1 Network device

Hub

Hub is a network device used to connect multiple computer in a network.

- All data is broadcasted to each device on the network. As it operate on physical layer 1.
- Transmission mode of HUB is **half duplex.**
  Half Duplex mean device only send or receive that data at one time.
  Full Duplex device can send or receive the data at same time.
  It is cheap , easy to setup.

Switches

Switch is a network device used to connect multiple computer in a network. It is more advance then HUB and Operate on Layer 2 , Only send the data to destination PC as we know it use MAC address to find devices. but cannot manage traffic between different VLANs .

- Transmission mode of HUB is FULL duplex.
  IT is expensive and difficult to setup.

Router

Router is a network device which is used to connect computer and devices directly to internet. Works on Layer 3 of OSI model having Ip address by it can connect to VLAN.

- Router use a process called routing to find the best path to send the data to destination PC.

A router is a device that directs data packets through the network. Here are its main functions:

1. **Path Determination**: It figures out the best route for data based on factors like speed and capacity.
2. **Data Forwarding**: It sends data to the next destination.
3. **Load Balancing**: It can send data along multiple paths to prevent overload and errors.

> **DHCP Server** (Dynamic Host Configuration Protocol) : Routers can assign IP addresses to devices on the network automatically, which simplifies network management.
> work on Layer 7.

What is Routing?

Routing is like choosing the best road to take when traveling from one place to another. In a computer network, it involves selecting the best path for data to travel between devices (nodes).

Routing table:- Routers maintain routing tables containing information about the best path for data packets to travel, facilitating accurate data transmission.

Why is Routing Important?

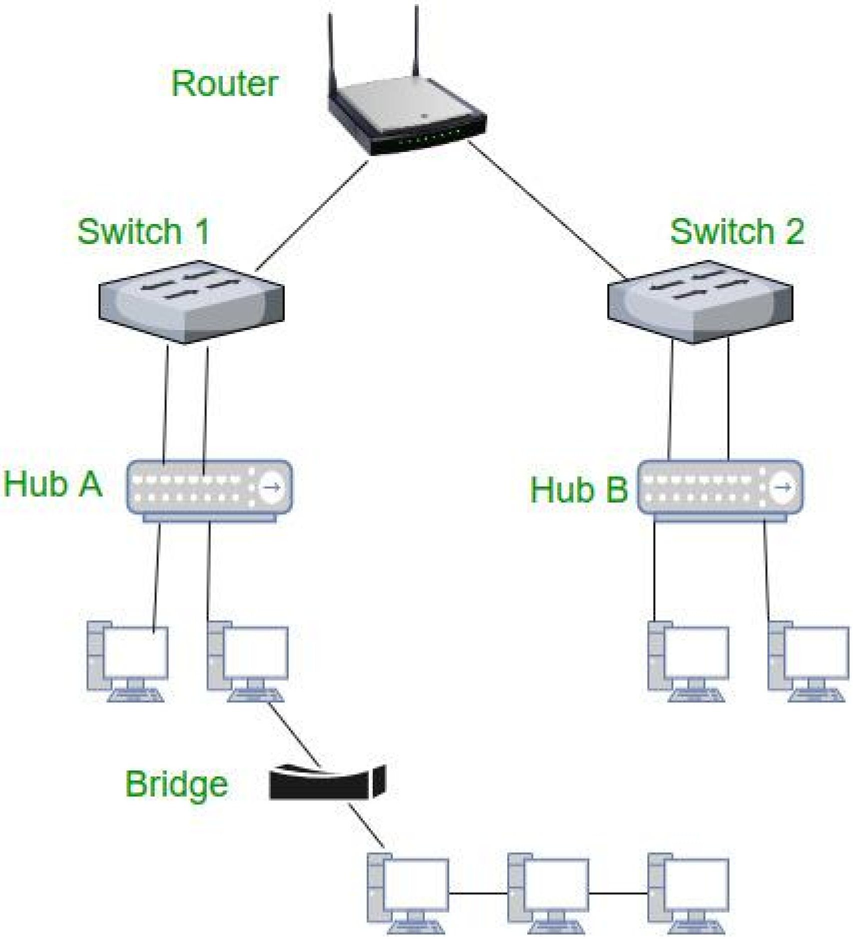
Routing helps manage data traffic efficiently, ensuring that information moves quickly without delays. Good routing minimizes issues like slow-loading websites or server crashes, keeping everything running smoothly.

Types of Routing

1. **Static Routing**: Manually set paths that don't change often. It's simple but can lead to problems if the network changes.
    - You have to set up all the server and pc manually in static routing and if 1 break you can't access the internet.
2. **Dynamic Routing**: Automatically adjusts paths based on current network conditions, making it more flexible and efficient.

Main Routing Protocols

- **Interior Gateway Protocols**: Manage routing within a single network. Used in Office or home.
    - **RIP**: Uses hop counts to find the shortest path (not commonly used anymore as it old have fault).
    - **OSPF**: Analyzes multiple factors for optimal paths.
- **Exterior Gateway Protocols**: Manage routing between different networks. used in www
    - **BGP**: Handles how data is routed over the internet between different networks.



DNS

- **DNS** is primarily concerned with the translation of domain names into IP addresses, enabling communication over the internet.
- **DNS Routing** optimizes how DNS queries are handled, directing them to the most appropriate servers for better performance and reliability.

Repeater

The repeater is the network device working at **layer 1** on OSI model.

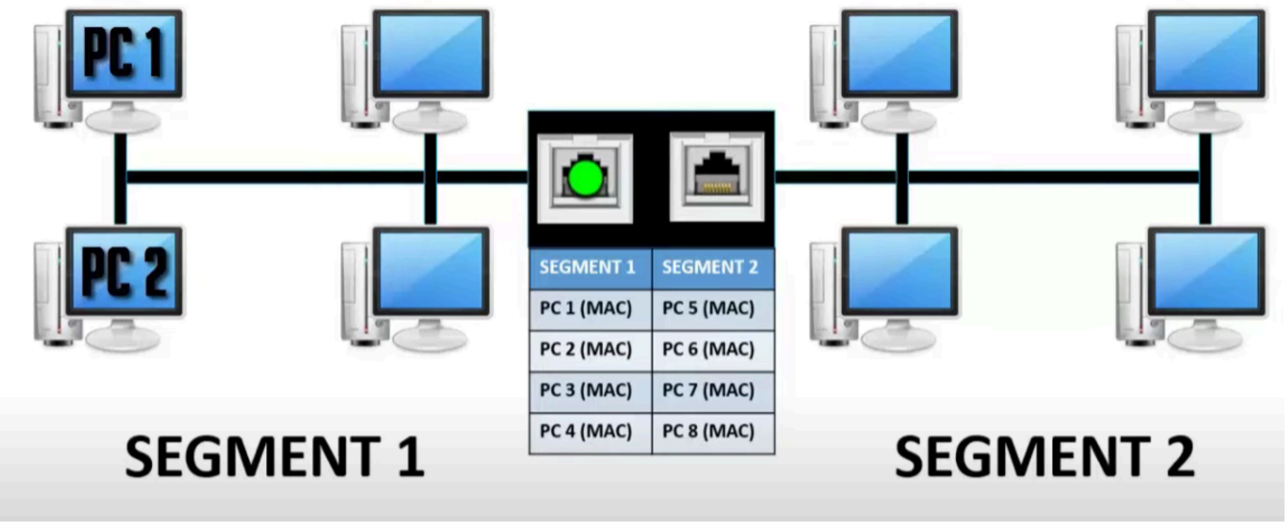
- There are only 2 ports on the repeater device. These ports transform the incoming signal into an outgoing signal and transmit it to the destination.
- It strengthens the weak signals on it and enables it to transmit data to longer distances. It is a device similar to a hub but does not have as many ports as a hub.

  > Can be used as wired or wireless.

Bridge

A bridge operates at the data link layer of the OSI model and is used to connect two or more local area networks (LANs) together. It forwards data packets based on their MAC addresses, allowing devices on different LANs to communicate with each other.

- IT operate on **physical and data link layer** both of OSI layer.
- By using it we can extend your LAN network.
- IT reduce the collision of data.
- It is intelligent device as at store all mac address in starting.
- Once the bridge broadcast a mess it don't have power to stop it.
- ITS EXPENSIVE AS WELL.
- Data transmission rata of data is slow then repeater.

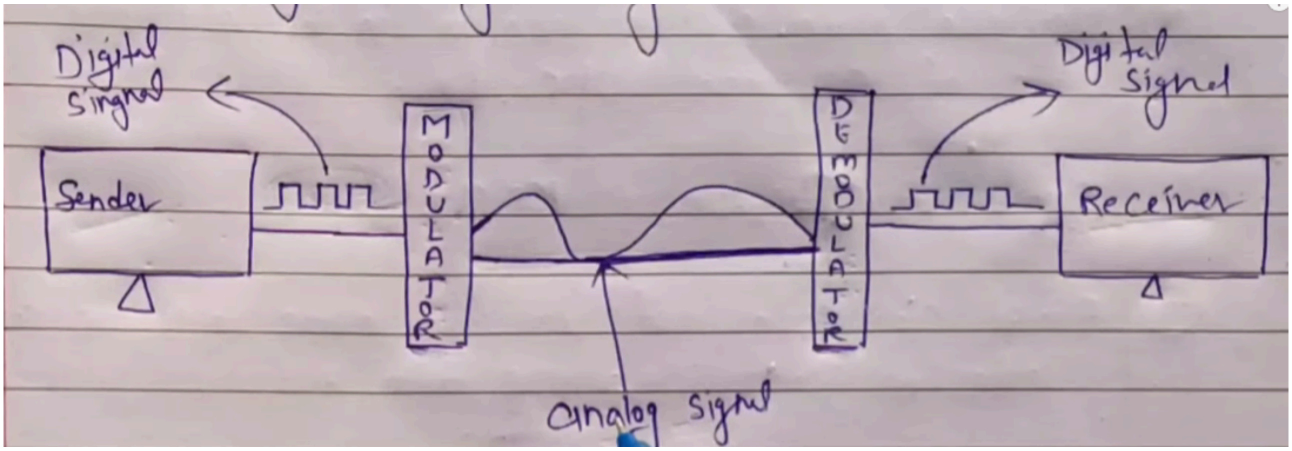


SEGMENT 1	SEGMENT 2
PC 1 (MAC)	PC 5 (MAC)
PC 2 (MAC)	PC 6 (MAC)
PC 3 (MAC)	PC 7 (MAC)
PC 4 (MAC)	PC 8 (MAC)

Modem

Modems stands for modulator and demodulator , it is a network device that is placed between the computers or telephone line.

- **Modulator :** Convert the digital signal of pc into analog and send further through cables.
- **Demodulator :** convert the receiving analog signal into digital signal and show the data to screen.



- IT allow computer to connect to internet.

Gateway

Gateway is one of the network equipment that can **work at every layer** according to the OSI model. IT connect two

- A gateway is a network node(device) that used to connect two dissimilar type of network or similar.
- Although it is similar to router devices in terms of its function, it differs from routers with its ability to work in every layer. In addition, there are **not only hardware but also software gateway** types.
- *IT connect two network which has different protocol.*
- we can't access internet without gateway .
- IF your pc is connected to a switch so switch work as your gateway.

> so if your pc connected to a hub it on layer 1 and work as your gateway , if you connected to switch it on work as your gateway . if router than so on . like it can operate on all layer. as we know gateway is software and hardware based both.

Difficult to manage , low data transmission rate, expensive but provide some security.

Access Points

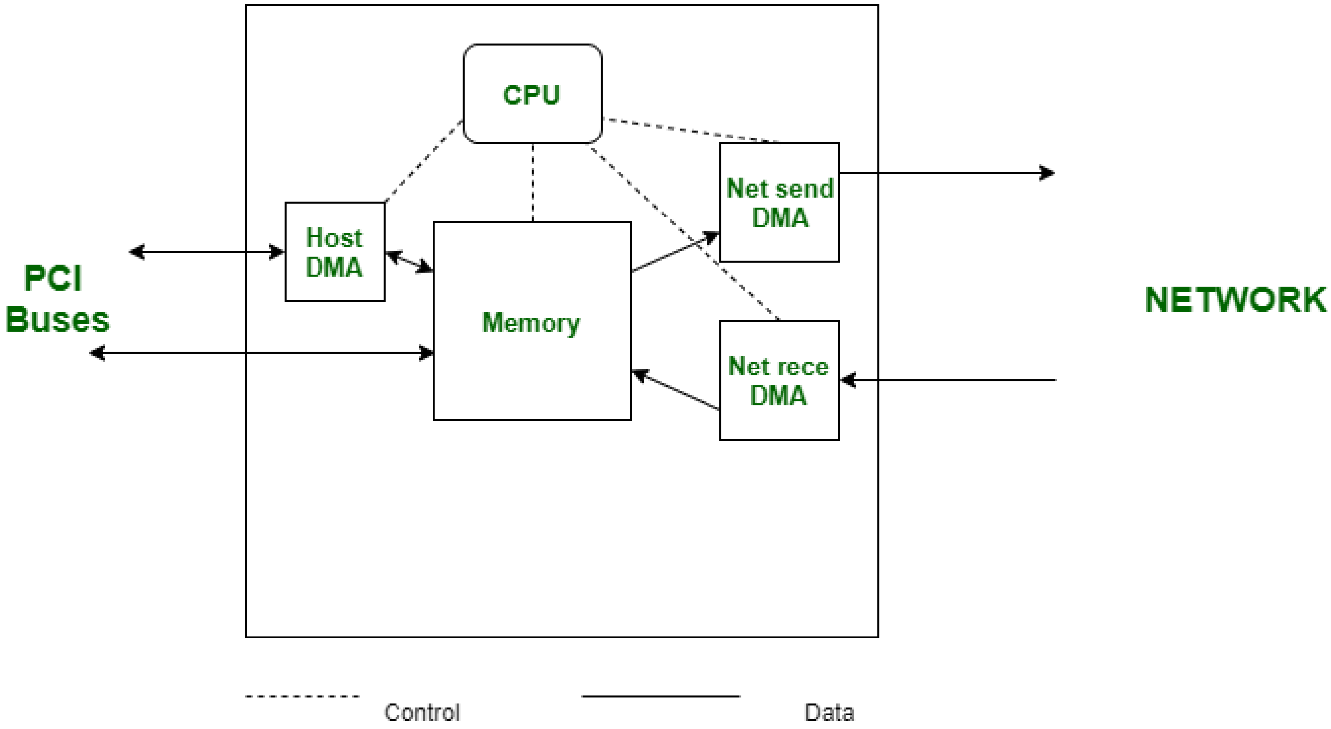
Wireless Access points (WAPs) are the wireless network hardware devices that are used to send Wi-Fi signals for providing wireless connectivity to the wireless devices in a specified area. They act as a bridge between wireless devices and the wired network infrastructure.

Wireless Access point:- A wireless access point (WAP or AP) is a device that allows wireless communication devices to connect to a wireless network using Wifi. Bluetooth or related standards. the WAP usually connect to a weird network (such as computer or printers) and wired devices on the network.

NIC

NIC : **Network interface card**

- These are hardware components installed in computers that enable them to connect to a computer.
  - A network interface card is a computer hardware computer design to allow computer to communicate other a computer network it is both on OSI layer 1 and layer 2 device, as it provide physical access to networking medium and provides a low level address system through the use of mac address.



Endpoints

Endpoints are also types of network hardware devices connected to the user ports of the switch in a computer network. **These devices are the ones who send and receive the data for the end users such devices include laptops, desktops, cameras, phones, etc.**

The increasing use of end-user devices like laptops, mobile phones, etc. by organizations all over the world to access their resources / their network remotely is also increasingly exposing endpoints to cyber threats and attacks.

Power over Ethernet (PoE)

PoE stands for Power over Ethernet. It's a technology that allows electrical power to be transmitted along with data over standard Ethernet cables.

This means devices like IP cameras, VoIP phones, and wireless access points can **receive power and data through** the same cable, simplifying installation and reducing the need for additional power sources.

Benefits of Network Hardware Devices

Network hardware devices, such as routers, switches, firewalls, and access points, provide numerous advantages that enhance connectivity, security, and performance in computer networks:

- **Improved Connectivity**: Devices like routers and switches enable seamless communication between multiple devices and networks, ensuring efficient data transfer.

- **Enhanced Security**: Firewalls protect networks from unauthorized access and cyber threats by monitoring and controlling incoming and outgoing traffic.

- **Increased Scalability**: Network devices allow businesses to easily expand their network infrastructure to accommodate growth without significant reconfiguration.

- **Flexible Networking**: Wireless access points (APs) offer greater flexibility in device placement, eliminating the need for physical cables and allowing easy access from various locations.

- **Simplified Management**: Managed switches and routers provide centralized control over network settings, making it easier to monitor performance and troubleshoot issues.

- **Broader Coverage**: Wireless access points extend the range of a network, providing connectivity in larger areas and eliminating dead zones.

- **Support for IoT Devices**: Modern network hardware can accommodate the growing number of Internet of Things (IoT) devices, ensuring reliable connectivity and data management.