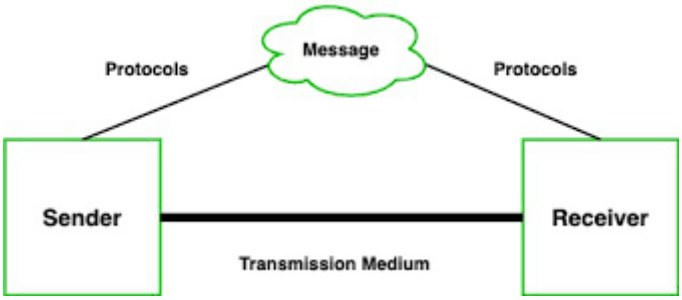
# Table of Contents

Introduction to data communication

Data communication is the process of transferring data from one place to another or between two locations. It allows electronic and digital data to move between two networks, no matter where the two are located geographically, what the data contains, or what format they are in [1].




Components of data communication.

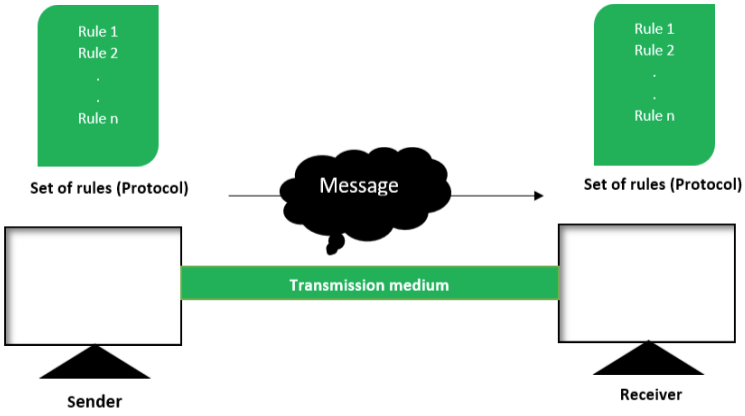
Message: This is the most useful asset of a data communication system. The message simply refers to data or piece of information which is to be communicated. A message could be in any form, it may be in the form of a text file, an audio file, a video file, etc.

Sender: To transfer message from source to destination, someone must be there who will play role of a source. Sender plays part of a source in data communication system. It is simple a device that sends data messages. The device could be in the form of a computer, mobile, telephone, laptop, video camera, or a workstation, etc.

Receiver: It is destination where finally message sent by source has arrived. It is a device that receives messages. Same as sender, receiver can also be in form of a computer, telephone mobile, workstation, etc.

Transmission Medium: In the entire process of data communication, there must be something which could act as a bridge between sender and receiver, Transmission medium plays that part. It is the physical path by which data or message travels from sender to receiver. Transmission medium could be guided (with wires) or unguided (without wires), for example, twisted pair cable, fiber optic cable, radio waves, microwaves, etc.

Set of rules (Protocol): To govern data communications, various sets of rules had been already designed by the designers of the communication systems, which represent a kind of agreement between communicating devices. These are defined as protocol. In simple terms, the protocol is a set of rules that govern data communication. If two different devices are connected but there is no protocol among them, there would not be any kind of communication between those two devices. Thus, the protocol is necessary for data communication to take place [1].




Importance of data communication

Global Connectivity: Data communication enables instant and efficient communication across the globe, allowing people and organizations to connect and collaborate regardless of geographical boundaries.

Business Operations: In business, data communication facilitates the exchange of information within an organization and with external stakeholders such as customers, suppliers, and partners. This includes emails, video conferences, file sharing, and more, all of which are vital for smooth operations and decision-making.

Information Sharing: Data communication allows for the rapid sharing of information, fostering collaboration and innovation. From research findings to market trends, timely access to data enables informed decision-making and drives progress in various fields.

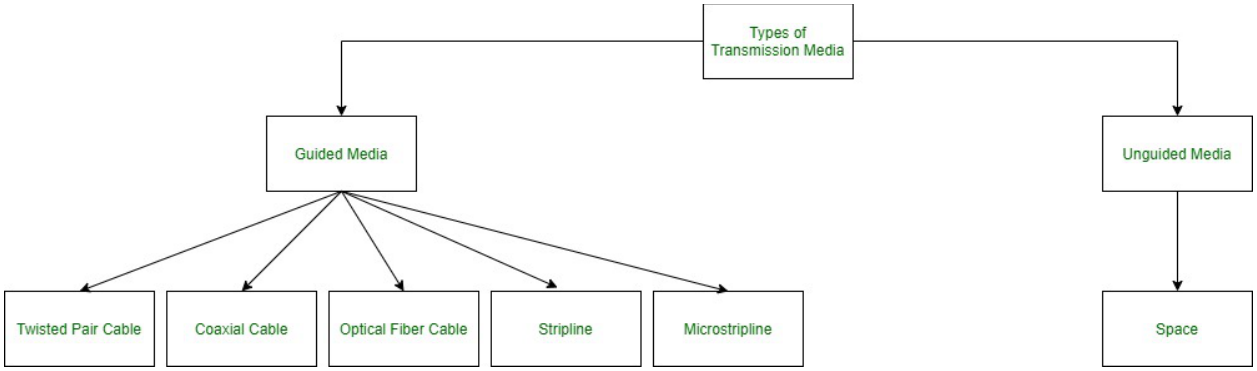
Economic Growth: The ability to transmit data efficiently contributes to economic growth by facilitating trade, enabling e-commerce, and supporting the development of new industries such as cloud computing, big data analytics, and Internet of Things (IoT) technologies.

Education and Research: Data communication is essential in education and research, enabling access to online resources, virtual classrooms, collaborative research projects, and the sharing of scholarly publications. It democratizes access to knowledge and supports lifelong learning.

Data transmission media

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types [2]:

Types of data transmission media




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

Features:

High Speed

Secure

Used for comparatively shorter distances.

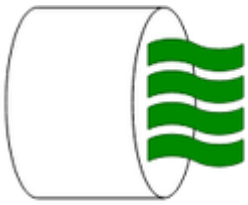
There are 3 major types of Guided Media:

(I) Twisted Pair Cable –

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

Unshielded Twisted Pair (UTP):

UTP consists of two insulated copper wires twisted around one another. This type of cable could block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.



Unshielded Twisted Pair

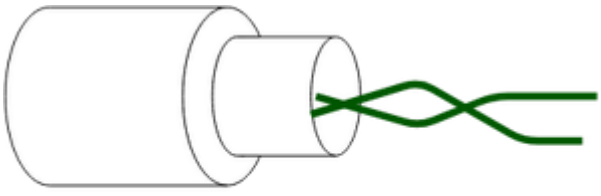
Advantages:

⇢ Least expensive⇢ Easy to install⇢ High-speed capacity

Disadvantages: ⇢ Susceptible to external interference⇢ Lower capacity and performance in comparison to STP⇢ Short distance transmission due to attenuation

Shielded Twisted Pair (STP):

This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Shielded Twisted Pair

Advantages: ⇢ Better performance at a higher data rate in comparison to UTP⇢ Eliminates crosstalk⇢ Comparatively faster

Disadvantages: ⇢ Comparatively difficult to install and manufacture⇢ More expensive⇢ Bulky

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

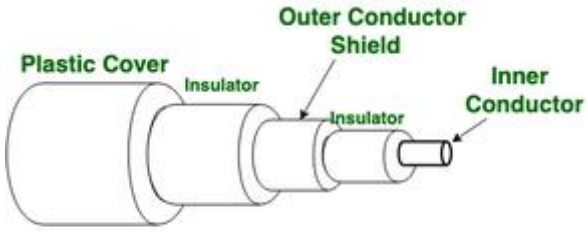



Figure of Coaxial Cable

Advantages:

1.High Bandwidth 2. Better noise Immunity 3. Easy to install and expand4.Inexpensive

Disadvantages: 1. Single cable failure can disrupt the entire network

Optical Fiber Cable –
It uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called cladding. It is used for the transmission of large volumes of data. The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

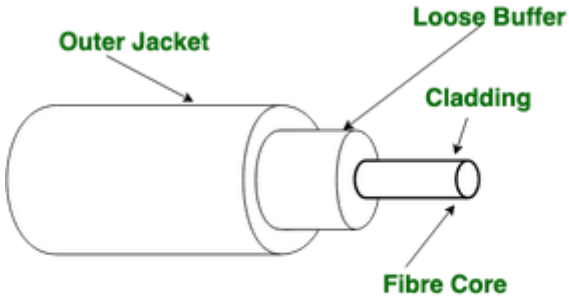



Figure of Optical Fibre Cable

Advantages:

1.Increased capacity and bandwidth 2. Lightweight 3. Less signal attenuation 4. Immunity to electromagnetic interference5.Resistance to corrosive materials

Disadvantages:

1.Difficult to install and maintain 2. High cost 3. Fragile.

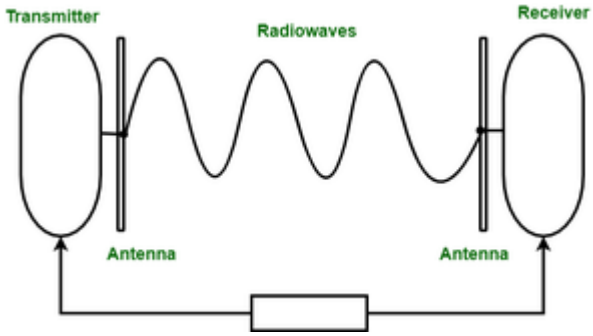
Unguided Media:

It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals. The signal is broadcast through air, Secure, Used for larger distances.

There are 3 types of Signals transmitted through unguided media:

(i) Radio waves –

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission. Further Categorized as (i) Terrestrial and (ii) Satellite.




(ii) Microwaves –

It is a line-of-sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

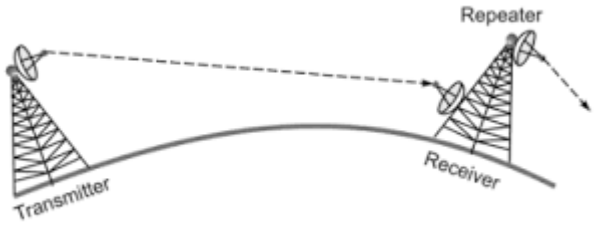
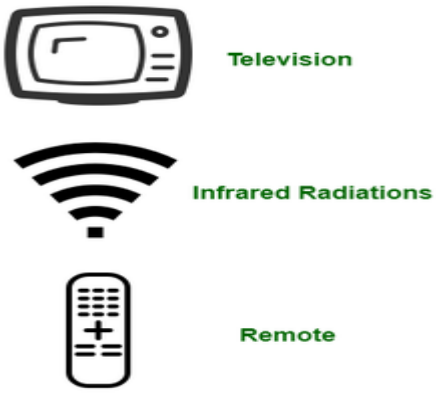



***Fig: Microwave Transmission***

(iii) Infrared –

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc [3].




Modulation

AM − It is known as amplitude modulation used to increase the amplitude of the signals.

FM − It is known as frequency modulation used to amplify the frequency of signals.

PM − Phase modulation is modulation in which the phase of the carrier wave is varied and is used for the transmission of signals.

Data transmission modes

Transmission mode means transferring data between two devices. It is also known as a communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected.

There are three types of transmission mode: -

These are explained as follows below.

1. Simplex Mode –
In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.

Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output [1].

Advantages:

There is no need for coordination between the transmitting and receiving devices, which simplifies the communication process.

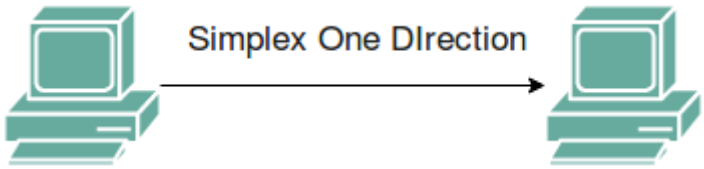
Simplex mode is particularly useful in situations where feedback or response is not required, such as broadcasting or surveillance.

Disadvantages:

Only one-way communication is possible.

There is no way to verify if the transmitted data has been received correctly.

Simplex mode is not suitable for applications that require bidirectional communication.



2. Half-Duplex Mode –

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sent, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie-talkie in which message is sent one at a time and messages are sent in both directions. Channel capacity=Bandwidth * Propagation Delay

Advantages:

Half-duplex mode allows for bidirectional communication, which is useful in situations where devices need to send and receive data.

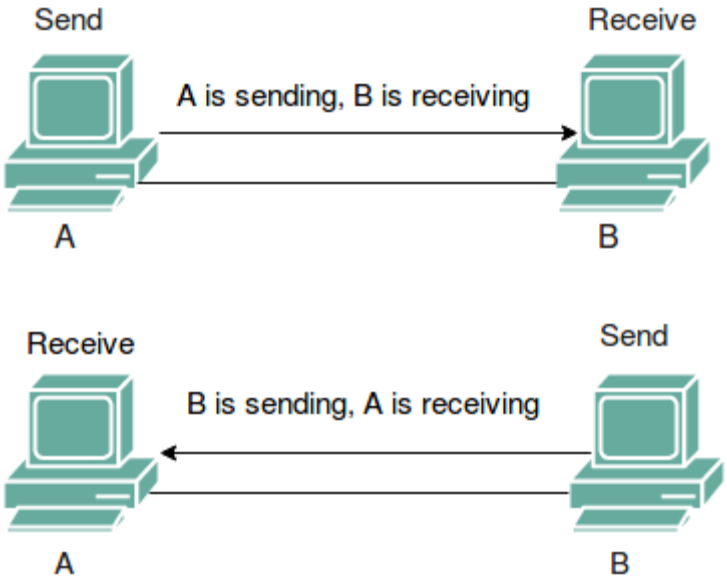
Half-duplex mode is less expensive than full-duplex mode, as it only requires one communication channel.

Disadvantages:

Half-duplex mode is less reliable than Full-Duplex mode, as both devices cannot transmit at the same time.

There is a delay between transmission and reception, which can cause problems in some applications.

There is a need for coordination between the transmitting and receiving devices, which can complicate the communication process [1].




3. Full-Duplex Mode –

In full-duplex mode, both stations can transmit and receive mail simultaneously. In fullduplex mode, signals going in one direction share the capacity of the link with signals going in another direction, this sharing can occur in two ways:

Either the link must contain two physically separate transmission paths, one for sending and the other for receiving.

Or the capacity is divided between signals traveling in both directions.

A full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

Example: Telephone Network in which there is communication between two people by a telephone line, through which both can talk and listen at the same time. Channel Capacity=2* Bandwidth*propagation Delay

Advantages:

Full-duplex mode allows for simultaneous bidirectional communication, which is ideal for real-time applications such as video conferencing or online gaming.

It is the most efficient mode of communication, as both devices can transmit and receive data simultaneously.

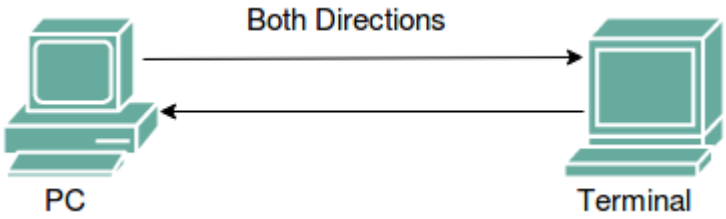
Full-duplex mode provides a high level of reliability and accuracy, as there is no need for error correction mechanisms.

Disadvantages:

Full-duplex mode is the most expensive mode, as it requires two communication channels.

It is more complex than simplex and half-duplex modes, as it requires two physically separate transmission paths or a division of channel capacity.

Full-duplex mode may not be suitable for all applications, as it requires a high level of bandwidth and may not be necessary for some types of communication [2].




Switching

In computer networking, Switching is the process of transferring data packets from one device to another in a network, or from one network to another, using specific devices called switches. A computer user experiences switching all the time for example, accessing the Internet from your computer device, whenever a user requests a webpage to open, the request is processed through switching of data packets only [4].

Types of Switching

There are three types of switching methods:

1.Message Switching 2. Circuit Switching

3.Packet Switching 4. Datagram Packet Switching

5.Virtual Circuit Packet Switching

1.Message Switching: This is an old switching technique that has become obsolete. In message switching technique, the entire data block/message is forwarded across the entire network thus, making it highly inefficient.

2.Circuit Switching: In this type of switching, a connection is established between the source and destination beforehand. This connection receives the complete bandwidth of the network until the data is transferred completely. This approach is better than message switching as it does not involve sending data to the entire network, instead of its destination only.

3.Packet Switching: This technique requires the data to be broken down into smaller components, data frames, or packets. These data frames are then transferred to their destinations according to the available resources in the network at a particular time. This switching type is used in modern computers and even the Internet. Here, each data frame contains additional information about the destination and other information required for proper transfer through network components.

4.Datagram Packet Switching: In Datagram Packet switching, each data frame is taken as an individual entity and thus, they are processed separately. Here, no connection is

established before data transmission occurs. Although this approach provides flexibility in data transfer, it may cause a loss of data frames or late delivery of the data frames.

5.Virtual-Circuit Packet Switching: In Virtual-Circuit Packet switching, a logical connection between the source and destination is made before transmitting any data. These logical connections are called virtual circuits. Each data frame follows these logical paths and provides a reliable way of transmitting data with less chance of data loss [4].

Point to point communication.

In telecommunications, a point-to-point connection is a communications link between two communication endpoints or nodes. A telephone call is an example of this, in which two phones are linked, and what one caller says can only be heard by the other. A "point-to-multipoint" or broadcast link, on the other hand, allows multiple nodes to receive information sent by a single node. Leased lines and microwave radio relays are also examples of point-to-point connections. In a point-to-point communication, there will be a transmitter and a receiver connected with a suitable connection. The capacity of the connecting channel remains unchanged throughout communication [4].

Types of Networks

Local Area Network (LAN) –

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN. Data is transmitted at a very fast rate as the number of computers linked is limited. The connections must be high-speed and relatively inexpensive hardware

(Such as hubs, network adapters, and Ethernet cables). LANs cover a smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, school, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted-pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Advantages:

Provides fast data transfer rates and high-speed communication.

Easy to set up and manage.

Can be used to share peripheral devices such as printers and scanners.

Provides increased security and fault tolerance compared to WANs.

Disadvantages:

Limited geographical coverage.

Limited scalability and may require significant infrastructure upgrades to accommodate growth.

May experience congestion and network performance issues with increased usage [4].

Metropolitan Area Network (MAN) –

MAN, or Metropolitan area Network covers a larger area than that covered by a LAN and a smaller area as compared to WAN. MAN has a range of 5-50km. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need high-speed connectivity. Speeds of MAN range in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.

Advantages:

Provides high-speed connectivity over a larger geographical area than LAN.

Can be used as an ISP for multiple customers.

Offers higher data transfer rates than WAN in some cases.

Disadvantages:

Can be expensive to set up and maintain.

May experience congestion and network performance issues with increased usage.

May have limited fault tolerance and security compared to LANs [4].

Wide Area Network (WAN) –
WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. WAN has a range of above 50 km. A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high-speed and relatively expensive.

Advantages:

Covers large geographical areas and can connect remote locations.

Provides connectivity to the internet.

Offers remote access to resources and applications.

Can be used to support multiple users and applications simultaneously.

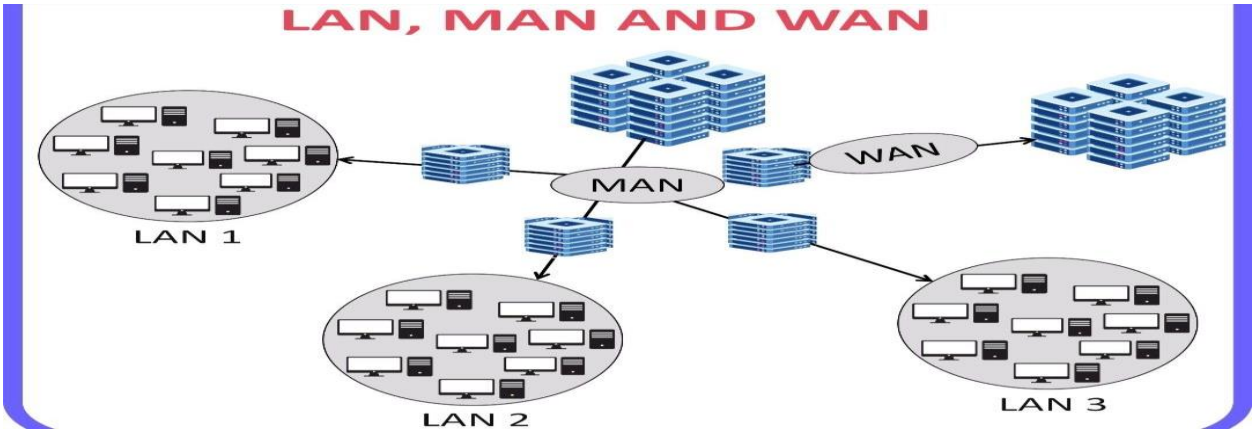
Disadvantages:

Can be expensive to set up and maintain.

Offers slower data transfer rates than LAN or MAN.

May experience higher latency and longer propagation delays due to longer distances and multiple network hops.

May have lower fault tolerance and security compared to LANs [4].




Network topology [1].

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as Network Topology. The various network topologies are:

1.Mesh Topology 2. Star Topology 3. Bus Topology 4. Ring Topology

5.Tree Topology 6. Hybrid Topology

Types of Network Topology

Bus Topology

In the case of Bus topology, all devices share a single communication line or cable. Bus topology may have problems while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning. Both ends of the shared channel have line terminator. The data is

sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point-to-point connection between hosts and hub. The hub device can be any of the following:

Layer-1 device such as hub or repeater.

Layer-2 device such as switch or bridge.

Layer-3 device such as router or gateway.

Star Topology

As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. All communication between hosts takes place through only the hub.

Ring Topology

In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host to the existing structure, the administrator may need only one more extra cable. Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

Mesh Topology

In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.

Full Mesh Topology

Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types: Full Mesh: All hosts have a point-to-point connection to every other host in the network. Thus, for every new host n(n-1)/2

connections are required. It provides the most reliable network structure among all network topologies.

Partially Mesh: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

Tree Topology

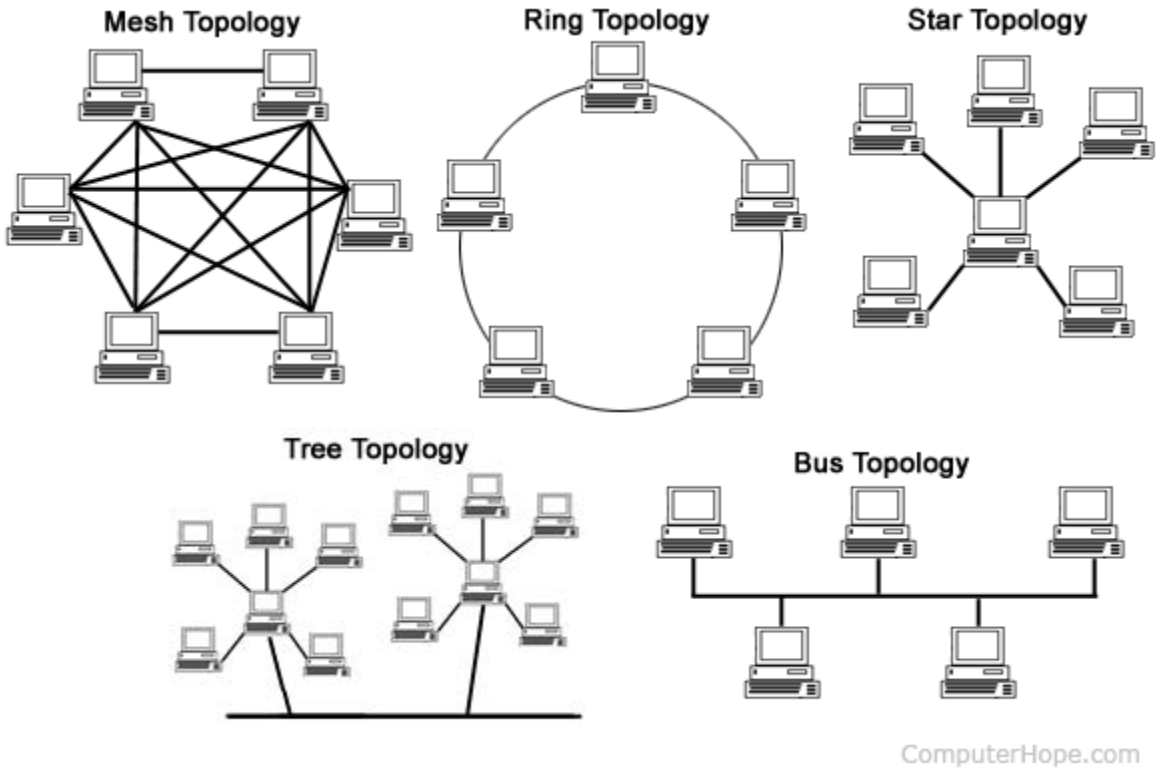
Also known as Hierarchical Topology, this is the most common form of network topology in use presently. This topology imitates extended Star topology and inherits properties of bus topology. This topology divides the network into multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is the access layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as the core layer, and is the central point of the network, i.e. root of the tree from which all nodes' forks.

Tree Topology

All neighboring hosts have point-to-point connections between them. Like the Bus topology, if the root goes down, then the entire network suffers even. Though it is not the single point of failure. Every connection serves as a point of failure, the failure of which divides the network into unreachable segments.

Hybrid Topology

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies. Combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. The Internet is the best example of the largest Hybrid topology.




Communication protocol

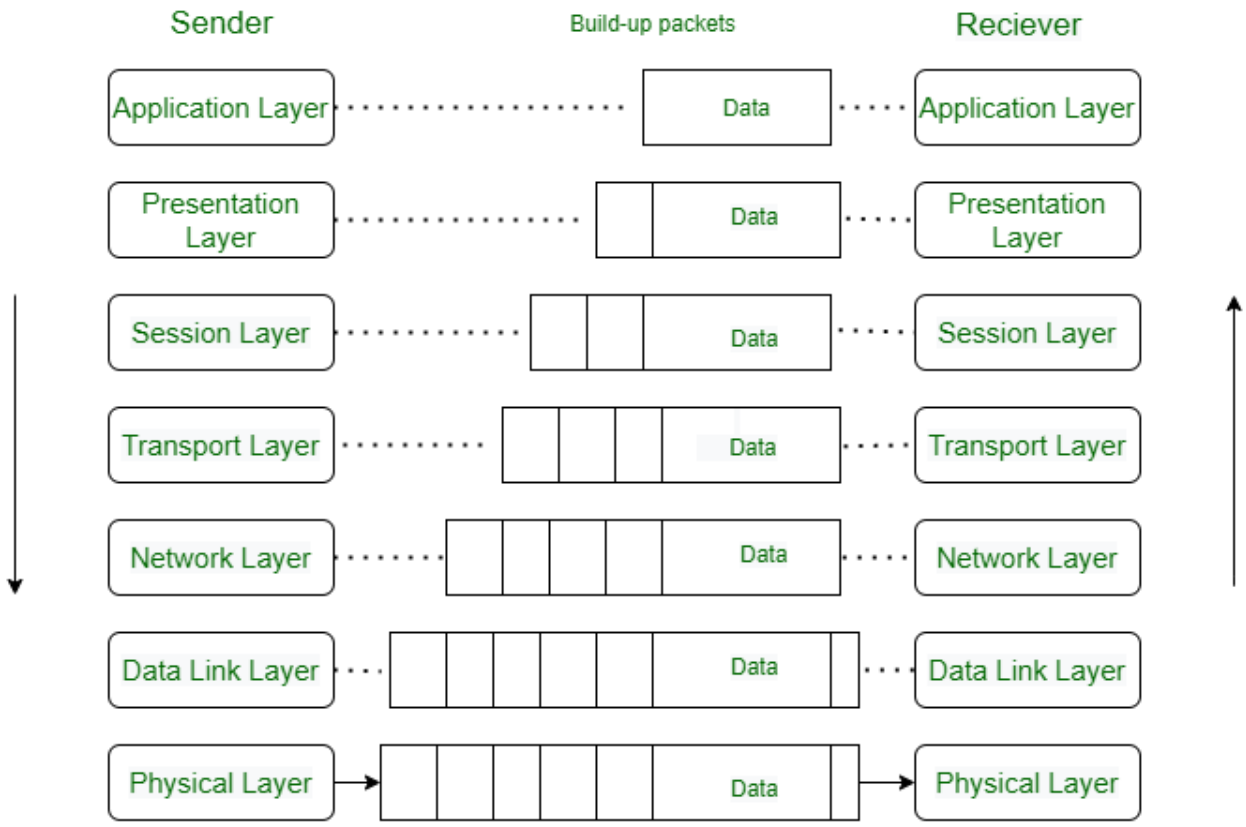
A communication protocol is a system of rules that allows two or more entities of a communications system to transmit information via any variation of a physical quantity. The protocol defines the rules, syntax, semantics, and synchronization of communication and possible error recovery methods. Protocols may be implemented by hardware, software, or a combination of both.

OSI MODEL [2]

What is OSI Model?

The OSI model, created in 1984 by ISO, is a reference framework that explains the process of transmitting data between computers. It is divided into seven layers that work together

to carry out specialized network functions, allowing for a more systematic approach to networking.



What are the 7 layers of the OSI Model?

The OSI model consists of seven abstraction layers arranged in a top-down order:

1.Physical Layer 2. Data Link Layer 3. Network Layer 4. Transport Layer

5.Session Layer 6. Presentation Layer 7. Application Layer

Physical Layer – Layer 1

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next.

Functions of the Physical Layer

Bit synchronization, Bit rate control, Physical topologies, Transmission mode

Hub, Repeater, Modem, and Cables are Physical Layer devices.

Network Layer, Data Link Layer, and Physical Layer are also known as Lower Layers or Hardware Layers.

Data Link Layer (DLL) – Layer 2

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.

The Data Link Layer is divided into two sublayers:

Functions of the Data Link Layer

Framing, Physical addressing, Error control, Flow Control Access control.

Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.

Switch & Bridge are Data Link Layer devices.

Network Layer – Layer 3

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

Functions of the Network Layer

Routing, Logical Addressing.

Segment in the Network layer is referred to as Packet.

Network layer is implemented by networking devices such as routers and switches.

Transport Layer – Layer 4

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as Segments. It is responsible for the End-to-End Delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

At the sender's side: The transport layer receives the formatted data from the upper layers, performs Segmentation, and implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

Functions of the Transport Layer

Segmentation and Reassembly, Service Point Addressing, Services Provided by Transport Layer, Connection-Oriented Service, Connectionless Service. Device or Protocol Use: TCP, UDP NetBIOS, PPTP

Session Layer – Layer 5

This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and ensures security.

Functions of the Session Layer

Session establishment, maintenance, and termination: The layer allows the two processes to establish, use and terminate a connection.

Synchronization: This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely, and data loss is avoided.

Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full duplex.

Presentation Layer – Layer 6

The presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

Functions of the Presentation Layer

Translation: For example, ASCII to EBCDIC.

Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext, and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

Compression: Reduces the number of bits that need to be transmitted on the network.

Note: Device or Protocol Use:  JPEG, MPEG, GIF

Application Layer – Layer 7

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which must be transferred over the network. This layer also serves as a window for the

application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.

Functions of the Application Layer

The main functions of the application layer are given below.

Network Virtual Terminal: It allows a user to log on to a remote host.

FTAM- File transfer access and management: This application allows a user to

access file in a remote host, retrieve files in remote host and manage or

control files from a remote computer.

Mail Services: Provide email service.

Directory Services: This application provides distributed database sources.

and access for global information about various objects and services.

Network devices.

Network Devices: Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example, Repeater, Hub, Bridge, Switch, Routers, Gateway, and NIC, etc.

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

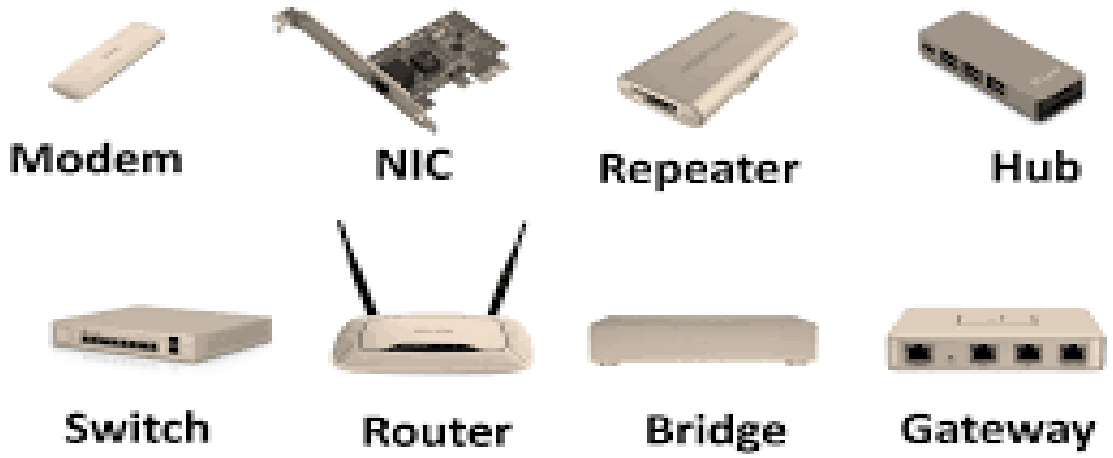
2. Hub – A hub is basically a multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.

In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

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

4.Routers – A router is a device that is like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updated routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

5. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency (many ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.




Types of Network Devices

References

[1] "geeksforgeeks," [Online]. Available: www.geeksforgeeks.org. [Accessed 29 02 2024].

[2] "Tutorial point," [Online]. Available: https://www.tutorialspoint.com/. [Accessed 29 02 2024].

[4] "chatgpt," [Online]. Available: www.chatgpt.com. [Accessed 29 02 2024].