1.COMPUTER NETWORKS

A computer network is a system that connects numerous independent computers in order to share information (data) and resources. The integration of computers and other different devices allows users to communicate more easily.

A computer network is a collection of two or more computer systems that are linked together. A network connection can be established using either cable or wireless media. Hardware and software are used to connect computers and tools in any network.

A computer network consists of various kinds of nodes. Servers, networking hardware, personal computers, and other specialized or general-purpose hosts can all be nodes in a computer network. Host names and network addresses are used to identify them.

2.What Do Computer Networks Do?

Computer Networks are one of the important aspects of Computer Science. In the early days, it is used for data transmission on telephone lines and had a very limited use, but nowadays, it is used in a variety of places.

Computer Networks help in providing better connectivity that helps nowadays. Modern computer networks have the following functionality like

-Computer Networks help in operating virtually.

-Computer Networks integrate on a large scale.

-Computer Networks respond very quickly in case of conditions change.

-Computer Networks help in providing data security.

3.Criteria of a Good Network

Performance: It can be measured in many ways, including transmit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of the network depends on a number of factors, including the number of users, the type of medium & Hardware

Reliability: In addition to accuracy is measured by frequency of failure, the time it takes a link to recover from failure, and the network's robustness in catastrophe.

Security: Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data loss.

4.Goals of Computer Networking

Programs do not have to execute on a single system because of resource and load sharing.

Reduced costs – Multiple machines can share printers, tape drives, and other peripherals.

Reliability – If one machine fails, another can take its place.

Scalability (it's simple to add more processors or computers)

Communication and mail (people living apart can work together)

Information Access (remote information access, access to the internet, e-mail, video conferencing, and online shopping)

Entertainment that is interactive (online games, videos, etc.)

5.Types of Computer Networks

Division Based on the Communication Medium

Wired Network: As we all know, "wired" refers to any physical medium made up of cables. Copper wire, twisted pair, or fiber optic cables are all options. A wired network employs wires to link devices to the Internet or another network, such as laptops or desktop PCs.

Wireless Network: "Wireless" means without wire, media that is made up of electromagnetic waves (EM Waves) or infrared waves. Antennas or sensors will be present on all wireless devices. Cellular phones, wireless sensors, TV remotes, satellite dish receivers, and laptops with WLAN cards are all examples of wireless devices. For data or voice communication, a wireless network uses radio frequency waves rather than wires.

6.Differences between LAN, MAN, and WAN

6.1Metropolitan 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:

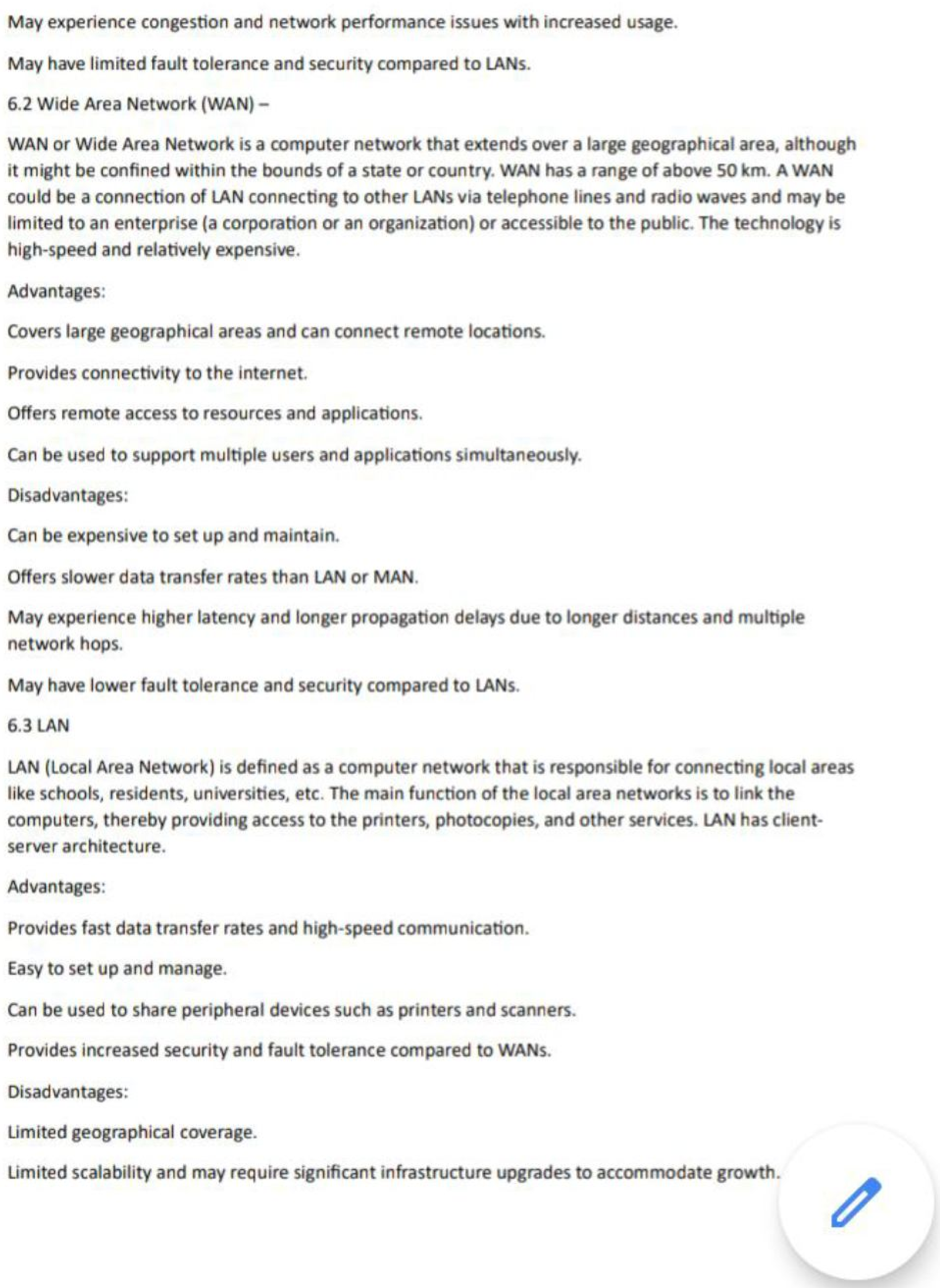
Provides high-speed connectivity over a larger geographical area than LAN.

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.

6.2 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.

6.3 LAN

LAN (Local Area Network) is defined as a computer network that is responsible for connecting local areas like schools, residents, universities, etc. The main function of the local area networks is to link the computers, thereby providing access to the printers, photocopies, and other services. LAN has client-server architecture.

Advantages:

Provides fast data transfer rates and high-speed communication.

Easy to set up and manage.

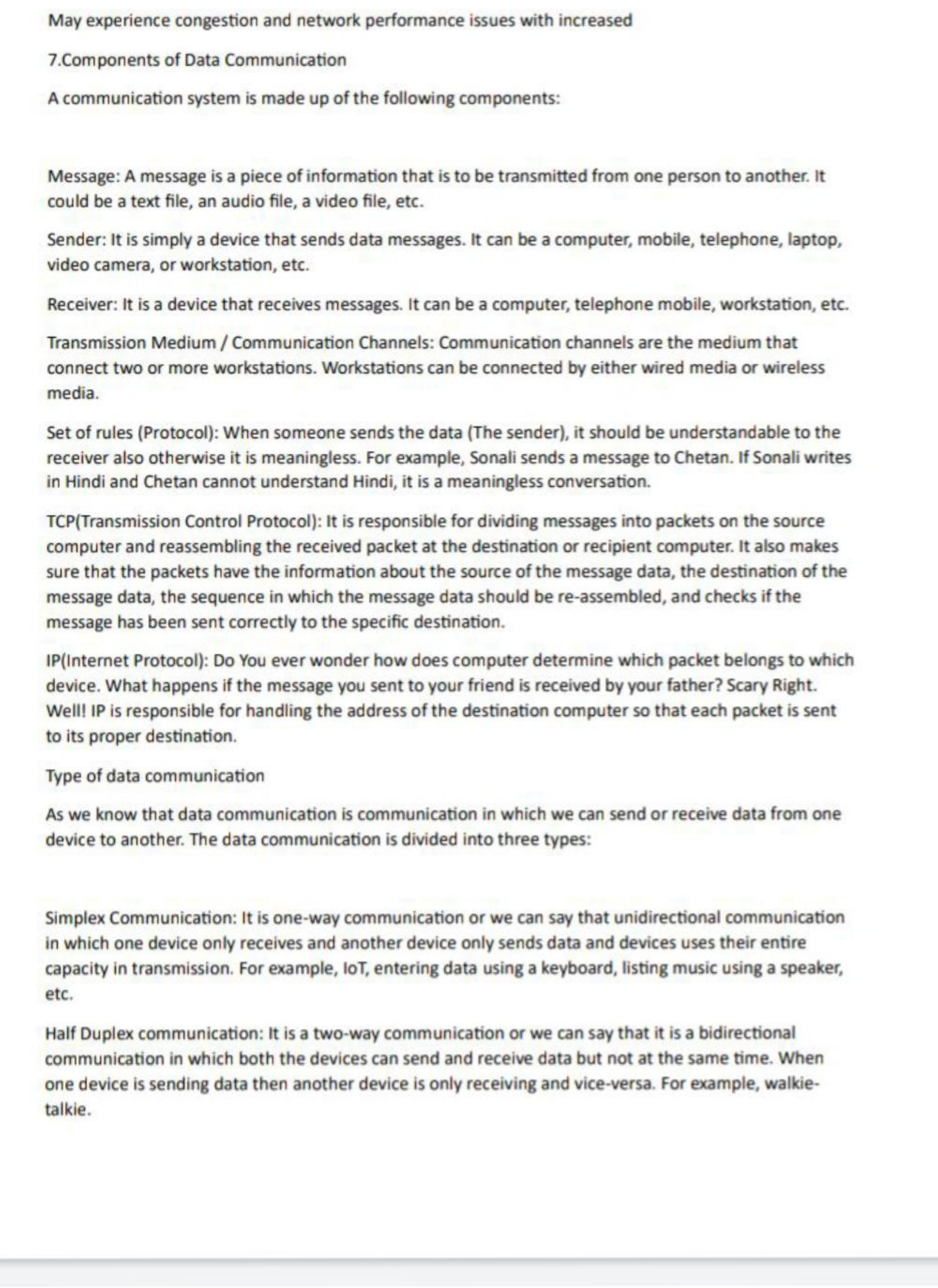
Can be used to share peripheral devices such as printers and scanners.

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

7.Components of Data Communication

A communication system is made up of the following components:

Message: A message is a piece of information that is to be transmitted from one person to another. It could be a text file, an audio file, a video file, etc.

Sender: It is simply a device that sends data messages. It can be a computer, mobile, telephone, laptop, video camera, or workstation, etc.

Receiver: It is a device that receives messages. It can be a computer, telephone mobile, workstation, etc.

Transmission Medium / Communication Channels: Communication channels are the medium that connect two or more workstations. Workstations can be connected by either wired media or wireless media.

Set of rules (Protocol): When someone sends the data (The sender), it should be understandable to the receiver also otherwise it is meaningless. For example, Sonali sends a message to Chetan. If Sonali writes in Hindi and Chetan cannot understand Hindi, it is a meaningless conversation.

TCP(Transmission Control Protocol): It is responsible for dividing messages into packets on the source computer and reassembling the received packet at the destination or recipient computer. It also makes sure that the packets have the information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination.

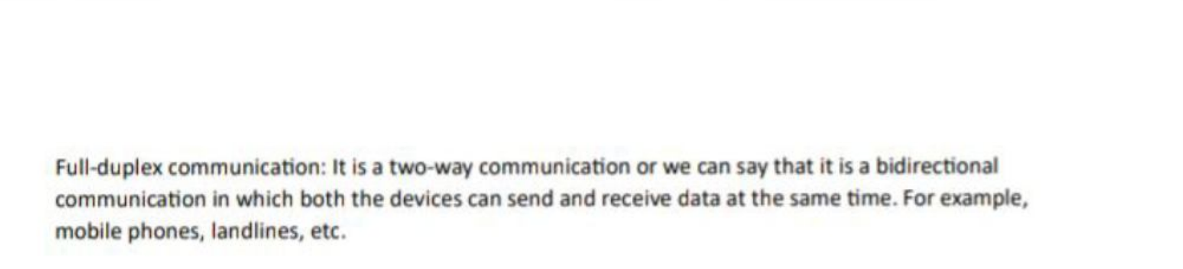
IP(Internet Protocol): Do You ever wonder how does computer determine which packet belongs to which device. What happens if the message you sent to your friend is received by your father? Scary Right. Well! IP is responsible for handling the address of the destination computer so that each packet is sent to its proper destination.

Type of data communication

As we know that data communication is communication in which we can send or receive data from one device to another. The data communication is divided into three types:

Simplex Communication: It is one-way communication or we can say that unidirectional communication in which one device only receives and another device only sends data and devices uses their entire capacity in transmission. For example, IoT, entering data using a keyboard, listing music using a speaker, etc.

Half Duplex communication: It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data but not at the same time. When one device is sending data then another device is only receiving and vice-versa. For example, walkie-talkie.



Full-duplex communication: It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data at the same time. For example, mobile phones, landlines, etc.

Type of data communication

As we know that data communication is communication in which we can send or receive data from one device to another. The data communication is divided into three types:

*Simplex Communication: It is one-way communication or we can say that unidirectional communication in which one device only receives and another device only sends data and devices uses their entire capacity in transmission. For example, IoT, entering data using a keyboard, listing music using a speaker, etc.

*Half Duplex communication: It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data but not at the same time. When one device is sending data then another device is only receiving and vice-versa. For example, walkie-talkie.

*Full-duplex communication: It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data at the same time. For example, mobile phones, landlines, etc.

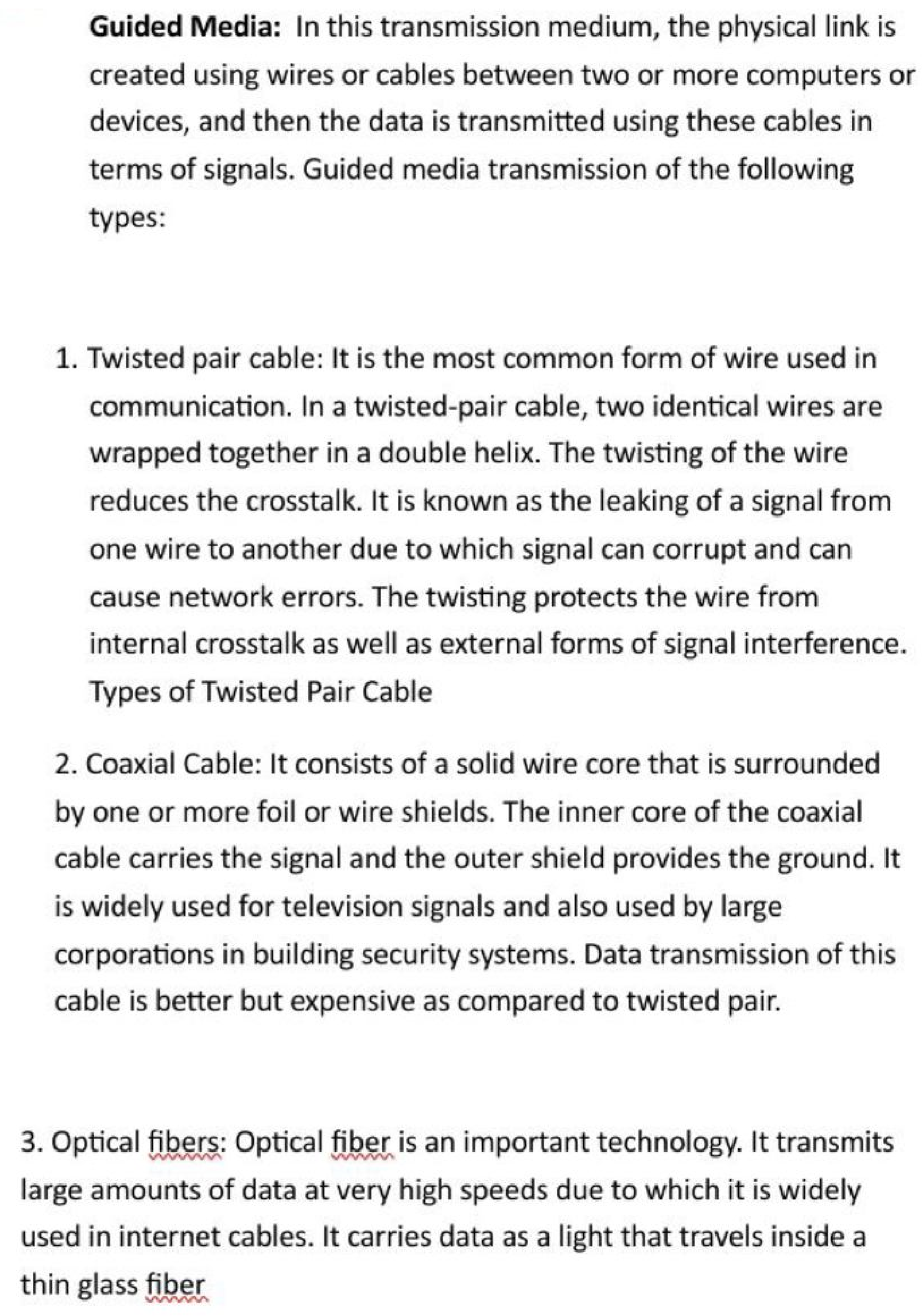
Communication Channels

Communication channels are the medium that connects two or more workstations. Workstations can be connected by either wired media or wireless media. It is also known as a transmission medium. The transmission medium or channel is a link that carries messages between two or more devices. We can group the communication media into two categories:

1.Guided media transmission

2.Unguided media transmission

Guided Media: In this transmission medium, the physical link is created using wires or cables between two or more computers or devices, and then the data is transmitted using these cables in terms of signals. Guided media transmission of the following types:



Guided Media: In this transmission medium, the physical link is created using wires or cables between two or more computers or devices, and then the data is transmitted using these cables in terms of signals. Guided media transmission of the following types:

1. Twisted pair cable: It is the most common form of wire used in communication. In a twisted-pair cable, two identical wires are wrapped together in a double helix. The twisting of the wire reduces the crosstalk. It is known as the leaking of a signal from one wire to another due to which signal can corrupt and can cause network errors. The twisting protects the wire from internal crosstalk as well as external forms of signal interference. Types of Twisted Pair Cable

2. Coaxial Cable: It consists of a solid wire core that is surrounded by one or more foil or wire shields. The inner core of the coaxial cable carries the signal and the outer shield provides the ground. It is widely used for television signals and also used by large corporations in building security systems. Data transmission of this cable is better but expensive as compared to twisted pair.

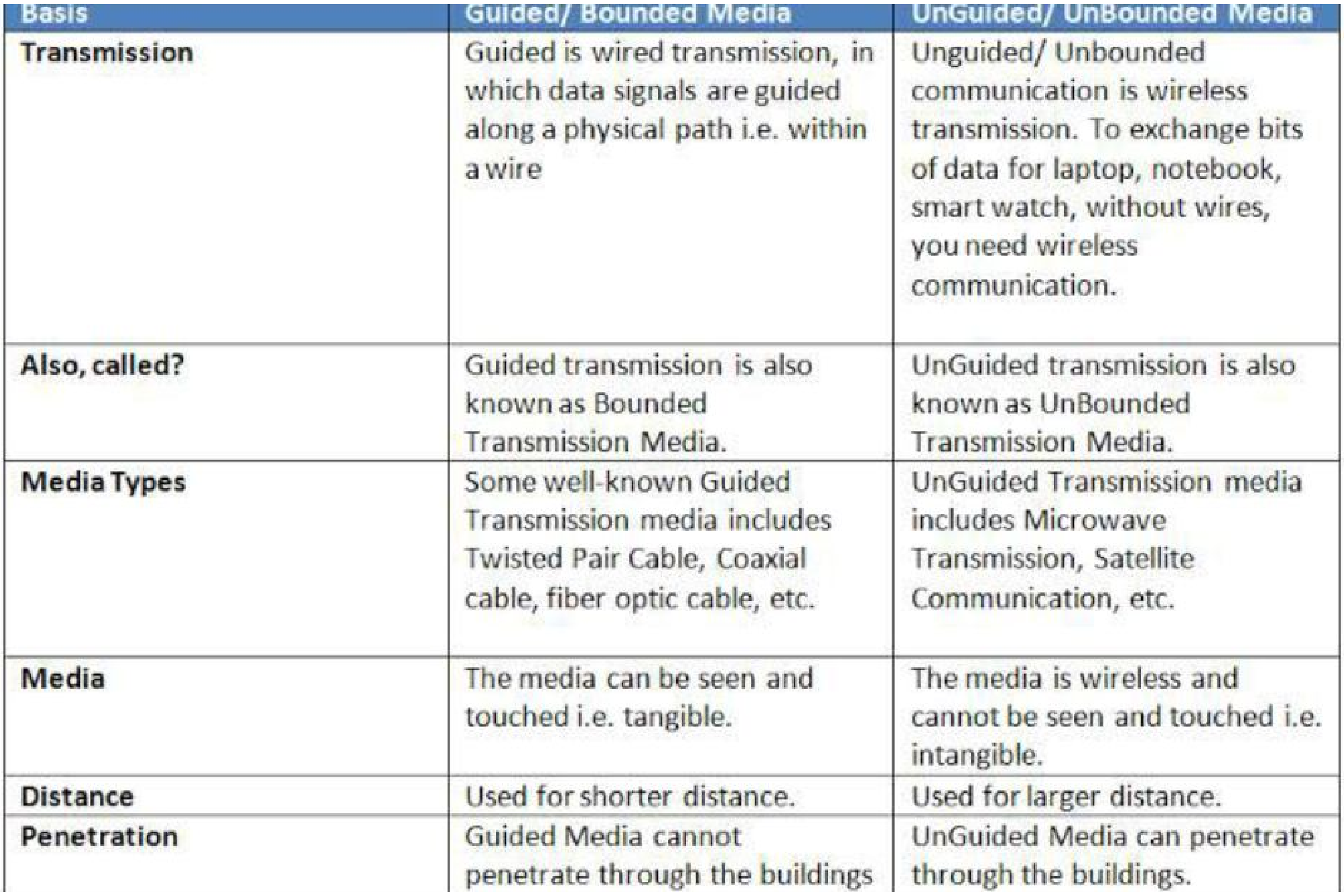
3. Optical fibers: Optical fiber is an important technology. It transmits large amounts of data at very high speeds due to which it is widely used in internet cables. It carries data as a light that travels inside a thin glass fiber

Unguided Media: The unguided transmission media is a transmission mode in which the signals are propagated from one device to another device wirelessly. Signals can wave through the air, water, or vacuum. It is generally used to transmit signals in all directions. Unguided Media is further divided into various parts :

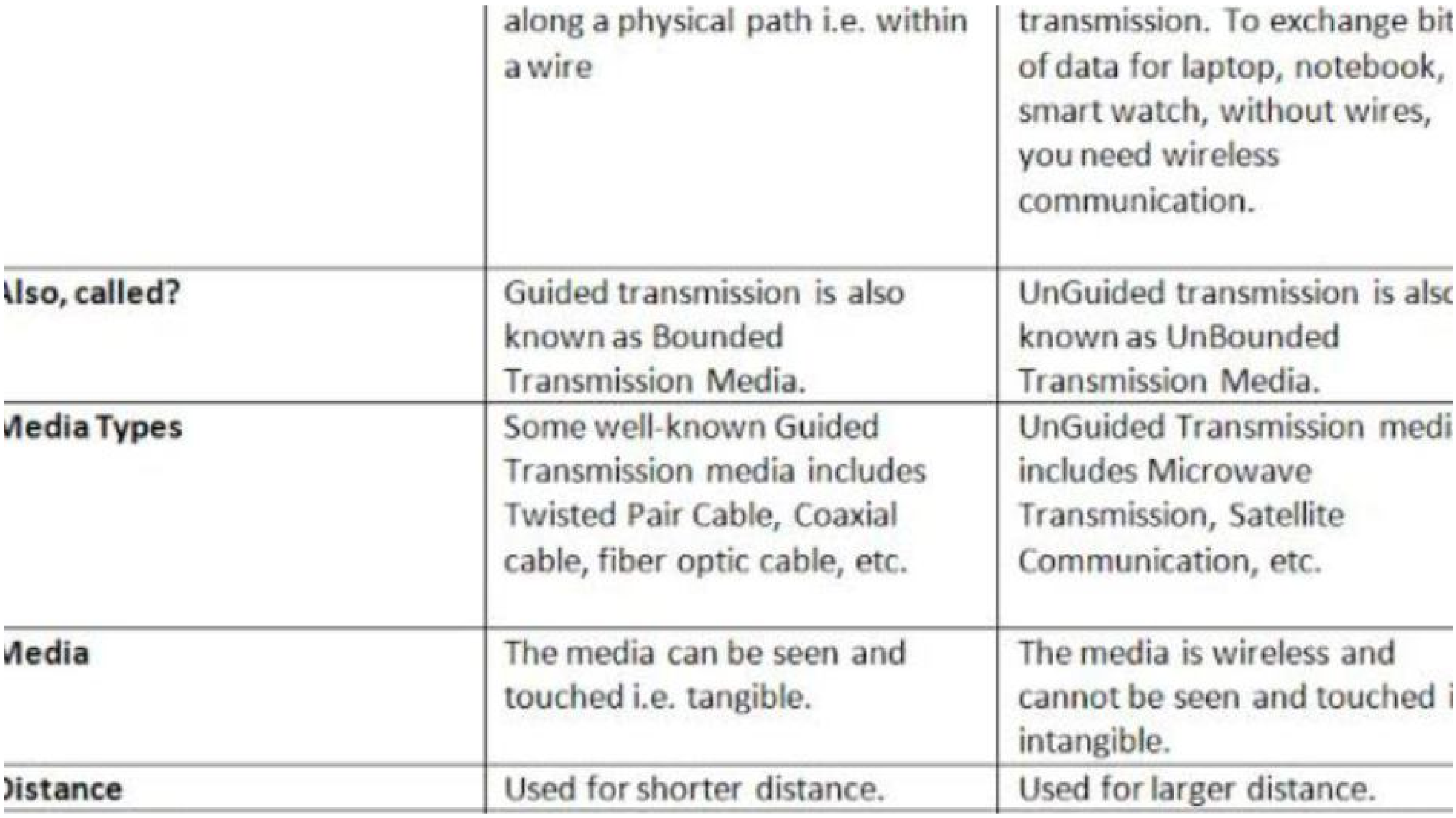
1. Microwave: Microwave offers communication without the use of cables. Microwave signals are just like radio and television signals. It is used in long-distance communication. Microwave transmission consists of a transmitter, receiver, and atmosphere. In microwave communication, there are parabolic antennas that are mounted on the towers to send a beam to another antenna. The higher the tower, the greater the range.

2. Radio wave: When communication is carried out by radio frequencies, then it is termed radio waves transmission. It offers mobility. It is consists of the transmitter and the receiver. Both use antennas to radiate and capture the radio signal.

3. Infrared: It is short-distance communication and can pass through any object. It is generally used in TV remotes, wireless mouse, etc.



Basis	Guided/ Bounded Media	UnGuided/ UnBounded Media
Transmission	Guided is wired transmission, in which data signals are guided along a physical path i.e. within a wire	Unguided/ Unbounded communication is wireless transmission. To exchange bits of data for laptop, notebook, smart watch, without wires, you need wireless communication.
Also, called?	Guided transmission is also known as Bounded Transmission Media.	UnGuided transmission is also known as UnBounded Transmission Media.
Media Types	Some well-known Guided Transmission media includes Twisted Pair Cable, Coaxial cable, fiber optic cable, etc.	UnGuided Transmission media includes Microwave Transmission, Satellite Communication, etc.
Media	The media can be seen and touched i.e. tangible.	The media is wireless and cannot be seen and touched i.e. intangible.
Distance	Used for shorter distance.	Used for larger distance.
Penetration	Guided Media cannot penetrate through the buildings	UnGuided Media can penetrate through the buildings.

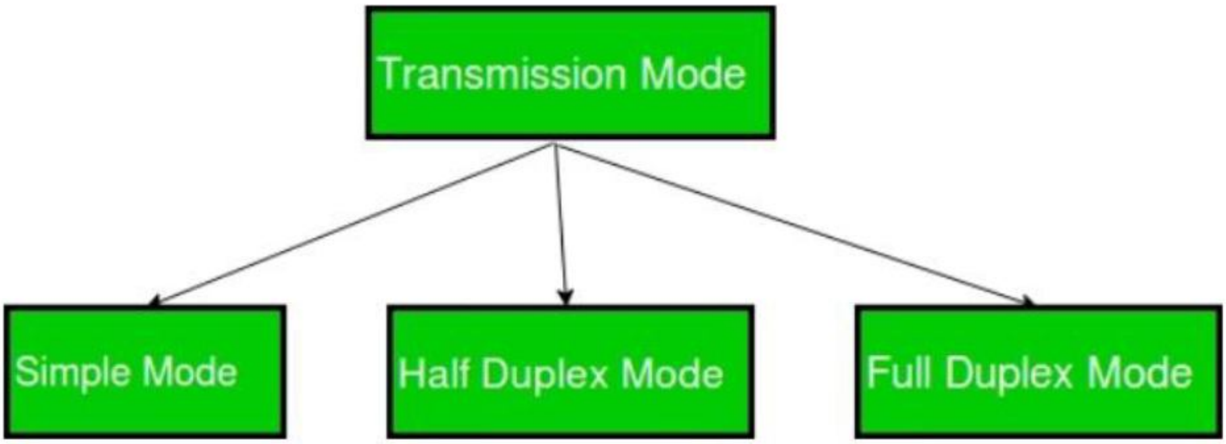


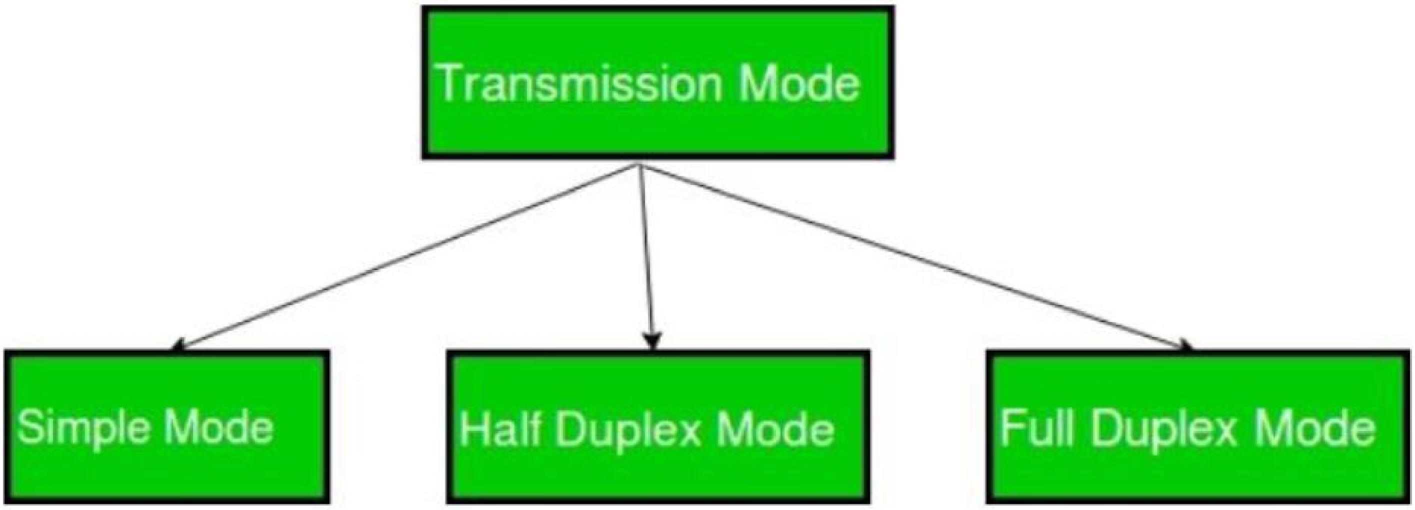
	along a physical path i.e. within a wire	transmission. To exchange bit of data for laptop, notebook, smart watch, without wires, you need wireless communication.
Also, called?	Guided transmission is also known as Bounded Transmission Media.	UnGuided transmission is alsc known as UnBounded Transmission Media.
Media Types	Some well-known Guided Transmission media includes Twisted Pair Cable, Coaxial cable, fiber optic cable, etc.	UnGuided Transmission medi includes Microwave Transmission, Satellite Communication, etc.
Media	The media can be seen and touched i.e. tangible.	The media is wireless and cannot be seen and touched i intangible.
Distance	Used for shorter distance.	Used for larger distance.

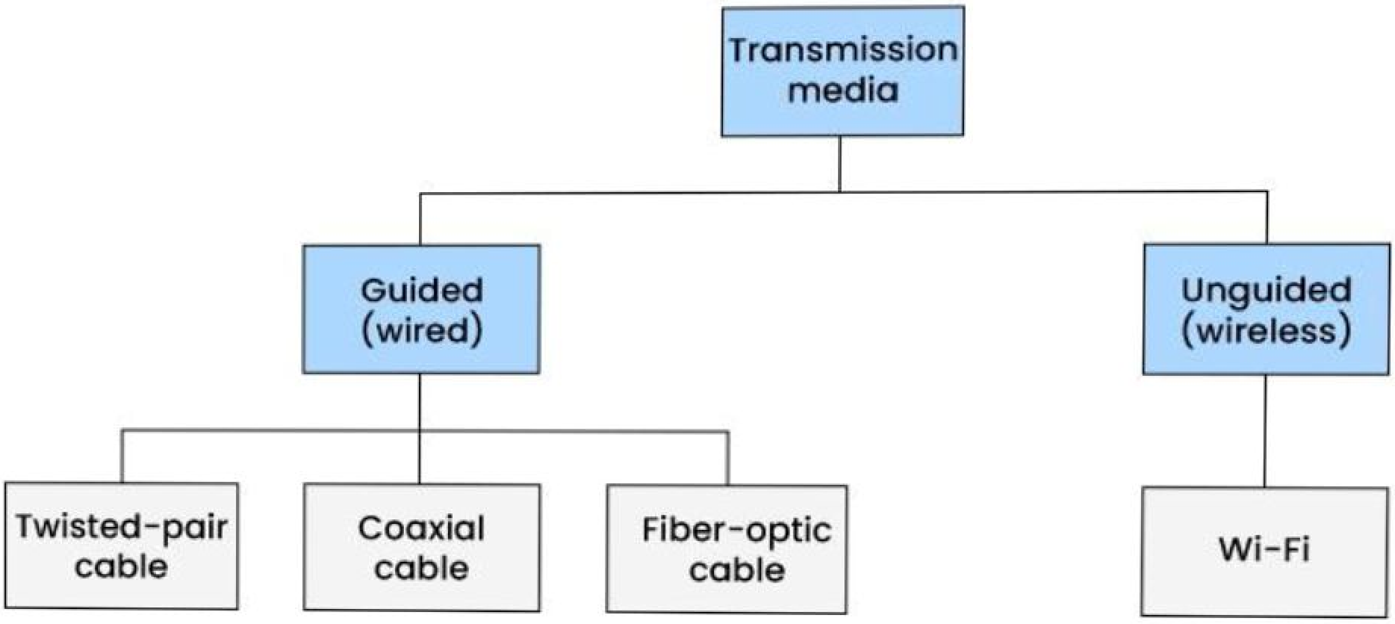
Transmission Modes in Computer Networks (Simplex, Half-Duplex and Full-Duplex)

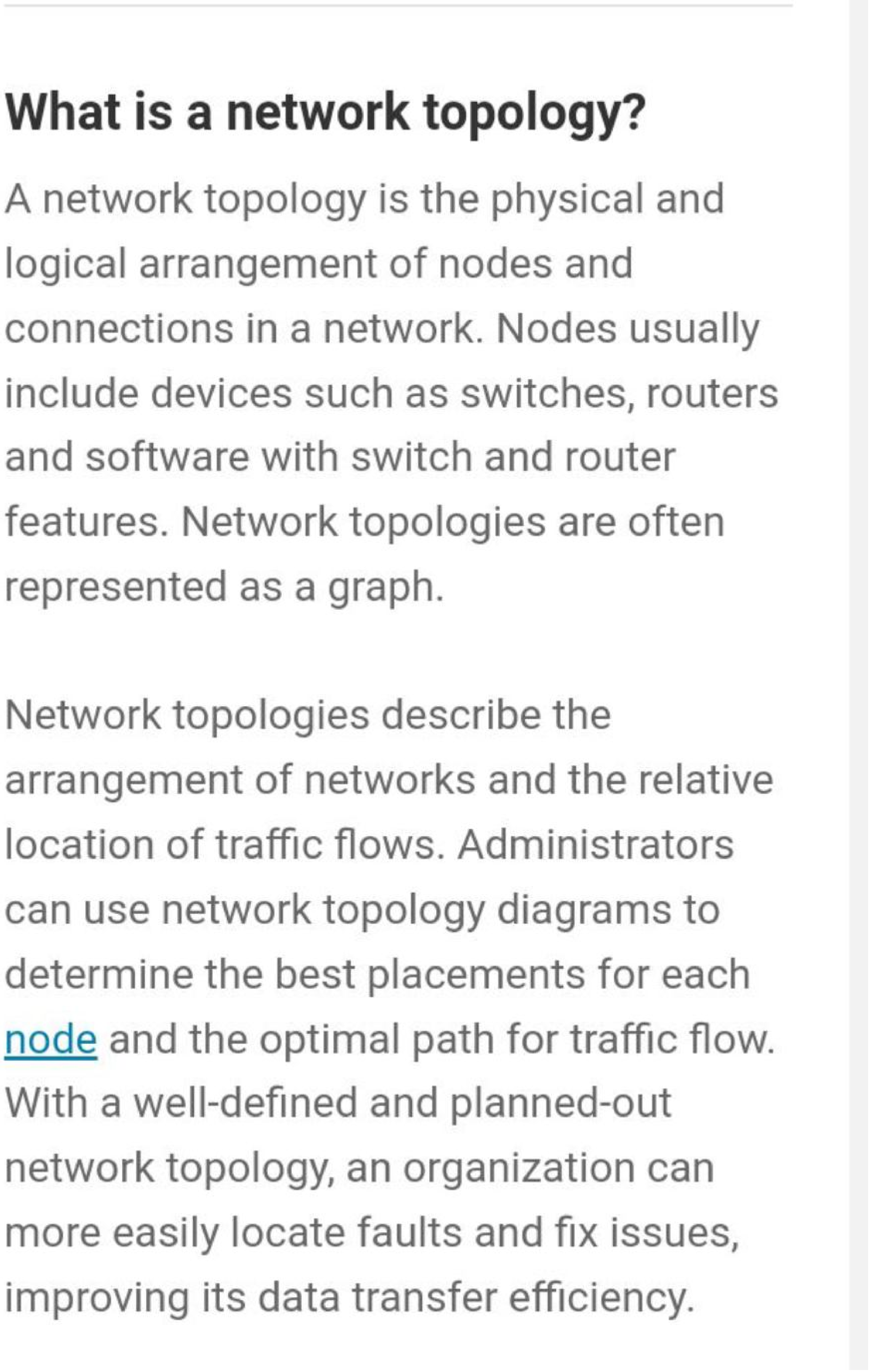
Transmission mode means transferring data between two devices. It is also known as a communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected.

There are three types of transmission mode:-




Transmission Mode
Simple Mode
Half Duplex Mode
Full Duplex Mode


Transmission media
Guided (wired)
Unguided (wireless)
Twisted-pair cable
Coaxial cable
Fiber-optic cable
Wi-Fi



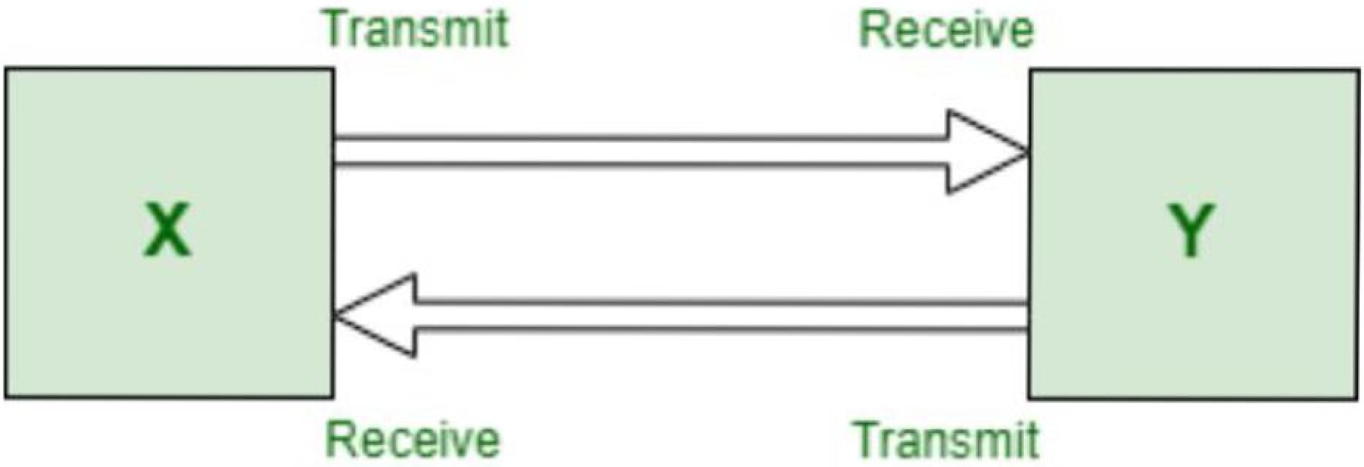
What is a network topology?

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 arrangement of networks and the relative location of traffic 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-out network topology, an organization can more easily locate faults and fix issues, improving its data transfer efficiency.

Point to Point Topology

Point-to-Point Topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.

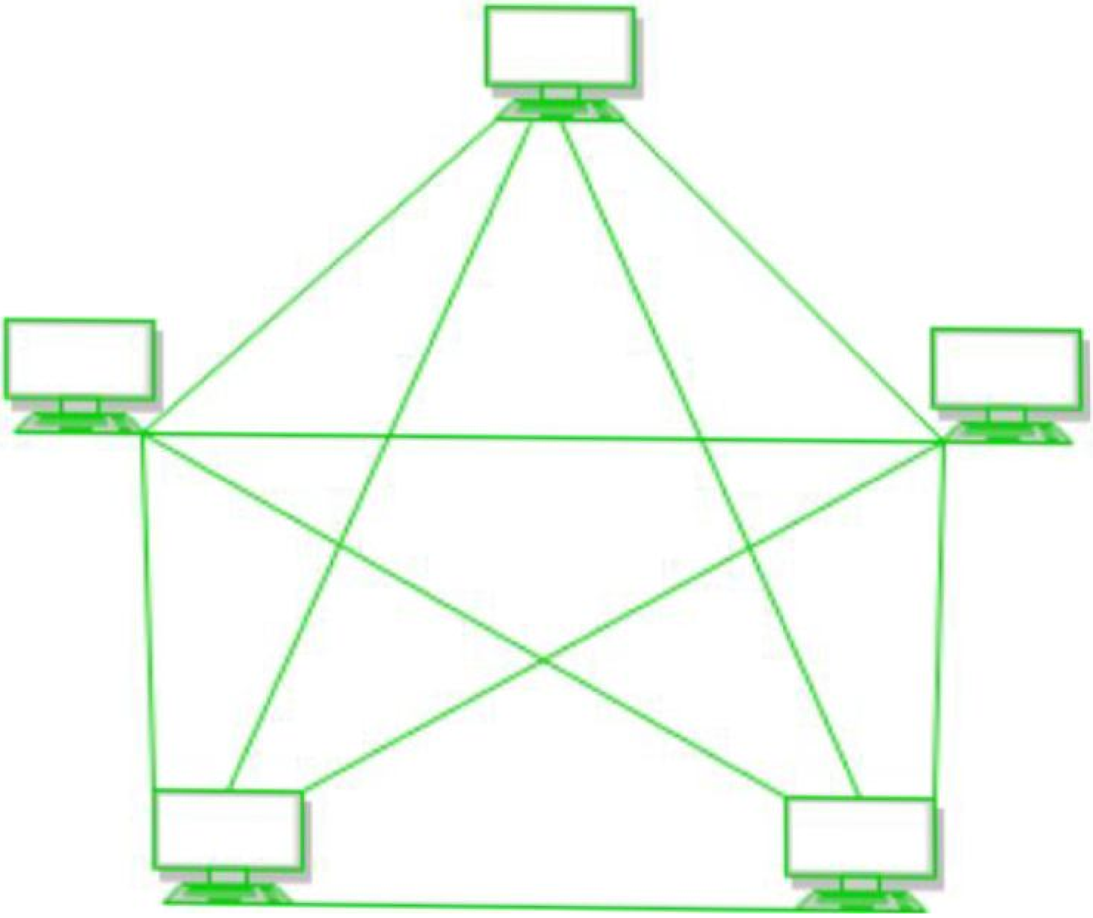
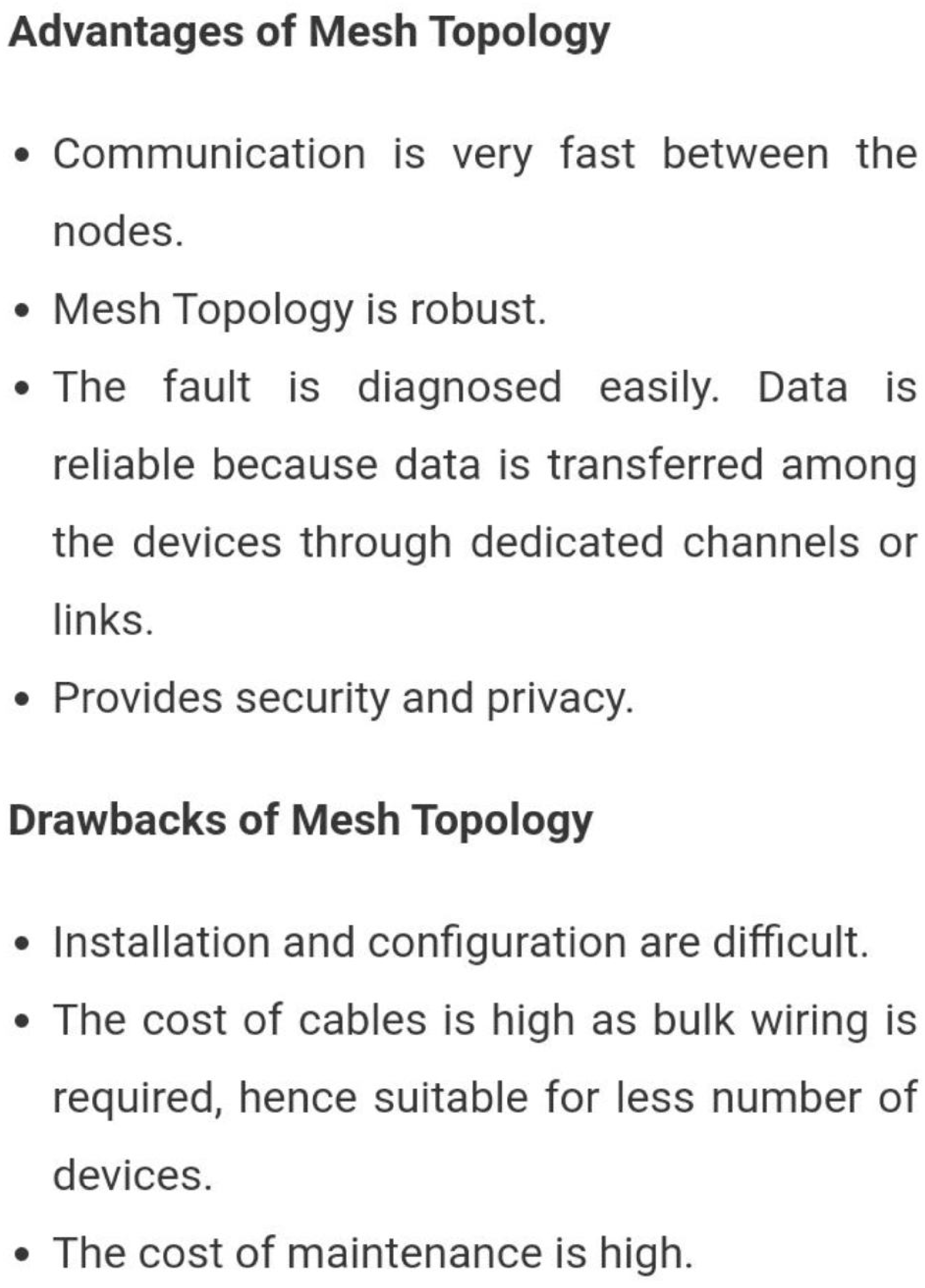


Figure 1: Every device is connected to another via dedicated channels. These channels are known as links.

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N * (N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is ${}^{N}C_{2}$ i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.



Advantages of Mesh Topology

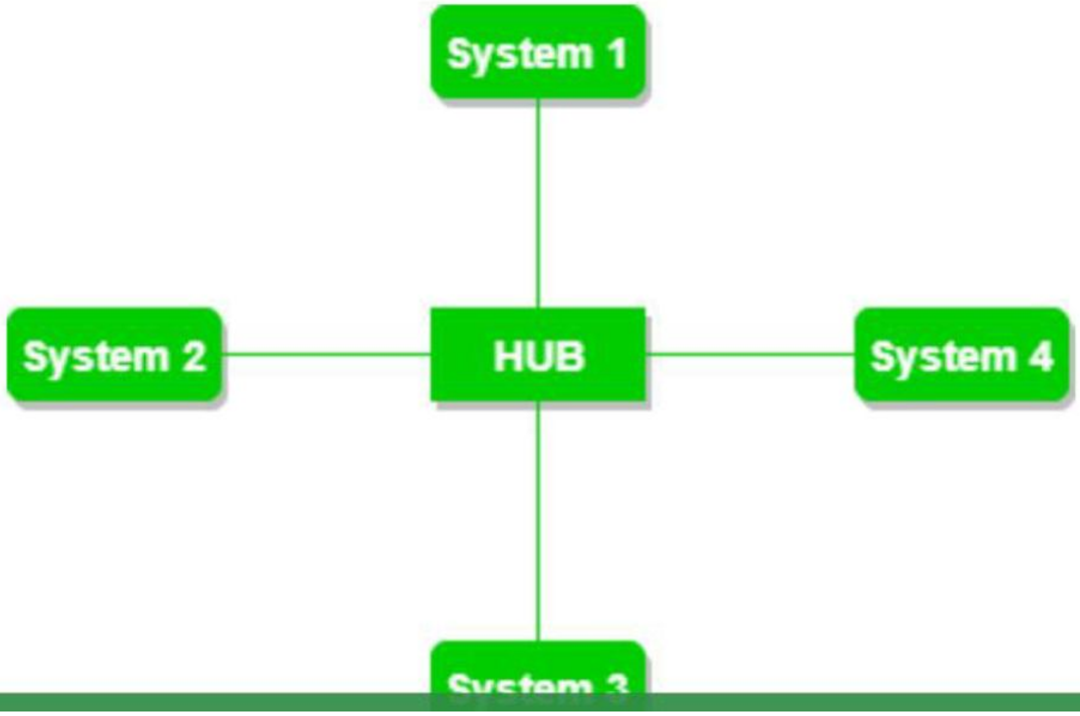
- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Drawbacks of Mesh Topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



Advantages of Star Topology

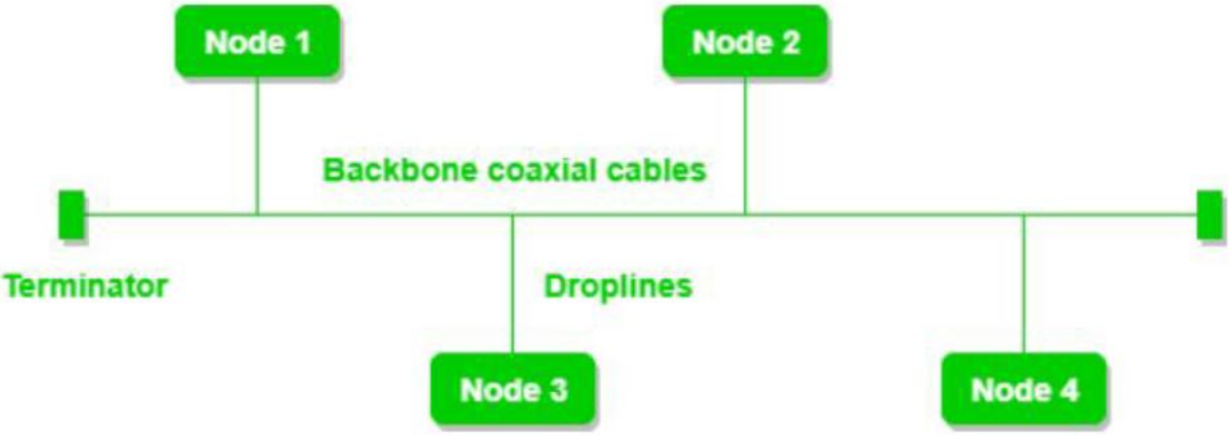
- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Drawbacks of Star Topology

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.

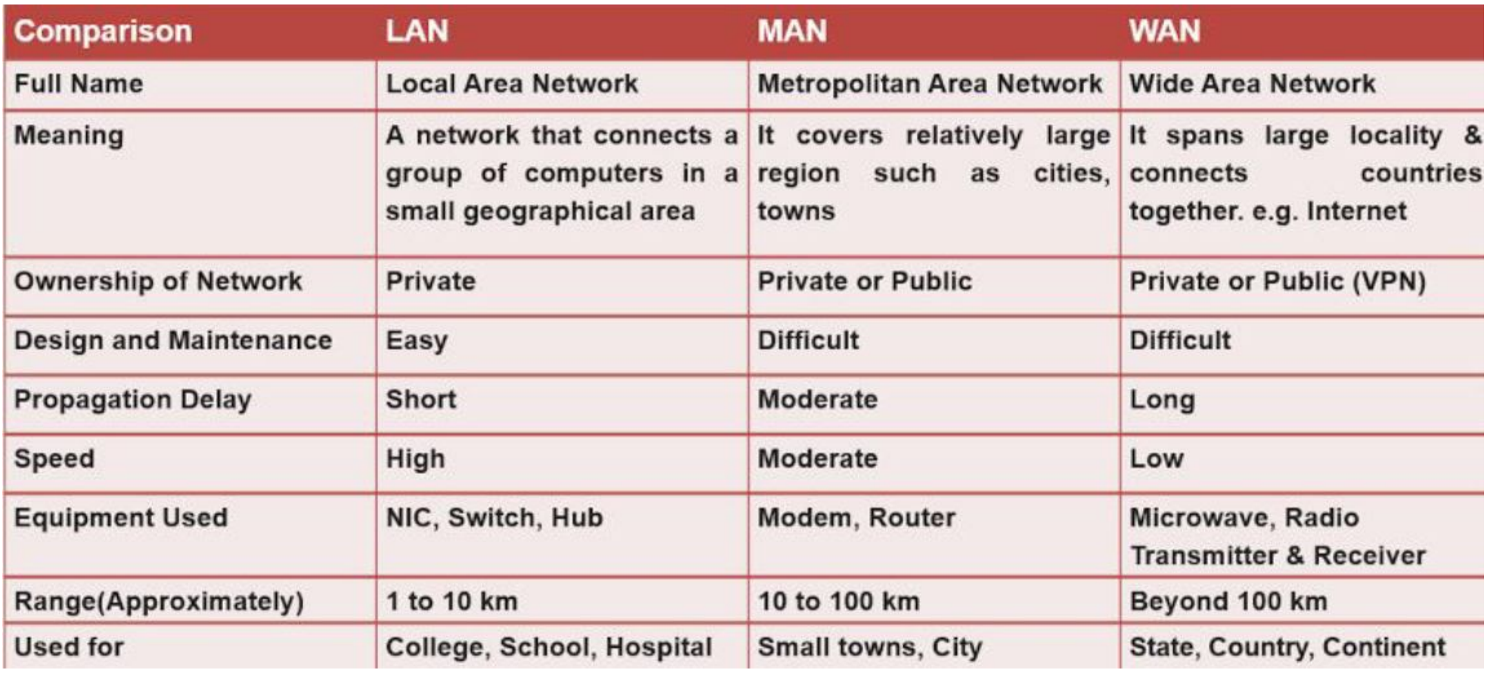


Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

Drawbacks of Bus Topology

- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.



Comparison	LAN	MAN	WAN
Full Name	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area	It covers relatively large region such as cities, towns	It spans large locality & connects countries together. e.g. Internet
Ownership of Network	Private	Private or Public	Private or Public (VPN)
Design and Maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Equipment Used	NIC, Switch, Hub	Modem, Router	Microwave, Radio Transmitter & Receiver
Range(Approximately)	1 to 10 km	10 to 100 km	Beyond 100 km
Used for	College, School, Hospital	Small towns, City	State, Country, Continent

SWITCHING TECHNIQUES

Switching techniques in computer networks refer to the methods used to forward data from one device to another within a network. The two primary switching techniques are circuit switching and packet switching, and there are variations within these categories.

1. **Circuit Switching:**
    - In circuit switching, a dedicated communication path is established between two devices for the duration of their conversation.
    - This path remains reserved exclusively for the two communicating parties until the conversation is complete.
    - Traditional telephone networks often use circuit switching.
2. **Packet Switching:**
    - In packet switching, data is broken down into smaller packets before transmission.
    - Each packet is sent independently and may take different routes to reach the destination.
    - Once all packets arrive at the destination, they are reassembled to reconstruct the original data.
    - Packet switching is more flexible and efficient than circuit switching.

    There are two main types of packet switching:

    - **Connectionless Packet Switching:**
        - Each packet is treated independently and can take different paths to reach the destination.
        - Example protocols include UDP (User Datagram Protocol) in the transport layer.
    - **Connection-Oriented Packet Switching:**
        - Before data transfer begins, a logical connection is established between the source and destination.
        - Example protocols include TCP (Transmission Control Protocol) in the transport layer.
3. **Message Switching:**
    - Message switching involves the entire message being sent from the source to the destination as a whole.
    - The message passes through a series of intermediate nodes, and each node stores and forwards the entire message.
    - This technique is less common due to its inefficiency.
4. **Cell Switching:**

- Cell switching is a technique used in Asynchronous Transfer Mode (ATM) networks.
- Data is broken down into fixed-size cells (53 bytes in the case of ATM) for transmission.
- Each cell is switched independently, and the network can handle various types of traffic efficiently.

The choice of switching technique depends on factors such as the type of network, the nature of the data being transmitted, and the required level of efficiency. Modern computer networks, especially the Internet, primarily rely on packet switching due to its flexibility and scalability.

INTERNET AND PROTOCOL

The Internet is a global network of interconnected computers and computer networks that communicate using a standardized set of protocols. Protocols are a set of rules or conventions that define how data is transmitted and received over a network. These protocols ensure that devices from different manufacturers can communicate with each other effectively. Several key protocols play crucial roles in the functioning of the Internet:

1. **Transmission Control Protocol (TCP):**
   - TCP is a connection-oriented protocol that ensures reliable and error-free delivery of data between devices on a network.
   - It breaks data into packets, numbers them, and ensures they are reassembled in the correct order at the destination.
2. **Internet Protocol (IP):**
   - IP is responsible for addressing and routing packets of data so that they can travel across networks and arrive at the correct destination.
   - There are two main versions of IP: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6).
3. **Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS):**
   - HTTP is used for transmitting and receiving information on the World Wide Web. It defines how web browsers and web servers communicate.
   - HTTPS is a secure version of HTTP that encrypts data during transmission, providing a secure connection for online transactions and sensitive information.
4. **File Transfer Protocol (FTP):**
   - FTP is a protocol used for transferring files between computers on a network. It allows users to upload and download files from servers.
5. **Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) / Internet Message Access Protocol (IMAP):**

- SMTP is used for sending emails, while POP and IMAP are used for retrieving emails from a mail server.
- POP is more focused on downloading emails to a local device, while IMAP allows users to manage emails on the server.

6. **Domain Name System (DNS):**
    - DNS translates human-readable domain names (e.g., www.example.com) into IP addresses that computers use to identify each other on the network.
7. **Border Gateway Protocol (BGP):**
    - BGP is a protocol used for routing and exchanging information between different autonomous systems (AS) on the Internet. It plays a crucial role in the global routing of data.

These protocols, among others, work together to enable the functioning of the Internet, allowing devices and networks from different vendors to communicate seamlessly. They form the foundation for various Internet services and applications, facilitating the exchange of data and information on a global scale.

OSI REFERENCE MODEL

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a communication or network system into seven abstraction layers. It was developed by the International Organization for Standardization (ISO) to facilitate communication between different systems and devices. The OSI model does not prescribe specific technologies or protocols but serves as a guideline for understanding and developing network protocols. The seven layers of the OSI model, from the lowest to the highest, are as follows:

1. **Physical Layer (Layer 1):**
    - This layer deals with the physical connection between devices. It defines the characteristics of the hardware, such as cables, connectors, and electrical signals. It is concerned with transmitting raw bits over a physical medium.
2. **Data Link Layer (Layer 2):**
    - The data link layer is responsible for creating a reliable link between two directly connected nodes. It handles issues such as framing, error detection, and flow control. Ethernet and PPP (Point-to-Point Protocol) operate at this layer.
3. **Network Layer (Layer 3):**
    - The network layer is concerned with logical addressing and routing. It determines the best path for data to travel from the source to the destination across a network. IP (Internet Protocol) operates at this layer.
4. **Transport Layer (Layer 4):**

- The transport layer is responsible for end-to-end communication and data flow control between devices on different networks. It ensures that data is delivered reliably and in the correct order. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are examples.

5. **Session Layer (Layer 5):**
    - The session layer establishes, maintains, and terminates communication sessions between applications. It manages dialogue control, ensuring that data is properly synchronized and organized for efficient communication.
6. **Presentation Layer (Layer 6):**
    - The presentation layer is responsible for translating data between the application layer and the lower layers. It deals with data encoding, encryption, and compression. It ensures that data is in a format that the application layer can understand.
7. **Application Layer (Layer 7):**
    - The application layer is the topmost layer and is closest to end-users. It provides network services directly to end-users and application processes. Protocols such as HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), and SMTP (Simple Mail Transfer Protocol) operate at this layer.

The OSI model helps in understanding and designing network architectures by breaking down the complex process of network communication into more manageable and standardized layers. It facilitates interoperability between different vendors' systems and promotes a modular approach to network design and implementation. While the OSI model is a valuable conceptual framework, in practice, the more widely used TCP/IP model is often referenced in the design and implementation of modern computer networks.

TCP/IP REFERENCE MODEL

The TCP/IP (Transmission Control Protocol/Internet Protocol) model, also known as the Internet protocol suite, is a conceptual framework used for the design and implementation of computer networks. It serves as the foundation for the development of the Internet. The TCP/IP model consists of four layers, which are often grouped into two categories: the Internet layer and the Transport layer.

1. **Link Layer (or Network Interface Layer):**
    - This layer is roughly equivalent to the combination of the Physical and Data Link layers in the OSI model. It deals with the physical connection between devices

and the framing of data for transmission over the local network. Ethernet, Wi-Fi, and PPP are examples of link layer technologies.

2. **Internet Layer:**
   - **Internet Protocol (IP):** Responsible for logical addressing (IP addresses) and routing of packets between devices on different networks. Both IPv4 and IPv6 are examples of network layer protocols.
   - **Internet Control Message Protocol (ICMP):** Used for error reporting, diagnostics, and management functions. Ping is an example of an ICMP tool.
   - **Internet Group Management Protocol (IGMP):** Used for managing multicast group memberships.
3. **Transport Layer:**
   - **Transmission Control Protocol (TCP):** Provides reliable, connection-oriented communication. It ensures the orderly and error-checked delivery of a stream of data.
   - **User Datagram Protocol (UDP):** Provides connectionless, unreliable communication. It is used when low overhead and fast communication are more important than guaranteed delivery.
4. **Application Layer:**
   - This layer corresponds to the top three layers (Session, Presentation, and Application) of the OSI model. It is responsible for providing network services directly to end-users and application processes.
   - **Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS) are examples of application layer protocols.**

The TCP/IP model is more widely used in practice than the OSI model, especially in the context of the Internet. It is a simpler model with fewer layers, making it easier to implement and understand. The TCP/IP suite is the protocol stack that underlies the entire Internet and is used for communication between a wide range of devices, including computers, routers, and other networked devices.

INTERNET SERVICES

1. **World Wide Web (WWW):**
   - The World Wide Web is a system of interconnected documents and resources linked by hyperlinks and URLs. Web browsers, such as Chrome, Firefox, and Safari, allow users to access and navigate the web.
2. **Email:**

- Email (Electronic Mail) is a widely used communication service for sending and receiving messages electronically. Popular email services include Gmail, Yahoo Mail, and Outlook.

3. **File Transfer:**
    - Services like File Transfer Protocol (FTP) and cloud storage platforms (e.g., Dropbox, Google Drive) enable users to upload, download, and share files over the Internet.
4. **Social Media:**
    - Social media platforms, such as Facebook, Twitter, Instagram, and LinkedIn, provide online spaces for users to connect, share content, and communicate with others.
5. **Instant Messaging and Chat:**
    - Services like WhatsApp, Facebook Messenger, and Slack offer real-time text, voice, and video communication, enabling instant messaging and collaboration.
6. **VoIP (Voice over Internet Protocol):**
    - VoIP services like Skype, Zoom, and Microsoft Teams allow users to make voice and video calls over the Internet, often at lower costs compared to traditional phone services.
7. **Streaming Services:**
    - Streaming services deliver audio and video content over the Internet. Examples include Netflix, Hulu, Spotify, and YouTube, offering on-demand access to a vast array of entertainment.
8. **Online Gaming:**
    - Online gaming services, such as Steam, Xbox Live, and PlayStation Network, allow users to play video games with others over the Internet.
9. **Search Engines:**
    - Search engines like Google, Bing, and Yahoo help users find information on the web by indexing and organizing vast amounts of content.
10. **E-commerce:**
    - Online shopping services, such as Amazon, eBay, and Alibaba, enable users to buy and sell goods and services over the Internet.
11. **Online Banking:**
    - Online banking services allow users to manage their finances, transfer funds, and perform other banking transactions through secure Internet connections.
12. **Educational Platforms:**
    - Platforms like Coursera, Khan Academy, and edX offer online courses and educational resources, allowing users to learn new skills and subjects.
13. **Web Hosting Services:**

- Web hosting services, like Bluehost, HostGator, and AWS, provide the infrastructure and tools for individuals and businesses to host websites and web applications.

14. **News and Information Services:**
    - Websites and apps from news organizations, such as BBC, CNN, and The New York Times, provide up-to-date information on current events.

These services collectively contribute to the diverse and dynamic nature of the Internet, shaping how individuals, businesses, and organizations interact and share information in the digital age.