Unit 5: Data Communication and Computer Network

Data Communication

Data communication refers to the exchange of digital information between two or more devices, using wired or wireless communication channels. It involves the transmission and reception of data through a communication medium, such as cables, radio waves, or optical fibers.

The data communication process involves several steps, including encoding, modulation, transmission, demodulation, decoding, and error detection and correction.

Data communication can occur over different types of networks, such as LANs (Local Area Networks), WANs (Wide Area Networks), and the internet. The devices involved in data communication can be computers, smartphones, tablets, servers, routers, switches, and other network devices.

Some common technologies used in data communication include Ethernet, Wi-Fi, Bluetooth, NFC (Near Field Communication), and cellular networks. Data communication plays a crucial role in many aspects of modern life, including business, education, entertainment, and social interactions.

Components of Data Communication

The components of data communication include:

1. Sender: The sender is the device or computer that originates the message or data to be transmitted.
2. Receiver: The receiver is the device or computer that receives the message or data transmitted by the sender.
3. Transmission medium: The transmission medium is the physical pathway or communication channel through which the data is transmitted, such as copper wires, fiber optic cables, or wireless radio waves.
4. Protocol: The protocol is the set of rules and procedures that govern the transmission of data between the sender and receiver, including the format of data, error detection and correction methods, and flow control.
5. Message: The message is the data or information that is transmitted between the sender and receiver.

Computer Network

A computer network is a collection of devices, such as computers, servers, printers, and other network-enabled devices, that are interconnected and can communicate with each other to share resources, data, and information.

Computer networks can be classified based on their size and geographic range, such as Local Area Networks (LANs), Metropolitan Area Networks (MANs), Wide Area Networks (WANs), and Personal Area Networks (PANs).

LANs typically cover a small area, such as a home, office, or building, and are often used to share resources and files among computers. MANs cover larger areas, such as a city, and are often used by organizations to connect multiple sites or offices within a city. WANs cover a larger geographic area, such as a country or the entire world, and are often used by organizations to connect multiple sites across different cities or countries.

Computer networks use various communication protocols and technologies, such as Ethernet, Wi-Fi, Bluetooth, and cellular networks, to enable devices to communicate with each other.

Some common types of computer networks include client-server networks, peer-to-peer networks, and cloud networks. Client-server networks are often used in businesses and organizations, where a central server provides resources and services to client devices. Peer-to-peer networks are often used for file-sharing and collaborative work among small groups. Cloud networks are used to store and access data and applications remotely over the internet.

Computer networks are essential in modern life, enabling communication, collaboration, and resource sharing among individuals and organizations.

Importance of Networking

Networking is important for several reasons:

1. Communication: Networking enables communication between devices, individuals, and organizations across different locations and time zones. It allows people to collaborate, share ideas, and work together on projects, regardless of where they are physically located.
2. Resource sharing: Networking allows resources such as printers, files, and databases to be shared among devices and users, which can lead to increased efficiency and productivity.

3. Access to information: Networking provides access to a vast amount of information and resources on the internet, including educational materials, research papers, and news.
4. Cost-effective: Networking can reduce costs by allowing devices and resources to be shared, which can eliminate the need for duplicate resources and devices.
5. Scalability: Networking can easily scale to accommodate new devices and users, making it suitable for businesses and organizations of all sizes.
6. Centralized management: Networking enables centralized management of devices, resources, and security, making it easier to monitor and control access to resources and information.
7. Innovation: Networking provides a platform for innovation and the development of new technologies and applications that can improve the way people live and work.

In summary, networking is essential for communication, resource sharing, access to information, cost-effectiveness, scalability, centralized management, and innovation, making it a crucial component of modern life and business.

Data Communication Media

Data communication media refer to the physical channels or pathways used to transmit data from one device to another. There are two main types of data communication media: guided and unguided.

1. Guided Media: Guided media, also known as wired media, refers to communication channels that use physical wires or cables to transmit data. Some examples of guided media include:

- Twisted-pair cables: These are commonly used for local area networks (LANs) and telephone systems, and consist of two or more copper wires twisted together to reduce interference.
- Coaxial cables: These cables consist of a copper wire surrounded by a layer of insulation, a woven shield, and an outer cover. They are often used for cable TV, internet, and other high-speed data transmissions.
- Fiber-optic cables: These cables use optical fibers made of glass or plastic to transmit data as light signals. They are commonly used for long-distance communication, high-speed internet, and cable TV.

2. Unguided Media: Unguided media, also known as wireless media, refers to communication channels that use radio waves or electromagnetic signals to transmit data. Some examples of unguided media include:

- Radio waves: These are commonly used for wireless communication, such as Wi-Fi and Bluetooth.

- Microwaves: These are used for long-distance communication, such as satellite communication and microwave radio links.
- Infrared waves: These are used for short-range communication, such as remote controls and infrared data transmission.

The choice of data communication media depends on several factors, including the distance between devices, the speed and bandwidth required, the cost, and the level of interference or security required.

Data Transmission across Media

Data transmission across media involves the process of transmitting data from a sender device to a receiver device over a physical communication channel, which can be either guided or unguided media. The process of data transmission across media involves the following steps:

1. Data encoding: Data encoding refers to the process of converting the raw data into a format suitable for transmission over the communication channel. This can include the use of digital signal processing techniques, modulation, and error-correction codes.
2. Transmission: Transmission is the process of sending the encoded data across the communication channel. This can involve the use of physical cables, optical fibers, or wireless signals, depending on the type of communication channel being used.
3. Reception: Reception involves receiving the transmitted data at the receiver end of the communication channel. This can involve the use of demodulation, error detection and correction, and digital signal processing techniques to recover the original data from the received signals.
4. Decoding: Decoding refers to the process of converting the received encoded data back into its original format. This can include the use of error-correction codes and other digital signal processing techniques to recover the original data.

The speed and reliability of data transmission across media can be affected by several factors, including the bandwidth of the communication channel, the quality of the transmission medium, the level of interference or noise in the communication channel, and the error-correction codes used to detect and correct transmission errors. To ensure reliable data transmission across media, it is important to use appropriate encoding, modulation, and error-correction techniques, and to carefully choose the most suitable communication channel for the type of data being transmitted.

Data Transmission and Data Networking

Data transmission refers to the process of transmitting digital or analog data from one device to another over a communication channel. The transmission can be either one-way or two-way, depending on the direction of data flow.

There are three main modes of data transmission:

1. Simplex: In simplex mode, data is transmitted in only one direction, from the sender to the receiver, and the receiver cannot send any data back to the sender. Examples of simplex mode include broadcast radio and television transmissions, where the sender broadcasts the signal and the receivers simply receive it.
2. Half-Duplex: In half-duplex mode, data can be transmitted in both directions, but only one device can transmit at a time. When one device is transmitting, the other device can only receive, and vice versa. This mode is commonly used in walkie-talkies and other two-way radios, where users take turns transmitting and receiving.
3. Full-Duplex: In full-duplex mode, data can be transmitted in both directions simultaneously, allowing for real-time two-way communication. This mode is commonly used in telephone networks and internet connections, where users can speak and listen at the same time or transmit and receive data simultaneously.

The choice of transmission mode depends on several factors, including the type of data being transmitted, the speed of transmission, the distance between the sender and receiver, and the level of control required over the communication channel.

Data Networking

Data networking refers to the process of connecting multiple devices together to share information and resources, such as files, printers, and internet connections. The goal of data networking is to enable devices to communicate with each other and exchange data in a fast, efficient, and secure manner.

Data networking is typically achieved using a combination of hardware and software components, including:

1. Network Interface Cards (NICs): These are hardware components that allow devices to connect to a network. They typically come in the form of a card that is installed inside a computer or device, and allow the device to send and receive data over the network.
2. Switches and routers: These are hardware components that are used to connect devices together and route data between them. Switches are used to connect devices within a local network, while routers are used to connect networks together.

3. Network protocols: These are sets of rules and procedures that govern how data is transmitted over a network. Examples of network protocols include TCP/IP, HTTP, and FTP.
4. Network security measures: These are software and hardware components that are used to protect a network from unauthorized access and malicious attacks. Examples of network security measures include firewalls, antivirus software, and encryption.

There are several types of data networks, including:

1. Local Area Network (LAN): A LAN is a network that covers a small geographic area, such as a home or office building. It typically consists of multiple devices connected together using switches or routers.
2. Wide Area Network (WAN): A WAN is a network that covers a larger geographic area, such as a city or country. It typically consists of multiple LANs connected together using routers.
3. Metropolitan Area Network (MAN): A MAN is a network that covers a medium-sized geographic area, such as a city or town. It typically consists of multiple LANs connected together using switches or routers.
4. Wireless network: A wireless network is a type of LAN or WAN that uses wireless signals to transmit data between devices. It is commonly used in homes, offices, and public places like coffee shops and airports.

Data networking has revolutionized the way we communicate and exchange information, enabling us to share data across vast distances in real-time. It has also opened up new opportunities for businesses, enabling them to improve their operations and collaborate more effectively.

Computer Network

A computer network is a group of interconnected computers and other devices that communicate and share resources with each other. The purpose of a computer network is to enable devices to share information and resources, such as files, printers, and internet connections.

Computer networks can be classified into different types based on their size and geographic scope. Some common types of computer networks include:

1. Local Area Network (LAN): A LAN is a network that covers a small geographic area, such as a home, office building, or school campus. It typically consists of multiple devices connected together using switches or routers.

2. Wide Area Network (WAN): A WAN is a network that covers a larger geographic area, such as a city, country, or even multiple countries. It typically consists of multiple LANs connected together using routers.
3. Metropolitan Area Network (MAN): A MAN is a network that covers a medium-sized geographic area, such as a city or town. It typically consists of multiple LANs connected together using switches or routers.
4. Wireless network: A wireless network is a type of LAN or WAN that uses wireless signals to transmit data between devices. It is commonly used in homes, offices, and public places like coffee shops and airports.

Computer networks can also be classified based on their topology, or the physical layout of devices in the network. Some common topologies include:

1. Bus topology: Devices are connected in a linear bus, with each device connected to the main communication line.

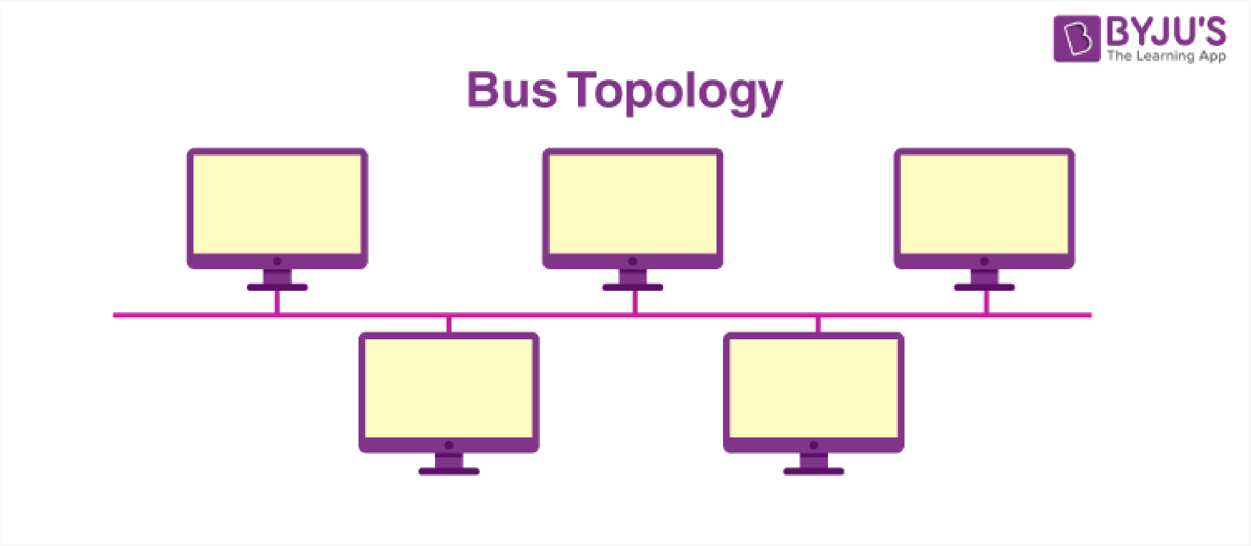


Image Source: https://byjus.com/gate/bus-topology-notes/

2. Star topology: Devices are connected to a central hub or switch, which acts as a central point of communication.

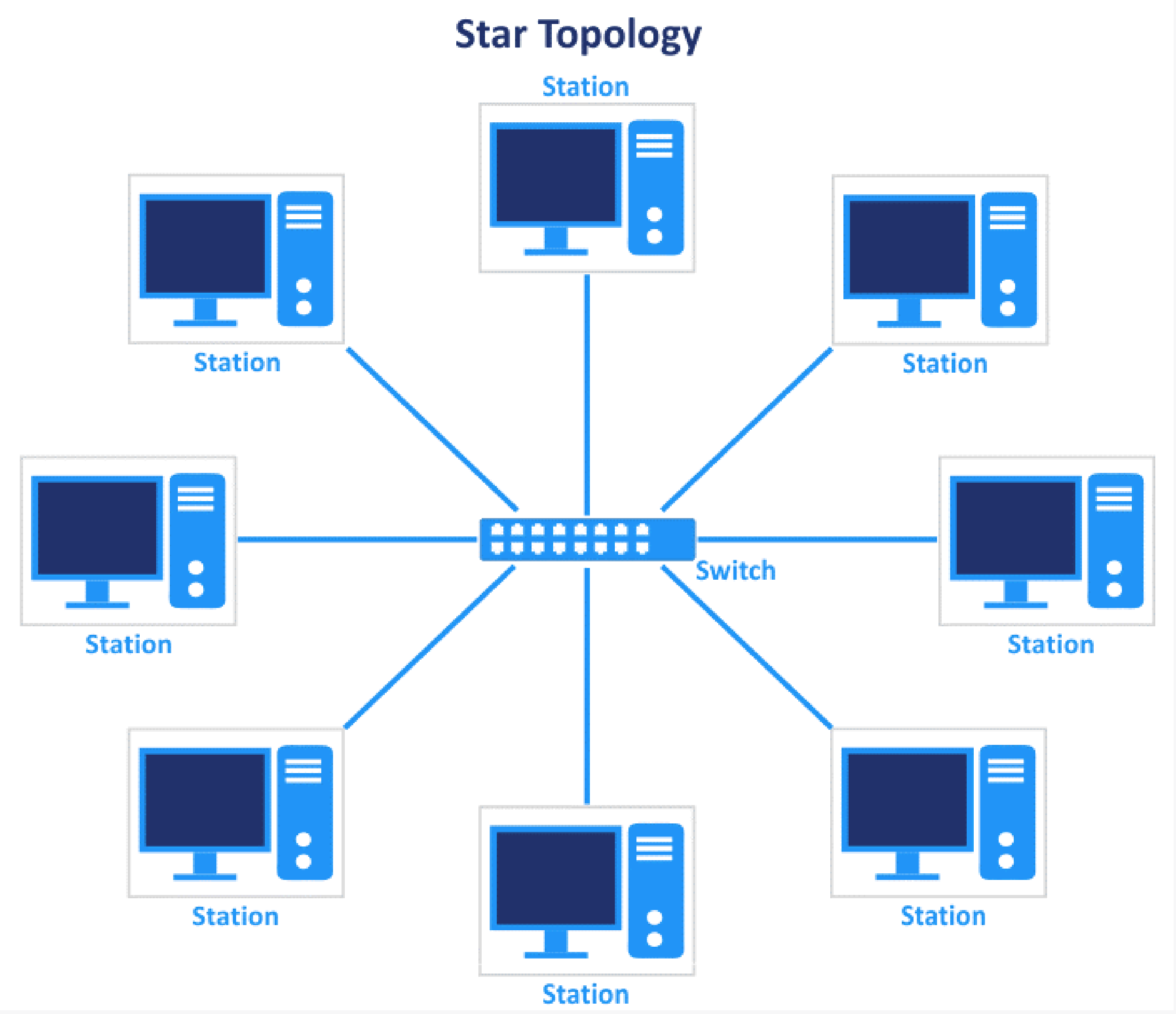


Image Source: https://www.nakivo.com/blog/wp-content/uploads/2021/04/The-star-network-topology.png

3. Ring topology: Devices are connected in a circular ring, with each device connected to the next device in the ring.

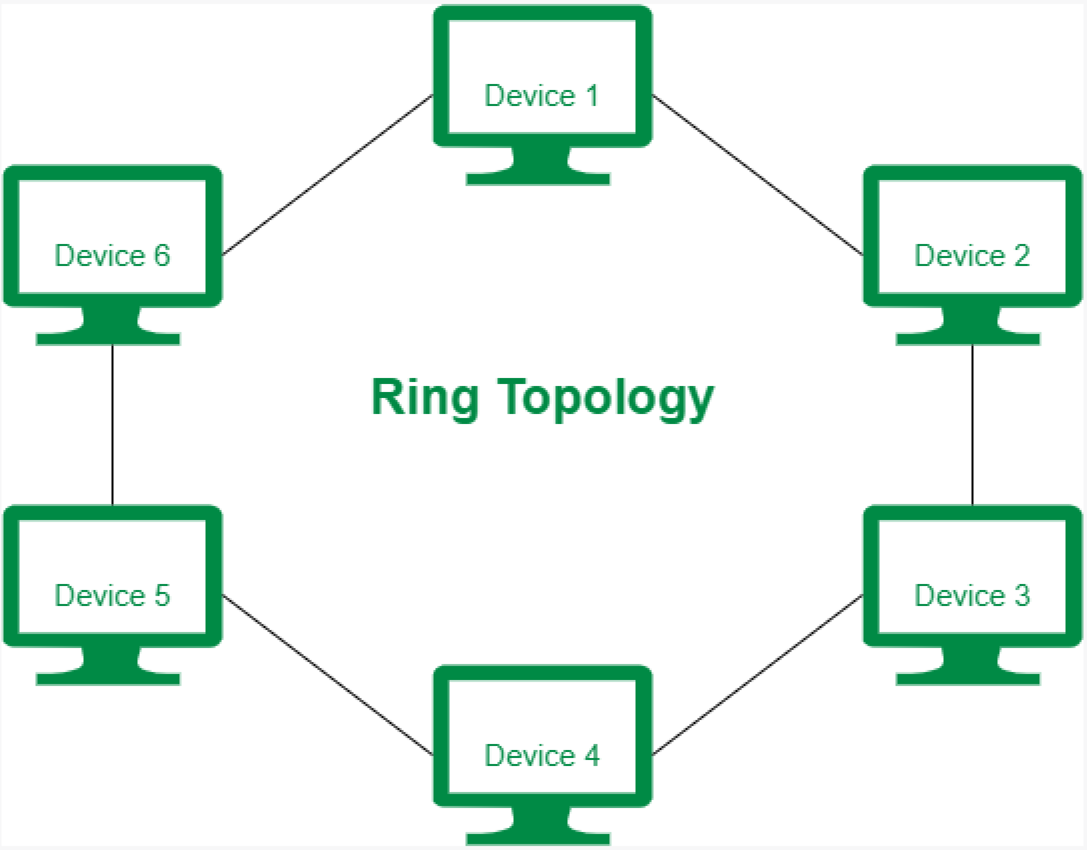


Image Source:
https://media.geeksforgeeks.org/wp-content/uploads/20200526102238/Untitled-Diagram-153-1.png

4. Mesh topology: Devices are connected to multiple other devices, forming a complex web-like structure.

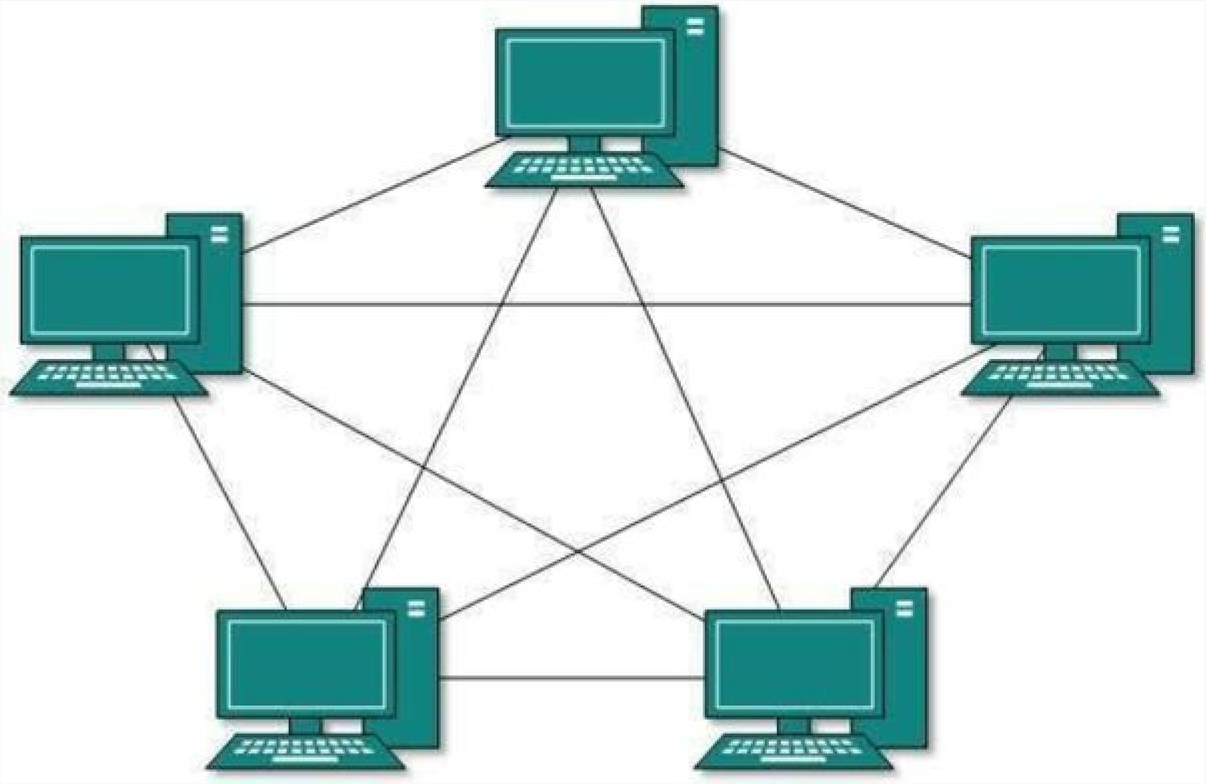


Image Source:
https://qph.cf2.quoracdn.net/main-qimg-89dce7c1b8d9c31ec8023c4abfb3056b-pjlq

Network Types

There are several types of computer networks based on their size, geographical scope, and topology. Here are some common network types:

1. LAN (Local Area Network)

   A Local Area Network (LAN) is a network that covers a small geographic area, such as a home, office, or school campus. A LAN typically consists of multiple devices connected together using switches or routers.

   The main advantage of a LAN is that it enables devices to share resources and communicate with each other. For example, devices on a LAN can share files, printers, and internet connections. This makes it easier for people to work together and collaborate on projects.

   LANs are commonly used in offices, schools, and homes. In an office setting, LANs are used to connect computers and other devices in a single building or group of buildings. In a home setting, LANs are used to connect computers, printers, and other devices together to share resources and access the internet.

2. MAN (Metropolitan Area Network)

   A Metropolitan Area Network (MAN) is a network that covers a medium-sized geographic area, such as a city or town. A MAN typically consists of multiple Local Area Networks (LANs) connected together using switches or routers.

   The main purpose of a MAN is to provide high-speed network connectivity to organizations and businesses within a specific geographic area. MANs are typically owned and operated by telecommunications companies or internet service providers (ISPs).

   MANs are commonly used by businesses, government agencies, and educational institutions that need to transfer large amounts of data between different locations within a city or town. For example, a university might use a MAN to connect different departments located in different buildings throughout a campus.

   MANs are also used by service providers to provide high-speed internet access to residential and business customers within a specific geographic area. The infrastructure required for a MAN can be expensive, so it is typically used in areas with high population density or where there is a high demand for high-speed internet access.

3. WAN (Wide Area Network)

   A Wide Area Network (WAN) is a network that covers a large geographic area, such as a city, country, or even multiple countries. A WAN typically consists of multiple Local

Area Networks (LANs) and Metropolitan Area Networks (MANs) connected together using routers and other networking devices.

The main purpose of a WAN is to provide long-distance communication and connectivity between geographically distant locations. WANs are used by organizations and businesses with multiple locations in different cities or countries that need to share resources and communicate with each other.

WANs are commonly used by large corporations, government agencies, and universities that need to transfer large amounts of data between different locations across the world. For example, a multinational corporation might use a WAN to connect its headquarters in one country with its branch offices in other countries.

WANs can be expensive to set up and maintain, as they require specialized networking equipment and high-speed communication links. However, they are essential for businesses and organizations that need to communicate and share information across long distances in real-time.

4. PAN (Personal Area Network)

A Personal Area Network (PAN) is a network that covers a small area, typically within a few meters of a person. A PAN is used for personal communication and connectivity between personal devices, such as smartphones, laptops, tablets, and wearable devices.

The main purpose of a PAN is to allow individuals to connect their personal devices together and share data between them. For example, a PAN can be used to transfer files, share internet connections, and synchronize data between different devices.

PANs can be created using wireless technologies such as Bluetooth, Wi-Fi, or Near Field Communication (NFC). These technologies allow devices to connect and communicate with each other without the need for cables or wires.

PANs are commonly used by individuals in their daily lives to connect their personal devices together and share data between them. For example, a person might use a PAN to connect their smartphone, laptop, and wearable fitness tracker together to share data and information.

Communication Protocols

A communication protocol is a set of rules and procedures used for transmitting data over a computer network. Communication protocols define the format, timing, sequencing, and error control of data transmission between devices on a network.

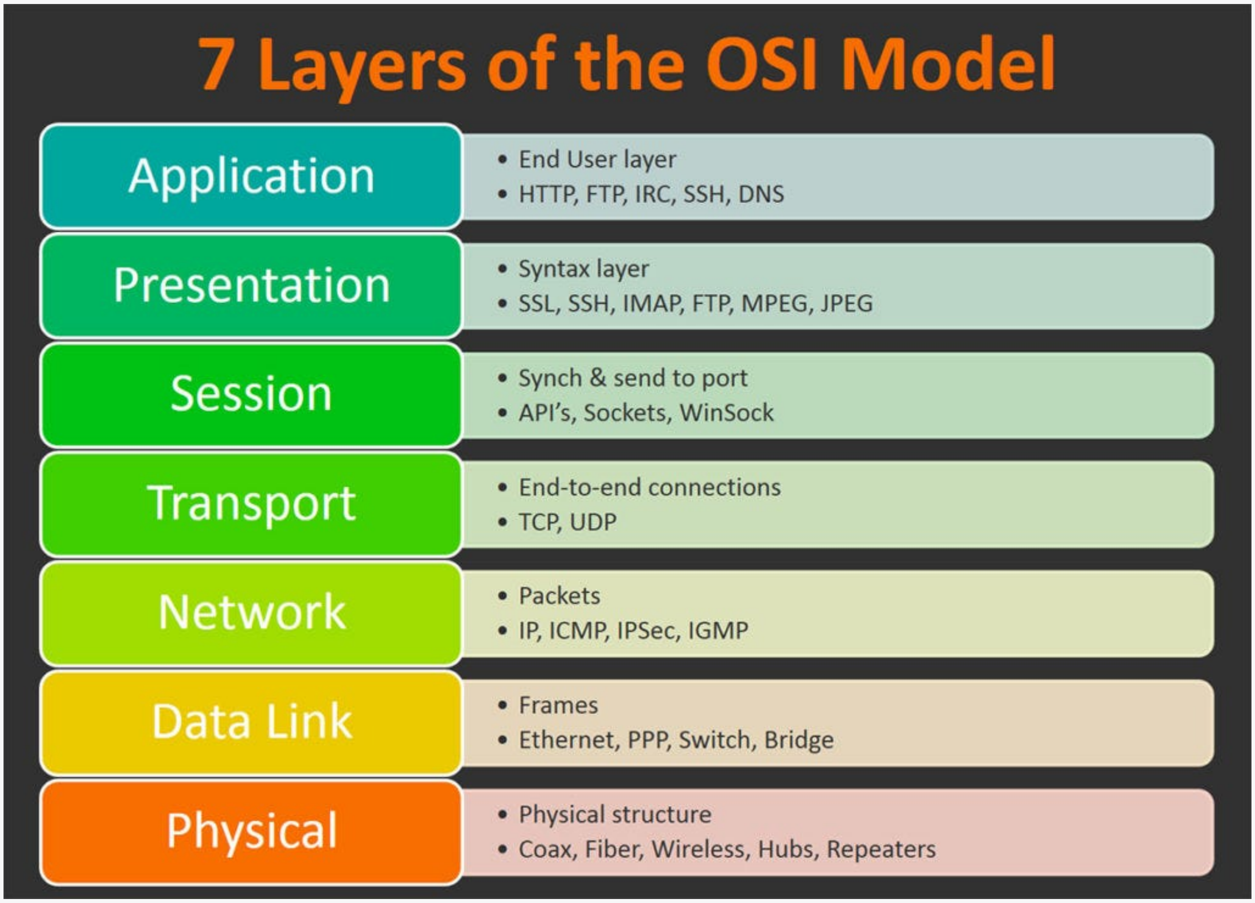
Communication protocols can be categorized into different layers, each of which deals with a specific aspect of the data transmission process. The most commonly used layered protocol model is the OSI (Open Systems Interconnection) model, which consists of seven layers:

1. Physical Layer: This layer is responsible for the physical transmission of data over the network. It defines the physical characteristics of the communication channel, including the cable type, data rate, and signal encoding. Examples of protocols that operate at this layer include Ethernet, Token Ring, and RS-232.
2. Data Link Layer: This layer is responsible for the reliable transmission of data between devices on a network. It provides error detection and correction, flow control, and access control. Examples of protocols that operate at this layer include the Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), and Ethernet.
3. Network Layer: This layer is responsible for routing data between different networks. It defines how data is transmitted from the source device to the destination device, and it provides services such as addressing and routing. Examples of protocols that operate at this layer include the Internet Protocol (IP), Internet Control Message Protocol (ICMP), and Address Resolution Protocol (ARP).
4. Transport Layer: This layer is responsible for ensuring the reliable delivery of data between applications running on different devices. It provides services such as segmentation, reassembly, flow control, and error recovery. Examples of protocols that operate at this layer include the Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP).
5. Session Layer: This layer is responsible for managing communication sessions between devices on a network. It establishes, manages, and terminates sessions between applications running on different devices. Examples of protocols that operate at this layer include the Remote Procedure Call (RPC) protocol and the Session Initiation Protocol (SIP).
6. Presentation Layer: This layer is responsible for the presentation of data to the application layer. It provides services such as data compression, encryption, and decryption. Examples of protocols that operate at this layer include the Secure Sockets

Layer (SSL), Transport Layer Security (TLS), and the Simple Network Management Protocol (SNMP).

7. Application Layer: This layer is responsible for providing services to applications running on different devices. It defines the protocols used by specific applications, such as email, file transfer, and web browsing. Examples of protocols that operate at this layer include the Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP).

Communication protocols are essential for ensuring that data is transmitted correctly and efficiently over a network. They provide a standardized way for devices on a network to communicate with each other and enable different devices and applications to work together seamlessly.



7 Layers of the OSI Model

Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters

Image Source:
https://miro.medium.com/v2/resize:fit:1024/1*17Zz6v0HWIzgiOzQYmO6lA.jpeg

Networking Hardware

Networking hardware refers to the physical devices used to build computer networks. These devices are designed to facilitate communication between different devices on the network and include the following:

1. Network Interface Card (NIC): A network interface card is a hardware component that enables a computer to connect to a network. It provides the computer with a physical interface to the network, allowing it to send and receive data.

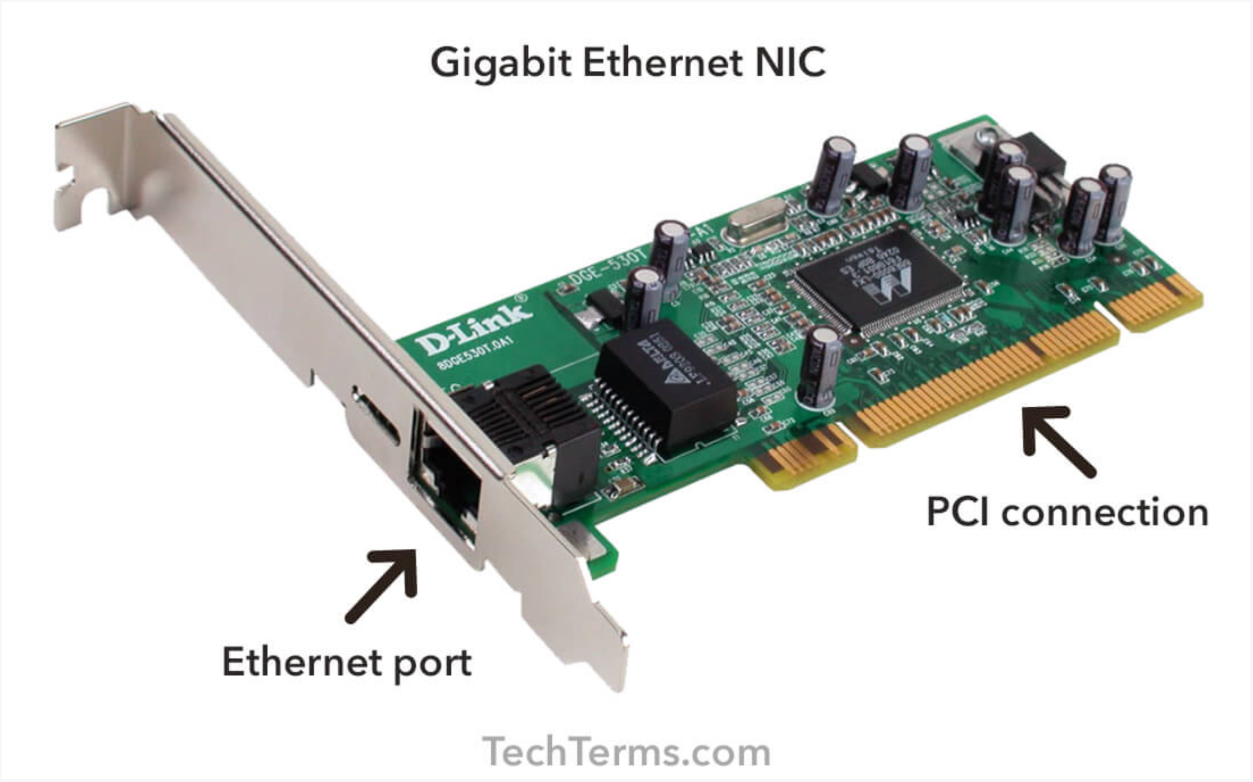
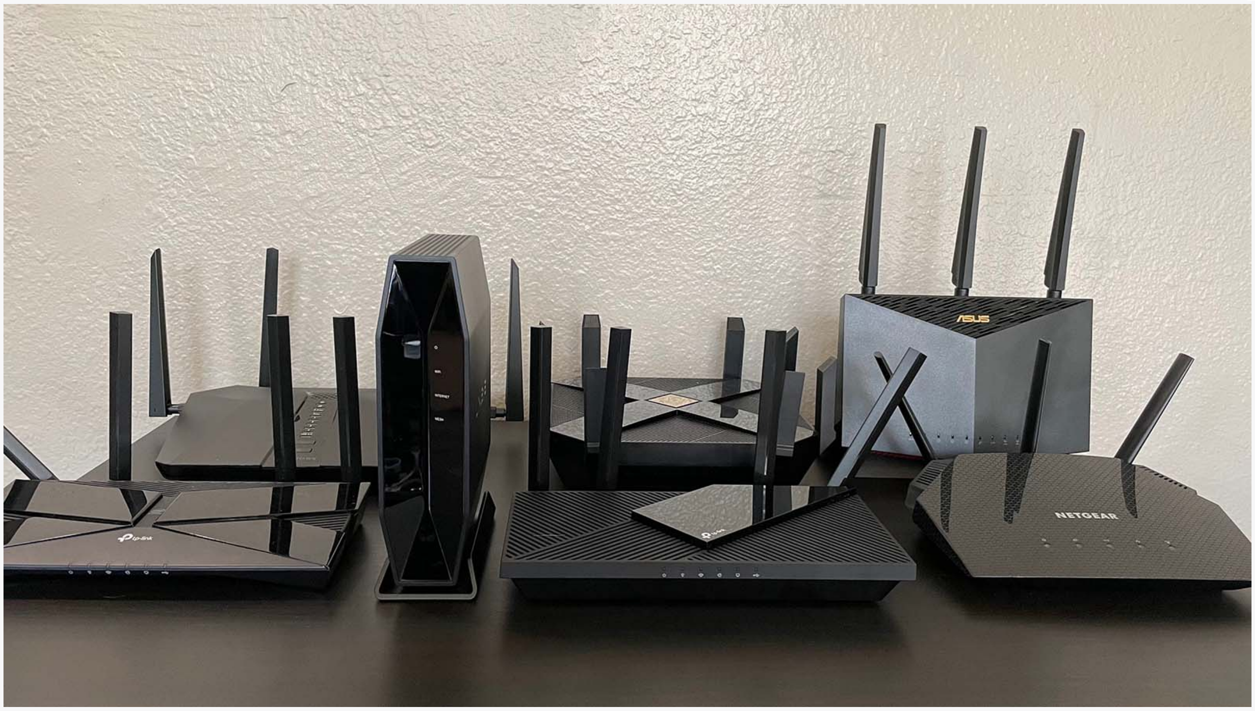


Image Source: https://techterms.com/img/lg/nic_98.jpg

2. Switches: Switches are devices that allow multiple devices on a network to communicate with each other. They are used to create local area networks (LANs) and provide a way to manage network traffic.

Image Source: https://www.cisco.com/c/dam/en/us/support/web/images/series/switches-350x-series-stackable-managed-switches.jpg

3. Routers: Routers are devices that connect multiple networks together and facilitate communication between devices on different networks. They are used to create wide area networks (WANs) and provide a way to manage network traffic.



4. Hubs: Hubs are devices that connect multiple devices on a network together. They are used to create small LANs and provide a way to manage network traffic.

Image Source: https://thecybersecuritymancom.files.wordpress.com/2018/01/hub4.png

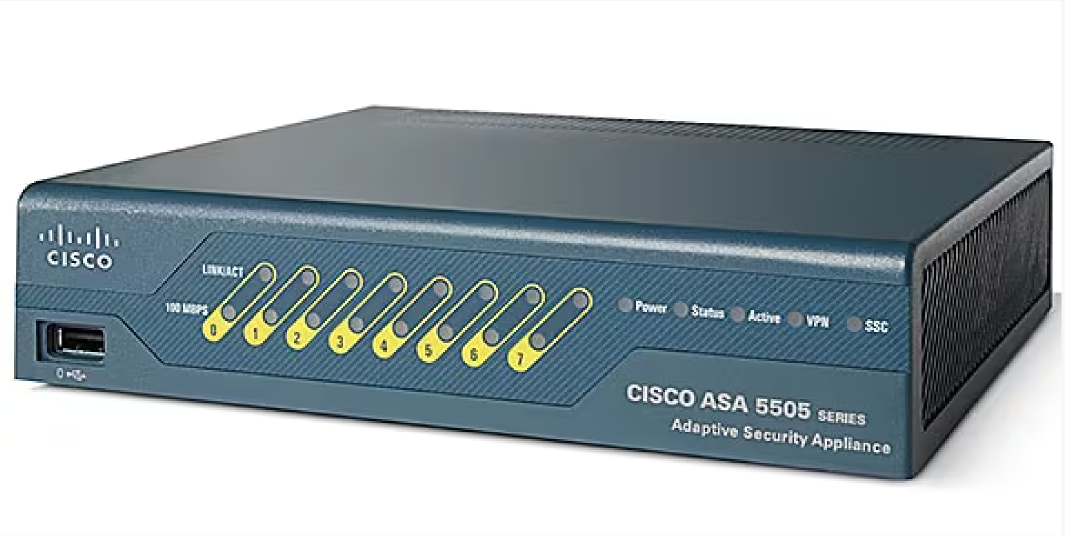
5. Modems: Modems are devices that allow computers to connect to the internet. They convert digital signals from a computer into analog signals that can be transmitted over a telephone line, cable, or satellite.

Image Source: https://static-01.daraz.com.np/p/81f2e3109175afc258ad0f65d809a620.jpg

6. Access Points: Access points are devices that allow wireless devices to connect to a network. They are used to create wireless LANs and provide a way to manage network traffic.

7. Repeaters: Repeaters are devices that amplify and regenerate signals as they travel along a network. They are used to extend the range of a network and improve signal quality.

8. Firewalls: Firewalls are devices that are used to protect a network from unauthorized access. They monitor incoming and outgoing network traffic and block any traffic that does not meet predefined security rules.



9. Load Balancers: Load balancers are devices that distribute network traffic across multiple servers or network devices. They are used to improve network performance and ensure that no single device is overloaded with traffic.

These are just a few examples of the hardware components used in computer networks. The specific hardware used will depend on the type and size of the network being created.

Wireless Networking

Wireless networking refers to the communication of data between devices without the use of physical wires or cables. Wireless networks use radio waves or infrared signals to transmit data between devices such as computers, smartphones, tablets, and other electronic devices.

Wireless networks can be classified into different types based on the range of coverage and the technology used. Some of the commonly used wireless networking technologies include Wi-Fi, Bluetooth, Zigbee, and NFC (Near Field Communication).

1. **Wi-Fi** is the most popular wireless networking technology used for connecting devices to the internet. It uses radio waves to transmit data over short distances and provides high-speed connectivity. Wi-Fi networks are commonly used in homes, offices, public places like airports, cafes, and hotels.
2. **Bluetooth** is another wireless networking technology that is used for short-range communication between devices. It is commonly used for connecting smartphones, tablets, and other portable devices to other devices such as speakers, headphones, and car stereos.
3. **Zigbee** is a wireless networking technology that is used for connecting devices in a home automation system. It is commonly used for connecting smart devices such as light bulbs, thermostats, and security systems.
4. **NFC** is a wireless networking technology that is used for short-range communication between devices. It is commonly used for mobile payments, contactless payments, and data transfer between devices.

Overall, wireless networking has become an essential part of modern life, and the demand for wireless connectivity continues to grow as technology advances.