Module 1

Syllabus

Introduction to Networks:
Network and uses of Networks, Types and topologies of Networks, TCP/IP Model, The OSI vs TCP/IP reference model, Architecture of Internet, Guided and wireless transmission media, Switching.

Data Communication:
The term "Data Communication" comprises two words: Data and Communication. Data can be any text, image, audio, video, or multimedia files. Communication is an act of sending or receiving data. Thus, data communication refers to the exchange of data between two or more networked or connected devices. These devices must be capable of sending and receiving data over a communication medium. Examples of such devices include personal computers, mobile phones, laptops, etc. As we can see in Figure, four different types of devices — computer, printer, server, and switch are connected to form the network. These devices are connected through a media to the network, carrying information from one end to another.

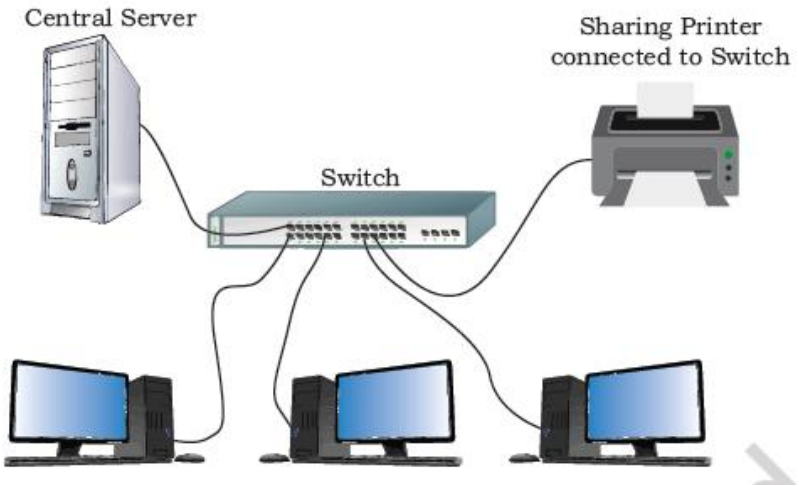


Figure 1.0 A simple network of computing devices

Concept of Data Communication

Whenever we talk about communication between two computing devices using a network, five most important aspects come to our mind. These are sender, receiver, communication medium, the message to be communicated, and certain rules called protocols to be followed during communication. The communication media is also called transmission media. Figure 1.1 shows the role of these five components in data communication.

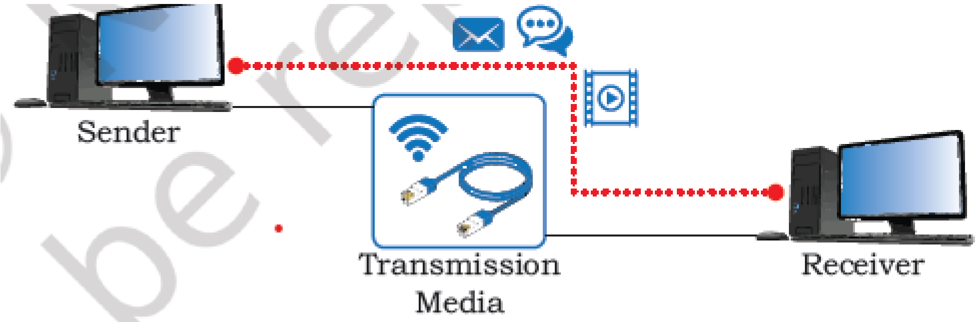


Figure 1.1 Concept of communication

Sender: A sender is a computer or any such device which is capable of sending data over a network. It can be a computer, mobile phone, smartwatch, walkie-talkie, video recording device, etc.

Receiver: A receiver is a computer or any such device which is capable of receiving data from the network. It can be any computer, printer, laptop, mobile phone, television, etc. In computer communication, the sender and receiver are known as nodes in a network.

Message: It is the data or information that needs to be exchanged between the sender and the receiver. Messages can be in the form of text, number, image, audio, video, multimedia, etc.

Communication media: It is the path through which the message travels between source and destination. It is also called medium or link which is either wired or wireless. For example, a television cable, telephone cable, ethernet cable, satellite link, microwaves, etc.

Protocols: It is a set of rules that need to be followed by the communicating parties in order to have successful and reliable data communication. You have already come across protocols such as Ethernet and HTTP.

Types of data communication

Data communication happens in the form of signals between two or more computing devices or nodes. The transfer of data happens over a point-to-point or multipoint communication channel. Data communication between different devices are broadly categorized into 3 types: Simplex communication, Half-duplex communication, and Full-duplex communication.

Simplex communication

It is a one-way or unidirectional communication between two devices in which one device is the sender and the other one is the receiver. Devices use the entire capacity of the link to transmit the data. It is like a one-way street where vehicles can move in only one direction. For example, data entered through a keyboard or audio sent to a speaker are one-way communications. With the advent of IoT, controlling home appliances is another example of simplex communication as shown in Figure 1.3. One can control fans, lights, fridge, oven, etc. while sitting in the office or driving a car.

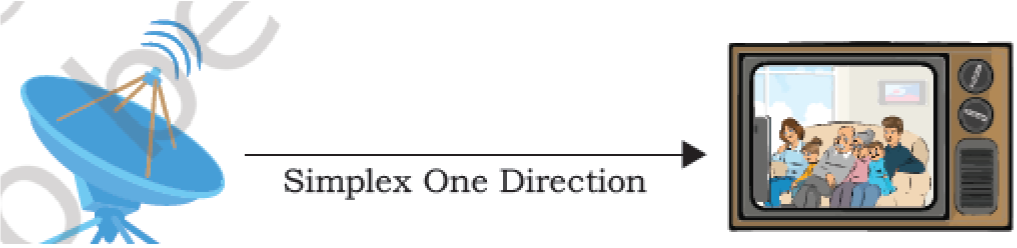


Figure 1.3 Simplex communication

Half-duplex Communication

It is two way or bidirectional communication between two devices in which both the devices can send and receive data or control signals in both directions, but not at the same time, as shown in Figure 1.4. While one device is sending data, the other one will receive and vice-versa. It is like sharing a one-way narrow bridge among vehicles moving in both directions. Vehicles cannot pass the bridge simultaneously. Basically, it is a simplex channel where the direction of transmission can be switched. Application of such type of communication can be found in walkie-talkie where one can press the push-to-talk button and talk. This enables the transmitter and turns off the receiver in that device and others can only listen.

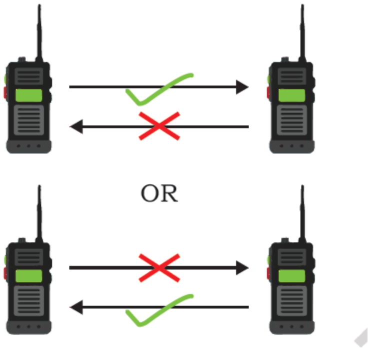


Figure 1.4 Half-duplex communication occurs in two different moments

Full-duplex Communication

It is two way or bidirectional communication in which both devices can send and receive data simultaneously, as shown in Figure 1.5. It is like a two way road where vehicles can go in both directions at the same time. This type of communication channel is employed to allow simultaneous communication, for example, in our mobile phones and landline telephones. The capacity of the transmission link is shared between the signals going in both directions. This can be done either by using two physically separate simplex lines — one for sending and other for receiving, or the capacity of the single channel is shared between the signals travelling in different directions.

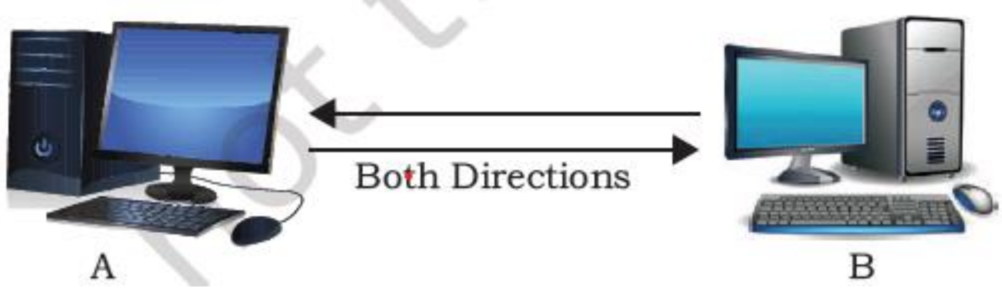


Figure 1.5 Full duplex Transmission of data

Transmission Medium

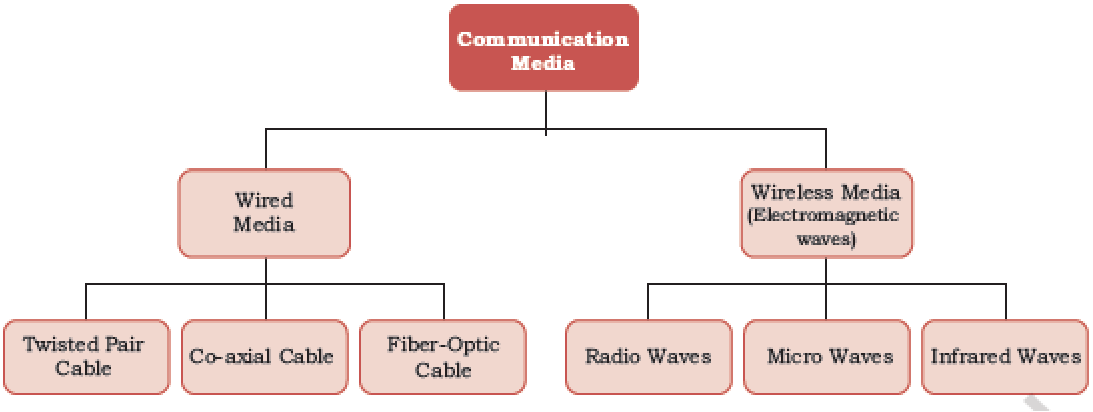


Figure 1.5 Classification of communication medium

Wired Transmission Media

Any physical link that can carry data in the form of signals belongs to the category of wired transmission media. Three commonly used guided/wired media for data transmission are, twisted pair, coaxial cable, and fiber optic cable. Twisted-pair and coaxial cable carry the electric signals whereas the optical fiber cable carries the light signals.

(A) Twisted Pair Cable

A twisted-pair consists of two copper wires twisted like a DNA helical structure. Both the copper wires are insulated with plastic covers. Usually, a number of such pairs are combined together and covered with a protective outer wrapping, as shown in Figure 1.6.

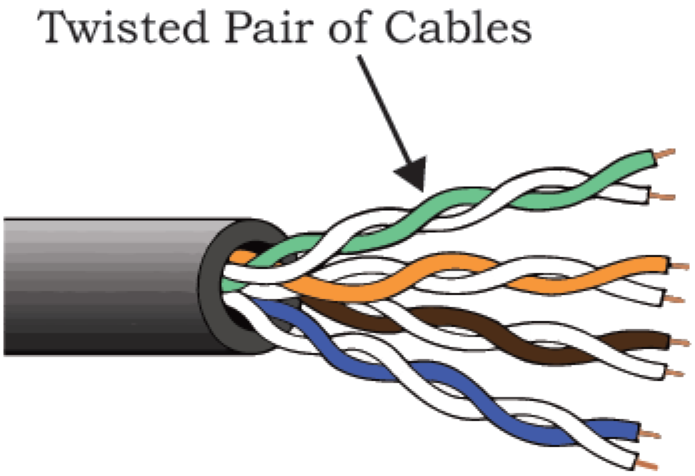


Figure 1.6 Twisted pair of cable

Each of the twisted pairs act as a single communication link. The use of twisted configuration minimises the effect of electrical interference from similar pairs close by. Twisted pairs are less expensive and most commonly used in telephone lines and LANs. These cables are of two types: Unshielded twisted-pair (UTP) and Shielded twisted-pair (STP), as shown in Figure 1.7.

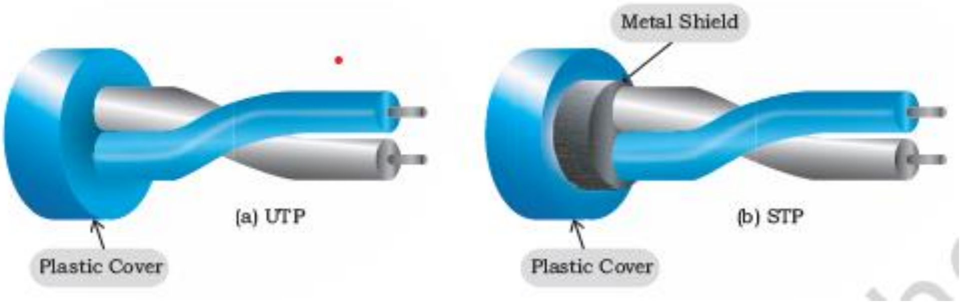


Figure 1.7 UTP Cable And STP cable

(B) Coaxial cable

Coaxial cable is another type of data transmission medium. It is better shielded and has more bandwidth than a twisted pair. As shown in Figure 1.8, it has a copper wire at the core of the cable which is surrounded with insulating material. The insulator is further surrounded with an outer conductor (usually a copper mesh). This outer conductor is wrapped in a plastic cover. The key to success of coaxial cable is its shielded design that allows the cable's copper core to transmit data quickly, without interference of environmental factors. These types of cables are used to carry signals of higher frequencies to a longer distance.

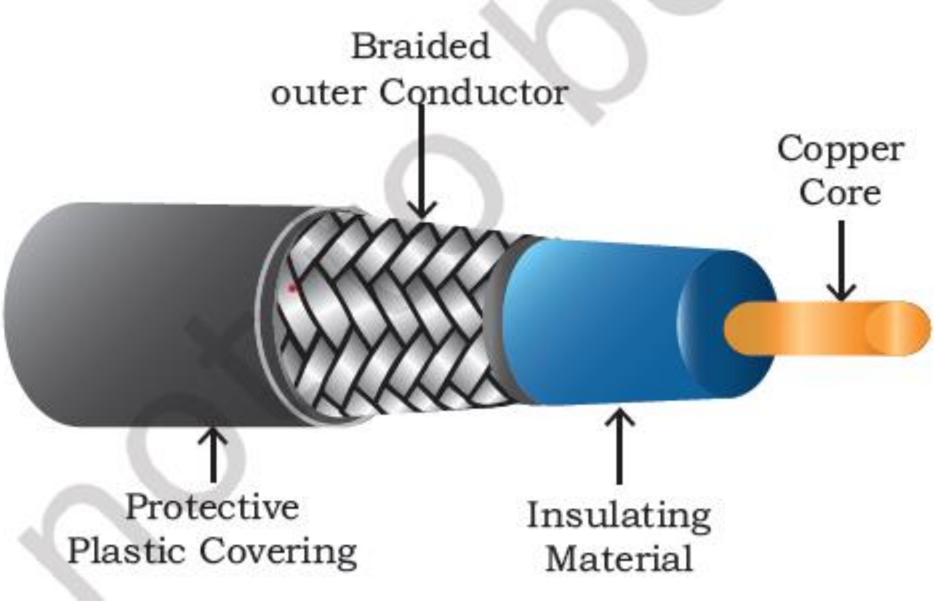


Figure 1.8 A Coaxial Cable

(C) Optical Fibre

The optical fiber cable carries data as light, which travels inside a thin fiber of glass (Figure 1.9). Optic fiber uses refraction to direct the light through the media. A thin transparent strand of glass at the centre is covered with a layer of less dense glass called cladding. This whole arrangement is covered with an outer jacket made of PVC or Teflon. Such types of cables are usually used in backbone networks. These cables are of light weight and have higher bandwidth which means higher data transfer rate. Signals can travel longer distances and electromagnetic noise cannot affect the cable. However, optic fibers are expensive and unidirectional. Two cables are required for full duplex communication.

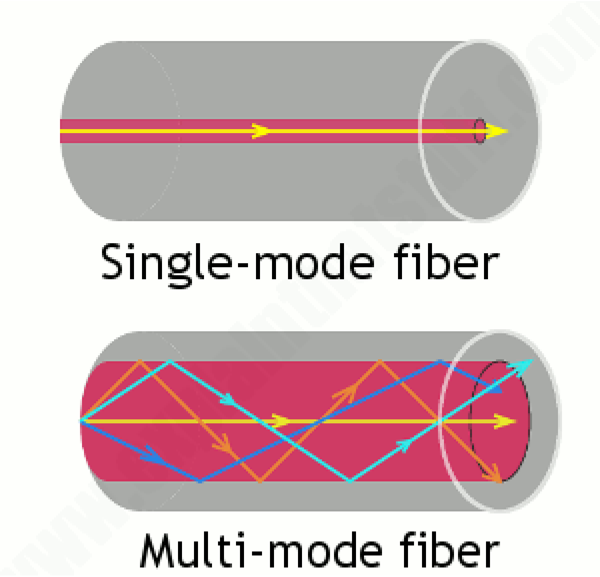
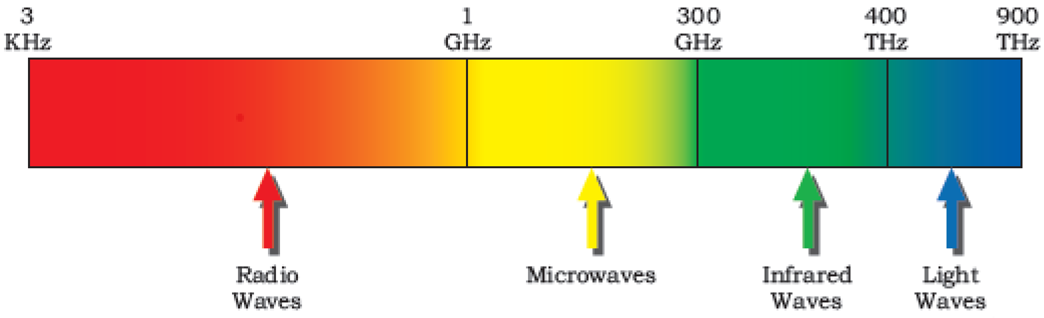


Figure 1.9 fiber optic cable

Wireless Transmission Media

In wireless communication technology, information In wireless communication technology, information travels in the form of electromagnetic signals through air. Electromagnetic spectrum of frequency ranging from 3 KHz to 900 THz is available for wireless communication (Figure 1.10). Wireless technologies allow communication between two or more devices in short to long distance without requiring any physical media. There are many types of wireless communication technologies such as Bluetooth, WiFi, WiMax etc.

The electromagnetic spectrum range (3KHz to 900THz) can be divided into 4 categories (Figure 1.10) - Radio waves, Microwaves, Infrared waves, and Visible or Light waves, according to their frequency ranges. Some of the properties of each wave are listed in Table 1.11 of these, three are useful for wireless communication.



1.10 Electromagnetic Wave Spectrum

Transmission Waves	**Properties**
Radio Waves	1. Waves of frequency range 3 KHz - 1 GHz 2. Omni-directional, these waves can move in all directions 3. Radio waves of frequency 300KHz-30MHz can travel long distance 4. Susceptible to interference 5. Radio waves of frequency 3-300KHz can penetrate walls 6. These waves are used in AM and FM radio, television, cordless phones.
Microwaves	1. Electromagnetic waves of frequency range 1GHz - 300GHz. 2. Unidirectional, can move in only one direction. 3. Cannot penetrate solid objects such as walls, hills or mountains. 4. Needs line-of-sight propagation i.e. both communicating antenna must be in the direction of each other. 5. Used in point-to-point communication or unicast communication such as radar and satellite. 6. Provide very large information-carrying capacity.
Infrared waves	1. Electromagnetic waves of frequency range 300GHz - 400THz. 2. Very high frequency waves. 3. Cannot penetrate solid objects such as walls. 4. Used for short-distance point-to-point communication such as mobile-to-mobile, mobile-to-printer, remote-control-to-TV, and Bluetooth-enabled devices to other devices like mouse, keyboards etc.

1.11Classification of transmission waves and their properties

Wireless Technologies

(A) Bluetooth

Bluetooth is a short-range wireless technology that can be used to connect mobile-phones, mouse, headphones, keyboards, computers, etc. wirelessly over a short distance. One can print documents with bluetooth- Enabled printers without a physical connection. All these bluetooth-enabled devices have a low cost transceiver chip. This chip uses the unlicensed frequency band of 2.4 GHz to transmit and receive data. These devices can send data within a range of 10 meters with a speed of 1 - 2 Mbps.

In Bluetooth technology, the communicating devices within a range of 10 meters build a personal area network called piconet. The devices in a piconet work in a master-slave configuration. A master device can communicate with up to 7 active slave devices at the same time.

Bluetooth technology allows up to 255 devices to build a network. Out of them, 8 devices can communicate at the same time and remaining devices can be inactive, waiting for a response command from the master device.

What is Network Topology?

Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

Types of Network Topology

Physical topology is the geometric representation of all the nodes in a network. There are six types of network topology which are Bus Topology, Ring Topology, Tree Topology, Star Topology, Mesh Topology, and Hybrid Topology.

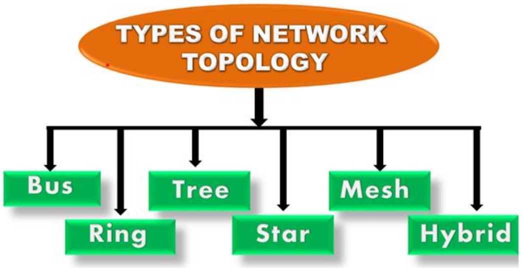
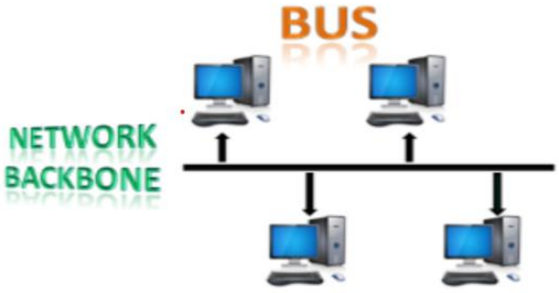


Figure 1.12 Types of Network Topology

Bus Topology



1.13 Bus Topology

- ✓ The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- ✓ Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- ✓ When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- ✓ The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- ✓ The configuration of a bus topology is quite simpler as compared to other topologies.

Advantages of Bus topology:

- ✓ **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- ✓ **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- ✓ **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- ✓ **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- ✓ **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- ✓ **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.

- ✓ **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- ✓ **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- ✓ **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

Ring Topology

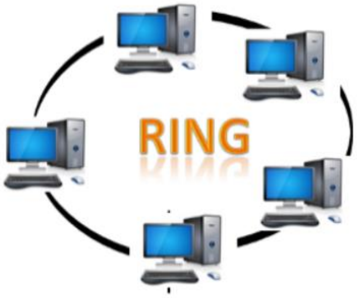


Figure 1.14 Ring Topology

- ✓ Ring topology is like a bus topology, but with connected ends.
- ✓ The node that receives the message from the previous computer will retransmit to the next node.
- ✓ The data flows in one direction, i.e., it is unidirectional.
- ✓ The data flows in a single loop continuously known as an endless loop.
- ✓ It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- ✓ The data in a ring topology flow in a clockwise direction.
- ✓ The most common access method of the ring topology is token passing.
  - o Token passing: It is a network access method in which token is passed from one node to another node.
  - o Token: It is a frame that circulates around the network.

Working of Token passing

- ✓ A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- ✓ The sender modifies the token by putting the address along with the data.
- ✓ The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- ✓ In a ring topology, a token is used as a carrier.

Advantages of Ring topology:

- ✓ **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- ✓ **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- ✓ **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- ✓ **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- ✓ **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- ✓ **Failure:** The breakdown in one station leads to the failure of the overall network.
- ✓ **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- ✓ **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

Star Topology

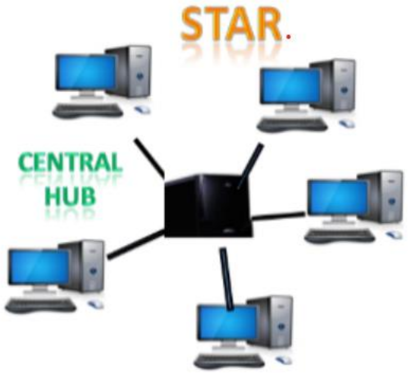


Figure 1.15 Star Topology

- ✓ Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.

- ✓ The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- ✓ Coaxial cable or RJ-45 cables are used to connect the computers.
- ✓ Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- ✓ Star topology is the most popular topology in network implementation.

Advantages of Star Topology

- ✓ **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- ✓ **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- ✓ **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- ✓ **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- ✓ **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- ✓ **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- ✓ **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star Topology

- ✓ A Central point of failure: If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- ✓ Cable: Sometimes cable routing becomes difficult when a significant amount of routing is required.

Tree topology

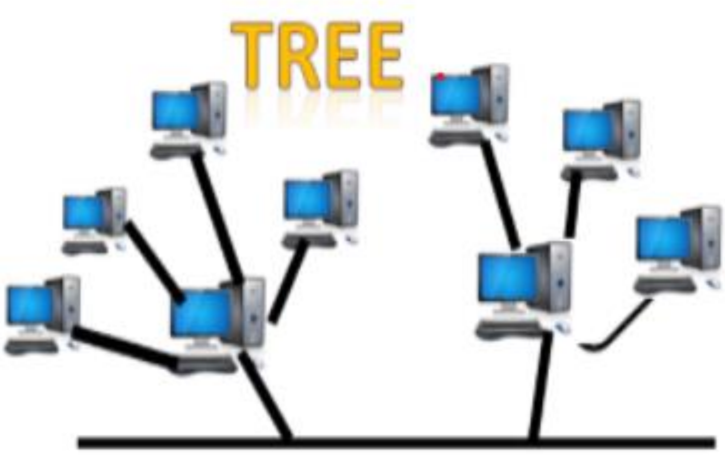


Figure 1.16 Tree Topology

- ✓ Tree topology combines the characteristics of bus topology and star topology.
- ✓ A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- ✓ The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- ✓ There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

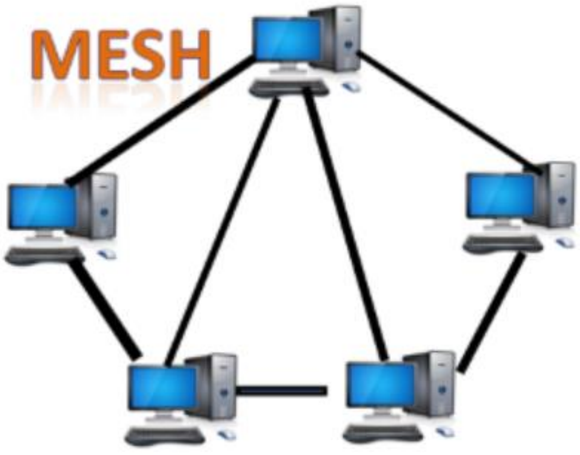
Advantages of Tree topology

- ✓ **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- ✓ **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- ✓ **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- ✓ **Error detection:** Error detection and error correction are very easy in a tree topology.
- ✓ **Limited failure:** The breakdown in one station does not affect the entire network.
- ✓ **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology

- ✓ Difficult troubleshooting: If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- ✓ High cost: Devices required for broadband transmission are very costly.
- ✓ Failure: A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- ✓ Reconfiguration difficult: If new devices are added, then it becomes difficult to reconfigure.

Mesh topology



1.17 Mesh Topology

- ✓ Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- ✓ There are multiple paths from one computer to another computer.
- ✓ It does not contain the switch, hub or any central computer which acts as a central point of communication.
- ✓ The Internet is an example of the mesh topology.
- ✓ Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- ✓ Mesh topology is mainly used for wireless networks.

Hybrid Topology

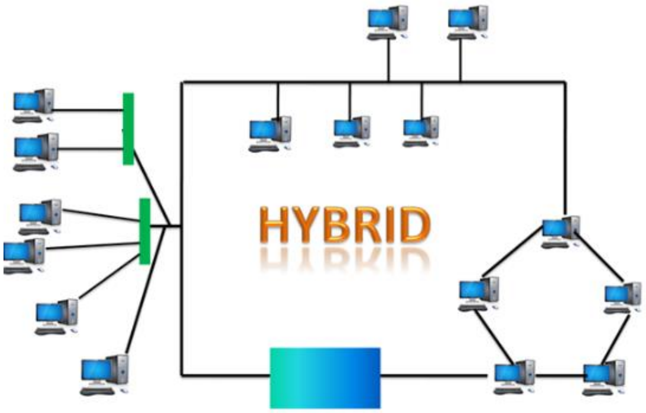


Figure 1.18 Hybrid Topology

- ✓ The combination of various different topologies is known as **Hybrid topology**.
- ✓ A Hybrid topology is a connection between different links and nodes to transfer the data.
- ✓ When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology

- ✓ **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- ✓ **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- ✓ **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- ✓ **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology

- ✓ Complex design: The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- ✓ Costly Hub: The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- ✓ Costly infrastructure: The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

TCP/IP Model

The TCP/IP model, also known as the Internet Protocol Suite, is a conceptual framework that describes the protocols and standards used for communication on the Internet. It consists of four layers, each responsible for specific functions. Let's explore each layer and its duties:

1. Application Layer:

The Application layer is the topmost layer in the TCP/IP model and is closest to the end-user. It provides network services and protocols that enable user applications to access network resources. Some of the protocols and services at this layer include:

- Hypertext Transfer Protocol (HTTP): Used for web browsing and accessing websites.

- Simple Mail Transfer Protocol (SMTP): Responsible for sending and receiving email.

- File Transfer Protocol (FTP): Used for transferring files between systems.

- Domain Name System (DNS): Translates domain names into IP addresses.

- Simple Network Management Protocol (SNMP): Used for network management and monitoring.

The Application layer handles application-specific data and encapsulates it into protocols that can be transmitted over the network.

2. Transport Layer:

The Transport layer is responsible for reliable and efficient data transfer between end systems. It ensures that data is transmitted accurately, in the correct order, and without errors. The primary protocols at this layer are:

- Transmission Control Protocol (TCP): Provides reliable, connection-oriented communication between applications. It breaks data into packets, ensures their reliable delivery, and handles flow control and congestion control.

- User Datagram Protocol (UDP): Provides unreliable, connectionless communication. It is faster but less reliable than TCP. It is often used for applications that can tolerate packet loss, such as streaming and real-time communication.

The Transport layer also handles port addressing to ensure that data reaches the correct application on the destination system.

3. Internet Layer:

The Internet layer is responsible for addressing, routing, and fragmenting data packets across different networks. It handles logical addressing using IP (Internet Protocol) addresses and performs routing functions to direct packets from the source to the destination. Key protocols at this layer include:

- Internet Protocol (IP): Provides the addressing and routing mechanisms for data packets.

- Internet Control Message Protocol (ICMP): Used for error reporting and diagnostic functions.

The Internet layer encapsulates data received from the Transport layer into IP packets and adds the necessary addressing information for delivery.

4. Network Interface Layer (also known as Link Layer):

The Network Interface layer is responsible for the physical transmission of data packets over the network medium. It deals with the protocols and hardware required to transmit data over specific types of networks, such as Ethernet, Wi-Fi, or DSL. This layer includes protocols like Ethernet, Wi-Fi, and Point-to-Point Protocol (PPP).

The Network Interface layer converts the IP packets received from the Internet layer into a format suitable for transmission over the physical network medium.

It's important to note that the TCP/IP model does not strictly adhere to the layered approach of the OSI model. The TCP/IP model combines certain functions of the OSI model into fewer layers to better reflect the protocols and architecture used on the Internet.

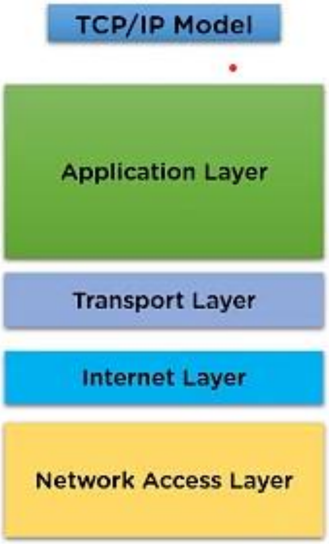
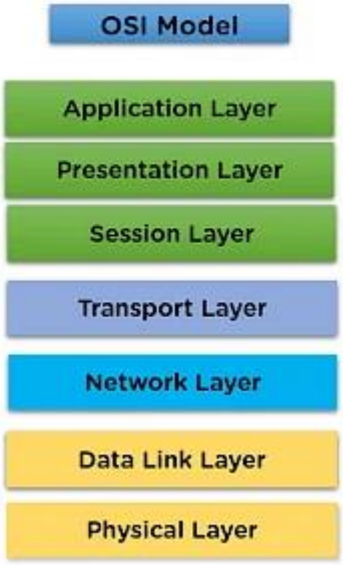


Figure 1.19 TCP/IP Model Layers

OSI Model

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a communication system into seven layers. Each layer has specific responsibilities and interacts with adjacent layers to facilitate communication between devices. Let's explore each layer and its duties:



1.20 OSI Model Layers

1. Physical Layer:

The Physical layer is the lowest layer in the OSI model and deals with the physical transmission of data. It defines the electrical, mechanical, and physical specifications for transmitting raw data over a communication medium. Key functions include:

- Transmission of bits over a communication medium (e.g., copper wires, optical fibers, wireless signals).

- Encoding and decoding of data into electrical or optical signals.

- Physical connection interfaces, such as connectors, cables, and physical characteristics like voltage levels and signaling rates.

The Physical layer ensures the reliable transmission of individual bits without concern for the meaning or structure of the data.

2. Data Link Layer:

The Data Link layer provides reliable point-to-point or point-to-multipoint data transmission within a local network. It is responsible for organizing bits into frames, detecting and correcting transmission errors, and managing access to the physical medium. Key functions include:

- Framing: Dividing the raw data into logical frames for transmission.

- Physical addressing: Assigning unique addresses to devices on the local network (MAC addresses).

- Error detection and correction: Verifying the integrity of transmitted data and retransmitting corrupted frames if necessary.

- Media access control: Regulating access to the shared network medium to prevent collisions (e.g., using protocols like Ethernet).

The Data Link layer establishes a reliable link between directly connected devices and ensures error-free transmission within the local network.

3. Network Layer:

The Network layer provides the functionality to route data across multiple networks or subnets. It is responsible for logical addressing, routing packets, and managing network congestion. Key functions include:

- Logical addressing: Assigning unique IP addresses to devices on the network.

- Routing: Determining the optimal path for data packets to reach their destination.

- Fragmentation and reassembly: Breaking large packets into smaller ones for transmission and reassembling them at the destination.

- Network congestion control: Managing network traffic to prevent congestion and ensure efficient data delivery.

The Network layer enables end-to-end communication between devices on different networks and ensures packets reach their intended destinations.

4. Transport Layer:

The Transport layer provides reliable, end-to-end data transfer between applications on different hosts. It ensures that data is delivered accurately, in the correct order, and without errors. Key functions include:

- Segmentation and reassembly: Breaking data into smaller segments for transmission and reassembling them at the destination.

- Flow control: Regulating the amount of data sent to prevent overwhelming the receiving device.

- Error detection and recovery: Verifying data integrity and retransmitting lost or corrupted segments.

- Multiplexing and demultiplexing: Managing multiple simultaneous data streams between different applications.

The Transport layer establishes a reliable connection between applications on different hosts and ensures the proper delivery of data.

5. Session Layer:

The Session layer establishes, maintains, and terminates communication sessions between applications. It manages the dialogue control and synchronization between devices. Key functions include:

- Session establishment, maintenance, and termination.

- Synchronization of data exchange between applications.

- Checkpointing and recovery: Allowing for the restoration of interrupted sessions.

The Session layer provides the mechanisms for establishing and managing communication sessions between applications.

6. Presentation Layer:

The Presentation layer handles the syntax and semantics of the information exchanged between applications. It is responsible for data formatting, compression, encryption, and decryption. Key functions include:

- Data translation and formatting (e.g., converting between different data formats or character encodings).

- Compression and decompression of data for efficient transmission.

- Encryption and decryption of data to ensure confidentiality and security.

The Presentation layer ensures that data sent by one application is understood by another application.

7. Application Layer:

The Application layer is the topmost layer in the OSI model and represents the actual applications and services used by end-users. It provides a platform for applications to access network services and interact with the underlying layers. Key functions include:

- High-level protocols for specific applications (e.g., HTTP, FTP, SMTP).

- Network services such as email, file transfer, remote login, and web browsing.

- User interfaces and application programming interfaces (APIs) for application development.

The Application layer is where end-user applications and services directly interact with the network.

It's important to note that while the OSI model provides a standardized framework, most modern networking implementations, such as the TCP/IP model, do not strictly adhere to its exact layering. However, the OSI model remains a valuable reference for understanding the various functions involved in network communication.

The OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model are two different conceptual models that describe network protocols and their interactions. Here are some key points of comparison between the two:

TCP/IP VS OSI

Number	TCP/IP	OSI
Number of Layers:	- TCP/IP Model: The TCP/IP model comprises four layers: Network Interface, Internet, Transport, and Application.	- OSI Model: The OSI model consists of seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
Development and Standards	- TCP/IP Model: The TCP/IP model predates the OSI model and was developed by the U.S. Department of Defense in the 1970s for their ARPANET project, which eventually became the foundation for the modern Internet. TCP/IP has become the de facto standard for networking protocols on the Internet.	- OSI Model: The OSI model was developed in the late 1970s and early 1980s by the International Organization for Standardization (ISO). It was an attempt to standardize network protocols and facilitate interoperability between different vendor systems.

Layer Functionality	- TCP/IP Model: The TCP/IP model has less strict layering and some overlapping functionality. It combines multiple functions of the OSI model into fewer layers, often with less well-defined boundaries.	- OSI Model: The OSI model defines a clear separation of functions into distinct layers, with each layer responsible for specific tasks. It emphasizes modularity and encapsulation, enabling easier implementation of new protocols.
Adoption and Practicality	- TCP/IP Model: The TCP/IP model has been widely adopted and is the basis for the Internet. Most modern networks, including the Internet itself, are built on TCP/IP protocols.	- OSI Model: Despite its initial intentions, the OSI model has not been widely implemented in practice. It remains more of a theoretical framework and is primarily used as a reference model for understanding networking concepts.
Compatibility	- TCP/IP Model: The TCP/IP model is specifically designed to work with TCP/IP protocols and aligns with the protocols used on the Internet.	- OSI Model: The OSI model is not directly compatible with TCP/IP protocols. However, it serves as a conceptual model that helps in understanding and designing network protocols and architectures.
Layer Names and Functions	While there are similarities between the layers of the two models, the mapping is not one-to-one. Here's a rough mapping of layers between the two models: - TCP/IP Network Interface layer corresponds to the Physical and Data Link layers of the OSI model. - TCP/IP Internet layer corresponds to the Network layer of the OSI model. - TCP/IP Transport layer corresponds to the Transport layer of the OSI model. - TCP/IP Application layer corresponds to the Session, Presentation, and Application layers of the OSI model.	

Architecture Of The Internet

The architecture of the Internet is ever-changing due to continuous changes in the technologies as well as the nature of the service provided. The heterogeneity and vastness of the Internet make it difficult to describe every aspect of its architecture. The overall architecture can be described in three levels –

1. Backbone ISP (Internet Service Provider)
2. Regional ISPs
3. Clients

The following diagram shows the three levels –

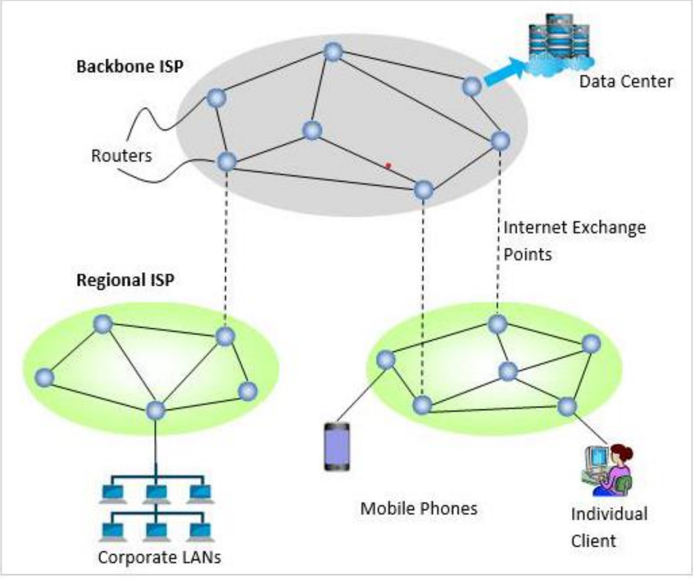


Figure 1.21 Architecture of Internet

Backbone ISP (Internet Service Provider) − Backbone ISPs are large international backbone networks. They are equipped with thousands of routers and store enormous amounts of information in data centers, connected through high bandwidth fiber optic links. Everyone needs to connect with a backbone ISP to access the entire Internet.

There are different ways through which a client can connect to the ISP. A commonly used way is DSL (Digital Subscriber Line) which reuses the telephone connection of the user for transmission of digital data. The user uses a dial-up connection instead of the telephone call. Connectivity is also done by sending signals over cable TV system that reuses unused cable TV channels for data transmission. For high-speed Internet access, the connectivity can be done through FTTH (Fiber to the Home), that uses optical fibers for transmitting data. Nowadays, most Internet access is done through the wireless connection to mobile phones from fixed subscribers, who transmit data within their coverage area.

Switching Technique

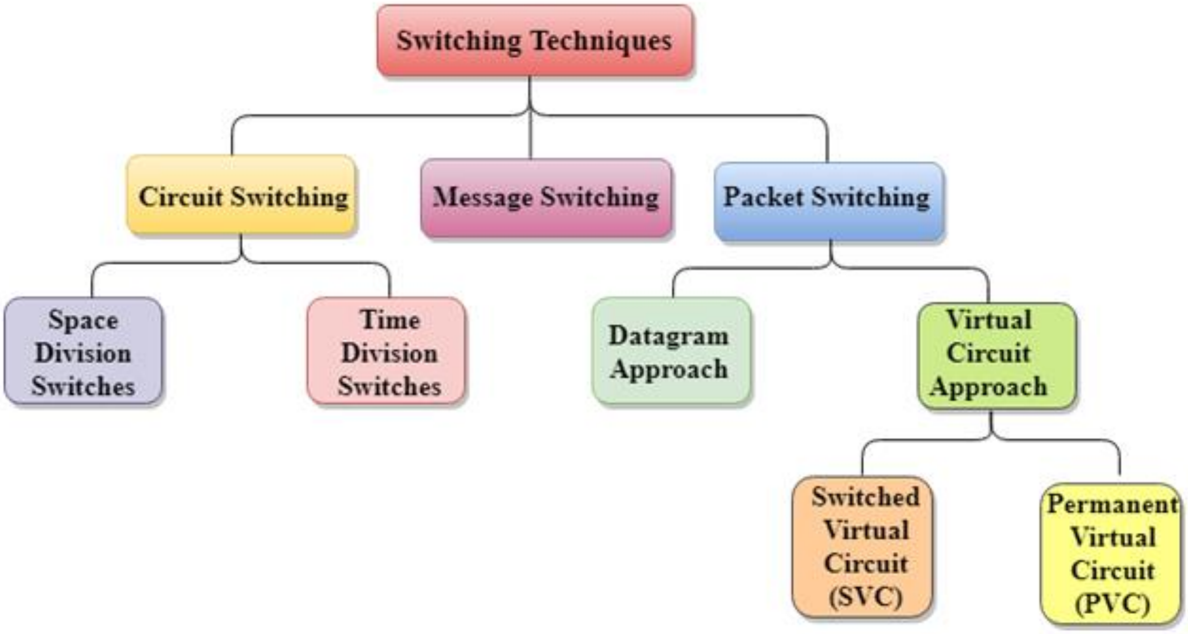


Figure 1.22 Different Switching Technique

Switching techniques refer to the methods used to establish connections and forward data packets within a network. There are several switching techniques commonly used in computer networks. Let's explore them in detail:

1. Circuit Switching:

Circuit switching is a switching technique that establishes a dedicated communication path between two endpoints for the duration of a connection. The path remains allocated exclusively to the connection, regardless of whether data is being transmitted or not. Key features of circuit switching include:

- Connection setup: Before data transmission begins, a dedicated path is established between the source and destination.
- Fixed bandwidth: The allocated bandwidth remains constant throughout the connection, regardless of the data rate required.
- Resources reservation: The required resources, including bandwidth and buffer space, are reserved for the duration of the connection.

Circuit switching is commonly used in traditional telephone networks, where a dedicated circuit is established for a phone call.

2. Packet Switching:

Packet switching is a switching technique that breaks data into smaller packets and transmits them independently over the network. Each packet is treated as an independent unit and can take different paths to reach the destination. Key features of packet switching include:

- Packetization: Data is divided into smaller packets, typically with a fixed maximum size.
- Store-and-forward: Each packet is individually received, stored temporarily, and forwarded to the next hop in the network.
- Variable bandwidth: Different packets can utilize varying amounts of available bandwidth.
- Statistical multiplexing: Multiple packets from different connections can be transmitted over the same link, sharing the available bandwidth.

Packet switching is commonly used in computer networks, including the Internet, as it allows efficient utilization of network resources and supports data transmission for multiple connections simultaneously.

3. Message Switching:

Message switching is a switching technique where data is transmitted in the form of complete messages or blocks. The entire message is stored and forwarded through the network, potentially taking different routes to reach the destination. Key features of message switching include:

- Message-based transmission: Data is transmitted in the form of complete messages or blocks.
- Store-and-forward: The complete message is received, stored temporarily, and forwarded to the next hop in the network.
- Store-and-forward delay: The delay introduced due to storing and forwarding complete messages can be significant.

Message switching was used in some early networking systems but has been largely replaced by packet switching due to its higher efficiency.

4. Virtual Circuit Switching:

Virtual circuit switching is a hybrid switching technique that combines the advantages of circuit switching and packet switching. It establishes a logical connection or "virtual circuit" between endpoints, but the data is transmitted in packets. Key features of virtual circuit switching include:

- Connection setup: A virtual circuit is established between the source and destination, similar to circuit switching.
- Packet-based transmission: Data is divided into packets and transmitted over the established virtual circuit, similar to packet switching.
- Resource reservation: Resources are reserved for the duration of the virtual circuit.

Virtual circuit switching provides the advantages of dedicated paths and guaranteed delivery of circuit switching, along with the flexibility and efficiency of packet switching.

These are the main switching techniques used in computer networks. The choice of switching technique depends on factors such as network requirements, traffic patterns, scalability, and the nature of the applications and services being used.