# DATA COMMUNICATIONS AND NETWORKING

**Transmission:**

The signals of data communication during transmission and reception may be in either analog or digital form. The digital signals travel from a communication device to the link via an **interface** or **line adapter** or **line driver**, while modems are used as an interface between a communication device and link for modulating signals (both analog and digital). These signals can be transmitted either serially or in parallel, depending on the type of transmission media being used.

**Serial Transmission:**

In this mode of transmission, message information is transmitted bit by bit over the link and the transmission speed of the transmitting site depends on the signaling speed. Both types of digital signals (data and control) are transmitted serially. The control signals are used for providing synchronization between two sites. The signaling rate is defined as the rate at which signaling per second is selected for the communication device and is usually expressed in baud. The time period of one signaling rate can be defined as the reciprocal of the baud. For example, if the signaling rate of a communication device is 300 baud, the time period of one signaling rate is 1/300 or .0033 sec. The communication circuit (containing electronic circuits like modulators/demodulators) must support the rapid change of the voltage levels (between logic 1s and 0s) during this time. The digital signal bits are sent during the signaling period. The number of bits to be transmitted during the signaling period could be one or more, depending on the signaling rate. If the number of bits (0s and 1s) during the signaling period is one, then the signaling rate is the same as that of the transmission speeds of bits/second (bps), but if the number of bits is more than one, then the baud may be more than the transmission speed of bps. The voltage values for describing logic 1s and 0s may be different depending on the signaling or coding methods used; e.g., we may have 0 and 5 volts ( in the case of TTLIC), -15 and 15 volts, or -3 and 3 volts ( in Ethernet LAN), etc.

**Parallel Transmission:**

In this transmission mode, each bit is assigned a specific, separate channel number and all bits are transmitted simultaneously over different channels. For every bit, a channel is defined. Thus for transmitting eight-bit data, eight channels are used. Both types of signals (data and control) are generated by different circuits and are also transmitted on different channels at the same time. The control signals provide synchronization between two sites and are sent on a separate channel to indicate different types of status (of transmitter and receiver) such as ready, busy, acknowledgement, etc. The number of data bits in the information to be sent by the data circuit defines the number of channel signals.

**Synchronous And Asynchronous Transmission**

One of the main problems with the transmission configurations (balanced or unbalanced) is the identification of characters being sent, and this problem becomes more serious in the case of serial configurations, as the bits are being sent continuously. On the receiving side, the node has to identify the bits for each of the transmitted characters. Further, the receiving node must be informed about the

transmission of data from the transmitting node. These nodes have to use some synchronizing bits between the characters, not only to identify the boundary of each character but also to provide synchronization between them.

In this mode of transmission, every character or symbol (expressed in ASCII or EBCDIC) is preceded by one "start" bit (spacing) and followed by one or more "stop" bit (marking) and is then transmitted over transmission channel. During the idle situation of the channel (no data is transmitted), logical 1s is constantly transmitted over the channel. The start bit indicates the receiver to activate the receiving mechanism for the reception, While the stop bit indicates the end of the present character or symbol. Due to this working concept, this mode of transmission is also known as start-stop transmission. The start and stop bits together provide synchronization between sending and receiving stations. This mode is very useful for sending text between terminals and computers asynchronously. The main advantage with this transmission is that it does not require any synchronization between sender and receiver.

**Simplex:**

In a simplex configuration, information always flows in one direction, similar to a radio broadcast system, one-way traffic system, etc. This type of operation usually depends on the characteristics of the computer/terminals being used and is independent of the characteristics of the communication link being used for the transmission. Examples are send-only terminals, receive-only terminals, etc.,

**Half-Duplex:**

A half-duplex configuration allows the transmission of a signal in one direction at a time. It usually depends on the characteristics of the terminals, data communication link, and modulation method, but it allows the transmission in only one direction at any time. The end of a signal in one direction is recognized by the other side, which may switch its mode to the transmission state. The turnaround and overhead time sometimes become serious problems and affect the throughput of the communication system. Typically, the turnaround time is in the range of 20-200 milliseconds and depends on propagation, capacitance, inductance, and resistance of the lines. The majority of the terminals offer half-duplex operations.

**Full-Duplex:**

A full-duplex configuration allows the transmission in both directions simultaneously. Since the turnaround time is eliminated (as the stations are not waiting for a response), the efficiency of the communication system is improved dramatically. Here we use two pairs of lines, and typically one pair of wires carries the data while another pair of wires carries the control signal. The operation depends on the characteristics of the communication devices being used. It is very useful in computer communication networks, especially with protocols of high-level data link layer control (HDLC), synchronous data link layer control (HDLC), synchronous data link layer control (SDLC), link access control - balanced (LAP-B), link access control -D channel (LAP-D), advanced data communication control procedures (ADCCP), digital data communication message protocol (DDCMP), and many other vendor-customized software.

**Front-End Processor:**

A specialized computer that performs the functions of line control, message handling, code conversion, and error control. The CPU does not have to perform these functions, thus making the system very fast. It provides asynchronous and/or synchronous ports for the system.

**Line Splitter:**

Usually, a line splitter is used at the exchange to provide the connection. By using a line splitter, one assigned line of exchange can be used by more than one location at the same time. That assigned line transmits information from a computer on the line to various terminals connected to different exchanges. Similarly, when these terminals want to transmit information, these are combined on that line and delivered to the computer. The point-to-point and multi-point connections can also be configured on leased lines using a line splitter.

**Multiplexing:**

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

As data and telecommunications usage increases, so does traffic. We can accommodate this increase by continuing to add individual lines each time a new channel is needed, or we can install higher-bandwidth links and use each to carry multiple signals. Today's technology includes high-bandwidth media such as optical fibre and terrestrial and satellite microwaves. Each of these has a bandwidth far in excess of that needed for the average transmission signal. If the bandwidth of a link is greater than the bandwidth needs of the devices connected to it, the bandwidth is wasted. An efficient system maximizes the utilization of all resources; bandwidth is one of the most precious resources we have in data communications. In a multiplexed system, n lines share the bandwidth of one link. The four lines on the left direct their transmission streams to a **multiplexer (MUX)**, which combines them into a single stream (many to one). At the receiving end, that stream is fed into a **Demultiplexer (DEMUX)**, which separates the stream back into its component transmissions (one to many) and directs them to their corresponding lines.

The word link refers to the physical path. The word channel refers to the portion of a link that carries a transmission between a given pair of lines. One link can have many (n) channels.

Signals are multiplexed by one of three basic techniques: frequency-division multiplexing (FDM), wave division multiplexing (WDM), and time-division multiplexing (TDM). The first two are techniques used for analog signals: the third for digital signals.

**TYPES OF MULTIPLEXING**

**1. Frequency Division Multiplexing (FDM)**

Frequency-division multiplexing is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signal travel. Channels must be

separated by strips of unused bandwidth (guard bands) to prevent signals from overlapping. In addition, carrier frequencies must not interfere with the original data frequencies. Failure to adhere to either condition can result in the unsuccessful recovery of the original signals.

**2. Wave Division Multiplexing (WDM)**

Wave-division multiplexing (WDM) is designed to use the high data rate capability of fiber-optic cable. The optic fiber data rate is higher than the data rate of metallic transmission cable. Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to connect several lines into one.

WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals transmitted through fiber-optic channels. The idea is the same: We are combining different signals of different frequencies; however, the difference is that frequencies are very high.

**3. Time Division Multiplexing (TDM)**

Time-Division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a link. Instead of sharing a portion of the bandwidth as in FDM, time is shared; each

connection occupies a portion of time in the link.

The data flow of each connection is divided into units, and the link combines one unit of each connection to make a frame. The size of the unit can be 1 bit or several bits. For n input connections, a frame is organized into minimum of n time slots, each slot carrying one unit from each connection.

**4. Inverse Multiplexing**

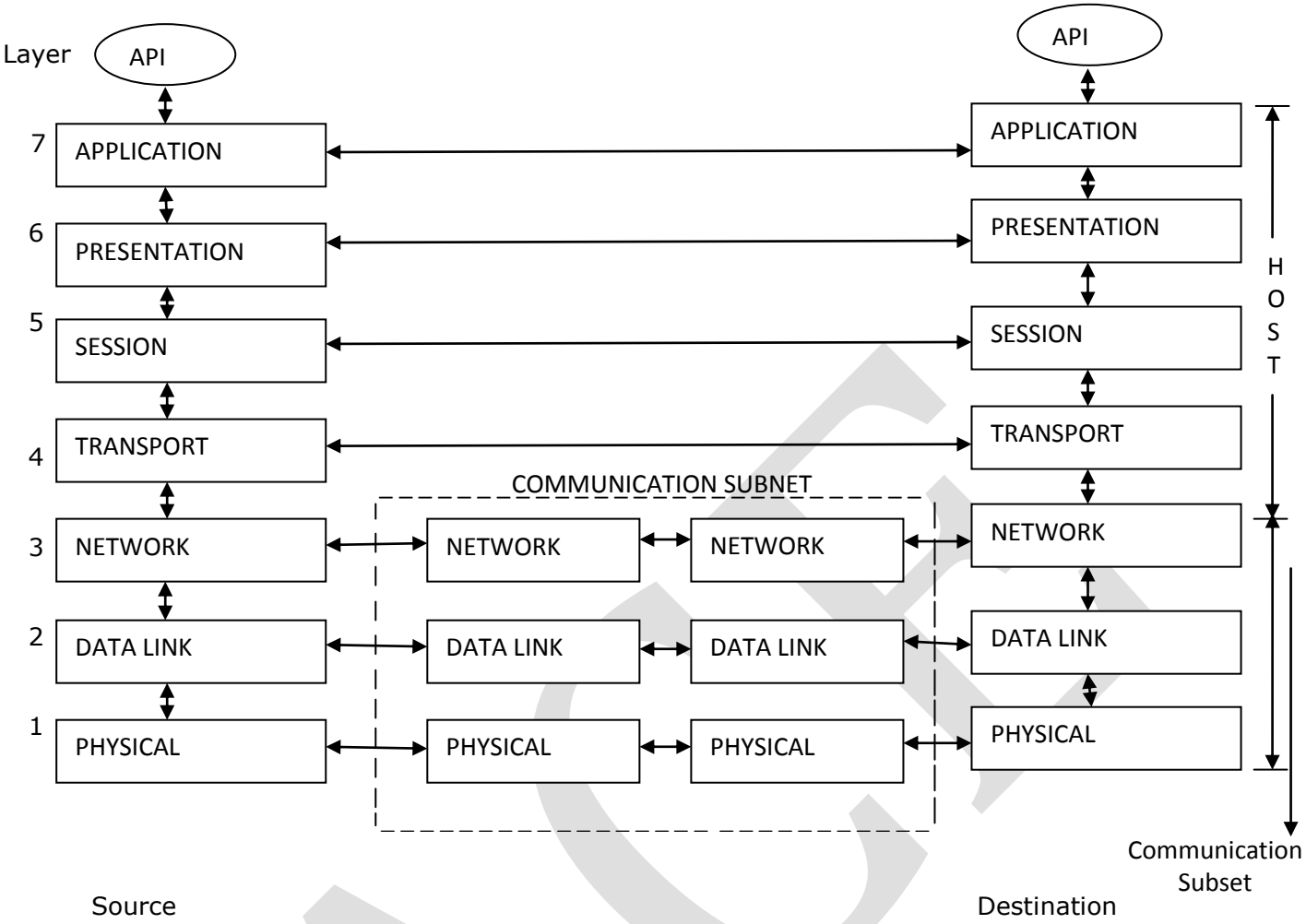
As its name implies, **inverse multiplexing** is the opposite of multiplexing. Inverse multiplexing takes the data stream from one high-speed line and breaks it into portions that can be sent across several lower-speed lines simultaneously, who no loss in the collective data rate.

**OSI MODEL**

The international standard defines a model composed of different layers (open system interconnection). It does not define any services or protocols for OSI but, instead, provides a framework for coordinating the development of various standards for interconnecting different systems. According to OSI, a system is defined as a collection of computers with their associated software and attached peripheral devices configured so that the information can be transferred across its connected devices. Obviously, a system which confirms to the OSI reference model is known as an open system.

**Physical layer**

The physical layer is mainly concerned with electrical, mechanical, procedural, and functional aspects of transmission media for information transmission and receiving over the network. It specifies the details of connecting cables, processing of digital signals, interfaces to different media, etc. the most popular standard for this layer of digital network interfaces X.21 (CCITT). Other standards for this layer include V.24 (CCITT) and RS-232 DCE/DTE interface (Electronics Industries Association (EIA)).




**Data link layer**

The data link layer is responsible for maintaining the integrity of data information between two sites. It offers a reliable channel for data transmitted over the transmission media. The protocols of this layer provide error recovery (error detection and error correction) to handle the errors caused by noisy media.

**Network layer**

The network layer provides communication between the user's PC and public or private networks. It defines addressing and routing (logical link) between source and destination sites. It also provides internet routing between two remote sites. This layer also makes sure that data packets are transmitted across the network correctly. X.25 is a standard for this layer; other proprietary networks providing an equivalent layer to this layer include IBM's SNA and DEC's DNA.

**Transport layer**

The transport layer offers network-independent service to higher layers and hides all details regarding the network being used for transmission. The upper layers have no idea about the type of network which is transmitting or receiving the data information. This layer breaks the message into smaller packets and provides the segmentation and reassembly, it also offers end-to-end error control and recovery.

**Session layer**

The session layer provides a session for data communication between two application processes. It also supports the synchronization between sites and defines checkpoints from which diagnostic tests can be performed in the event of failure. It establishes the length of the session during which users log in and log out.

**Presentation layer**

The presentation layer represents the data information in appropriate form to be acceptable to the lower layers of the network. Two standard representation schemes for character representation are ASCII (plain text) and EBCDIC (IBM plain text), which are usually supported by most of the networks. The presentation layer provides different formatting styles to the data information and associated compatibility between various cooperating processes. It also convert the information (bit stream) into video, audio, and other formats. All the application entities of the application layer are also translated or mapped into suitable entities by this layer.

**Application layer**

The application layer provides an interface between application entities and the user's computer. This layer offers services to a variety of aspects of data communication between the user's computer and application entities including terminal handling, file handling, text interchange, job transfer, and manipulation. For each of these aspects, a number of standards have been defined, and a collection of these standards is known as the specific application service elements (SASE). Within each of these aspects of application, quite a number of standards have been defined and are continuously being defined to cater to different upcoming applications from various technologies. For example, a large number of terminal handling standards have been defined, such as basic class, form, graphics, and images. The application layer offers a variety of applications such as e-mail, data transfers, file transfer, digitized video, audio, data, remote login, and other Internet services.

**Piggybacking**

Piggybacking is a bi-directional data transmission technique in the network layer (OSI model). It takes the most of the sent data frames from receiver to emitter, adding the confirmation that the data frame sent by the sender was received successfully (ACK acknowledge). This practically means, that instead of sending an acknowledgement in an individual frame it is piggy-backed on the data frame.

**Poll And Select**

This technique is basically used in a master-slave configuration of a distributed network system. The primary node in the system polls for a secondary nodes to respond. Based on the responses from secondary, the primary selects one node to communicate with. This technique is based on the concept of poll and select.

**Automatic Repeat Request (ARQ)**

Most protocols for the data link layer support error detection and error recovery over a transmission line or link. This error-control technique provides error recovery after the error is detected by ARQ at the receiving site, the receiver requests the sending site to retransmit the protocol data unit

(PDU). The combination of error detection and error recovery results in a reliable data link. Three versions of ARQ have been defined: Stop-and-wait ARQ, Go-back-N, and Go-back-selective.

**(i) Stop-and-wait ARQ:** A sending station sends a frame (protocol data unit) to the destination station and waits until it receives an acknowledgement from the destination station. This means that there can be only one frame over the channel at any time.

**(ii) Go-back-N ARQ:** A sending station sends more than one frame which is controlled by the upper limit of the maximum value. If an error is detected in any frame (when an acknowledgement arrives at the sending station) or the acknowledgement is lost or it is timed out, in all three cases, the sending station will retransmit the same frame until it is received error free on the receiving side. All the frames behind the error frames are discarded and hence have to be retransmitted.

**(iii) Go-back-select ARQ:** This version of ARQ is similar to Go-back-N-ARQ, with the only difference being that here the frames behind the error frame are stored in a buffer at the receiving site (as opposed to discarding in Go-back-N ARQ) until the error frame is received error free.

**INTERFACING**

Most digital data-processing devices have limited data-transmission capability. Typically, they generate a simple digital signal, such as NRZ-L, and the distance across which they can transmit data is limited. Consequently, it is rare for such a device (terminal, computer) to attach directly to a transmission or networking facility.

The devices we are discussing, which include terminals and computers, are generally referred to as data terminal equipment (DTE). A DTE makes use of the transmission system through the mediation of data circuit-terminating equipment (DCE). An example of the latter is a modem.

There are various international standards for the physical layer interface (commonly known as DTE/DCE interface) on the network market. The most common and important interfaces are EIA RS-232, EIA RS-530 (with RS-422-A and 423-A), and X.21.

**EIA RS-232 DTE/DCE interface**

The Electronic Industry Association $(\mathrm{EIA})^{9}$ has defined the RS-232 standard interface of the DTE with DCE which is connected to the analog public telephone system. Since these lines or related lines with telephone requirements and specifications are nowadays heavily used for data communication. The RS-232 DTE/DCE interface supports both transmission (synchronous and asynchronous) schemes for data communication and can also be used for other types of interfacing. It contains a 25-pin, D-shaped connector which can be easily plugged into the modem socket and which is also known as a DB-25 connector.

**EIA RS-232-D DTE/DCE interface**

The RS-232-D $interface^{9}$ provides all functions (described earlier) for establishing connection between DTE and DCE, namely, initialization of the interconnection circuit for establishing the link between DTE and DCE, transmission of data and control across the circuits, timing and control signals to provide synchronization between them, maintenance and controlling of data transfer between them, etc. it establishes an unbalanced connection between DTE and DCE, and, as such, voltages and currents flow through the ground circuits in one direction and return through the ground (return path). Their values are defined with respect to the ground (which is common to both transmitting and

receiving circuits at two nodes). Further, the RS-232-D always establishes a circuit for data transmission in only one direction at a time; hence, it supports half duplex operation. All the signals (data, control, timing, etc.) flow through the same circuit(primary). If we can provide a second circuit (secondary at lower speed) between DTE and DCE, then full-duplex operation can also be supported by RS-232-D.

**EIA RS-232-C DTE/DCE interface**

The RS-232-C interface, now renamed RS-232-D, defines the electrical and mechanical characteristics of the interface between the DTE and the DCE using serial binary communication. In this version of the interface, the prefix D (after the interface was renamed RS-232-D), in fact, indicates its conformance with CCITT V.24, V.28, and ISO 2110.

The RS-232-C interface has the following characteristics:

- Most common DTE/DCE interface
- One of the most successful standards
- Unbalanced electrical transmission
- Bipolar 3-25 V
- 50 ft maximum data rate
- 20-kbps maximum data rate
- 21 interchange circuits
- Data
- Control
- Timing
- 25-pin connector

**RS-449 (RS-422-A and RS-423-A) interface**

As mentioned above, the RS-232 interface can be used for only a limited distance (less than 15 m) with a maximum speed of 20 kbps due to noise (ground looping currents, shielding, capacitances, inductance, etc.,). In addition to these factors, the quality and reliability of the circuit also affect the actual data rate. A new standard known as an RS-449 (RS-442-A and RS-423-A) interface overcomes this problem by using different distance electrical circuits RS-422-A (balance circuit) and RS-423-A (unbalanced circuit) between DTE and DCE, making it useful for a longer distance with a higher data rate (up to 2.5 Mbps).

The RS-449 interface 12 has the following characteristics:

- A new family of physical interface (DTE/DCE) standards
- Defined by RS-449, RS-422-A, and RS-423-A
- RS-44912
- Defines mechanical, functional, and procedural functions
- Has 30 interchange circuits
- Has 37-pin connector (uses ISO 4902 mechanical connector) (Figure 10.7(a))
- Offers a bit rate up to 2.5 Mbps
- Has plan for transition from 232-C and 232-D

- Compatible with CCITT V.24, CCITT V.54, CCITT X.21 bits
- RS-422-A10
- Compatible with X.27
- Balanced electrical transmission
- Can be used for a distance of up to 1.5 km
- 100-kbps data rate at 1.5-km distance
- 10-Mbps data rate at 15km

**USER DATAGRAM PROTOCOL**

The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite, the set of network protocols used for the internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths. The protocol was designed by David P.Reed in 1980 and formally defined in RFC 768

A number of UDP's attributes make it especially suited for certain applications.

- It is transaction-oriented, suitable for simple query-response protocols such as the Domain Name System or the Network Time Protocol
- It provides datagrams, suitable for modeling other protocols such as in IP tunneling or Remote Procedure Call and the Network File System.
- It is simple, suitable for bootstrapping or other purposes without ba full protocol stack, such as the DHCP and Trivial File Transfer Protocol.
- It is stateless, suitable for very large numbers of clients, such as in streaming media applications for example IPTV
- The lack of retransmission delays makes it suitable for real-time applications such as Voice over IP, online games, and many protocols built on top of the Real Time Streaming Protocol.
- Works well in unidirectional communication, suitable for broadcast information such as in many kinds of service discovery and shared information such as broadcast time or Routing Information Protocol

**Datagram:** A datagram is a basic transfer unit associated with a packet-switched network in which the delivery, arrival time, and order of arrival are not guaranteed by the network service.

**Structure of a datagram:** Each datagram has two components. A header and a data payload. The header contains all the information sufficient for routing from the originating equipment to the destination without relying on prior exchanges between the equipment and the network. Headers may include source and destination addresses as well as a type field. The payload is the data to be transported. This process of nesting data payloads in a tagged header is called encapsulation.

**Use in the Internet Protocol:** The Internet protocol defines standards for several types of datagrams.

Datagram service is a service provided by IP at the Internet layer. It is a connectionless, best effort, unreliable, message delivery services. Many higher level protocols including TCP (a connection –

oriented services) depend on IP's Datagram service, laying additional functionality on top. UDP uses IP's Datagram service as well.

The term datagram is often considered synonymous to packet but there some nuances. The term datagram is generally reserved for packets of an unreliable service that does not notify the user if delivery fails, while the term packet applies to any message formatted as a packet. For example, Internet Protocol (IP) provides an unreliable service and UDP packets are generally called datagrams.

If a datagram fragments, then its fragments may be referred to as packets, but not as datagrams. [4] TCP refers to its fragments as TCP segments, not packets [5] presumably to distinguish them from unreliable fragments.

**MODULATION**

Modulation is an operation which translates a modulating signal (corresponding to information or message) into another signal using a constant carrier signal of high frequency. The modulation supports adaptation (to any unfavourable atmospheric conditions, noisy environment, etc.) for high quality of reception of the signals and allows multiple transmissions of signals over a common transmission medium simultaneously. Demodulation or detection is also a nonlinear process, although we might use linear circuits for linear zing due to obvious reasons (linear circuits offer stable response and inexpensive and less complex than these processes).

One of the main advantages of the modulation process is that it overcomes noises and can transmit the signal over a larger distance and, hence, offers a good quality of transmission. Further, several sub channels can be transmitted over the communication link via another process termed multiplexing

There are two main classes of modulation techniques:

- Analog modulation (AM)
- Digital Modulation (DM)

**Analog Modulation**

Analog modulation can be defined as either analog or digital, depending on (1) the carrier waveform (sinusoidal or pulse), (2) the type of transmission (analog or digital), and (3) the type of modulation based on change of parameters (amplitude, frequency, phase of modulating signal). For digital data communication, analog modulation requires the digital data to first be converted to analog before the modulated signal is transmitted.

**Analog Modulation for analog signals**

An analog signal can be described by three main parameters or basic characteristics: amplitude, frequency, and phase in time domain, and, accordingly, we have three modulation techniques:

- Amplitude modulation
- Frequency modulation
- Phase modulation

**Amplitude Modulation (AM)**

This is one of the earliest forms of modulation and one of the most commonly used modulation techniques. In this modulation, the amplitude of a carrier signal is changed in accordance with the

instantaneous value of lower-frequency modulating signals. The AM process generates a modulated signal which has twice the bandwidth of the modulating signal. It is obtained by multiplying a sinusoidal information signal with a constant term of the carrier signal, and this multiplication produces three sinusoidal components: **carrier, lower sideband,** and **upper sideband.** The bandwidth of each sideband is the same as that of the modulating signal. A standard AM signal is considered to be highly inefficient for radio frequency (RF) power to send the information through signals. In spite of this problem, AM is popular due to the ease with which AM signals can be demodulated or detected.

**Frequency modulation (FM)**

In this modulation process, the carrier frequency changes in accordance with an instantaneous value of the base band modulating (carrier amplitude remains unchanged) Due to immunity to noises, FM is used for high-fidelity commercial broadcasting (FM radios). The immunity to noise can in fact be seen only at the receiving side, as the demodulation process maintains the amplitude of the signal at the constant value. The FM process contains a large number of sidebands and defines amplitude of modulating signals as derivation of carrier signal from allotted centre frequency. (This is usually controlled by the FCC in the U.S.; in other countries, it is controlled by respective government agency.) For example, a carrier frequency range of any commercial broadcasting station cannot be more than 150 KHz; i.e., frequency deviation of each side of the centre frequency will be 75 KHz. If we have a modulating frequency of, say, 20 KHz, the channel bandwidth of that station for the broadcasting may be around 200 KHz. This modulation process is very useful for radio-frequency (RF) transmission over wireless communication links (e.g., microwave link, satellite link, etc.) and can utilize the link bandwidth effectively by multiplexing the frequencies of a few gigahertzes with a bandwidth of transmission in the range of 4 to 6MHz.

**Phase modulation (PM)**

In this type of modulation, the phase of the carrier signal varies linearly according to the instantaneous value of the base band modulating signal. The instantaneous frequency deviation is proportional to the derivative of the modulating signal.

These two types of modulation are collectively considered angular modulation. Features of angular modulation include

- Noise immunity at high modulation index.
- Larger available bandwidth than AM and available at all times.

In applications where a stable frequency of carrier signal is required (e.g., telemetry, fixed bandwidth transmission, etc.,). The phase modulation is preferred over the frequency modulation. This requires the transmitter to generate a stable frequency of the carrier thus making the transmitter more complex and expensive. In a way, this helps during the demodulation process at the receiving side, as the frequency of the carrier signal is stable.

**MODEM**

An interface between devices which need to share data across the network; generally consists of a transmitter and receiver. It transmits data from computer/ terminal connected to one side of the modem, while the other side is connected to the telephone line. It changes the characteristics of

signals so that it is compatible with the telephone channel. Two main types of basic modems have been defined as asynchronous and synchronous to support appropriate transmission modes.

**Quick-Pack**

Uses a data compression algorithm to increase throughput by converting the baud rate of the host to a slower modem. It allows the PC to send the data at a normal rate of 9600 bps and adjusts this rate to the transmission rate of a 1200/2400 dial-up modem automatically. In other words, it maps the 9600-bps data rate of a PC to match the slower dial-up modem rates of 1200/2400 bps. This modem product uses a standard ACT data compression technique. A typical connection using this unit is shown in Figure 3.15 (A). It supports asynchronous transmission (ASCII) and full duplex and is compatible with different classes of MNP (microcosm network protocol).

**Microcom Network Protocol (MNP)**

MNP is an error-correcting communications protocol for asynchronous data (interactive and file transfer applications). It can be used over dial-up lines via 1200/2400-bps modems. It conforms to OSI model's data link layer (for providing reliable data transfer). Traditional modems cannot provide error-free data transfer because the transmission includes noise and distortions introduced by voice-grade telephone circuits. This protocol has become the de *facto* standard of the industry. It has defined five versions (classes) of protocols, and each version or class of MNP interacts with each other and offers efficient operations over the media.

- **Class I:** uses an asynchronous byte-oriented block method of data exchange. It is seldom used.
- **Class II:** adds full duplex and offers throughput of 2000 bps from 2400-bps modems.
- **Class III:** uses a synchronous bit-oriented full duplex data packet. It eliminates start and stop bits and offers throughput of 2600 bps from 2400-bps modems.
- **Class IV:** adds adaptive size packet assembly and data phase packet format optimization and offers 2900 bps from 2400-bps modems.
- **Class V:** adds data compression, which uses a real-time adoption algorithm to compress the data and offers 4800 bps from 2400-bps modems.

**BELL MODEMS**

Bell modems are very popular widely accepted in North America and other countries. In fact, physical layer specifications in North America are defined on the basis of Bell modem specifications. For automatic dial-and-answer modems, Bell 103/212A specifications are widely used by different vendors, while Bell 103, 113, 201 C , 208 A/B, and 212 A specifications have been adopted by many manufacturers. Each of these modems has different data rates and baud rates and use different types of modulation techniques.

**TYPES OF MODEMS**

**Low-speed modems**

The maximum data rate of these modems is 600 bps and can be used over voice-grade, dial-up, or private lines for unlimited distances. These modems, in general, use frequency shift keying (FSK). The sender modem usually uses low frequency values for 1 and 0, while the receiver modem uses

higher frequency values for its 1 and 0 to send acknowledgement to the sender, as shown figure 3.17. The low-speed modems are useful for keyboard terminals. These modems are compatible to CCITT V 21.

**Medium-speed modems**

These modems provide data rates between 1200 and 3600 bps and can be used for the same applications as those of low-speed modems. These modems also use frequency shift keying (FSK) and support a bit rate in the range of 1200-3600 bps; however, 1200 bps is very common.

**High-speed modems**

These modems are used for the same applications as low-speed and medium-speed modems. These are very popular with the RS-232 physical layer interface. The transmission bit rate is between 4800bps and 19.2 kbps.

**Wide-band modems**

These modems are use more than one transmission line to send the data. The bit rate of each line is added to provide the total bit rate of over 19.2 kbps on each side of the telephone line.

**Null modem**

Asynchronous devices (mainframes, terminals, PCs, printers) may be connected by a modem eliminator (eliminating the use of a pair of modems). The devices are connected by cables. The null modem (crossover) cable includes both modem and cable and can support a length of 15m for local applications. The cable is usually immune to noises and is not available for a higher distance than the standard 15m.

**INTEGRITY**

Integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, either accidental or malicious. As more and more monetary exchanges occur over the Internet, integrity is crucial. For example, it would be disastrous if a request for transferring $100 changed to a request for $10,000 or $100,000. The integrity of the message must be preserved in a secure communication.

**TOKEN PASSING**

In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a predecessor and a successor. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.

In this method, a special packet called a token circulates through the ring. The possession of the token gives the station the right to access the channel and send its data. When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round. In this process, when station receives the token and has no data to send, it just passes the data to the next station.

Token management is needed for this access method. Stations must be limited in the time they can have possession of the token. The token must be monitored to ensure it has not been lost or destroyed. For example, if a station that is holding the token fails, the token will disappear from the network. Another function of token management is to assign priorities to the stations and to the types of data being transmitted. And finally, token management is needed to make low-priority stations release the token to the higher priority stations.

**LOGICAL RING**

In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one.

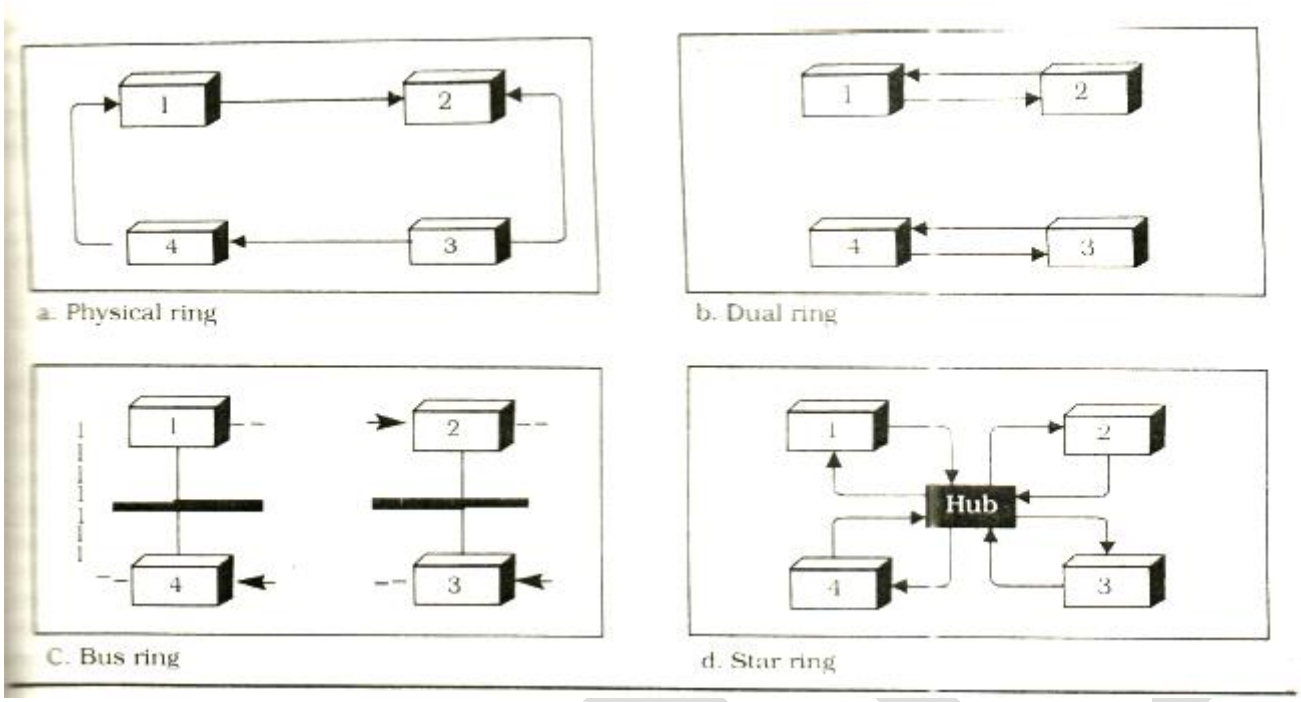
Logical ring and physical topology in token-passing access method

In the physical ring topology, when a station sends the token to its successor, the token cannot be seen by other stations; the successor is the next one in line. This means that the token does not have to have the address of the next successor. The problem with this topology is that if one of the links-the medium between two adjacent stations fails, the whole system fails.

The **dual ring** topology uses a second (auxiliary) ring which operates in the reverse direction compared with the main ring. The second ring is for emergencies only( such as a spare tire for a car). If one of the links in the main ring fails, the system automatically combines the two rings to form a temporary ring. After the failed link is restored, the auxiliary ring becomes idle again. Note that for this topology to work, each station needs to have two transmitter ports and two receiver ports. The high-speed Token Ring networks called FDDI (Fiber Distributed Data Interface) and CDDI (Copper Distributed Data Interface) use this topology.

In the bus ring topology, also called a **token bus,** the stations are connected to a single cable called a bus. They, however, make a logical ring, because each station knows the address of its successor (and also predecessor for token management purposes). When a station has finished sending its data, it releases the token and inserts the address of its successor in the token. Only the station with the address matching the destination address of the token gets the token to access the shared media. The Token Bus LAN, standardized by IEEE, uses this topology.

In a **Star ring** topology, the physical topology is a star. There is a hub, however, that acts as the connector. The writing inside the hub makes the ring; the stations are connected to this ring through the two wire connections. This topology makes the network less prone to failure because if a link goes down, it will be bypassed by the hub and the rest of the stations can operate. Also adding and removing stations from the ring is easier. This topology is still used in the Token Ring LAN designed by IBM.




**REPEATER**

A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern. The repeater then sends the refreshed signal. A repeater can extend the physical of a LAN.

A repeater does not actually connect two LANs; it connects two segments of the same LAN. The segments connected are still part of one single LAN. A repeater is not a device that can connect two LANs of different protocols.

A repeater can overcome the 10Base5 Ethernet length restriction. In this standard, the length of the cable is limited to 500 m. To extend this length, we divide the cable into segments and install repeaters between segments. Note that the whole network is still considered one LAN, but the portions of the network separated by repeaters are called segments. The repeater acts as a two-port node, but operates only in the physical layer. When it receives a frame from any of the ports, it regenerates and forwards it to the other port.

It is tempting to compare a repeater to an amplifier, but the comparison is inaccurate. An amplifier cannot discriminate between the intended signal and noise; it amplifies equally everything fed into it. A repeater does not amplify the signal; it regenerates the signal. When it receives a weekend or corrupted signal, it creates a copy, bit for bit, at the original strength.

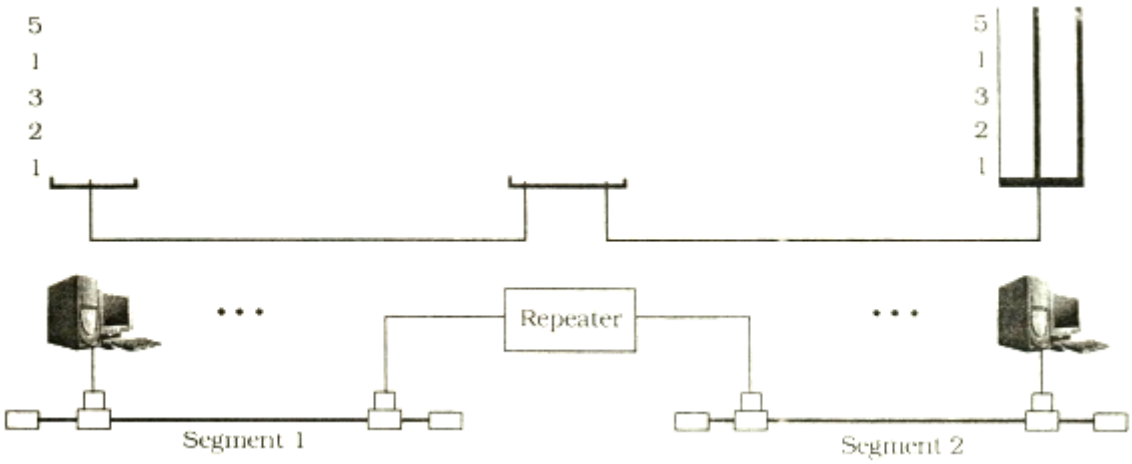
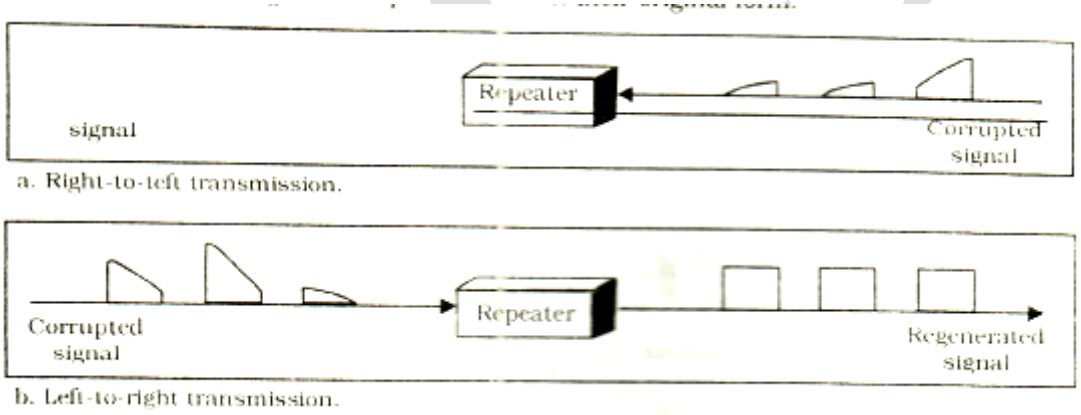



**Figure: A Repeater Connecting Two Segments of a LAN**

The location of a repeater on a link is vital. A repeater must be placed so that a signal reaches it before any noise changes the meaning of any of its bits. A little noise can alter the precision of a bit's voltage without destroying its identify if the corrupted bit travels much farther, however, accumulated noise can change its meaning completely. At that point, the original voltage is not recoverable, and the error needs to be corrected. A repeater placed on the line before the legibility of the signal becomes lost can still read the signal well enough to determine the intended voltage and replicate them in their original form.

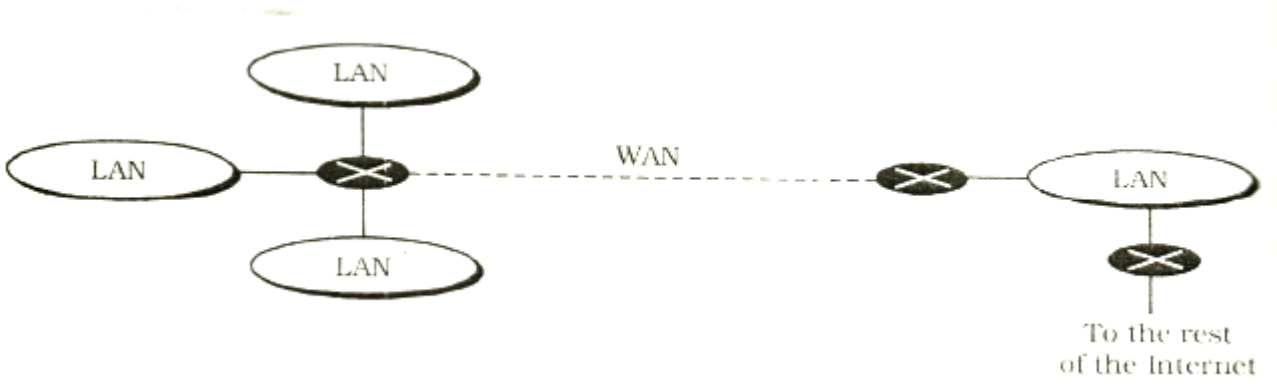



**ROUTER**

A router provides interconnection between two different networks. The router, an internetworking unit (device), is compatible with the three lower layers. Unlike bridges, it supports at least three lower layers. Unlike bridges, it supports at least three physical links (in general, it supports other links, too). This device is similar to a bridge for interconnecting different LANs, except that it is used in other types of networks such as WANs FDDIs, and other high-speed networks. It operates at the network layer. It can be used to connect LANs to WANs, MANs to WANs, LANs to LANs, and so on. A message frame transmitted over a LAN goes to all the nodes. At the network layer, hardware devices do the routing for sending a frame to other connected networks. By looking at the address defined in the frame, each node determines if the frame belongs to it. If so, the router accepts this frame.

The router defines the route for a frame to be transmitted to a destination. It is possible that the router will define more than one route for any frame to a destination, and the frame has to go through a number of routers. Each frame must contain two addresses: the destination address and the

address of the next node along the route. The second address changes as it moves from one router to another. The routing strategies deal basically with the determination of the next node to which the frame must be sent. Routers are most commonly used for interconnecting networks from a single vendor or interconnecting networks which are based on the same network architecture. Here, the physical and data link layer protocols may be different, but higher-layer protocols must be the same.




**GATEWAY**

A gateway is used to interconnect different networks and, as such, must offer high-level protocol conversion. It must offer message format conversion, as messages from different networks have different formats, sizes, and coding. it must provide address translation, as different networks use different addressing schemes. Finally, because these networks are using a different set of protocols for their layers, the gateway must provide conversions for different functions (implemented differently in different networks), such as flow control, error control, and error recovery. Since gateways provide interconnection between different networks, they are flexible, expensive, and complex. The conversions of protocols have to be performed on the basis of layers.

A gateway provides interface between two different networks having different protocols and provides mapping between their protocols. It operates at layer 7 of OSI-RM. Typically, a PC may be connected through a gateway to a mainframe or other computer having different protocols so that the packets can be sent to it and the mainframe resources can be used.

For an incoming packet, a gateway determines the output link. It offers connection-oriented configuration-based protocols (like X.25), and the decision to route the packets is made only after the connection is established. It defines an internal path during the duration of a call. In the case of connectionless service, the address of every incoming packet must be examined. Routing determination makes routing strategies and its processing cause overhead over connection-oriented configurations. Since it operates at the network layer, it can easily transform or map the address of one LAN to another one, making it slower. This device for internetworking is usually used in WANs, where response time is slow and it is not required to handle more than 10,000 packets per second. Internetworking between dissimilar LANs can be defined for both connection-oriented and connectionless services. A gateway connected between the Internet and the network of the destination (target network) receives the Internet e-mail and forwards it to the destination. As said earlier, the message is broken into IP packets. The gateway receives it and uses TCP to reconstruct the IP packet

into the complete message. It then provides mapping to the message into the protocol being used at the destination.

**BRIDGE**

A bridge operates in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) address (source and destination) contained in the frame.

A bridge has filtering capability. It can check destination address of a frame and decide if the frame should be forwarded or dropped. If the frame is to be forwarded, the destination must specify the port. A bridge has a table that maps addresses to ports.

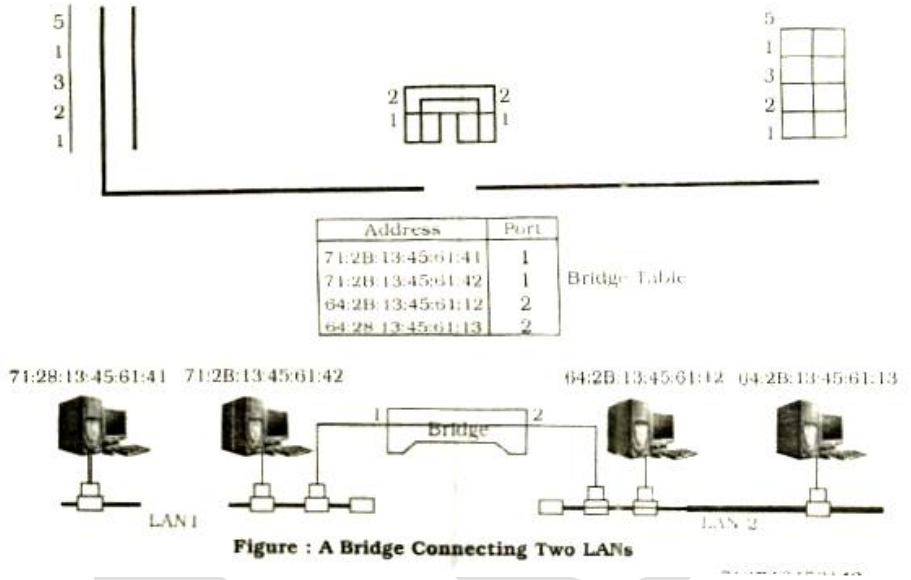



**Figure : A Bridge Connecting Two LANs**

Example shows two LANs are connected by a bridge. If a frame destined for station 712B13456142 arrives a port 1, the bridge consults its table to find the departing port. According to its table, frames for 712B13456142 leave through port 1; therefore, there is no need for forwarding, and the frame is dropped. On the other hand, if a frame for 712B13456141 arrives at port 2, the departing port is port 1 and the frame is forwarded. In the first case, LAN2 remains free of traffic; in the second case, both LANs have traffic. In our example, we show a two-port bridge; in reality a bridge usually has more ports.

**HUB**

**Passive Hubs:**

A passive hub is just a connector. It connects the wires coming from different branches. In a star topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point. This type of a hub is part of the media; its location in the Internet model is below the physical layer.

**Active Hubs**:

An active hub is actually a multipart repeater. It is normally used to create connections between stations in a physical star topology. We have seen examples of hubs in some Ethernet implement-actions (IOBase-T, for example). However, hubs can also be used to create multiple levels of hierarchy; the hierarchical use of hubs removes the length limitation of IOBase-T (100 m).

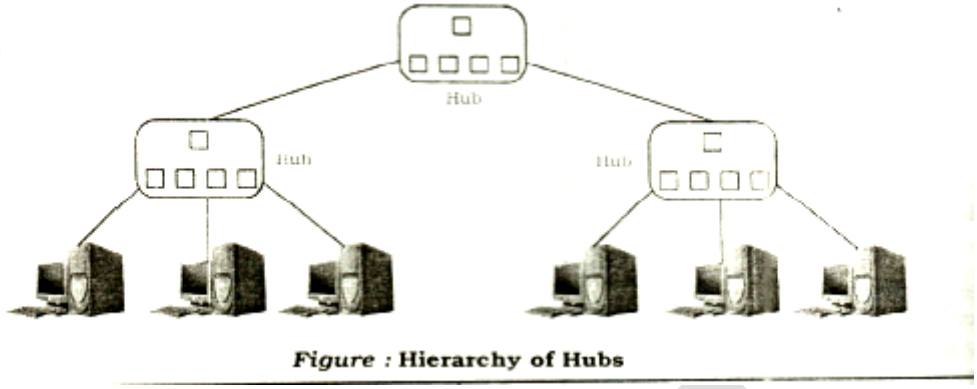



*Figure :* **Hierarchy of Hubs**

**Handshaking**

In information technology, telecommunications, and related fields, handshaking is an automated process of negotiation, that dynamically sets parameters of a communications channel established between two entities before normal communication over the channel begins. It follows the physical establishment of the channel and precedes normal information transfer.

It is usually a process that takes place when a computer is about to communicate with a foreign device to establish rules for communication. When a computer communicates with another device like a modem, printer, or network server, it needs to handshake with it to establish a connection.

Handshaking can be used to negotiate parameters that are acceptable to equipment and systems at both ends of the communication channel, including, but not limited to, information transfer rate, coding alphabet, parity, interrupt procedure, and other protocol or hardware features. Handshaking is technique of communication between two entities.

A simple handshaking protocol might only involve the receiver sending a message meaning "I received your last message and I am ready for you to send me another one." A more complex handshaking protocol might allow the sender to ask the receiver if he is ready to receive or for the receiver to reply with a negative acknowledgement meaning "I did not receive your last message correctly, please resend it" (e.g. if the data was corrupted en route).

**Common Types of Handshakes:**

Three way handshake

Establishing a normal TCP connection requires three separate steps:

1. The first host ('A') sends the second host ('B') a "synchronize" (SYN) message, which Bob receives.
2. 'B' replies with a synchronize-acknowledgement (SYN-ACK) message, which 'A' receives.
3. 'A' replies with an acknowledgement message, which 'B' receives, and doesn't need to reply to.

In this setup, the synchronize messages, act as service requires from one server to the other, while the acknowledgement messages return to the requesting server to let it know the message was received.

**ACID**

In computer science, ACID (atomicity, consistency, isolation, durability) is a set of properties that guarantee that database transactions are processed reliably. In the context of databases, a single logical operation on the data is called a transaction. For example, a transfer of funds from one bank account to another, even though that might involve multiple changes (such as debiting one account and crediting another), is a single transaction.

******* IACE *******