scheme. Since IPv4 IP addresses use 32-bit addresses, there are a possible ~4.2 billion (2^32) possible IP addresses. Have we used them all up?

No, but there are some address ranges that can’t be used for technical/legacy reasons. Even if those technical/legacy reasons could be overcome, the IPv4 address space is still very constrained for a quickly growing Internet. In April 2010, the Regional Internet Registries (the “authorities”) said that only 8% of the IPv4 addresses are unallocated and the remaining are expected to run within years.

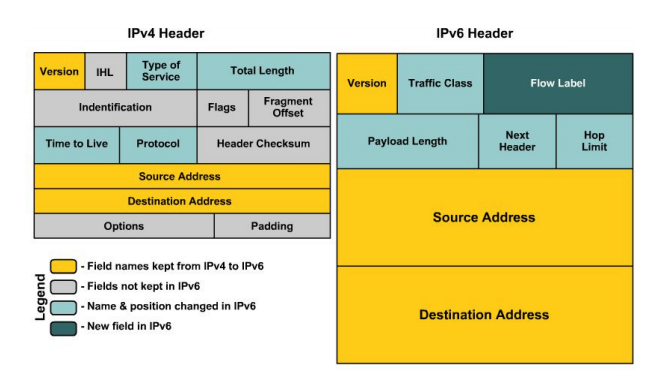
**The main incentives to move to IPv6 are:**

-IPv6 gives us 128 bits for address space that is (2^128) unique addresses.

-IPv6 has built-in features for mobility.

-IPv6 has built-in support for IPSec.

-IPv6 supports for smooth transition from IPv4



The following list describes the function of each header field.

**Version** – 4-bit Version number of Internet Protocol = 6.

**Traffic Class** – 8-bit traffic class field. The nodes that originate a packet must identify different classes or different priorities of IPv6 packets. The nodes use the Traffic Class field in the IPv6 header to make this identification. The routers that forward the packets also use the Traffic Class field for the same purpose.

**Flow Label** – 20-bit field. The IPv6 routers must handle the packets belonging to the same flow in a similar fashion. All packets that belong to the same flow must be sent with the same source address, same destination address.

**Payload Length** – The 16-bit payload length field contains the length of the data field in octets/bits following the IPv6 packet header. The 16-bit Payload length field puts an upper limit on the maximum packet payload to 64 kilobytes.

**Next Header** – 8-bit selector. Identifies the type of header that immediately follows the IPv6 header. wing the IPv6 header and located at the beginning of the data field (payload) of the IPv6 packet. This field usually specifies the transport layer protocol used by a packet's payload. The two most common kinds of Next Headers are TCP (6) and UDP (17), but many other headers are also possible. Similar to the Protocol field in IPv4.

**Hop Limit** – 8-bit integer. This field specifies the maximum no of hops ( Routers ) the packet can travel before it is dropped.

**Source Address** – 128 bits. The address of the initial sender of the packet.

**Destination Address** – 128 bits. The address of the intended recipient of the packet.

## **11.2 VPN and IP security**

**VPN**

A virtual private network (VPN) is programming that creates a safe, encrypted connection. Typically, it is used over a less secure network, such as the public internet. It uses tunneling protocols to encrypt data at the sending end, and decrypt it at the receiving end. The originating and receiving network addresses are also encrypted to provide better security for online activities. It can also be used to provide remote employees.

**How a VPN works**

At its most basic level, VPN tunneling creates a point-to-point connection that cannot be accessed by unauthorized users. To actually create the tunnel, the endpoint device needs to be running a VPN client (software application) locally or in the cloud. The client runs in the background. It is not noticeable to the end user, unless there are performance issues.

The performance can be affected by many factors, like speed of users' internet connections, the protocol types an internet provider may use, and the type of encryption it uses. In the enterprise, performance can also be affected by poor quality of service (QoS) outside the control of an organization's information technology (IT) department.

**VPN protocols**

VPN protocols ensure an appropriate level of security to connected systems, when the underlying network infrastructure alone cannot provide it. There are several different protocols used to secure and encrypt users and corporate data. They include:

* IP security (IPsec)
* Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
* Point-To-Point Tunneling Protocol (PPTP)
* Layer 2 Tunneling Protocol (L2TP)
* OpenVPN

**Types of VPN**

**Remote access VPN**

Remote access clients connect to a VPN gateway server on the organization's network. The gateway requires the device to authenticate its identity before granting access to internal network resources. This type usually relies on either IP Security (IPsec) or Secure Sockets Layer (SSL) to secure the connection.

**Site-to-site VPN**

In contrast, a site-to-site VPN uses a gateway device to connect an entire network in one location to a network in another location. End-node devices in the remote location do not need VPN clients because the gateway handles the connection.

**Mobile VPN**

In a mobile VPN, the server still sits at the edge of the company network, enabling secure tunneled access by authenticated, authorized clients. Mobile VPN tunnels are not tied to physical IP addresses, however. Instead, each tunnel is bound to a logical IP address. That logical IP address sticks to the mobile device no matter where it may roam.

**Hardware VPN**

Hardware VPNs offer a number of advantages over strictly software-based VPNs. In addition to enhanced security, hardware VPNs can provide load balancing for large client loads.

**VPN appliance**

A VPN appliance, also known as a VPN gateway appliance, is a network device with enhanced security features. Also known as an SSL (Secure Sockets Layer) VPN appliance, it is a router that provides protection, authorization, authentication and encryption for VPNs.

**Dynamic multipoint virtual private network (DMVPN)**

A dynamic multipoint virtual private network (DMVPN) exchanges data between sites without needing to pass through an organization's headquarter VPN server or router. A DMVPN creates a mesh VPN service that runs on VPN routers and firewall concentrators. Each remote site has a router configured to connect to the company’s headquarters device (hub), providing access to the resources available. When two spokes are required to exchange data between each other.

**IP Security**

The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

**Uses of IP Security –**

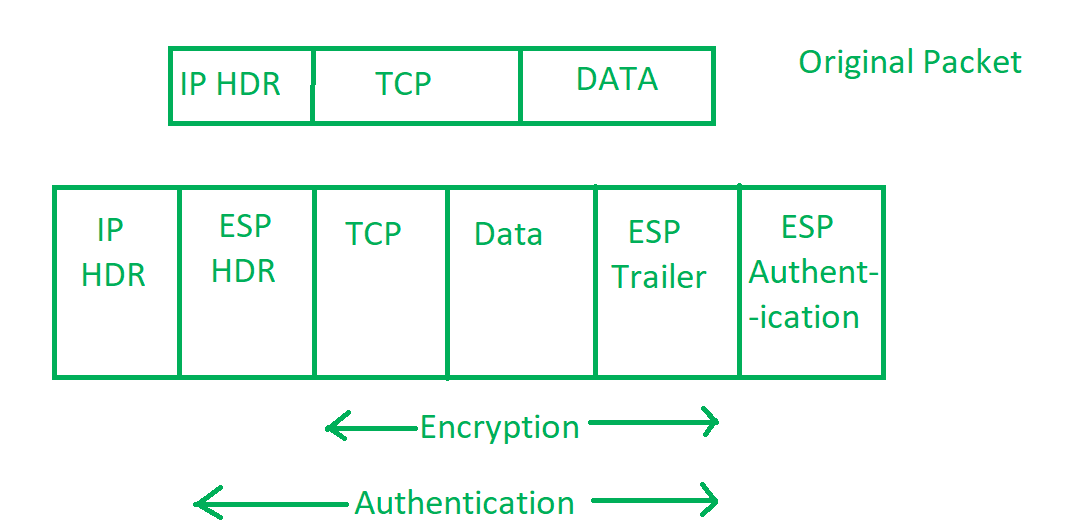
IPsec can be used to do the following things:

* To encrypt application layer data.
* To provide security for routers sending routing data across the public internet.
* To provide authentication without encryption, like to authenticate that the data originates from a known sender.
* To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

**Components of IP Security –**

It has the following components:

1. **Encapsulating Security Payload (ESP) –** It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH) –** It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection protects against unauthorized transmission of packets. It does not protect data’s confidentiality.  
     
     
   
3. **Internet Key Exchange (IKE) –**

It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication.  


**Working of IP Security –**

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet applies an appropriate encryption. The incoming packets are also checked by the host whether they are encrypted properly or not.
2. Then the **IKE Phase 1** starts in which the 2 hosts( using IPsec ) authenticate themselves to each other to start a secure channel. It has 2 modes. The **Main mode** which provides the greater security and the **Aggressive mode** which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
4. Now, the **IKE Phase 2** is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.
5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
6. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

## **11.3 Routing protocol**

Definition - What does Routing Protocol mean?

A routing protocol uses software and routing algorithms to determine optimal network data transfer and communication paths between network nodes. Routing protocols facilitate router communication and overall network topology understanding.

A routing protocol is also known as a routing policy

Types of routing protocol

1. **Distance Vector Routing Protocol**

These protocols select the best path in the basis of hop counts to reach a destination network in the particular direction.

**Features**

* Updates of the network are exchanged periodically.
* Updates (routing information) is always broadcast.
* Full routing tables are sent in updates.
* Routers always trust on routing information received from neighbor routers. This is also known as routing on rumors.

**Disadvantages**

* As the routing information is exchanged periodically, unnecessary traffic is generated which consumes available bandwidth.
* As full routing tables are exchanged, therefore it has security issues. If an authorized person enters the network, then the whole topology will be very easy to understand.
* Also broadcasting on the network periodically creates unnecessary traffic.

**2. Link State Routing Protocol –** These protocols know more about the Internetwork than any other distance vector routing protocol. These are also known as SPF (Shortest Path First) protocol. OSPF is an example of link state routing protocol.

**Features**

* Hello messages, also known as keep-alive messages are used for neighbor discovery and recovery.
* Concept of triggered updates are used i.e updates are triggered only when there is a topology change .
* Only that much updates are exchanged which is requested by the neighbor router.

Link state routing protocol maintains three tables namely:

1. **Neighbor table-** the table which contains information about the neighbors of the router only, i.e, to which adjacency has been formed.
2. **Topology table-** This table contains information about the whole topology i.e contains both best and backup routes to particular advertised networks.
3. **Routing table-** This table contains all the best routes to the advertised network.

**Advantages**

* As it maintains separate tables for both the best route and the backup routes ( whole topology) therefore it has more knowledge of the inter network than any other distance vector routing protocol.
* Concept of triggered updates are used therefore no more unnecessary bandwidth consumption is seen like in distance vector routing protocol.
* Partial updates are triggered when there is a topology change, not a full update like distance vector routing protocol where the whole routing table is exchanged.

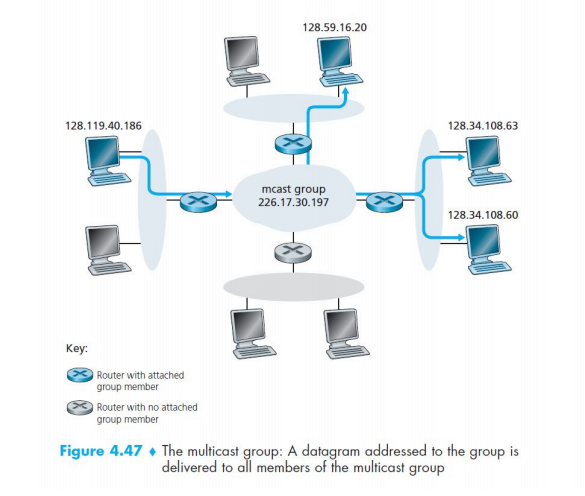
**3. Advanced Distance vector routing protocol –** It is also known as hybrid routing protocol which uses the concept of both distance vector and link state routing protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) is an example of this class if routing protocol. EIGRP acts as a link state routing protocol as it uses the concept of Hello protocol for neighbor discovery and forming adjacency. Also, partial updates are triggered when a change occurs. EIGRP acts as a distance vector routing protocol as it learns routes from directly connected neighbors.

## **11.4 Multicasting**

**Multicast Routing**

Multicast service, in which a multicast packet is delivered to only a subset of network nodes. A number of emerging network applications require the delivery of packets from one or more senders to a group of receivers. These applications include bulk data transfer (for example, the transfer of a software upgrade from the software developer to users needing the upgrade), streaming continuous media (for example, the transfer of the audio, video, and text of a live lecture to a set of distributed lecture participants), shared data applications (for example, a whiteboard or teleconferencing application that is shared among many distributed participants), data feeds (for example, stock quotes), Web cache updating, and interactive gaming (for example, distributed interactive virtual environments or multiplayer games).

On the Internet, if we need to send a message to multiple pc ( a group) then to identify these groups of pc a single identifier is used. This single identifier is a class D multicast IP address. The group of receivers associated with a class D address is referred to as a multicast group. The multicast group abstraction is illustrated in Figure 4.47. Here, four hosts (shown in shaded color) are associated with the multicast group address of 226.17.30.197 and will receive all datagrams addressed to that multicast address.



# **12. Data modems [2 hrs]**

## **12.1 Concept of modulation**

**Modulation**Process of combining low frequency signal with very high frequency radio waves called as carrier web. It is performed at the transmitting end. The result wave of modulation is called a modulated wave. Wave being modulated is called a message signal or modulating signal or base band signal.

**Need for modulation**

* **Long range transmission**

Transmits message over a longer distance is necessary to modulate the signal before transmission

Frequency is directly proportional to distance.

* **Practical antenna size**

WiFi communication, size of antenna (receiving and transmitting) depends on the frequency of the signal

Frequency is indirectly proportional to size of antenna

* **Reduction of low interface**

Noise reduction cannot be zero but with several modulation schemes it can be minimized

## 

## **12.2 AM, FM, PM**

**AM**

The amplitude of the carrier wave is varied according to the message signal. 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.

**FM**

In FM transmission, the frequency of the carrier signal is modulated to follow the changing voltage level (amplitude) of the modulating signal.

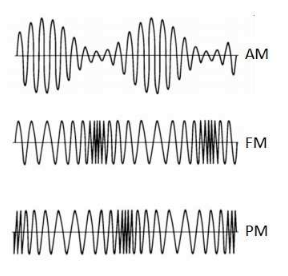
The peak amplitude and phase of the carrier signal remain constant, but as the amplitude of the information signal changes, the frequency of the carrier changes correspondingly.

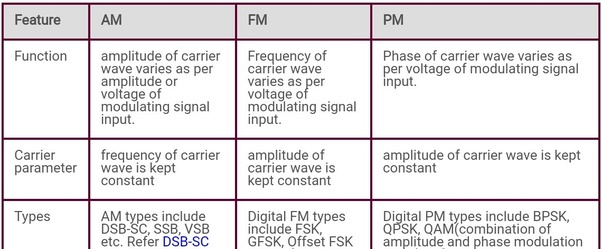
**PM**

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. In FM, the instantaneous change in the carrier frequency is proportional to the amplitude of the modulating signal; in PM the instantaneous change in the carrier frequency is proportional to the derivative of the amplitude of the modulating signal.

|  | AM | FM | PM |
| --- | --- | --- | --- |
| Advantages | AM signals are reflected back to earth from the ionosphere layer. Due to this fact, AM signals can reach far places which are thousands of miles from source. Hence AM radio has coverage wider compared to FM radio. | In FM, recovered voice depends on frequency and not amplitude. Hence the effects of noise are minimized in FM.  FM bandwidth covers all the frequency range which humans can hear. Hence FM radio has a better quality of sound in comparison with AM radio. | Phase modulation (PM) is a simple contrast to Frequency modulation (FM).  It is used to find out the velocity of a target by removing Doppler data. This needs a constant carrier which is achievable during phase modulation however not in FM (frequency modulation).  The main benefit of this modulation is signal modulation because it permits computers for communicating on high-speed using a telephone system.  When the information is being transmitted without intrusion then the speed rates can be observed.  And one more advantage of PM (phase modulation) is improved immunity toward the noise. |
| Disadvantages | The most natural as well as man made radio noise are of AM type. The AM receivers do not have any means to reject this kind of noise.  Weak AM signals have low magnitude compared to strong signals. This requires the AM receiver to have circuitry to compensate for signal level difference. | At higher frequency, FM modulated signals pass through the ionosphere and do not get reflected. Hence FM has lesser coverage compared to AM signals. | Phase modulation needs two signals by a phase variation among them. Through this, both the two patterns are required like a reference as well as a signal.  This type of modulation requires hardware which is more complex due to its conversion technique.  Phase ambiguity arrives if we exceed index pi radian of modulation (1800).  Phase modulation index can be enhanced by employing frequency multiplier. |

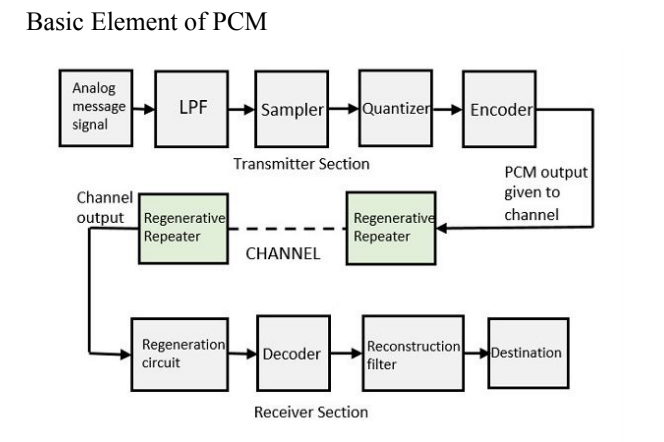




**Pulse Code Modulation**

Pulse code modulation converts analog signal information into a binary sequence, i.e 0 or 1. In PCM the message signal is represented by a sequence of coded pulses. This message is achieved by representing the signal in discrete form in both time and amplitude. Instead of pulse train PCM produces a series of numbers of digits. Each one of these digit binary codes represent the approximate amplitude of the signal sample at that instant. It is the standard form of digital audio in computers, compact discs, digital telephony and other digital audio applications.

**Basic Element of PCM**

****

**LPF**

This filter eliminates the higher frequency component present in the input analog signal which is greater than the highest frequency of the message signal

**Sampler**

This is the technique which helps to collect the sample data instantaneous value of message signal so as to reconstruct the original signal.

**Quantizer**

Quantization is the process of reducing the excessive bits and confining the data. It reduces the redundant bits and completes the value.

**Encoder**

The digitization of analog signals is done by an encoder; it represents each quantized level by a binary code. The sampling done here is by using samples and hold process. There are three sections, LPF samples quantizer will act as an analog to digital converter encoding to minimize the bandwidth used.

**Regenerative Repeater**

The section increases the signal strength and the output of the channel also has one regenerative repeater circuit which compensates the signal loss and reconstruction of the signal.

**Decoder**

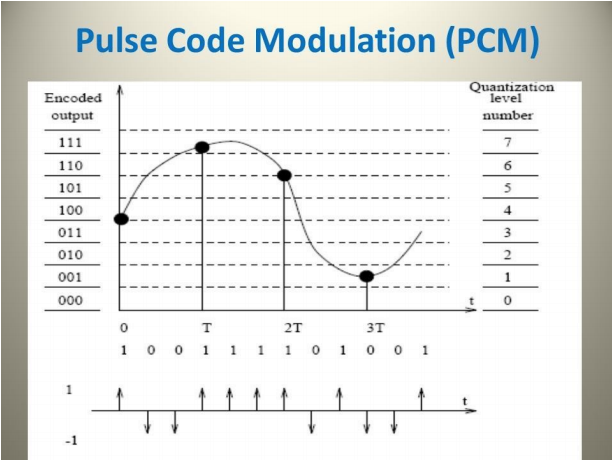
Decoder circuit decodes the pulse coded waveform to reproduce the original signal.

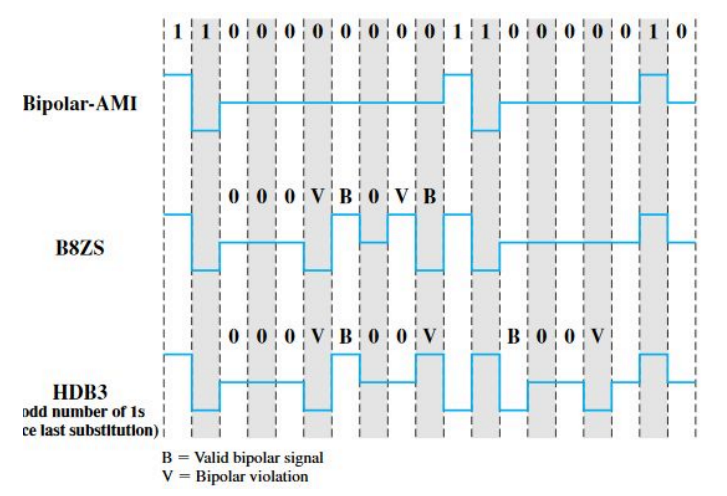
**Reconstruction Filter**

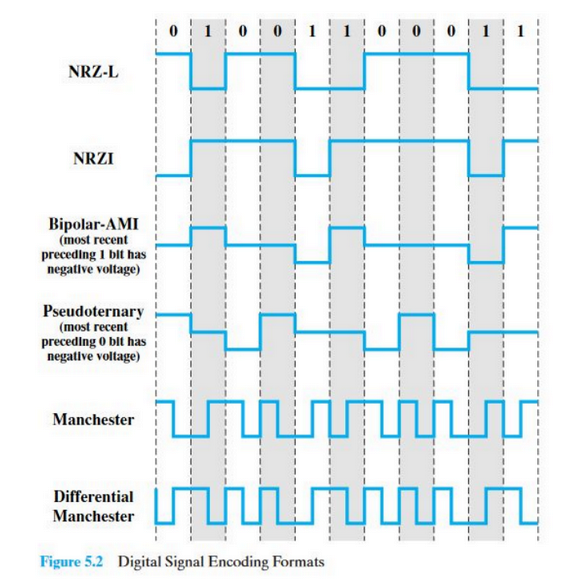
A LPF is employed to get back the original signal called reconstruction filter.

**Quantization**

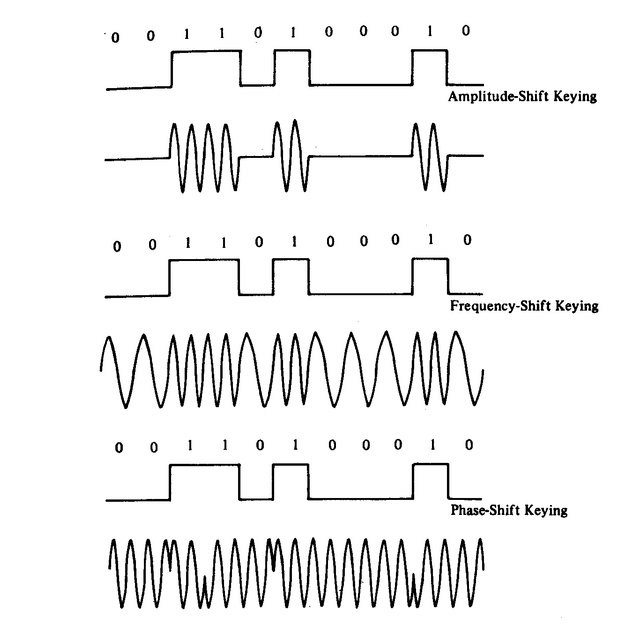
Quantization is the process of converting infinite no of possibilities to a finite no of possibilities to a finite no of condition. It is the process of round off. It converts the sampled signal into an approximated signal.







## **12.3 FSK, PSK, ASK**



**FSK**

Frequency Shift Keying (FSK) is a frequency modulation scheme (conveys information over a carrier wave by varying its instantaneous frequency) in which digital information is transmitted through discrete frequency changes of a carrier wave.

**PSK**

Phase Shift Keying (PSK) is a method of digital communication in which the phase of a transmitted signal is varied to transmit information. There are several methods that can be used to do PSK.

**ASK**

**Amplitude Shift Keying** is a type of Amplitude Modulation which represents the binary data in the form of variations in the amplitude of a signal.

Any modulated signal has a high frequency carrier. The binary signal when ASK modulated, gives a **zero** value for **Low** input while it gives the **carrier output** for **High** input.

**Signal-to-Noise ratio (S/N or SNR)**

In analog and digital communications, signal-to-noise ratio, often written S/N or SNR, is a measure of signal strength relative to background noise. The ratio is usually measured in decibels (dB) using a signal-to-noise ratio formula. If the incoming signal strength in microvolts is Vs, and the noise level, also in microvolts, is Vn, then the signal-to-noise ratio, S/N, in **decibels** is given by the formula:

***S/N = 20 log10(Vs/Vn)***

***S/N=20log10(As/Vn)***

***S/N=10log10(Ps/Pn)***

***Expressed in dB Where V=Voltage, A=Amplitude, P=Power, s=signal, n=noise.***

Example, suppose that Vs = 10.0 microvolts and Vn = 1.00 microvolt. Then:

S/N = 20 log10(10.0) = 20.0 dB

**Channel Capacity**

Shannon -Hartley theorem gives the maximum rate at which a signal can be transmitted over a specific bandwidth in presence of a noise.

The formula is

**Capacity = bandwidth \* log2(1 + SNR)**

**C = B \* log2(1+ S/N)**

where C is the achievable channel capacity, B is the bandwidth of the line( in **Hz or bits/second**, S is the average signal power and N is the average noise power.

For a typical telephone line with a signal-to-noise ratio of 30dB and an audio bandwidth of 3kHz, we get a maximum data rate of: **C = 3000 \* log2(1001)** which is a little less than 30 kbps.

For a satellite TV channel with a signal-to noise ratio of 20 dB and a video bandwidth of 10MHz, we get a maximum data rate of:

**C=10000000 \* log2(101)**

which is about 66 Mbps.