CSC 418: COMPUTER NETWORK & COMMUNICATION (3 CREDIT UNITS)

COURSE CONTENT

Introduction, Evolutionary trends of computer networks, computer network topology: Tree, Bus, Star, Ring and Hybrid. Measure of communication, channel characteristics, transmission media, noise and distortion, modulation and demodulation, multiplexing: TDM, FDM, and FCM. Parallel and serial transmission, Data switching techniques, Computer network Examples and design consideration, Open System Interconnection, Protocols, Standards and Controls, Description of network e.g. ARPANET, etc

INTRODUCTION

In the past, messages were carried using basic methods, for example, by runners or carrier pigeons. This was adequate for distances and data rates of the age. Nowadays, people communicate with each other using modern communication systems which are based on electrical communication. Such a technology allows the transmission of signals over very long distances at very high speeds. Examples of electronic communication systems are: telephones, TVs, mobiles, faxes, computer networks, etc.

A network is a set of devices, which is often referred to as nodes connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. Network enables the interconnected devices to share information and resources. This interconnection could either be established using cables (wired) or without cables (wireless).

Evolutionary Trends of Computer Networks

The US Department of Defence established Advanced Research Project Agency (ARPA) in the late 1960s, which created a small network called ARPANET for the purpose of research. The development of contemporary network was sparked by the creation of the first packet switched network. As a result, it enabled sharing of resources and collaborative research among various universities and research centres.

In the 1970s Ethernet was created at Xeros PARC, computers within a constrained geographical area were enabled to share resources and communicate using standard LAN protocol.

In the late 1970s and early 1980s, the Transmission Control Protocol/Internet Protocol (TCP/IP) was developed by Vinton Clerf and Robert Kahn paving way for the birth of the internet. TCP/IP is a network protocol for reliable data transmission that ensures compatibility between different networks. Its adoption allowed network connection, forming the global network of networks known as the internet.

During the 1980s, the internet expanded beyond academic and research institutions. Commercial networks and Internet Service Providers (ISPs) emerged, connecting businesses and individuals to the internet. The expansion led to the creation of Wide Area Network (WAN) linking different LANs and extended over larger geographical area.

In 1989, Tim Berners-Lee invented the World Wide Web (WWW), introducing hypertext and URLs for easy navigation and information retrieval on the internet. The www revolutionized the way information is accessed and shared, leading to explosion in the growth of websites and online services.

In the 1990s, significant advancement was recorded with the introduction of faster protocols such as HTTP and SSL/TLS in addition to the introduction of web browsers. Protocols are used to establish encrypted connection between a server and a browser allowing secured transfer of sensitive information like credit card over the internet. The emergence of mobile devices and wireless technology further contributed to the growth of the internet, allowing people to connect to the internet on the go.

In recent years, networking technology has continued to evolve; the deployment of high-speed broadband with 3G, 4G and now 5G wireless networks and the proliferation of Internet of Things (IoT) devices have brought further transformations. Concepts like Soft Defined Networking (SDN) and virtualization have gained prominence offering more flexibility, scalability and control over network infrastructures.

Networking Fundamentals

a) Data

Data refers to the raw facts that are collected. Data exist in different forms, including:

- Text: Text includes alphabets in lower case letters, upper case letters or a combination of both.
- Numbers: Numbers are represented in form of digits.

- Images: a photographic or trace objects that represent the underlying pixel data
- Audio: This is data in form of sound that can be recorded and transmitted
- Video: This is data in form of moving visual images.

b) Information

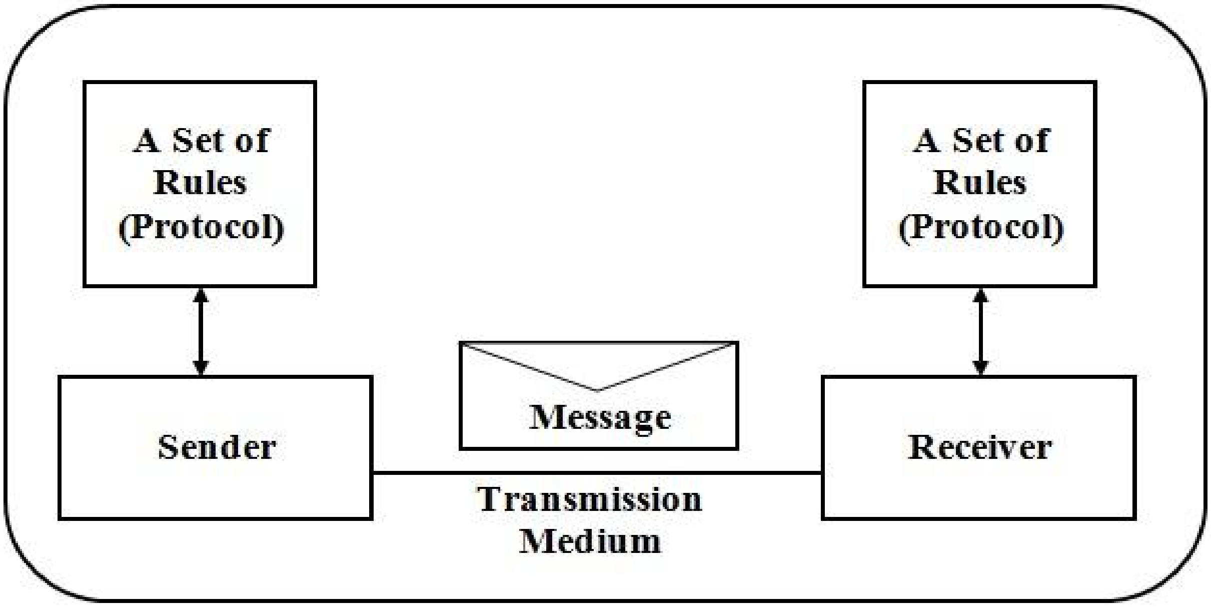
Information refers to processed data that is used in decision making.

c) Data Communication

Data Communication is a process of exchanging data or information. Data sharing can be local or remote. Local communication usually occurs between components in a particular location or point while remote communication takes place between devices separated over a distance.

Components of Data Communications

A data communications system has five (5) components



- Message: The message is the information (data) to be communicated by the sender. It could exist in form of text, numbers, graphics, audio, and video.
- Sender: The sender is the device that sends the data or message. It can be a computer, workstation, telephone, camera, etc.
- Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone, camera, etc.

- Transmission Medium: The transmission medium is the physical path by which a message travels from sender to receiver.
- Protocol: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

Data Transmission Modes

Data transmission between two devices can occur in one of three modes; it can be simplex, half-duplex, or full-duplex:

1. Simplex: This is a communication channel that sends information in one direction only, a device can only send or receive information but not both. Information is said to be unidirectional, examples microphone, speaker, keyboard and monitor.

2. Half-duplex: In half-duplex, a device can send and receive information but the sender and receiver do not communicate simultaneously; the communication is one direction at a time. Examples of half-duplex devices are walkie-talkie, two-way radio transmitter, television and radio broadcasting.

3. Full-Duplex: In full-duplex, a device can send and receive information simultaneously, the communication is in both directions at the same time, example: telephone.

CATEGORIES OF NETWORK

1. Local Area Network (LAN)

Local Area Network is a small network limited to a particular location. It may be privately owned and could exist within an office in a room or a building. It is widely used to connect personal computers and workstations in offices and factories to share information or devices like printer. It can be distinguished from other kinds of networks by size, transmission technology, and topology.

2. Metropolitan Area Network (MAN)

Metropolitan Area Network is a regional connectivity typically within a campus or small geographical area. It is designed to extend over an entire city. It may be a single network, such as cable television network, or it may be a means of connecting a number of LANs into a large network, so that resources may be shared LAN–to–LAN as well as device to device. For example, a company can use a MAN to connect the LANs in all of its branch offices within a city.

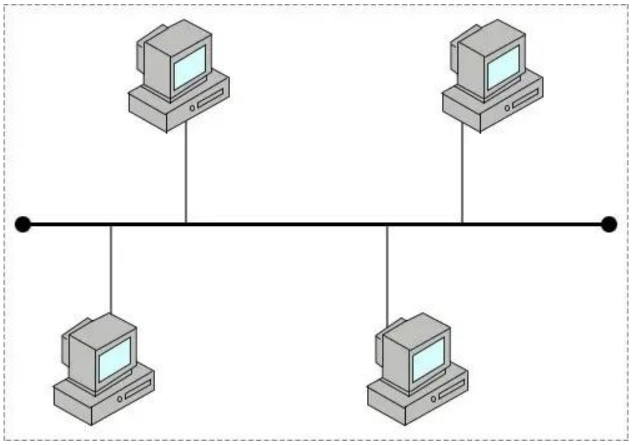
3. Wide Area Network (WAN)

Wide Area Network provides no limit of distance. It provides long distance transmission of data over large geographical areas that may span across countries, continents or even the whole world. In most WAN, the subnet consists of two distinct components; transmission lines (channels) and routers. The transmission lines are used for moving bits between machines, whereas routers are used to connect two or more transmission lines together.

NETWORK TOPOLOGY

A network topology is the physical and logical arrangement of nodes and connections in a network. Nodes usually include devices such as switches, routers and software with switch and router features. Network topologies are often represented as a graph. Network topologies describe the physical structure of networks and the relative location of data flows. Administrators can use network topology diagrams to determine the best placements for each node and the optimal path for traffic flow. With a well-defined and planned network topology, network administrators can more easily locate faults and fix issues, improving its data transfer efficiency.

1. Bus Topology



The bus topology is a multi-point configuration in which a long cable acts as a backbone to link all the devices in the network. Every node is connected in series along a single cable and data transmission is through the backbone of the network. Advantages of a bus topology include use of installation. A disadvantage includes difficult reconfiguration and fault isolation.

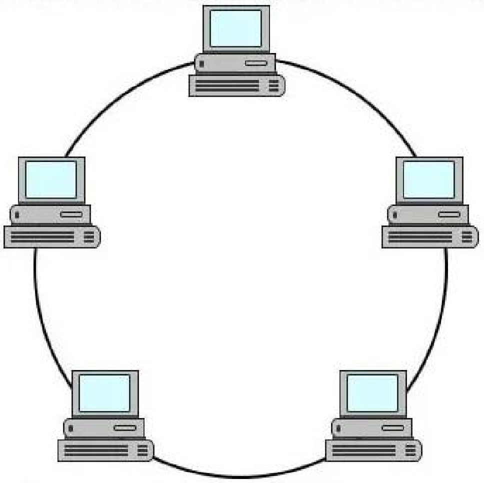
Advantages of Bus Topology

i. It is easy to set up, handle and implement.
ii. It is best suited for small networks.
iii. It is not expensive.

Disadvantages of Bus Topology

i. Cable length is limited, thus limiting the number of network nodes that can be connected.
ii. It performs well only for a limited number of nodes. When the number of devices connected to the bus increases, the efficiency decreases.
iii. It is suitable for networks with low traffic. High traffic increases the load on the bus which results to decline in efficiency.
iv. It is heavily dependent on the central bus, so fault in the bus leads to overall network failure.
v. It is difficult to isolate faults in the network nodes.
vi. Each device on the network “sees” all the data being transmitted, thus posing a security risk.

2. Ring Topology



In ring topology, the nodes are arranged in a circular form with data traveling around the circle in one direction. When one node sends data to another, the data passes through each intermediate node on the ring until it reaches its destination. A signal is passed along the ring in one direction from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

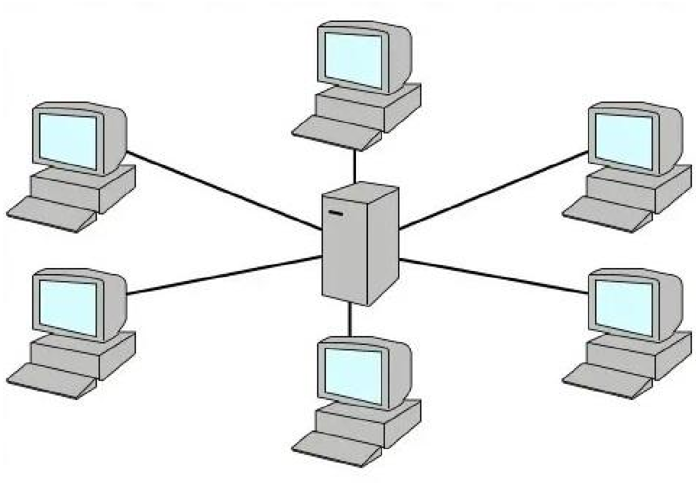
Advantages of Ring Topology

i. A central server is not required for the management of the network.
ii. The traffic is unidirectional and the data transmission at high speed.
iii. It is better with handling loads.
iv. The adding or removing of network nodes is easy, as the process requires changing only two connections.
v. It is easy to identify faults in network nodes.
vi. Each node has the opportunity to transmit data. Thus, it is a very organized network topology.

Disadvantages of Ring Topology

i. The failure of a single node in the network causes the entire network to fail since data transmitted between two nodes passes through all the intermediate nodes.
ii. The movement or changes made to the network nodes affect the entire network's performance.
iii. Data transmission from one node to another passes through all the intermediate nodes, which could lead to security breach.
iv. Data transmission slower and the speed declines with an increase in the number of nodes.
v. There is heavy dependency on the cables connecting the network nodes in the ring.

3. Star Topology



The star topology connects all of the peripheral nodes (computers, etc.) to a central node, which reduces the probability of a network failure. A failure of a transmission line linking any peripheral node to the central node will result in the isolation of that peripheral node from all others, but the remaining peripheral nodes will be unaffected. However, the disadvantage is that the failure of the central node will cause the failure of all of the peripheral nodes.

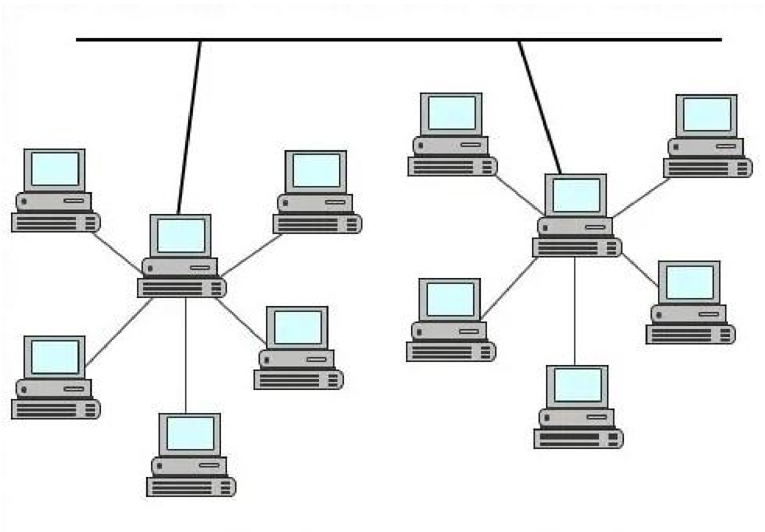
Advantages of Star Topology

i. Due to its centralized nature, the topology offers simplicity of operation.
ii. It also achieves isolation of each device in the network.
iii. Adding or removing network nodes is easy and does not affect the entire network.
iv. It is easy to detect faults in the network devices.
v. It poses a lesser security risk.
vi. The use of a high-capacity central hub enables traffic load to be handled properly.

Disadvantages of Star Topology

i. The network depends on a central hub; hence, failure of the central hub leads to the failure of the entire network.
ii. The number of nodes that can be added depends on the capacity of the central hub.
iii. The setup cost is expensive.

4. Tree Topology



In a tree topology the nodes are arranged in hierarchical order. As in a star topology, nodes are linked to a central hub that controls the traffic to the network.

However, not every device is directly plugs to the central hub. The majority of devices connect to a secondary hub that in turn is connected to the central hub.

It can be viewed as a collection of star networks arranged in a hierarchy. It has a central root node that is connected to one or more nodes of a lower hierarchy. In a symmetrical hierarchy, each node in the network has a specific number of nodes connected to those at a lower level. The root node is connected to one or more secondary nodes, which are connected to tertiary nodes, thus forming a hierarchical or tree structure.

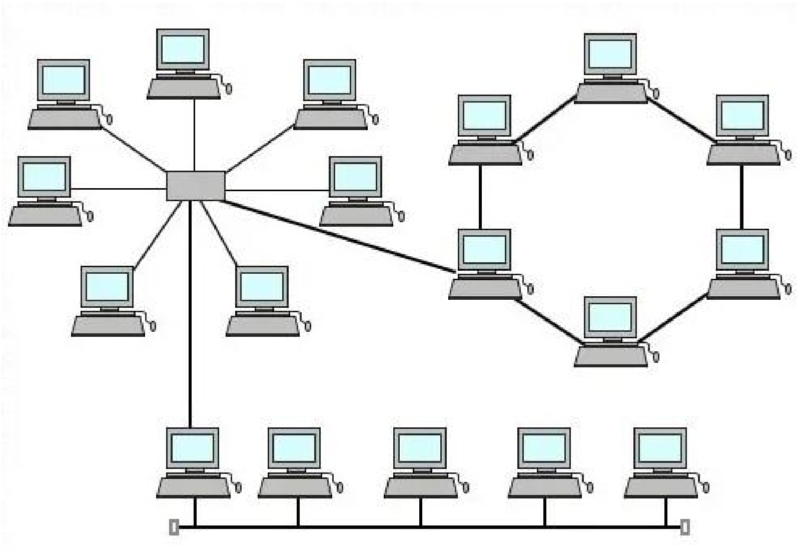
Advantages of Tree Topology

i. It is most suited in networking multiple departments an organization, where each unit (star segment) functions separately and is also connected with the main node (root node).
ii. The advantages of centralization that are achieved in a star topology are inherited by the individual star segments in a tree network.
iii. Each star segment gets a dedicated link from the central bus. Thus, the failure of one segment does not affect the rest of the network.
iv. Fault identification is quite easy.
v. Scalability is easily achieved by the addition of more nodes.

Disadvantages of Tree Topology

i. The network depends heavily on a central bus with multiple segments connected to bus; its failure affects the entire network.
ii. Owing to its size and complexity, maintenance is not easy and costs are high.
iii. The network configuration is difficult in comparison to other topologies.
iv. Even though it is scalable, the number of nodes that can be added depends on the capacity of the central bus and on the cable type.

5. Hybrid Topology



Hybrid network topology is a combination of two or more basic network structures like bus, star, and ring topologies in such a way that the resulting network does not exhibit one of the standard topologies. It typically provides exceptional flexibility, as they can accommodate a number of setups. It has the advantage of making a network easily expandable.

Advantages of Hybrid Topology

i. It is extremely flexible and reliable.
ii. It is easily scalable as the networks are built in a fashion which enables easy integration of new components.
iii. Detecting and handling fault are easy.
iv. It is suitable for large networks.
v. The data transmission is very fast.

Disadvantages of Hybrid Topology

i. It is expensive to install and implement because it has more hardware requirements.
ii. Implementation and configuration are very complex.
iii. Any issue with the backbone of any of the incorporated topology affects the performance of the entire network.

TRANSMISSION MEDIA

Transmission media is a communication channel that transmits information from the source/transmitter to the receiver. It is a physical path for data transfer through electromagnetic signals. Anything that can carry information from a source to a destination can be referred to as a transmission medium. For example, the transmission medium for two people having a dinner conversation is the air or telephone for long distance communication. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane. In data communications the definition is more specific, information is transmitted in the form of bits through local area network usually through free space, metallic cable, or fiber-optic cable.

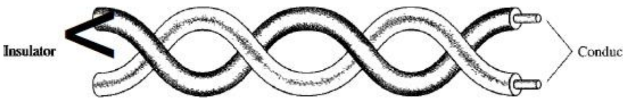
There are two categories of transmission media in computer networks, which include the Guided and the Unguided media.

1. Guided Transmission Media

These media consist of wires through which the data is transferred. Guided media is a physical link between transmitter and recipient devices. Signals are directed in a narrow pathway using physical links. Guided media are also known as wired or bounded media, signals traveling along any of these media is directed and restrained by the physical limits of the medium. Examples are twisted-pair cable, coaxial cable, and fiber-optic cable.

a) Twisted Pair Cable

These are the most widely used transmission medium cables. It consists of two insulated conductors of a single circuit twisted together to improve electromagnetic compatibility and packed together in protective sheaths.



Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly repelled. Twisted-pair cables are used in telephone lines to provide voice and data channels, they are also used in local area network.

Advantages

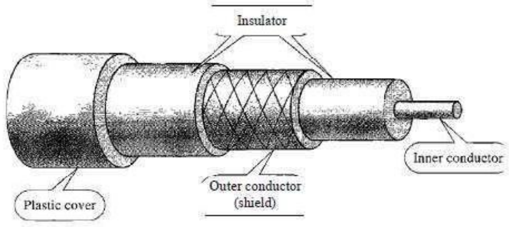
i. They have fast transmission rate.
ii. They can be used for both analog and digital transmissions.
iii. They are least expensive for short distances.
iv. They are reliable and easy to install.

Disadvantages

i. Their signals cannot travel long distances without repeaters.
ii. They are not durable because they are very thin and hence easily break.
iii. They are not suitable for broadband connections.
iv. They are susceptible to external interference such as electromagnetic interference.

b) Fiber Optic Cable

Fiber-optic cables are made of glass or plastic and transmit signals in the form of light. Its core is made of fiber rather than copper and it is more often used for long-distance communications. Compared to other materials, these cables can carry huge amounts of data and run for miles without using signal repeaters.



Due to lesser requirements, they have less maintenance costs and it improves the reliability of the communication system. These can be unidirectional as well as bidirectional in nature. Fiber-optic cables are often found in backbone networks because its wide bandwidth is cost effective.

Advantages

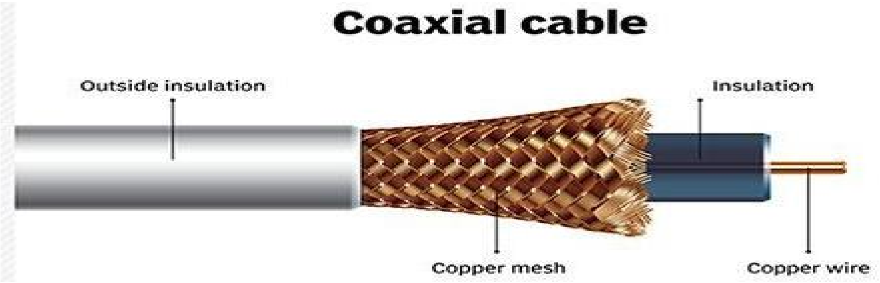
i. Fiber-optic cable can support higher bandwidths than either twisted-pair or coaxial cable.
ii. It is suitable for long distance transmission.
iii. It is e easy to install and maintain.
iv. It is resistance to electromagnetic interference.
v. Glass is more resistant to corrosive materials than copper.
vi. Fiber-optic is less bulky; they are much lighter than copper cables.

Disadvantages

i. They are fragile, thus easily damaged.
ii. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
iii. The cable and the interfaces are relatively more expensive.

Coaxial Cable

Coaxial cables are made of PVC/Teflon and consist of two parallel conductors that are separately insulated. They transmit information in baseband mode and broadband mode and equally have the ability to carry high frequency electrical signals without any big loss.



Coaxial cable carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Coaxial cable was widely used in analog telephone networks. Cable TV networks also use coaxial cables. Coaxial cable is also used in traditional Ethernet LANs.

Advantages

i. It supports high bandwidth signal transmission.
ii. It is less susceptible to noise or interference.
iii. It is easy to install and also very durable.

Disadvantage

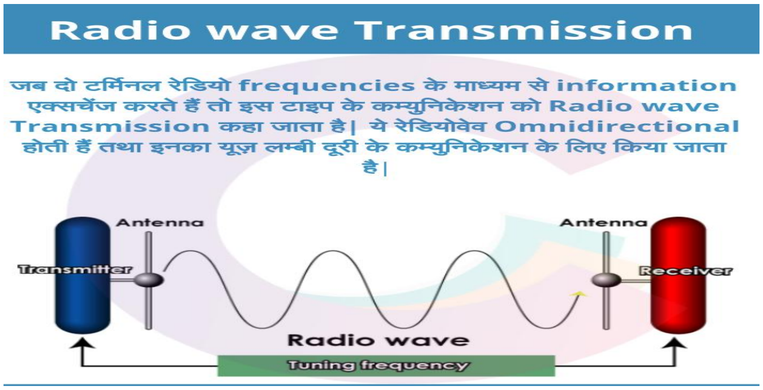
i. It is too bulky because it has multiple layers.
ii. It is expensive to install for longer distances because of its thickness and stiffness.
iii. It needs to be grounded to limit interference.
iv. Suitable for short distance, using coaxial cables over long distances can result to signal loss.

2. Unguided Transmission Media

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as unbounded or wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them. There is no physical connectivity between transmitter and receiver. These types of transmission media are used for longer distances however they are less secure than guided media. There are three main types of unguided transmission media, they include:

a) Radio Waves

Radio waves are transmitted in every direction throughout free space. They are said to be omni-directional, which means that signal transmits by radio waves are propagated in all directions. Radio waves can cover large areas and even penetrate obstacles such as buildings and walls. The frequency of these waves ranges between 3 kHz to 1GHz. The omni-directional characteristics of radio waves make them very useful for multicasting, in which there is one sender but many receivers. Examples of multicasting include AM and FM radio, television, maritime radio, cordless phones, and paging.



Radio wave Transmission

जब दो टर्मिनल रेडियो frequencies के माध्यम से information एक्सचेंज करते हैं तो इस टाइप के कम्युनिकेशन को Radio wave Transmission कहा जाता है| ये रेडियोवेव Omnidirectional होती हैं तथा इनका यूज़ लम्बी दूरी के कम्युनिकेशन के लिए किया जाता है|

Advantages

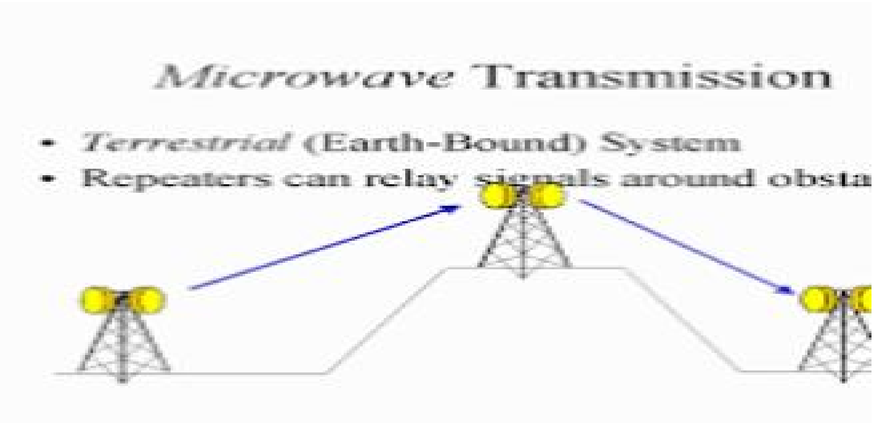
i. They are easy to generate.
ii. These waves are useful in multi-casting, i.e. transmitting from one sender to multiple receivers.
iii. They can cover large areas and even penetrate obstacles such as buildings and walls.

Disadvantages

i. Issues such as interference might arise when another signal with the same bandwidth or frequency is sent.
ii. It cannot isolate a communication to just inside or outside a building.
iii. Radio wave band is relatively narrow leading to low data rate for digital communications.

b) Microwaves

Microwaves are unidirectional electromagnetic waves with frequencies between 1 and 400 GHz and provide bandwidth between the ranges of 1 to 10 Mbps. Antenna transmitting microwave waves has to be focused, which means that the sending and receiving antennas need to be aligned. This is why it is known as line-of-sight transmission. Microwaves distance covered by the signal is proportional to the height of the antenna. It is suitable for shorter distance transmissions; for travelling longer distances, the height of the tower should be increased. They have applications in mobile phones and televisions.



Microwave Transmission

- *Terrestrial* (Earth-Bound) System
- Repeaters can relay signals around obsta

Advantages

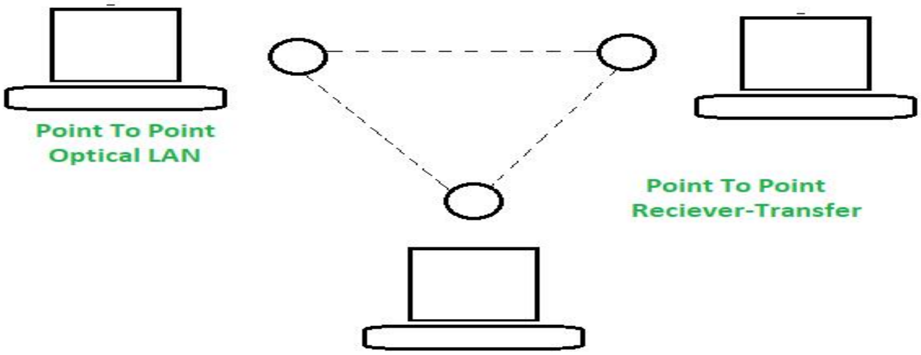
i. It has high bandwidth; hence a large amount of information can be transmitted using it.
ii. It is often more reliable than other forms of wireless communication, such as satellite or cellular connections.
iii. Its transmissions can be encrypted, making it more secure than some other forms of wireless communication.

Disadvantages

i. It is easily disrupted by bad weather like heavy rain, snow, or fog.
ii. Microwave transmission requires a clear line of sight between the transmitter and receiver, which can be affected by buildings or natural obstacles.
iii. The cost of implementing the communication infrastructure is too much high.
iv. Some studies have suggested that prolonged exposure to microwaves from transmission towers could be harmful to human health.
v. Microwave transmissions can easily be disrupted by other electronic devices, such as radar systems that operate on the same frequency within the same area.

c) Infrared

Infrared wave is useful for only very short distance communication. Unlike radio waves, they do not have the ability to penetrate barriers like walls. It prevents interference between one system and another; that means a short-range communication system in one room cannot be affected by another system in the same or nearby room. Since they have larger bandwidth, the data transfer rate is very high for infrared waves. They have less interference and are more secure. Infrared signals are basically used for communication between wireless devices like remote controls, keyboards, mice, printers.



Point -To-Point infrared media in a network

Advantages

i. Signal transmission is fast.
ii. There is no interference between devices within the same area.
iii. It is capable of detecting signal in the presence or absence of light.
iv. It is highly immune to noise.
v. It offers secure transmission because of point to point mode of communication.

Disadvantages

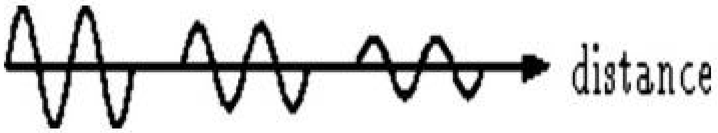
i. It is not suitable for long distance communication.
ii. Its signals cannot penetrate obstacles like walls and doors, limiting their use in transmission.
iii. It does not support the high data transfer rates, hence not suitable for broadband connections.

Transmission Impairment in Data Communication

In the data communication system, signals go through transmission medium. Some imperfections in these transmission mediums cause imperfections the signals sent to the receiver. These are referred to as signal or transmission impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium; that is, what is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise.

a) Attenuation

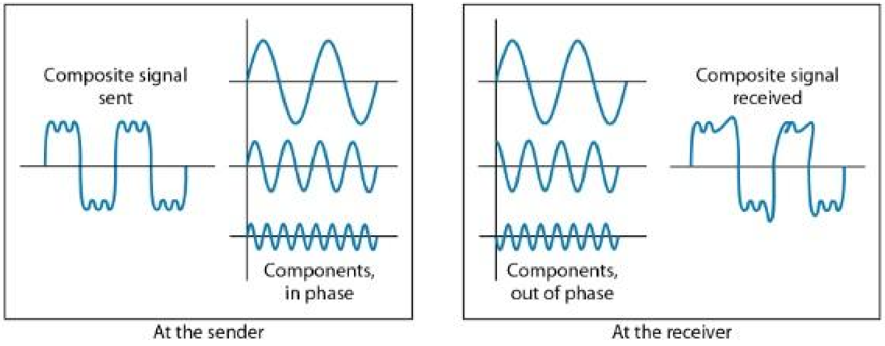
Attenuation refers to the reduction (loss) of energy in a signal as it travels over distance through a medium, due to the resistance of the medium. The weakened signal is commonly known as an attenuated signal. To eliminate this loss, amplifiers are employed to boost the signal and restore its original strength. This process helps compensate for the energy lost during transmission.



That is why a wire carrying electric signals becomes warm or hot after a while since some of the electrical energy in the signal is converted to heat. Attenuation makes it challenging to receive the signal at the receiver end. The environment plays a significant role in causing this attenuation by creating resistance, which reduces the signal strength as it tries to overcome this resistance.

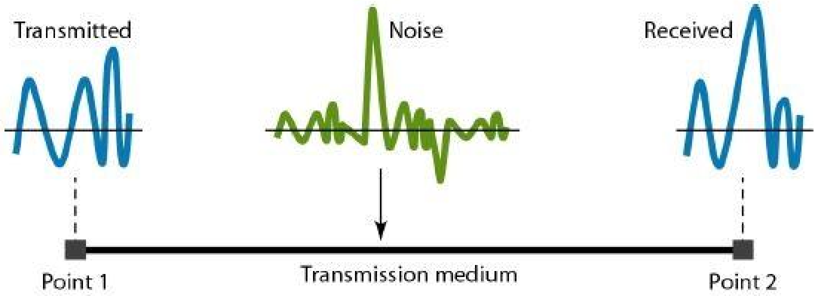
b) Distortion

Distortion refers to alterations in signal form or shape during transmission. It can occur in a composite signal made of different frequencies. When transmitting a composite signal, any delay between its frequency components can cause the component to reach the receiver with a different delay constraint than its original. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. This can alter the shape of the original signal, and the delay can occur due to various reasons, such as environmental parameters or the distance between the transmitter and receiver.
It is commonly found in signals generated or received by computer, video signals and data cables such as network cables.



c) Noise

Noise refers to the unwanted signal that interferes with the original signal. Noise usually is introduces to a generated signal, it alters the signal that is eventually transmitted to the receiver.



Various forms of noise are induced noise, thermal noise, crosstalk noise, and impulse noise. These types of noise have the potential to corrupt the signal and cause issues.

- Induces Noise

- Thermal noise is the noise caused by the random movements of electrons in cables or conductors generating an additional signal that alters the signal being transmitted.

- Crosstalk noise is caused by electromagnetic interference (EMI) between adjacent network cables or conductors. When two or more cables are placed close to each other, the electrical signals in one cable can induce an unwanted signal in the adjacent cable. It can be reduced by using twisted pair cables, which have a special winding pattern that reduces interference, and other shielding techniques.

- Impulse noise is a sudden, short-duration burst of interference. It can be caused by external factors like electrical surges, lightning strikes, or electromagnetic pulses. These sudden changes can overload the network and cause alterations or even damage to the equipment. It can be reduced by using surge protectors and other protective measures that can absorb or redirect the excess energy.
- Inter-modulation noise is caused when two or more signals with different frequencies mix together and create new frequencies that can interfere with or distort the original signals.

  The interaction between multiple signals occurs mostly in a nonlinear devices or mediums. It can be reduced by using filters and other signal processing techniques that can separate and isolate the different frequencies.

Noise is a major factor that limits the speed of communication. To study the efficiency (performance) of a communication processes, it is important to analyze the noise signal. Signal-to-Noise Ratio (SNR) is used for this purpose.

MODULATION AND DEMODULATION

Modulation

Modulation is the process by which some parameters of a carrier wave such as amplitude, frequency or phase is changed according to the signal containing information in order to convert a low-frequency signal to high frequency to have better transmission.

A carrier wave is a high-frequency signal that has constant amplitude and frequency and is generated from a radio frequency oscillator. It is sometimes referred to as an empty signal because it is a signal that does not contain information and is used to modulate an original signal that contains information to be transmitted over a long distance.

Simply transmitting a baseband signal (message signal) to longer distances causes various unwanted alterations in the signal itself. Modulation is used to eliminate unwanted parameters that cause variation in the message signal. Modulation schemes can be in analog or digital form.

a) Analog Modulation

An analog scheme has an input wave that varies continuously like a sine wave. Examples include:

i. Amplitude Modulation (AM): The strength or intensity of the signal carrier is varied to represent the data being added to the signal.
ii. Frequency Modulation (FM): The frequency of the carrier waveform is varied to reflect the frequency of the data.
iii. Phase Modulation (PM): The phase of the carrier waveform is varied to reflect changes in the frequency of the data. In PM, the frequency is unchanged while the phase is changed relative to the base carrier frequency. It is similar to FM.
iv. Polarization Modulation: The angle of rotation of an optical carrier signal is varied to reflect transmitted data.

b) Digital Modulation

Digital modulation scheme, voice is sampled at some rate and then compressed and turned into a bit stream, and this in turn is created into a particular kind of wave which is then superimposed on the carrier signal. Examples are:

i. Phase-shift Keying (PSK) is a digital modulation process which conveys data by changing (modulating) the phase of a constant frequency carrier wave. The modulation is accomplished by varying the sine and cosine inputs at a precise time. It is widely used for wireless LANs, RFID and Bluetooth communication.

ii. Frequency-shift Keying (FSK) is a frequency modulation scheme in which digital information is encoded on a carrier signal by periodically shifting the frequency of the carrier between several discrete frequencies. The technology is used for communication systems such as telemetry, weather balloon radiosondes, caller ID, garage door openers, and low frequency radio transmission in the VLF and ELF bands. The simplest FSK is binary FSK (BFSK), in which the carrier is shifted between two discrete frequencies to transmit binary (0s and 1s) information.

iii. Amplitude-shift Keying (ASK) is a form of amplitude modulation that represents digital data as variations in the amplitude of a carrier wave. In an ASK system, a symbol, representing one or more bits, is sent by transmitting a fixed-amplitude carrier wave at a fixed frequency for a specific time duration. For example, if each symbol represents a single bit, then the carrier signal could be transmitted at nominal amplitude when the input value is 1, but transmitted at reduced amplitude or not at all when the input value is 0.

iv. Quadrature Amplitude Modulation (QAM) is a digital modulation method related to analog modulation methods widely used in modern telecommunications to transmit information. It conveys two analog message signals, or two digital bit streams, by changing (modulating) the amplitudes of two carrier waves, using the amplitude-shift keying (ASK) digital modulation scheme or amplitude modulation (AM) analog modulation scheme. The two carrier waves are of the same frequency and are out of phase with each other by 90°, a condition known as orthogonality or quadrature. The transmitted signal is created by adding the two carrier waves together. At the receiver, the two waves can be coherently separated (demodulated) because of their quadrature.

Demodulation

Demodulation is the process by which receiver regains the original message signal from the modulated one; that is, the process of separating a message signal from a carrier signal. It is the reverse of modulation. It is also necessary in order to recover the original message signal after modulating it to allow proper and long-distance signal transmission.

Demodulation is done at the receiver section. A demodulator that is responsible for demodulation then it is predefined that it is placed at the receiver end of a communication system.

A modem is a device that is used for both modulation and demodulation, hence modem was the name derived from MOdulator and DEModulator. Several techniques are used for the process of modulation and demodulation, the implementation depends on the area of need.

Difference between Modulation and Demodulation

- Modulation and demodulation are reversal processes of each other. Thus, is done at the two ends of a communication system.

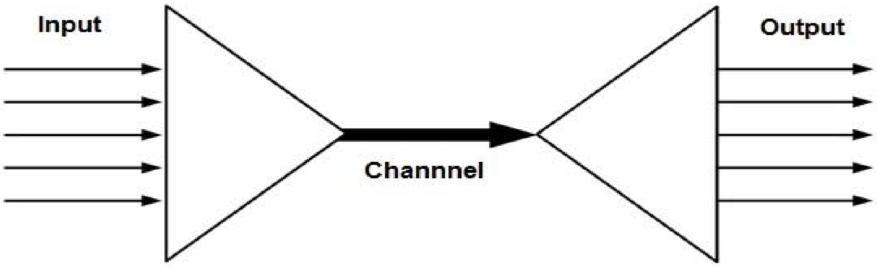
- The major difference between modulation and demodulation is that modulation is the act of altering the parameters of the carrier signal according to message signal for convenient data transmission. On the contrary, demodulation is done in order to recover the original message signal from a modulated signal.

- Another crucial difference between modulation and demodulation is that modulation is done at the transmitting end while demodulation occurs at the receiving end.

- Modulation essentially occurs to transmit data to a longer distance. Demodulation takes place to retain the original form of the signal.
- In modulation, the message signal is added on a carrier wave for transmission while in demodulation, the message is separated from the carrier signal.

MULTIPLEXING

Multiplexing is a process in which two or more signals can be transmitted over the same communication channel simultaneously. It is a method by which multiple analog or digital signals are combined into one signal over a shared medium. The multiplexing allows the same channel to be used by many signals. This is possible only with modulation. Hence, many TV channels can broadcast simultaneously without getting mixed with each other as they use different carrier frequencies. It is referred to as frequency division multiplexing.



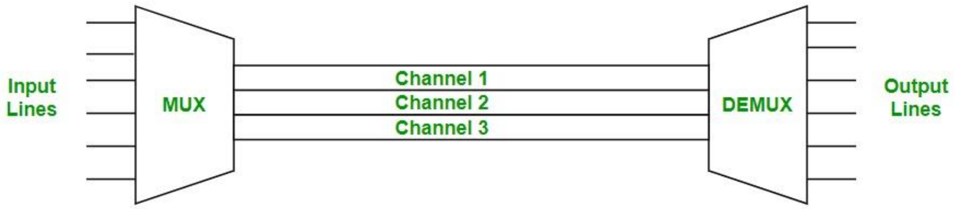
Multiplexing originated in telegraphy in the 1870s, and is now widely applied in communications. The main purpose is to share a scarce resource such as a physical transmission medium like a cable. For example, in telecommunications, several telephone calls may be carried using one wire.

The multiplexing divides the capacity of the communication channel into several logical channels, one for each message signal or data stream to be transferred. A reverse process, known as demultiplexing, extracts the original channels on the receiver end. A device that performs the multiplexing is called a multiplexer (MUX), and a device that performs the reverse process is called a demultiplexer (DEMUX or DMX).

Types of Multiplexing

1. Frequency-division Multiplexing (FDM)

Frequency division multiplexing is a type of multiplexing where the bandwidth of a single physical medium is divided into a number of smaller, independent frequency channels. The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices. Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal. It is basically used in radio and television transmissions.



FDM introduces a lot of inter-channel cross-talk, due to the fact that the bandwidth is divided into different frequency channels. In order to prevent the inter-channel cross talk, unused strips of bandwidth must be placed between each channel; these unused strips are known as guard bands.

Advantages of FDM:

i. It is used for analog signals.
ii. A Large number of signals can be sent through an FDM simultaneously.
iii. It does not require any synchronization between sender and receiver.

Disadvantages of FDM:

i. It is used only when low-speed channels are required.
ii. It suffers the problem of crosstalk.
iii. A large number of modulators is required.
iv. It requires a high bandwidth channel.

2. Time-division Multiplexing (TDM)

Time-division multiplexing is defined as is a digital multiplexing technique time is shared. The total time available in the channel is distributed among different users; therefore, each user is allocated a different time interval known as a time slot at which data is to be transmitted by the sender. This cycle of time slots is referred to as a frame. The sender takes control of the channel for a fixed amount of time. There is no simultaneous data transmission; rather the data is transmitted one-by-one. All signals operate with the same frequency (bandwidth) at different time. Even though, TDM can be used to multiplex both digital and analog signals, it is mainly used to multiplex digital signals.
TDM was first developed in the 19th century for applications in telegraphy to route multiple transmissions simultaneously over a single transmission line but its most common application was found in digital telephony later in the 20th century. These include:

i. Plesiochronous digital hierarchy (PDH)
ii. Synchronous digital hierarchy (SDH)
iii. Synchronous optical networking (SONET)
iv. Integrated Services Digital Network (ISDN)

PDH technology was used in telecommunications networks to transport large quantities of data over digital transport equipment such as fibre optic and microwave radio systems.

ISDN is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the digitalized circuits of public switched telephone network. It has largely been replaced with digital subscriber line (DSL) systems of much higher performance. DSL is a technology that is used to transmit digital data over telephone lines. It uses higher frequency bands for data transfer and is commonly used in telecommunications for Internet access.

SDH and SONET are standardized protocols that transfer multiple digital bit streams synchronously over optical fiber using lasers or highly coherent light from light-emitting diodes (LEDs). Data can also be transferred at low transmission rates via an electrical interface.

Advantages of TDM

i. TDM requires less bandwidth than FDM due to its compact and efficient transmission of signals.
ii. It is more resistant to noise and distortion since the signals are transmitted in discrete and digital form.
iii. It is more flexible and scalable, as the number and size of the time slots can be adjusted and allocated dynamically.

Disadvantages of TDM

i. There is need of synchronization between the sender and the receiver, as the signals must be sent in a specific order and timing.
ii. Analog signals cannot be handled without conversion, as they must be sampled and quantized by time.
iii. It can suffer from time delay and jitter due to the buffering and switching of signals by time.

There are two types of Time Division Multiplexing, they are:

a) Synchronous Time Division Multiplexing

Synchronous TDM is commonly used in digital telecommunications networks, that allows multiple signals to be transmitted over a single communication line but each signal is transmitted in fixed time slots synchronized with the transmitter's clock. This ensures that each signal is transmitted at the same rate and in the correct order.

Synchronous TDM does not guarantee that the full capacity of a link is used. It is more likely that only a portion of the time slots is in use at a given instant. Because the time slots are pre-assigned and fixed, whenever a connected device is not transmitting the corresponding slot is empty and that much of the path is wasted.

b) Asynchronous or Statistical Time Division Multiplexing

Asynchronous TDM allows a number of lower speed input lines to be multiplexed to a single higher speed line; that is, it allows bandwidth to be split over one line but unlike synchronous TDM, the total speed of the input can be greater than the capacity of the path.

In asynchronous TDM, the number of time slots in a frame (m) is based on a statistical analysis of the number of input lines that are likely to be transmitting at any given time. Rather than being pre-assigned, each slot is available to any of the attached input lines that has data to send. Thus, asynchronous TDM is designed to avoid type of waste associated with synchronous TDM.

Asynchronous TDM allows a number of lower speed input lines to be multiplexed to a single higher speed line. Unlike synchronous TDM, asynchronous TDM the total speed of the input lines can be greater than the capacity of the path. In a synchronous system, if there are n input lines, the frame contains a fixed number of at least n time slots.

3. Space-division Multiplexing

In wired communication, space-division multiplexing, which is also referred to as space-division multiple access (SDMA) is the use of separate point-to-point electrical conductors for each transmitted channel. Examples include an analogue stereo audio cable, with a pair of wires for the left channel and another for the right channel, and a multi-pair telephone cable, a switched star network such as a telephone access network, a switched Ethernet network, and a mesh network.

Methods of Data Transmission

There are two methods used for transferring data between media which are given below: Serial Transmission and Parallel Transmission.

1. Parallel Transmission

Parallel transmission is a method of transferring multiple binary digits (bits) simultaneously using multiple conductors. It transmits quickly since it utilizes several input and output lines for sending the data. Parallel transmission is faster than serial transmission to transmit the bits but it is used for short distance data transfer.

A parallel interface comprises of parallel wires that individually contain data and other cables that allow the transmitter and receiver to communicate.

2. Serial Transmission

Serial transmission is the process of sending data sequentially, one bit at a time, over a communication channel or computer bus. Data is transferred bit by bit from one digital device to another in two directions (bi-directional), 8 bits are transferred at a time having a start and stop bit known as the parity bit, which are 0 and 1 respectively. It is used for all long-haul communication and most computer networks, where cost of cable and synchronization difficulties makes parallel communication impractical. Serial data cables are utilized to send data across extended distances.

Serial computer buses have become more common even at shorter distances, as improved signal integrity and transmission speeds in newer serial technologies have begun to outweigh the parallel bus's advantage of simplicity.

Long distance communication and most computer networks employ serial communication and majority of communication systems use serial mode. Serial networks may be extended over vast distances for far less money since fewer physical wires are required.

Keyboard and mouse cables and ports are almost invariably serial—such as PS/2 port, Apple Desktop Bus and USB. Cables that carry digital video are also mostly serial—such as coax cable plugged into a HD-SDI port, a webcam plugged into a USB port or FireWire port, Ethernet cable connecting an IP camera to a Power over Ethernet port, FPD-Link, digital telephone lines (ex. ISDN), etc. There are mainly two types of serial transmission. They include Synchronous Serial transmission and Asynchronous Serial Transmission.

i. Synchronous Serial transmission does not add extra bit during transmission; rather, data is conveyed in the form of frames that comprise numerous bytes.

ii. Asynchronous transmission adds an extra bit to every byte to notify the recipient of the appearance of new data. Typically, the start bit is 0, and the stop bit is 1. ATM connections can be categorized into two types:

    - Point–to–point connections: These are the connections which connect two ATM end–systems. Such connections can be unidirectional or bidirectional.
    - Point–to–multipoint connection: These are the connections which connect a single source end–system known as the root node, to multiple destination end–systems (known as leaves).

DATA SWITCHING

Data switching is a process of transferring data packets from a source to a destination device through series of connected networks. It involves the use of a switch, which allows for the transfer of data between different devices. The switch acts as a central hub that connects all the devices in the network and enables the transfer of data between them. It is a mechanism used in computer networks to determine the best route for data transmission in a large network where there are multiple paths that link senders and receivers.

Data switching allows communications equipment and circuits, to be shared among users. Each user has sole access to a circuit during network use. It is responsible for the efficient management of information flow between multiple devices connected to a network. Data switching is an integral part of modern-day networking, as it allows for the transfer of data between different devices in a seamless and efficient manner.

Data Switching Techniques

There are three main types of data switching, which:

- Circuit switching
- Packet switching
- Message switching

1. Circuit Switching

This was the first type of data transfer mechanism used. Circuit switching is used in the telephone networks to transmit voice and data signals. In a synchronous transmission, which involves transmission of voice, a synchronized connection must be made between the sender and receiver because there must be a constant time interval between each successive bit, character, or event. To enable synchronized transmission, circuit switching establishes a dedicated connection between the sender and the receiver involved in the data transfer over the network.

2. Packet Switching

Packet switching ensures that the network is utilized at all times. It does this by sending signals even in the small unused segments of the transmission – for example, between the words of a conversation or when a caller is put on hold. However, in packet switching, there can be variations in the timing when the digital bits are received. For normal voice and data communications, this is not a problem, but for broadband signals, such as television, it is a huge problem that causes the picture to jerk and the audio to be out of synchronization with the picture. Data to be sent is broken down into small packets. Each packet contains data and header information for control e.g., routing. At each node the packet is received, stored briefly and passed on. At each node, the packets may be put on a queue for further movement into the network.

3. Message Switching

In message switching, there is no physical path between the sender and receiver. When the sender has the structure of data to be transmitted, it is saved in the first switching office, i.e., router and then the data is forwarded. Each block is inspected for errors and then sent accordingly.

OPEN SYSTEMS INTERCONNECTION (OSI) MODEL

The Open Systems Interconnection (OSI) model is a conceptual model from the International Organization for Standardization (ISO) that provides a common basis for the coordination of standards development for the purpose of systems interconnection. It is a conceptual model used by networking professionals to represent how data is sent or received over a network. It describes how applications communicate over a network and focuses on providing a visual design of how each communications layer is built on top of the other, starting with the physical cabling, all the way to applications that communicate with other devices on a network.

The model partitions the flow of data in a communication system into seven abstraction layers to describe networked communication from the physical implementation of transmitting bits across a communications medium to the highest-level representation of data of a distributed application. Each layer in the OSI model has well-defined functions and the methods of each layer communicate and interact with those of the layers immediately above and below. Each intermediate layer serves a class of functionality to the layer above it and is served by the layer below it.

The purpose of the OSI reference model is to guide technology vendors and developers so the digital communications products and software programs they create can interoperate and to promote a clear framework that describes the functions of a networking or telecommunications system in use.

In the OSI reference model, there are seven different abstraction layers; namely, Physical, Data Link, Network, Transport, Session, Presentation, and Application.

1. The Physical Layer

This layer is responsible for sending computer bits from one device to another along the network using electrical, mechanical or procedural interfaces. It determines how physical connections to a network are set up and how bits are represented into predictable signals as they are transmitted either electrically, optically or via radio waves.

2. The Data-Link Layer

The data link layer provides a link (node-to-node data transfer) between two directly connected nodes. It detects and possibly corrects problems that may occur in the physical layer as a result of bit transmission errors. It defines the protocol to establish and terminate a connection between two physically connected devices. It also defines the protocol for flow control between them.

It handles moving data into and out of a physical link in a network. It ensures that the pace of the data flow does not overwhelm the sending and receiving devices. This layer also permits the transmission of data to the network layer.

3. Network Layer

The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. It provides the functional and procedural means of transferring packets from a node one network to a node in another network.

Network layer protocols accomplish this by packaging data with correct network address information, selecting the appropriate network routes and forwarding the packaged data up the stack to the transport layer. It finds the best physical path for the data to reach its destination; this is known as routing.

4. Transport Layer

The transport layer is responsible for transferring data across a network (end-to-end communication between the two devices) and provides error-checking mechanisms and data flow controls. It determines how much data to send, where it gets sent and at what rate.

Its functions include taking data from the session layer and breaking it up into chunks called segments before sending it to network layer. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can utilize.

The transport layer performs error control on the receiving end by ensuring that the data received is complete and requesting a re-transmission if the data is incomplete.

5. The Session Layer

This is the layer that is responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session after data transmission to avoid wasting resources.

The session layer also provides for full-duplex, half-duplex, or simplex operation, and establishes procedures for checkpoint, suspending, restarting, and terminating a session between two related streams of data, such as an audio and a video stream in a web-conferencing application.

Checkpoint is a mechanism used to synchronize data transfer; for example, if a 100 megabyte file is being transferred, this layer could set a checkpoint every 5 megabytes. In the case of a break in transmission after about 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

6. Presentation Layer

This layer is primarily responsible for preparing data so that it can be used by the application layer. It makes the data presentable for applications to utilize by translating, encrypting and compressing the data. Basically, it formats data for the application layer based on the semantics or syntax the application allows.

If the devices are communicating over an encrypted connection, this layer is responsible for adding the encryption on the sender’s end as well as decoding the encryption on the receiver's end so that it can present the application layer with readable data.

Large amount of data received could be compressed before delivering it to session layer. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

7. Application Layer

The application layer is the layer of the OSI model that is closest to the end user, which means that there is a direct interaction between the layer and the user using software applications that implements a component of communication between the client and server, such as File Explorer. Software applications like web browsers and email clients rely on the application layer to initiate communications.

Its functions typically include file sharing, message handling, and database access through the most common protocols at the application layer such as Hypertext Transfer Protocol (HTTP), File Transfer protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

COMMUNICATION PROTOCOLS

Communication protocols are a set of rules that govern exchange of information in an easy, reliable and secure way. It allows connected devices to communicate with each other, irrespective of internal and structural differences. It determines what is being communicated, how it is being communicated, and when it is being communicated.

A protocol is like a common language for computers. The computers within a network use vastly different software and hardware; however, the use of protocols enables them to communicate with each other.

Without protocols, computers and other devices would not know how to interact with each other. To successfully send and receive information, devices on both sides of a communication exchange must accept and follow protocol conventions. Support for these network protocols can be built into the software, hardware or both. There are different kinds of protocols that are used in networks for communication, they include:

1. Transmission Control Protocol (TCP)

Transmission Control Protocol (TCP) is a communications standard that enables application programs and computing devices to exchange messages over a network.

It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.

TCP is one of the basic standards that define the rules of the internet and is included within the standards defined by the Internet Engineering Task Force (IETF). It is one of the most commonly used protocols within digital network communications and ensures end-to-end data delivery.

TCP organizes data so that it can be transmitted between a server and a client. It guarantees the integrity of the data being communicated over a network. Before it transmits data, TCP establishes a connection between a source and its destination, which it ensures remains live until communication begins. It then breaks large amounts of data into smaller packets, while ensuring data integrity is in place throughout the process.

2. Hypertext Transfer Protocol (HTTP)

The Hypertext Transfer Protocol (HTTP) is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. It is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser. It functions as a request–response protocol in the client-server based models. Its newer and secure variant named HTTPS has been adopted by almost all websites.

3. File Transfer Protocol (FTP)

This is a network protocol that is used to transfer files from one device to another over an unencrypted TCP/IP connection. It is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. It basically transfers web page files from a source to a destination that acts as a server for other computers on the internet. It is commonly integrated into web browsers to make data transfers more reliably and efficiently.

Many organizations use FTP because of its ability to send large files or lots of files at once in a way that is fast and efficient. Unfortunately, this efficiency comes at the cost of security because it transmits all data in plain text. There is a secure version of FTP called File Transfer Protocol Secure Sockets Layer (FTPS), which uses SSL encryption to obscure the transferred data.

3. Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is an internet standard communication protocol for electronic mail transmission; that is, it is used in sending and receiving email messages. It is used most commonly by email clients like Gmail, Outlook, Yahoo Mail, etc to send messages to remote servers.

SMTP can send and receive email, but email clients typically use a program with SMTP for sending email. Because SMTP is limited in its ability to queue messages at the receiving end, it is usually used with either Post Office Protocol 3 (POP3) or Internet Message Access Protocol (IMAP), which lets the user save messages in a server mailbox and download them periodically from a server. SMTP is typically limited to and relied on to send messages from a sender to a recipient while POP and IMAP are used to retrieve the emails on the end user's side.

4. Post Office Protocol 3 (POP3)

Post Office Protocol 3 (POP3) is an application-layer Internet standard protocol used by e-mail clients to retrieve e-mail from a mail server. It provides access via an Internet Protocol (IP) network for a user client application to a mailbox maintained on a mail server. The protocol supports list, retrieve and delete operations for messages. POP3 clients also have an option to leave mail on the server after retrieval, and in this mode of operation, clients will only download new messages.

POP3 is actually an older protocol that was originally designed to be used on only one computer. Unlike modern protocols that use two-way synchronization, POP3 only supports one-way email synchronization, it only allowing users to download emails from a server to a client. Because of this, POP3 accounts lack most of the basic functionality that can be found in more modern services.

5. Internet Message Access Protocol (IMAP)

Internet Message Access Protocol (IMAP) is also an internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection. It was designed with the goal of permitting complete management of an email box by multiple email clients; therefore clients generally leave messages on the server until the user explicitly deletes them. Many web mail service providers such as Gmail and Outlook also provide support for both IMAP and POP3.

With IMAP accounts, messages are stored in a remote server. Users can log in via multiple email clients on computers or mobile device and read the same messages. All changes made in the mailbox will be synced across multiple devices and messages will only be removed from the server if the user deletes the email.

6. Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) is one of the main protocols of the internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP, which is part of the Transport Layer of the TCP/IP suite. It has many applications such as emails, FTP, streaming media, etc.

7. Internet Protocol (IP)

Internet Protocol (IP) is a type of protocol that allows data to be sent from one computer to another on the internet. Each computer, which is known as a host has a unique address called IP address that uniquely identifies it from all other computers on the internet. It is used for addressing and routing data packets so that they can reach their destination. One of the core protocols that runs on top of IP is the Transmission Control Protocol (TCP), which is often why IP is also referred to as TCP/IP.

8. User Datagram Protocol (UDP)

User Datagram Protocol is a communications protocol for time-sensitive applications like gaming, playing videos, or Domain Name System (DNS) lookups. UDP provides faster communication because it does not spend time forming a firm connection with the destination before transferring the data. Because establishing the connection takes time, eliminating this step results in faster data transfer speeds.

However, UDP can also cause data packets to get lost as they go from the source to the destination. It can also make it relatively easy for a hacker to execute a distributed denial-of-service (DDoS) attack.

NETWORK STANDARDS AND CONTROLS

Network standards are established specifications that ensure compatibility and interoperability among different devices, vendors, and applications on a network. These standards define the physical, electrical, and functional characteristics of network components such as cables, connectors, signals, frequencies, and protocols.

They provide guidelines to manufacturers, vendors, government agencies and other service providers to ensure that different devices and systems communicate with each other on a network, regardless of their hardware, software, or location. They also ensure consistency, efficiency, and quality of products and services for users and applications.

These standards define the physical, electrical, and functional characteristics of network components, such as cables, connectors, signals, frequencies, and protocols.

They provide common framework for data transmission, without which network communication would be chaotic, unreliable, and insecure. There are two types of standards: formal and de facto:

- A formal standard is developed by an official industry or government body. Formal standards typically take several years to develop, during which time technology changes, making them less useful. For example, there are formal standards for applications such as Web browsers (e.g., HTTP, HTML), for network layer software (e.g., IP), data link layer software (e.g., Ethernet IEEE 802.3), and for physical hardware (e.g., V.90 modems).

- De facto standards are those that emerge in the marketplace and are supported by several vendors but have no official standing. For example, Microsoft Windows is a product of one company and has not been formally recognized by any standards organization, yet it is a de facto standard. In the communications industry, de facto standards often become formal standards once they have been widely accepted.

1. American National Standards Institute (ANSI)

The American National Standards Institute (or ANSI) is a United States-based organization responsible for US standards and assessment systems. The standards established by this group are geared towards strengthening the US position in the international global economy. These standards govern the computer and technology industry. ANSI is the main body responsible for coordinating and publishing information on standards in the networking and technology industry in the United States. There are about 13,000 standards under their control.

One of the most common and long-standing standards they have established is the American Standard Code for Information Interchange (ASCII). This is a standard that is responsible for the codes used to represent text used in computers, telecommunication equipment, and other digital devices.

2. International Organization for Standardization (ISO)

This is one of the most important standards bodies that which makes technical recommendations about data communication interfaces. ISO is based in Geneva, Switzerland. The membership is composed of the national standards organizations of each ISO member country.

3. International Telecommunication Union - Telecommunication Standardization Sector (ITU-T)

ITU is a specialized agency of the United Nations responsible for many matters related to information and communication technologies. It was originally established as the International Telegraph Union, which drafted the earliest international standards and regulations governing international telegraph networks.

ITU promotes the shared global use of the radio spectrum, facilitates international cooperation in assigning satellite orbits, assists in developing and coordinating worldwide technical standards, and works to improve telecommunication infrastructure in the developing world. It is also active in the areas of broadband Internet, wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, TV broadcasting, amateur radio, and next-generation networks. It is Geneva, Switzerland, with global membership including 193 countries and around 900 businesses, academic institutions, and international and regional organizations both public and private sectors that operate computer or communications networks or build network software and equipment, examples Google, AT&T, Slack Technology.

4. Institute of Electrical and Electronics Engineers (IEEE)

This is an organization of electrical engineering and electronics dedicated to advancing technological innovation and creating standards in a wide area of industries including power and energy, healthcare, telecommunications, and networking. Important IEEE networking standards include IEEE 802.3, which encompasses many popular networking technologies including Ethernet. They promote the development and application of electro-technology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of their members.

Importance of Network Standards

i. Interoperability: Standards ensure that different devices and systems can work together seamlessly, regardless of who manufactured them. Without standards, it would be difficult to connect devices from different vendors and get them to communicate with each other.

ii. Compatibility: Standards ensure that new devices and systems can be added to an existing network without causing problems. If a new device is not built to the same standards as the rest of the network, it may not be compatible and could cause issues such as data loss or security breaches.

iii. Cost-effectiveness: Adopting standards can help reduce costs by allowing companies to use off-the-shelf components and equipment that have been tested and proven to work with other devices on the network. This can be more cost-effective than developing custom solutions for every aspect of the network.

iv. Safety: Standards help ensure the safety of network users by establishing guidelines for the design and operation of network components. For example, electrical safety standards help prevent fire and other hazards.

v. Performance: Standards can help optimize the performance of a network by specifying how devices should transmit and receive data. For example, standards for networking protocols can help ensure that data is transmitted efficiently and without errors.