COMPUTER NETWORKS

By: Sagar Chhabriya (Batch CS-2k22)

SEM-5

SUBMITTED TO
Sir Mohammad Faiz Lakhani

Contents

Networking History

ARPANET: The First Network (Advanced Research Projects Agency Network)

In 1969, ARPANET, the first computer network, was created by the U.S. Department of Defense. Its primary purpose was to ensure communication during a nuclear war. ARPANET initially connected four universities, but by 1972, it expanded to include 40 machines. ARPANET laid the foundation for the modern Internet.

The Internet

ARPANET expanded over time to link U.S. defense-related universities. It eventually included connections with institutions like University College London and Norway's Royal Radar Network. This global network of networks was named the **"Internet"** by Vinton Cerf, Yogen Dalal, and Carl Sunshine, researchers from Stanford University. They also developed the key protocols, such as **TCP**, which are still essential for communication on the Internet today.

What is Computer Networking?

Computer networking refers to the practice of connecting multiple computing devices that can exchange data and share resources. These networks enable devices to communicate with each other, providing the backbone for services like the Internet, file sharing, and online communication.

Communications Protocols

Devices in a network use a system of rules known as **communications protocols** to transmit information. These protocols define the rules and methods for data exchange over both physical and wireless technologies, ensuring that the data is transferred accurately and efficiently between devices.

How Does a Computer Network Work?

In a computer network, the devices, known as **nodes**, follow specific rules, called **protocols**, to send and receive data. The **network architecture** defines how the parts of the network interact. It includes the physical devices, the arrangement of components, and the protocols that govern how the devices communicate. Essentially, the architecture ensures that data flows smoothly and securely across the network.

Modern Computer Networks

Modern computer networks have evolved to meet the needs of a connected world. Some of the key features of contemporary networks include:

1. **Operate Virtually**: Modern networks create virtual connections over physical ones, enabling flexibility and scalability.
2. **Integrate Large Networks**: Networks can now be integrated and managed on a large scale, allowing efficient communication across wide geographic areas.
3. **Respond Quickly**: Software-driven networks can adjust in real time to manage traffic and optimize performance.
4. **Ensure Security**: Built-in security features and support for additional protections are standard, ensuring the integrity and privacy of communications.

Data Communication

What is Data Communication?

Data communication refers to the process of transferring data between two or more devices over a transmission medium. This involves both sending and receiving data. Data communication plays a vital role in enabling various services, such as the Internet, email, and instant messaging.

Transmission

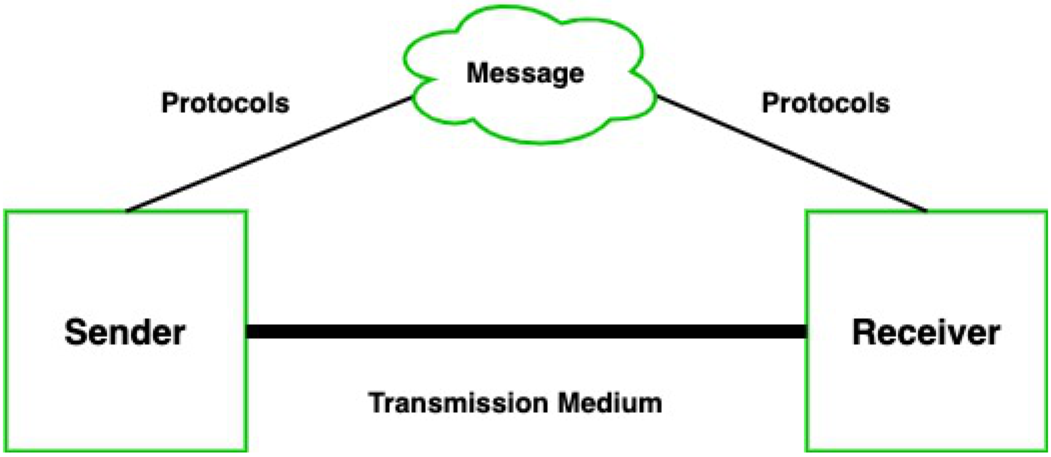
Transmission is a critical component of data communication, referring to the act of sending data from one location to another. This can involve physical media (e.g., cables) or wireless methods (e.g., Wi-Fi, Bluetooth).

Components of Data Communication

Data communication involves five key components:

1. **Message**: The information being transmitted, which could be in the form of text, audio, video, or other data types.
2. **Sender**: The device that initiates the transmission of the message (e.g., a computer or mobile phone).
3. **Receiver**: The device that receives the transmitted message (e.g., another computer or mobile phone).
4. **Transmission Medium / Communication Channels**: The path over which the data travels, which can be wired (e.g., fiber optic cables, copper wires) or wireless (e.g., radio waves, satellite signals).

5. **Set of Rules (Protocols)**: The agreed-upon guidelines that ensure the message is correctly interpreted by both the sender and the receiver. These rules can include languages, data formats, and specific communication protocols like **HTTP** or **TCP/IP**.



Types of Data Transmission

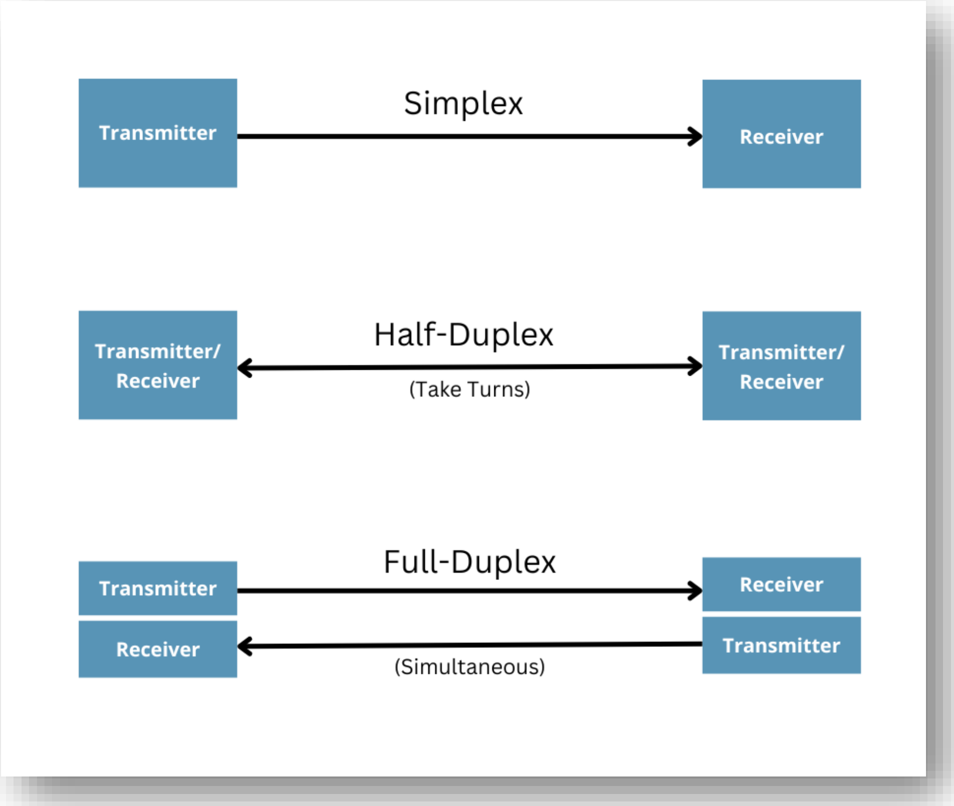
Data transmission refers to the communication of sending or receiving data between devices. It can be categorized into two types:

Simplex (One-Way Communication)

- **Simplex Communication** is one-way communication where one device sends data, and the other only receives.
  Example: A keyboard sending input to a computer or listening to music through speakers.

Duplex (Two-Way Communication)

- **Half Duplex Communication** allows two-way communication, but not at the same time. Devices can send and receive data, but not simultaneously.
  Example: Walkie-talkies, where users can talk and listen, but not at the same time.
- **Full Duplex Communication** allows two-way communication where devices can send and receive data simultaneously.
  Example: Mobile phones and landlines.



Synchronous vs. Asynchronous Transmission

1. **Synchronous Transmission**
   - In synchronous transmission, data flows continuously with timing signals, keeping both sender and receiver in sync.
   - **Advantage**: Faster data transfer as it flows without interruption.
   - **Disadvantage**: Requires precise timing between sender and receiver.
2. **Asynchronous Transmission**
   - In asynchronous transmission, data is sent in separate packets with start and stop signals, meaning the sender and receiver don't need to be in sync.
   - **Advantage**: Flexible and easy to set up.
   - **Disadvantage**: Slower due to additional signals for synchronization.

Signal Types

1. **Analog Signal**
   - Analog signals are continuous waves that vary smoothly to represent information. **Example**: Radio waves.

2. **Digital Signal**
    - Digital signals are discrete pulses representing information in binary form (0s and 1s). **Example**: Data transferred over Ethernet cables.

Network Protocols

Network protocols are a set of rules that govern communication between devices in a network. Here are some common protocols:

1. **IP (Internet Protocol)** - Directs data packets to the correct address on a network.
2. **TCP/IP (Transmission Control Protocol/Internet Protocol)** - Ensures data is sent and received correctly over the internet.
3. **FTP (File Transfer Protocol)** - Used for transferring files between computers.
4. **HTTP (Hypertext Transfer Protocol)** - Used to transfer web pages from the server to the browser.
5. **ICMP (Internet Control Message Protocol)** - Sends error messages and operational information about network connections.
6. **POP3 (Post Office Protocol version 3)** - Used to retrieve email from a server.
7. **TCP** - Breaks messages into smaller packets and reassembles them at the receiving end.

How Network Protocols Work

Network protocols help devices communicate over a network. The **OSI Model** is commonly used to understand the role of each protocol. It has seven layers, with each layer handling specific aspects of communication.

Network Connectivity Devices

Several network devices help establish and maintain communication between devices on a network. These include:

1. **Router**
    - A router connects different networks together (e.g., a home network to the internet). **Packet Tracer Command**: router(config)# ip address [IP address] [subnet mask]

2. **Switch**

   - A switch connects multiple devices in the same network and directs data using MAC addresses.

     Packet Tracer Command: switch(config)# mac-address-table static [MAC address] vlan [vlan id]

3. **Hub**

   - A hub connects devices and sends data to all devices, which is less efficient than a switch.

4. **Modem**

   - A modem converts digital data into a format suitable for transmission over telephone lines.

5. **Access Point (AP)**

   - An access point provides wireless connectivity to a wired network, allowing devices to connect without cables.

6. **Network Interface Card (NIC)**

   - A NIC allows a device to connect to a network, either wired or wireless.

7. **Firewall**
    - A firewall protects the network by monitoring and controlling incoming and outgoing traffic based on security rules.
8. **Repeater**
    - A repeater amplifies signals to extend the range of a network.
9. **Bridge**
    - A bridge connects multiple Local Area Networks (LANs) to create a larger network.

Broadcast vs Unicast

In networking, data can be sent in two ways: broadcast or unicast.

- **Broadcast**
    - **Definition**: Sends data to all devices on a network.
    - **Example**: ARP (Address Resolution Protocol) sends data to all devices to resolve IP addresses to MAC addresses.
    - **Efficiency**: Can cause network congestion in large networks.
- **Unicast**
    - **Definition**: Sends data from one device to a specific destination device.
    - **Example**: Accessing a website or sending an email.
    - **Efficiency**: More efficient as data is only sent to the target device.

What is a MAC Address?

A **MAC (Media Access Control) address** is a unique identifier assigned to a device's network interface controller (NIC). It is a 48-bit hexadecimal address, often written in the format MM:MM:MM:SS:SS:SS. Each device on a network has a unique MAC address, just like a fingerprint.

ARP (Address Resolution Protocol)

ARP is used to find a device's MAC address when you only know its IP address.
Example: If a computer knows an IP address but needs to send data to the device's MAC address, it uses ARP.

RARP (Reverse Address Resolution Protocol)

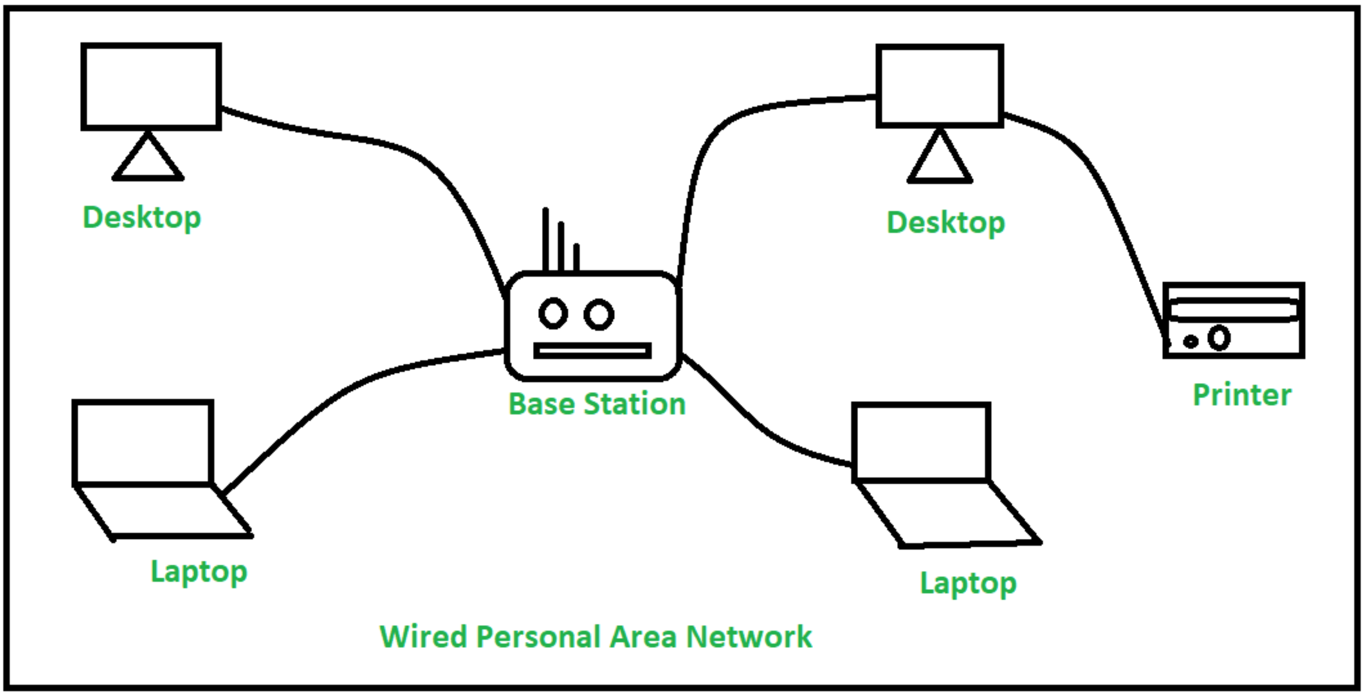
RARP is used to find the IP address of a device when you only know its MAC address.
Example: A device with a known MAC address requests its IP address from a RARP server.

Classification of Computer Network Architectures

1. **Client-Server Architecture**
   - In this model, servers provide resources and manage tasks, while clients request resources from servers.
     Example: A company's central server provides data that employees can access.
2. **Peer-to-Peer (P2P) Architecture**
   - All computers in this model have equal roles and can share resources with each other. No central server is needed.
     Example: Multiple computers working together to render 3D graphics.

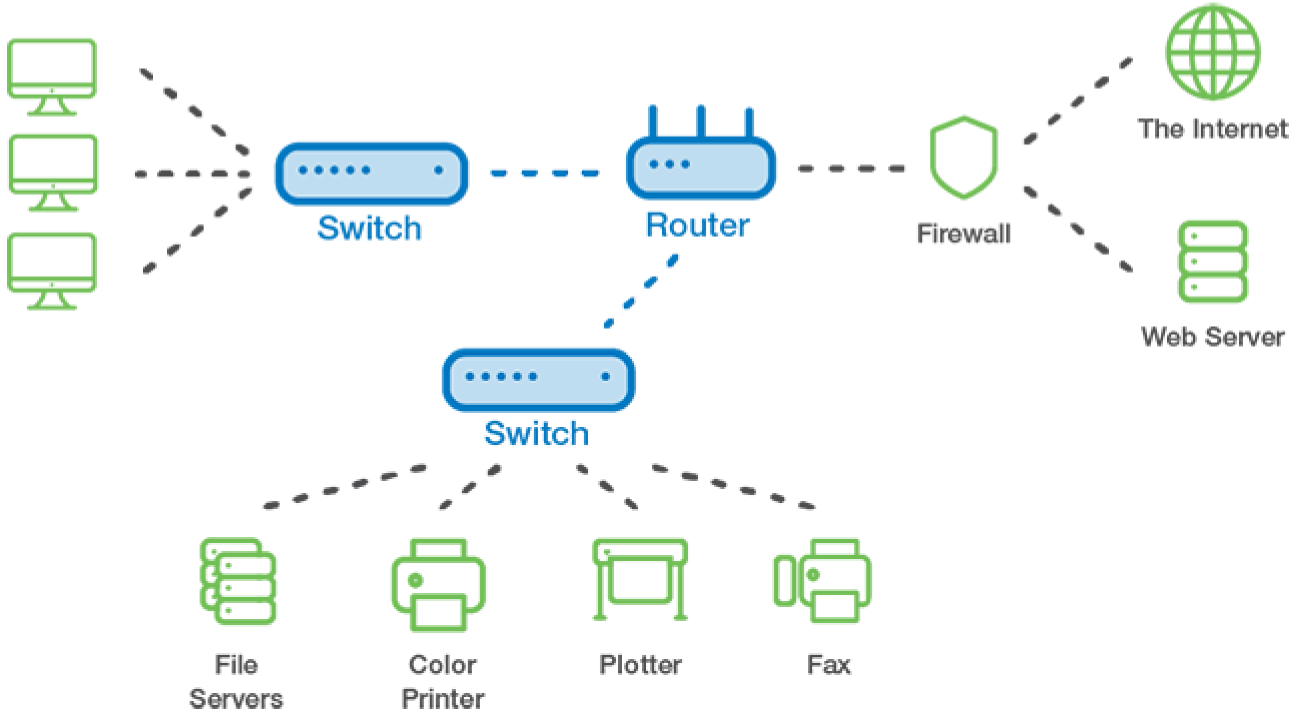
Types of Networks According to Geographical Coverage

1. **PAN (Personal Area Network)**
   - A small network connecting personal devices within a short range.
     Example: Bluetooth connections between a smartphone and wireless headphones.



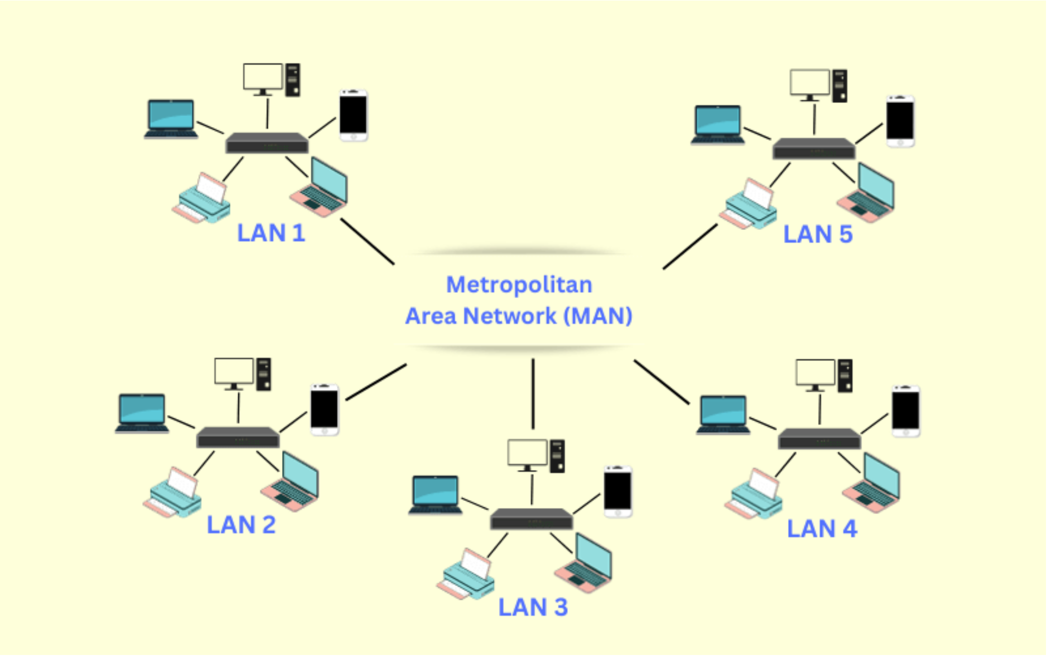
2. **LAN (Local Area Network)**

   - A network that connects devices within a limited area such as a home or office. **Example**: The network in an office connecting computers and printers.



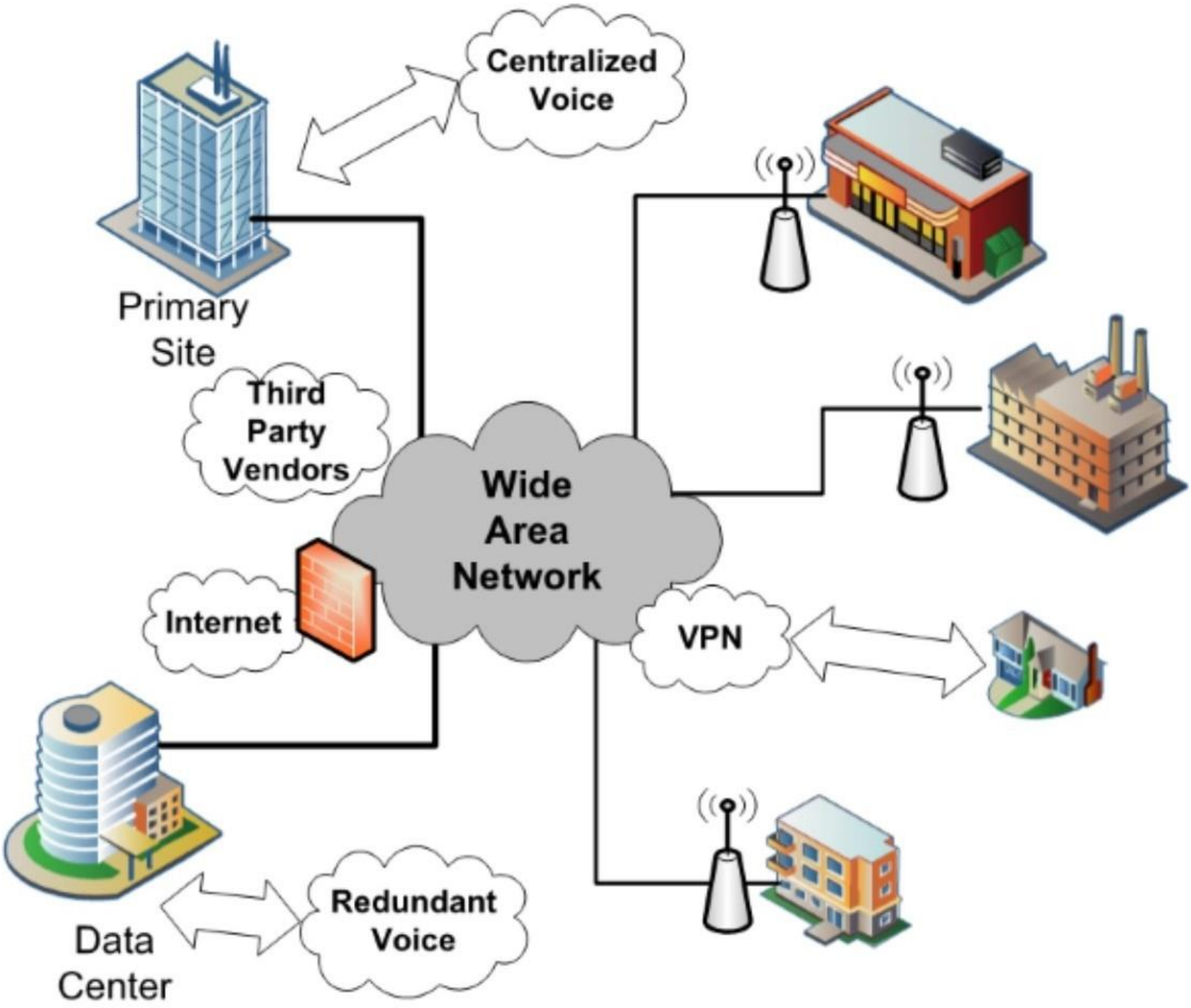
3. **MAN (Metropolitan Area Network)**

   - A network covering a city or a large campus. **Example**: A university's network across a city.



4. **WAN (Wide Area Network)**

   - A network covering a large geographic area, such as a country or continent. **Example**: The internet, connecting networks globally.



Network Topology

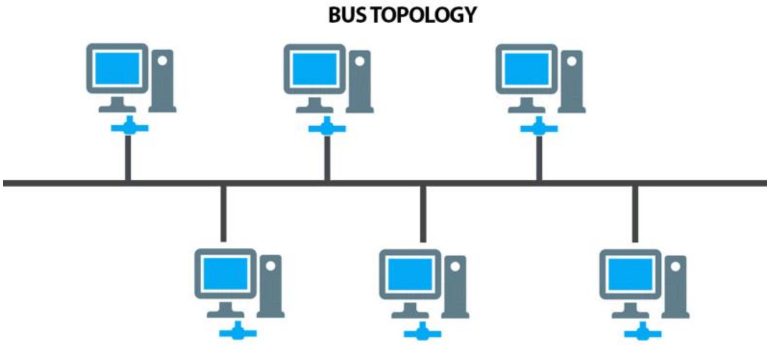
A **network topology** refers to the physical and logical arrangement of the nodes (devices) and connections (cables or wireless links) in a network. It determines how network devices, such as computers, routers, switches, and other components, are organized and connected to each other. The topology also defines how data flows within the network and how devices interact. There are two main types of topologies:

1. **Physical Topology**: Refers to the actual layout of the devices and cables in a network. It shows how the devices are physically connected.
2. **Logical Topology**: Describes how data moves within the network, focusing on the flow of information between devices, which may be different from the physical layout.

The choice of topology influences the network's performance, scalability, fault tolerance, and overall reliability.

Types of Network Topologies

1. **Bus Topology**
   - **Description**: In a bus topology, all devices are connected to a single central cable, called the bus. Data sent by any device travels along the bus to all other devices. This is a simple and cost-effective topology, though it can suffer from performance issues as more devices are added.
   - **Example**: Older Ethernet networks using coaxial cables.



Advantages:

- Easy to install and extend.
- Requires less cable than other topologies.

Disadvantages:

- Limited cable length and number of devices.
- A failure in the main cable can bring down the entire network.

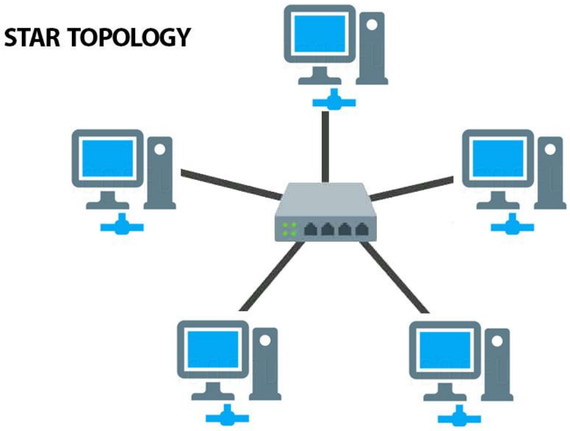
2. **Star Topology**
   - **Description**: In a star topology, each device is connected to a central hub or switch. The hub or switch manages and routes data between devices. If one device fails, the rest of the network continues to function normally.
   - **Example**: Modern office networks where computers and printers connect to a central switch or router.

Advantages:

- Easy to add or remove devices without disrupting the network.
- Centralized management.

Disadvantages:

- The failure of the central hub or switch brings down the entire network.



3. **Ring Topology**

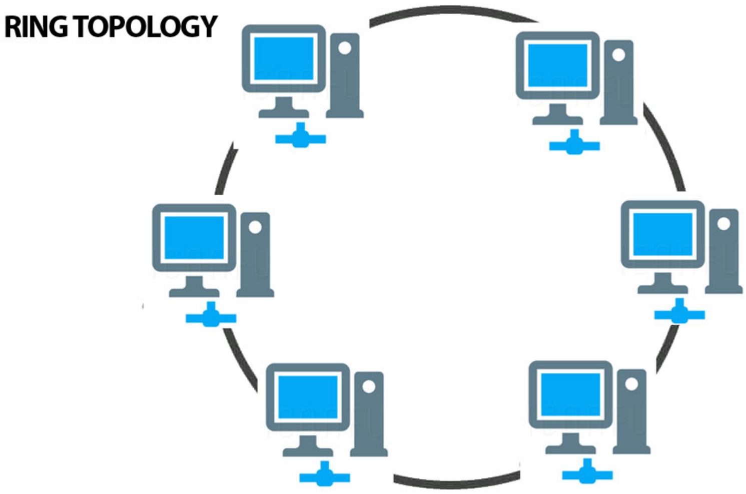
- **Description**: Devices in a ring topology are connected in a circular fashion, with each device connected to two other devices. Data travels in one direction around the ring (or both directions in a dual-ring setup). Token Ring is an example of this type of network, where devices pass a token to control access to the network.
- **Example**: Older networks, such as Token Ring networks.

Advantages:

- Data transmission is relatively fast, as there's a direct path.
- Works well for smaller networks.

Disadvantages:

- If one device or connection fails, the entire network can be disrupted.
- Difficult to troubleshoot and expand.



4. **Mesh Topology**

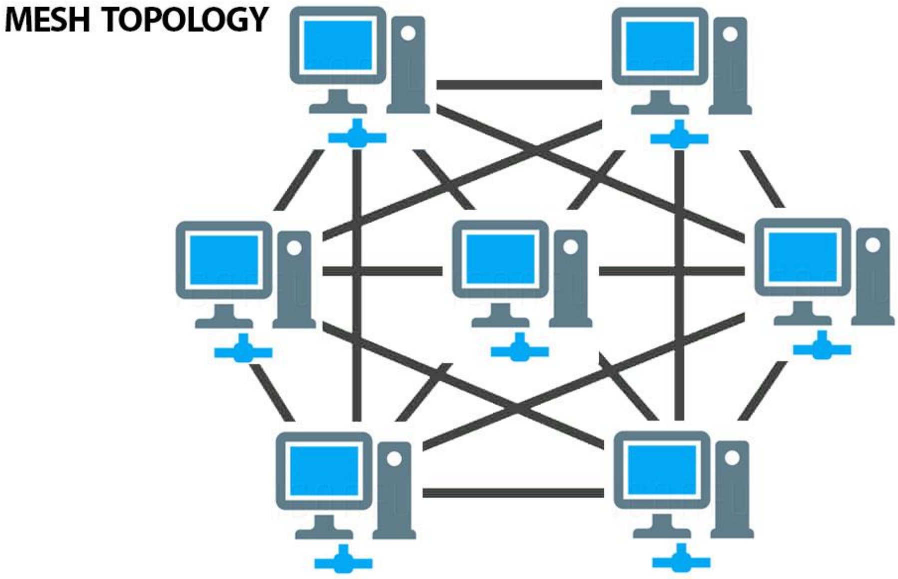
   - **Description**: In a mesh topology, each device is interconnected with every other device, providing multiple paths for data to travel. This topology is highly redundant and resilient, meaning the network can withstand failures. Mesh networks can be fully meshed (where every device is connected to every other device) or partially meshed (some devices are connected to multiple others).
   - **Example**: The internet, where routers are connected with redundant paths to ensure reliability and fault tolerance.

Advantages:

- High fault tolerance, as multiple paths are available.
- Data can be transmitted simultaneously between devices.

Disadvantages:

- Expensive to implement due to the large number of connections.
- Complex to maintain.



5. **Tree Topology**

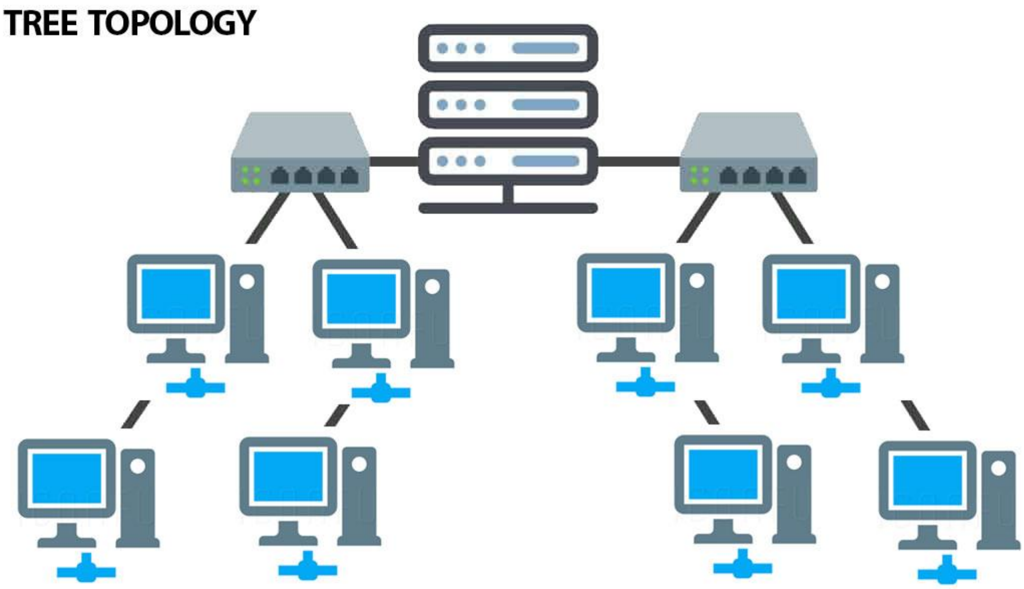
- **Description**: Tree topology is a hybrid that combines elements of bus and star topologies. Devices are grouped into star-configured networks (branches), which are then connected to a central backbone (bus). This hierarchical structure is ideal for large organizations or campuses.
- **Example**: Large corporate networks where departments have their own star networks connected to a central backbone.

Advantages:

- Scalable and hierarchical, ideal for large networks.
- Easy to isolate network faults.

Disadvantages:

- The backbone cable is a single point of failure.
- Expensive to implement.



6. **Hybrid Topology**

    - **Description**: A hybrid topology combines two or more different topologies to take advantage of the strengths of each. For example, a network may use star topology within departments and connect these stars using a bus or ring topology for inter-department communication.

    - **Example**: A corporate network that uses star topology within departments and bus topology for inter-department connections.

Advantages:

- Flexible and adaptable to different needs.
- Can be tailored to optimize performance.

Disadvantages:

- More complex to design and manage.
- Can be costly due to the use of multiple topologies.

Cover up

- **Bus Topology**: All devices share a common central cable. Simple but prone to failure.
- **Star Topology**: Devices are connected to a central hub or switch. Easy to manage but reliant on the central hub.
- **Ring Topology**: Devices are connected in a circular fashion. Reliable but vulnerable to single-point failures.
- **Mesh Topology**: Devices are interconnected, providing multiple paths for data. Highly fault-tolerant but expensive and complex.
- **Tree Topology**: Combines star and bus topologies, ideal for large networks.
- **Hybrid Topology**: A combination of different topologies to leverage the benefits of each.

Networking Addresses

Networking addresses are identifiers used to uniquely identify devices on a network, allowing them to communicate with each other. There are two main types of addresses:

1. **IP Address (Logical Address)**: This address is used to identify devices in a network, including computers, routers, and other devices. It is the logical address assigned to a device for communication over the internet or a local network.

2. **MAC Address (Physical Address)**: This is a unique hardware address assigned to a network interface card (NIC) in a device. It operates at the Data Link Layer of the OSI model and is used for communication within the same network segment (local network).

Types of IP Addresses

- **Public IP Address**: A unique IP address assigned to devices that are directly accessible from the internet. These are typically assigned by the Internet Service Provider (ISP).

- **Private IP Address**: An IP address used within a private network and not routable on the public internet. These are reserved for local network usage and are part of certain IP address ranges (e.g., 192.168.x.x, 10.x.x.x).

IPv4 and IPv6 Addresses

- **IPv4 (Internet Protocol version 4)**:
  - **Format**: An IPv4 address consists of 32 bits, divided into 4 octets (each ranging from 0 to 255), represented as four decimal numbers separated by periods. Example: 192.168.1.1.
  - **Total Addresses**: IPv4 can support a total of **2^32** (about 4 billion) unique addresses.

- **IPv6 (Internet Protocol version 6)**:
  - **Format**: IPv6 addresses are 128 bits long and are written as eight groups of four hexadecimal digits, separated by colons. Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
  - **Total Addresses**: IPv6 can support **2^128** (about 3 trillion) unique addresses, allowing for a vast number of devices to be connected globally.

DTE and DCE

- **DTE (Data Terminal Equipment)**: These are devices that serve as endpoints in data communication networks, such as computers, printers, or other devices that generate or consume data. These devices communicate through data interfaces.

- **DCE (Data Communication Equipment)**: These are devices that facilitate data transmission between DTEs. Examples include modems, routers, and switches. DCE devices convert data formats and manage communication between DTEs.

Routing

- **Routing**: Routing refers to the process of selecting paths in a network to send data from a source to a destination.
- **Dynamic Routing**: In dynamic routing, routes are automatically adjusted based on network changes using routing protocols like **OSPF** (Open Shortest Path First) and **BGP** (Border Gateway Protocol). These protocols help routers determine the best paths dynamically.
- **Static Routing**: In static routing, routes are manually configured by the network administrator. These routes remain fixed and do not change unless updated manually.

What is an IPv4 Address?

An **IPv4 address** is a unique identifier assigned to each device on a network. It acts like a "home address" for your device, allowing it to communicate with other devices on the network. It is divided into two parts:

- **Network ID**: Identifies the network to which the device belongs.
- **Host ID**: Identifies the specific device within that network.

Example: The address 192.168.1.1 consists of a network ID (192.168.1) and a host ID (1).

Need for Classful Addressing

In the early days of IP networking, IP addresses were divided into fixed-size blocks, leading to inefficiency. For example, an organization might have needed a Class A network but only had a few devices, wasting a large number of available addresses.

The need for classful addressing led to the creation of **subnetting**, which divides the address space more efficiently based on the size of the network.

IP Address Classes (IPv4)

The **32-bit IPv4 address** is divided into five classes. These classes are designed for different types of networks:

1. **Class A**:
   - **Range**: 1.0.0.0 to 126.255.255.255.
   - **Network ID**: 8 bits.
   - **Host ID**: 24 bits.
   - **Purpose**: For large networks, offering a significant number of hosts.

Example: 10.0.0.0

2. **Class B**:
   - **Range**: 128.0.0.0 to 191.255.255.255.
   - **Network ID**: 14 bits.
   - **Host ID**: 16 bits.
   - **Purpose**: For medium-sized networks.

Example: 172.16.0.0

3. **Class C**:
   - **Range**: 192.0.0.0 to 223.255.255.255.
   - **Network ID**: 24 bits.
   - **Host ID**: 8 bits.
   - **Purpose**: For small networks.

Example: 192.168.1.0

4. **Class D**:
   - **Range**: 224.0.0.0 to 239.255.255.255.
   - **Purpose**: Reserved for multicast addressing.
5. **Class E**:
   - **Range**: 240.0.0.0 to 255.255.255.255.
   - **Purpose**: Reserved for future or experimental use.

Baseband vs Broadband

- **Baseband**: Refers to communication using a single channel at a time. It is typically used in situations where data is sent over a single frequency range, such as Ethernet.
- **Broadband**: Refers to the ability to send multiple channels of data simultaneously over a wide range of frequencies, allowing for more data to be transmitted at once. It is used in technologies like DSL, cable, and fiber-optic networks.

Special Address: Loopback (127.0.0.1)

- **127.0.0.1** is reserved for the **loopback address**. It is used to test the network stack on the local machine. Any packets sent to this address are looped back to the local device, and it's commonly used for troubleshooting and testing purposes.

Subnetting

Subnetting is the process of dividing a single IP address into smaller subnets to improve network performance and security. It allows an organization to efficiently use IP address space and manage traffic within different segments of the network.

Transmission Media

Transmission media are the physical pathways used to transmit data from one point to another in a network. They are classified into two main categories:

1. Guided Media (Wired)

Guided media involves a physical pathway through which the data travels, typically using cables or wires. The data is transmitted through a fixed path, and examples include:

- **Coaxial Cable**: A cable that consists of a central conductor, an insulating layer, a metal shield, and an outer cover. It transmits data using electrical signals. Commonly used for cable TV, internet connections, and other forms of data transmission.
- **Twisted Pair Cable**: This cable consists of pairs of insulated wires twisted together. The twisting helps to reduce electromagnetic interference. There are two types of twisted pair cables:
  - **Shielded Twisted Pair (STP)**: These cables have a braided shield around them, offering protection against external interference.
  - **Unshielded Twisted Pair (UTP)**: These cables lack the shielding, relying solely on the twisting of wires for reducing interference.
  - **Categories**: Twisted pair cables are categorized into different types (e.g., Cat5, Cat6, Cat7), with higher categories offering better performance and faster data transmission.
- **Fiber Optic Cable**: Made of glass or plastic fibers, this cable transmits data in the form of light signals. Fiber optic cables are known for their high speed and capacity, making them ideal for long-distance communication, including high-speed internet connections.

2. Unguided Media (Wireless)

In unguided media, data is transmitted through free space using electromagnetic waves. Examples of unguided media include:

- **Radio Waves**: These electromagnetic waves are used for wireless communication, such as radio broadcasting, TV signals, and Wi-Fi. They can travel through the air and are commonly used for long-range communication.
  - **Applications**: Mobile communication, wireless networking, radar, and navigation.
  - **Advantages**: Long-distance communication, portability, and reliable connections.
  - **Disadvantages**: Prone to interference, affected by atmospheric disturbances, limited bandwidth, and potential health risks from prolonged exposure.

    - **Role of Antenna**: Antennas are used to transmit and receive radio waves. They convert electrical signals into electromagnetic waves and vice versa.

- **Microwave Transmission**: This uses high-frequency electromagnetic waves for data transmission over long distances. Microwaves can travel through the air or be transmitted via satellite, providing long-range communication capabilities.
    - **Applications**: Communication between distant locations, satellite communications, broadcasting, etc.
- **Infrared Waves**: These are a type of electromagnetic radiation, often used for short-range communication. Infrared waves require special transceiver devices to send and receive signals.
    - **Applications**: Wireless keyboards, mice, TV remote controls, and night vision technologies.
- **Satellite Microwaves**: These microwaves are transmitted between the Earth and satellites orbiting in space. They are crucial for global communication and broadcasting services.
    - **Applications**: Satellite television, global internet services, GPS systems.

Key Concepts in Transmission Media

- **Bandwidth**: This refers to the amount of data that can be transmitted through a medium over a period of time, typically measured in kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps). Higher bandwidth means more data can be transmitted in a given time.

Transmission Media Comparison

Transmission Media	Type	Advantages	Disadvantages
Coaxial Cable	Guided (Wired)	Durable, reliable, good for TV and internet	Susceptible to interference, bulkier than fiber
Twisted Pair Cable	Guided (Wired)	Cheap, easy to install	Lower bandwidth, subject to interference
Fiber Optic Cable	Guided (Wired)	High-speed, long-distance, immune to interference	Expensive, harder to install
Radio Waves	Unguided (Wireless)	Long-range, portable	Limited bandwidth, interference, health risks
Microwaves	Unguided (Wireless)	High data rates, long-distance communication	Affected by weather, requires line-of-sight
Infrared Waves	Unguided (Wireless)	Short-range, low interference	Limited range, requires line-of-sight

Summary of Applications and Advantages

- **Coaxial Cable**: Widely used in cable TV networks and internet connections, providing reliable transmission with good shielding against interference.
- **Twisted Pair Cable**: Common in local area networks (LANs), especially in offices and homes. With different categories, twisted pair cables provide flexible solutions for varying data transmission speeds.
- **Fiber Optic Cable**: Offers high-speed transmission and is less prone to interference, ideal for long-distance and high-performance communication.
- **Radio Waves**: Used for wireless communication, from radio and TV broadcasting to Wi-Fi and mobile phone communication.
- **Microwave Transmission**: Vital for long-distance data transmission, especially when fiber optic cables cannot be used, such as in remote or hard-to-reach areas.
- **Infrared Waves**: Used for short-range communication systems like remote controls, wireless peripherals, and sensors.

Each type of transmission medium offers specific advantages and is chosen based on the distance, speed, cost, and environment of the communication needs.

OSI Model: Open Systems Interconnection

The **OSI (Open Systems Interconnection) model** is a theoretical framework that standardizes how different networking protocols interact to facilitate communication between devices on a network. It was developed by the **International Organization for Standardization (ISO)** in **1984** to guide the development and understanding of network communication.

Why OSI Model?

The OSI model provides a universal language for computer networks, allowing devices and systems from different manufacturers to communicate effectively. It helps in understanding and troubleshooting network communications by dividing the process into manageable layers.

7 Layers of the OSI Model

The OSI model has **7 layers**, each with a specific function in the communication process. These layers work together to ensure that data can be transmitted from one network to another in a reliable, secure, and efficient manner.

1. Physical Layer (Layer 1)

- **Function**: This layer deals with the transmission of raw bits (1s and 0s) over a physical medium like cables, fiber optics, or wireless radio waves. It includes the hardware that enables the transmission of data.
- **Examples**: Cables (Ethernet, fiber optic), network interface cards (NICs), switches, routers.

2. Data Link Layer (Layer 2)

- **Function**: Responsible for creating a reliable link between two directly connected nodes. It handles framing, addressing (MAC addresses), and error detection/correction.
- **Example**: Ethernet, Wi-Fi, PPP (Point-to-Point Protocol).
    - **Error Checking**: Ensures data integrity using techniques like checksums.
    - **Framing**: Data is framed into packets for transmission.

3. Network Layer (Layer 3)

- **Function**: The network layer is responsible for routing data from the source to the destination across different networks. It breaks data into packets and handles logical addressing (IP addresses).
- **Examples**: Routers, IP (Internet Protocol), IPv4/IPv6.
    - **Routing**: Determines the best path for data to travel.
    - **Addressing**: Logical addressing using IP addresses.

4. Transport Layer (Layer 4)

- **Function**: This layer ensures reliable data transfer between two hosts. It handles error detection, correction, and flow control. It also manages segmentation and reassembly of data.

- **Examples**: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
    - **Error Checking**: Ensures that data is sent correctly and requests retransmissions if needed.
    - **Segmentation**: Breaks data into smaller segments for efficient transmission.

5. Session Layer (Layer 5)

- **Function**: This layer establishes, manages, and terminates communication sessions between applications on the sender and receiver devices. It ensures that data is synchronized and in the correct order.
- **Examples**: NetBIOS, RPC (Remote Procedure Call).
    - **Session Management**: Handles the opening, closing, and managing of communication sessions.

6. Presentation Layer (Layer 6)

- **Function**: This layer is responsible for translating data into a format that the application layer can understand. It handles data encryption, compression, and translation between different data formats.
- **Examples**: SSL/TLS (encryption), JPEG, GIF, ASCII.
    - **Data Translation**: Converts data into a readable format.
    - **Encryption and Compression**: Secures data by encrypting it and reduces the size for efficient transmission.

7. Application Layer (Layer 7)

- **Function**: The topmost layer provides the interface for user applications to interact with the network. It handles high-level protocols and serves as the bridge between the end-user and the network services.
- **Examples**: HTTP, FTP, SMTP, DNS.
    - **Application Interaction**: Allows users to interact with the network (e.g., sending an email, browsing the web).

Real-life Example: Sending an Email (Layer-by-Layer Breakdown)

Luffy sends an email to Zoro:

1. **Application Layer (Layer 7)**: Luffy uses an email application (e.g., Gmail or Outlook) to write his email.
2. **Presentation Layer (Layer 6)**: The application formats the email, encrypts it if necessary, and prepares it for transmission.

3. **Session Layer (Layer 5)**: A connection is established between Luffy's email client and Zoro's email client over the internet.
4. **Transport Layer (Layer 4)**: The email data is broken into smaller segments. Sequence numbers and error-checking information are added to ensure reliable delivery.
5. **Network Layer (Layer 3)**: The email data is addressed with IP addresses and routed through the internet to Zoro's mail server.
6. **Data Link Layer (Layer 2)**: The data is framed, and MAC addresses are added to the frames for local delivery within the network. Error detection is applied to ensure data integrity.
7. **Physical Layer (Layer 1)**: The email data is transmitted as electrical or optical signals over cables or wireless connections.

Once Zoro receives the email, the process is reversed, and the email content is decrypted and displayed in Zoro's email application.

Advantages of the OSI Model

1. **Modular Structure**: By dividing network functions into separate layers, the OSI model provides clarity and modularity, allowing for easier troubleshooting, design, and understanding.
2. **Standardization**: It standardizes communication functions, ensuring that different systems and devices can communicate with each other regardless of the manufacturer.
3. **Simplifies Troubleshooting**: By isolating issues within specific layers, network administrators can identify and focus on the problem layer, reducing troubleshooting complexity.
4. **Flexibility**: Network protocols can evolve without affecting the entire system, as the OSI model's layered approach allows each layer to function independently.

TCP/IP Model: Practical Oriented Model

The **TCP/IP model** is a simpler, more practical approach to network communication that was developed by the U.S. Department of Defense. It is often considered more aligned with real-world networking.

Key Differences Between OSI and TCP/IP Models:

1. **OSI Model**:
   - 7 Layers.
   - Theoretical model used for standardizing network communications.
   - Divides functionalities into separate layers for better clarity.
2. **TCP/IP Model**:
   - 4 Layers:

        - **Application Layer** (combined layers 5, 6, 7 of OSI)
        - **Transport Layer** (same as OSI)
        - **Network Layer** (same as OSI)
        - **Network Access Layer** (combines OSI's physical and data link layers)
    - Practical model based on real-world protocols.
    - Simpler structure with fewer layers.

Example: In TCP/IP, the Application Layer combines the OSI's **Session**, **Presentation**, and **Application** layers. The **Network Access Layer** combines the **Data Link** and **Physical** layers.

Network Impairments and Causes

In networking, signals travel through transmission media to reach their destination, but these signals often undergo changes as they move, resulting in impairments that affect the quality and reliability of communication. When signals travel, they can degrade, become distorted, or suffer from interference, leading to the phenomenon that "what is sent is not necessarily what is received." These impairments can be caused by various factors:

1. Attenuation (Signal Weakening)

Attenuation refers to the weakening of a signal as it moves through the transmission medium, such as cables or air. The further a signal has to travel, the more it will lose strength. As a result, the signal may become too weak to be received clearly at the other end, especially over long distances.

To counteract this, amplifiers can be used to boost the signal along the way, but even amplifiers have their limitations. Attenuation can significantly affect the quality of communication, leading to the need for repeaters and amplifiers to maintain signal strength.

2. Distortion (Shape or Form Change)

Distortion occurs when a signal changes its shape or form as it travels through the transmission medium. This is particularly noticeable when a composite signal, consisting of multiple frequencies, is transmitted. Distortion can cause parts of the signal to shift in frequency or become misaligned, which can result in errors in the received data.

The impact of distortion can be significant, especially in high-speed communication systems where maintaining the integrity of the signal is critical. Distortion can lead to loss of data or incorrect interpretation of the transmitted message.

3. Noise (Unwanted Signals)

Noise refers to any unwanted signal that interferes with the transmission, making it difficult to decode the original message. Noise can come in various forms, including:

- **Thermal Noise**: This type of noise is caused by the random motion of electrons in the transmission medium, such as copper wires. It results in additional signals that weren't originally sent by the transmitter.
- **Induced Noise**: Induced noise is generated by external devices like motors or appliances, which act as antennas and induce electrical signals into nearby cables or networks. This unwanted noise can significantly disrupt the clarity of the signal.
- **Crosstalk**: This happens when signals from one wire interfere with signals on an adjacent wire. Essentially, one wire acts as a transmitter while the other acts as a receiver, leading to signal leakage and potential errors.

- **Impulse Noise**: This is a sudden spike or burst of high-energy signal that occurs in very short bursts, often caused by external events such as lightning, power line disturbances, or electrical surges. Impulse noise can severely corrupt the signal, causing data loss or damage.

Networking Devices and Protocols

Hub and Switches:

Network devices like hubs and switches play a crucial role in managing data flow in a network. These devices may use an **IOS (Internet Operating System)**, which is a specialized operating system that helps manage network traffic, ensure correct routing, and maintain the network's performance.

Spanning Tree Protocol (STP):

The **Spanning Tree Protocol (STP)** is essential for preventing loops in Ethernet networks. In any network topology with redundant paths, loops can occur, causing infinite cycles of data that can severely degrade network performance. STP prevents such loops by identifying redundant paths and disabling them, ensuring that there is only one active path between any two devices.

STP determines the **root bridge** and assigns roles (e.g., root, bridge, and blocking) to each device based on MAC addresses, thus managing data flow in the network.

For example:

- **Root Bridge**: The device with the smallest MAC address is chosen as the root.
- **Bridge**: Devices that are part of the network and help forward traffic.
- **Block**: Devices that block redundant paths to prevent loops.

Each switch in the network has a unique **MAC address** (48 bits, in hexadecimal format), and STP uses this address to decide which paths should be active and which should be blocked. STP ensures efficient and loop-free operation of the network.

Time to Live (TTL)

The **Time to Live (TTL)** field in IP packets controls how long a packet is allowed to circulate within the network before being discarded. Each time a packet passes through a router or network device, its TTL value is decremented by one. If the TTL value reaches zero, the packet is dropped, preventing it from circulating indefinitely due to routing errors or loops.

TTL plays a critical role in avoiding network congestion caused by endless loops, as well as ensuring that old, outdated packets are not processed repeatedly. It helps optimize network performance and resource management.

What is a VLAN?

A **VLAN (Virtual Local Area Network)** is a logical subgroup within a physical network that allows network administrators to segment networks into smaller, isolated groups regardless of their physical location. VLANs are used to divide a larger network into multiple smaller networks, each with its own broadcast domain, which is beneficial for performance, security, and management.

In a typical physical network, all devices connected to a switch belong to the same network and can communicate directly with each other. However, with VLANs, network devices can be grouped together virtually, even if they are on different physical switches. Devices in different VLANs cannot communicate with each other unless there is a **router** or a **Layer 3 switch** to route the traffic between VLANs.

When and Why is VLAN Used?

VLANs are used in various scenarios to optimize the network infrastructure:

1. **Segregating Network Traffic:**
    - **Separation of departments**: For instance, a company might create separate VLANs for its HR, Finance, and IT departments. Each department's network traffic will be isolated from others, preventing unauthorized access and improving performance.
    - **Security**: VLANs enhance security by preventing unauthorized users or devices from accessing sensitive data or systems. For example, a VLAN could separate the **guest network** from the **corporate network** to ensure guest users cannot access internal resources.
    - **Traffic Management**: VLANs are often used to improve traffic management. For example, traffic for **voice** and **data** can be segregated into different VLANs to ensure that voice traffic gets higher priority, improving voice quality.
2. **Improved Network Performance:**
    - By segmenting a network into smaller VLANs, broadcast traffic is limited to each VLAN, reducing congestion in the overall network and improving performance. This is particularly helpful in large networks with a high volume of broadcast traffic.
3. **Better Resource Management:**
    - VLANs allow for easier allocation of resources. For example, you can prioritize certain types of traffic (such as VoIP or video conferencing) to ensure that those services have enough bandwidth.
4. **Cost Savings:**
    - VLANs enable organizations to use the same physical infrastructure (such as switches and cables) for multiple virtual networks, saving on hardware and reducing the need for additional network equipment.

Advantages of VLANs:

- **Improved Network Performance:** VLANs help in reducing the size of broadcast domains, which lowers network congestion and improves overall network performance.
- **Better Security:** By isolating network segments, VLANs prevent unauthorized access and reduce the risk of attacks.
- **More Efficient Network Management:** Network administrators can better control network traffic and resources.
- **Cost Savings:** VLANs allow multiple virtual networks to share the same physical infrastructure, reducing the need for additional network equipment.
- **Simplified Network Configuration:** VLANs make it easier to configure and manage network settings for specific groups of users or devices.

How to Configure VLAN and InterVLAN Routing in Cisco Packet Tracer

Here are the basic steps for configuring VLANs and InterVLAN routing in **Cisco Packet Tracer**:

1. Create the Network Topology

- In **Cisco Packet Tracer**, start by creating the physical network topology.
- Add **Cisco switches**, **routers**, and **end devices (PCs, laptops)**.
- Connect the devices using **Ethernet cables**.

2. Configure VLANs on the Switch

- Select a **switch** in the topology.
- Go to the **CLI (Command Line Interface)** of the switch and configure VLANs.

Here’s how to configure VLANs on the switch:

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name HR
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name IT
Switch(config-vlan)# exit

Switch(config)# vlan 30
Switch(config-vlan)# name Finance
Switch(config-vlan)# exit
```

- This command creates three VLANs: **HR (VLAN 10)**, **IT (VLAN 20)**, and **Finance (VLAN 30)**.

3. Assign Ports to VLANs

- After creating the VLANs, assign switch ports to each VLAN. This is done by specifying the port number that will be part of each VLAN.

```
Switch(config)# interface range fa0/1 - 10
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10

Switch(config)# interface range fa0/11 - 20
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20

Switch(config)# interface range fa0/21 - 30
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 30
```

- Here, ports fa0/1 - fa0/10 are assigned to **VLAN 10 (HR)**, fa0/11 - fa0/20 to **VLAN 20 (IT)**, and fa0/21 - fa0/30 to **VLAN 30 (Finance)**.

4. Configure Router for InterVLAN Routing

- To enable communication between different VLANs, you need to configure **InterVLAN Routing** on a **router** or a **Layer 3 switch**.
- Use **Router-on-a-Stick** configuration, where a single router interface is used to route traffic between VLANs. You need to create **subinterfaces** for each VLAN on the router.

```
Router> enable
Router# configure terminal
Router(config)# interface gig0/0.10
Router(config-if)# encapsulation dot1Q 10
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# no shutdown

Router(config)# interface gig0/0.20
Router(config-if)# encapsulation dot1Q 20
Router(config-if)# ip address 192.168.20.1 255.255.255.0
Router(config-if)# no shutdown

Router(config)# interface gig0/0.30
Router(config-if)# encapsulation dot1Q 30
Router(config-if)# ip address 192.168.30.1 255.255.255.0
Router(config-if)# no shutdown
```

- In this example, the router interface gig0/0 has subinterfaces for each VLAN, and each subinterface has an IP address in the corresponding subnet. The dot1Q encapsulation type is used to allow the router to understand VLAN tags.

5. Configure PCs with Appropriate IP Addresses

- Each PC should have an IP address in the subnet corresponding to its VLAN. For example:
    - **VLAN 10 (HR)** PCs should have IP addresses in the 192.168.10.0/24 subnet.
    - **VLAN 20 (IT)** PCs should have IP addresses in the 192.168.20.0/24 subnet.
    - **VLAN 30 (Finance)** PCs should have IP addresses in the 192.168.30.0/24 subnet.
- Set the default gateway for each PC to the respective router subinterface IP address.

6. Test Connectivity

- Use the **ping** command to test connectivity between PCs in different VLANs. If configured correctly, the PCs should be able to communicate across VLANs through the router.

```
PC1> ping 192.168.20.2

PC1> ping 192.168.30.2
```

- These pings test if PCs in different VLANs can communicate with each other via the router.

Inter-VLAN Communication Overview

Inter-VLAN communication enables devices from different VLANs to communicate with each other. Since VLANs isolate traffic, devices in separate VLANs cannot communicate directly unless there is a routing device (such as a router or Layer 3 switch) to route the traffic between them. This is typically achieved through **Router-on-a-Stick** configuration, where a router uses a single physical interface to route traffic between multiple VLANs by creating subinterfaces.

Steps for Configuring Inter-VLAN Communication in Packet Tracer

Step 1: Create VLANs

First, create two VLANs (VLAN 10 and VLAN 20) on the switch.

On Switch 1 (VTP Server):

```
Switch1> enable
Switch1# config terminal
Switch1(config)# vlan 10
Switch1(config-vlan)# name marketing
Switch1(config-vlan)# exit

Switch1(config)# vlan 20
Switch1(config-vlan)# name hr
Switch1(config-vlan)# exit
```

On Switch 2:

```
Switch2> enable
Switch2# config terminal
Switch2(config)# vlan 10
Switch2(config-vlan)# name marketing
Switch2(config-vlan)# exit

Switch2(config)# vlan 20
Switch2(config-vlan)# name hr
Switch2(config-vlan)# exit
```

Step 2: Assign Ports to VLANs

Assign specific ports to the VLANs. For example, ports fa0/1, fa0/2, and fa0/3 on Switch 1 will be assigned to VLAN 10, and ports fa0/4, fa0/5, and fa0/6 on Switch 2 will be assigned to VLAN 20.

On Switch 1:

```
Switch1(config)# interface range fa0/1 - 3

Switch1(config-if-range)# switchport mode access

Switch1(config-if-range)# switchport access vlan 10
```

On Switch 2:

```
Switch2(config)# interface range fa0/1 - 3

Switch2(config-if-range)# switchport mode access

Switch2(config-if-range)# switchport access vlan 20
```

Step 3: Assign IPs and Gateways to Devices

Each device within a VLAN must be assigned an IP address that falls within the subnet of the VLAN. Additionally, the default gateway should be configured to allow the devices to communicate between VLANs.

1. **For Devices in VLAN 10 (Marketing)**:
   - IP Address: 192.168.10.10
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 192.168.10.1 (assigned by the router)
2. **For Devices in VLAN 20 (HR)**:
   - IP Address: 192.168.20.10
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 192.168.20.1 (assigned by the router)

Step 4: Configure Router for Inter-VLAN Routing

Inter-VLAN routing is done using the **Router-on-a-Stick** configuration, where the router's single physical interface is divided into subinterfaces for each VLAN. The router performs routing between VLANs using these subinterfaces.

1. **Router Configuration**:
   - Enter the router’s CLI:
   - Router> enable
   - Router# config terminal
   - **Create subinterfaces for VLAN 10 and VLAN 20**:
   - Router(config)# interface fa0/0.10
   - Router(config-if)# encapsulation dot1Q 10
   - Router(config-if)# ip address 192.168.10.1 255.255.255.0

- Router(config-if)# no shutdown
- Router(config-if)# exit
-
- Router(config)# interface fa0/0.20
- Router(config-if)# encapsulation dot1Q 20
- Router(config-if)# ip address 192.168.20.1 255.255.255.0
- Router(config-if)# no shutdown
- Router(config-if)# exit
- The **encapsulation dot1Q** command enables **802.1Q encapsulation**, which allows the router to differentiate between VLANs on the same physical interface. The subinterface .10 handles VLAN 10 traffic, and .20 handles VLAN 20 traffic.

Step 5: Testing Inter-VLAN Communication

- Once the router and switches are configured, you can test inter-VLAN communication.
- **On PC in VLAN 10**, try to ping the **PC in VLAN 20** to verify that the router is routing traffic correctly between VLANs.

For example:

- **PC in VLAN 10**:
- ping 192.168.20.10
- **PC in VLAN 20**:
- ping 192.168.10.10

If the devices can ping each other, inter-VLAN routing is successfully configured.

Router-on-a-Stick Overview

In a **Router-on-a-Stick** setup, a single physical router interface is divided into multiple logical subinterfaces. Each subinterface corresponds to a specific VLAN, and the router routes traffic between the VLANs. This setup saves hardware resources and is commonly used in smaller networks.

VTP (VLAN Trunking Protocol)

VTP simplifies VLAN management by allowing VLAN configuration changes to be automatically propagated across multiple switches within the same VTP domain.

- **VTP Server**: Manages VLANs and propagates changes to VTP clients.
- **VTP Client**: Receives VLAN updates from the VTP server but cannot create or delete VLANs.

Steps to Configure VTP:

On Switch 1 (VTP Server):

```
Switch1> enable
Switch1# config terminal
Switch1(config)# vtp mode server
Switch1(config)# vtp domain your_domain_name
Switch1(config)# vlan 10
Switch1(config-vlan)# name marketing
Switch1(config-vlan)# exit
Switch1(config)# vlan 20
Switch1(config-vlan)# name hr
Switch1(config-vlan)# exit
```

On Switch 2 (VTP Client):

```
Switch2> enable
Switch2# config terminal
Switch2(config)# vtp mode client
Switch2(config)# vtp domain your_domain_name
```

Switch 2 will automatically receive the VLANs from Switch 1. This eliminates the need to manually configure VLANs on each switch, simplifying VLAN management in larger networks.

Subject Work Code

The code for the Networking subject is available on GitHub. You can access and review the code repository using the following link:

GitHub Repository: Networking - Sukkur IBA CS

Please refer to this link for all related code and further development details.