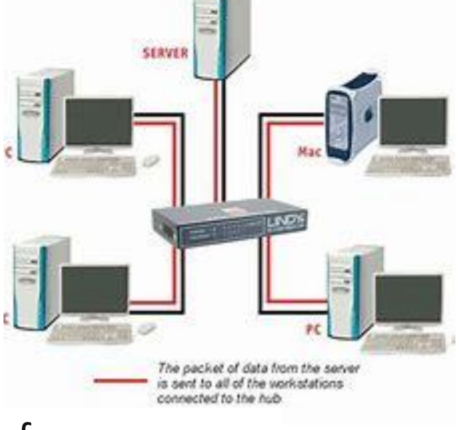
Computer Network

Various Network devices:

1) **NIC (Network Interface Card)**

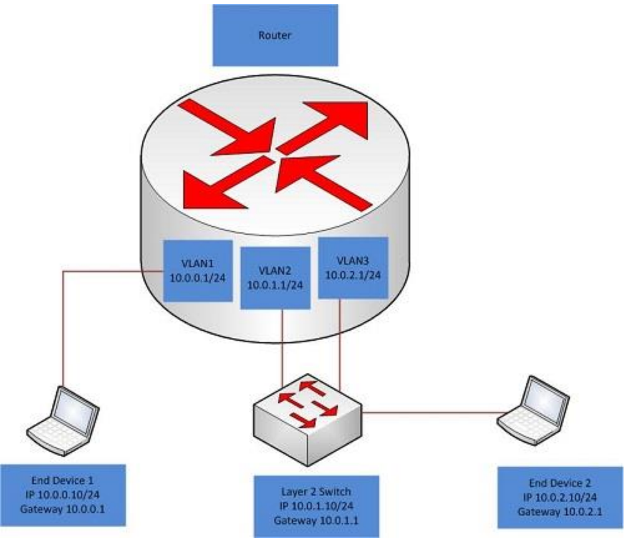
- NIC is hardware component used to connect a computer with another computer onto a network
- The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).
- It can support a transfer rate of 10,100 to 1000 Mb/s
- There are two types of NIC:
    1) Wired NIC: The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data
    2) Wireless NIC**:** The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.


SERVER
C
Mac
C
PC
LINDY
The packet of data from the server is sent to all of the workstations connected to the hub

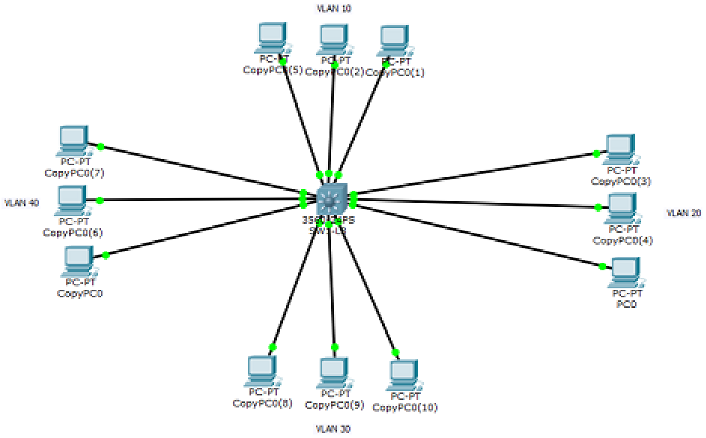
2)HUB

- Hubs are used to create small Home Networks.
- Hubs are used for monitoring the networks.
- Hubs are used in Organizations and Computer Labs for connectivity.
- It Makes one device or peripheral available throughout the whole network
- A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.
- The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

3) Layer 2 and Layer 3 Switches

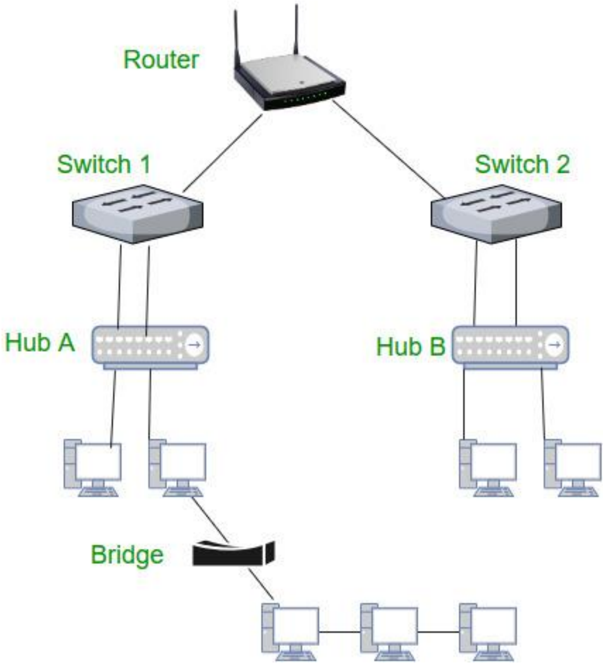


- Layer 2 switches basically do switch only, which means they operate using devices' MAC addresses to redirect the data packets from the source port to the destination port. It does that by maintaining a MAC address table to remember which ports have which MAC addresses assigned. A MAC address operates within the Layer 2 of the OSI reference model. A MAC address simply differentiates one device from another with each device being assigned a unique MAC address. It utilizes hardware-based switching techniques to manage traffic in a LAN (Local Area Network). As switching occurs at Layer 2, the process is quite faster because all it does is sorting MAC addresses at a physical layer. In simple terms, a Layer 2 switch acts as a bridge between multiple devices.



- A Layer 3 switch is exactly the opposite of what a Layer 2 switch does. Layer 2 switches were not able to route data packets at layer 3. Unlike Layer 2 switches, Layer 3 does routing using IP addresses. It’s a specialized hardware device used in routing data packets. Layer 3 switches have fast switching capabilities and they have higher port density. They are significant upgrades over the traditional routers to provide better performance and the main advantage of using Layer 3 switches is that they can route data packets without making extra network hops, thus making it faster than routers. However, they lack some added functionalities of a router. Layer 3 switches are commonly used in large scale enterprises. Simply put, a Layer 3 switch is nothing but a high-speed router but without WAN connectivity.

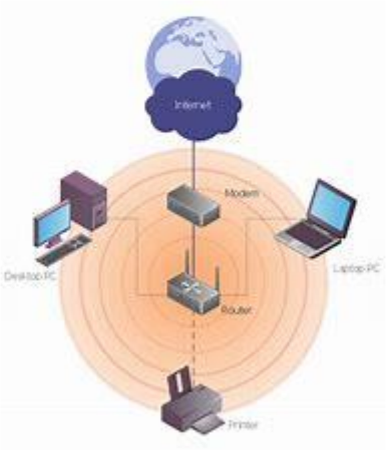
4) Bridge



- A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments
- Bridging is distinct from routing. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network. In the OSI model, bridging is performed in the data link layer (layer 2).
- If one or more segments of the bridged network are wireless, the device is known as a wireless bridge.
- The bridge is a networking device which is used to divide LAN into multiple segments.
- Bridge works under data link layer on OSI model.
- It stores the MAC address of PC available in a network.
- The bridge is used to reduce network traffic.

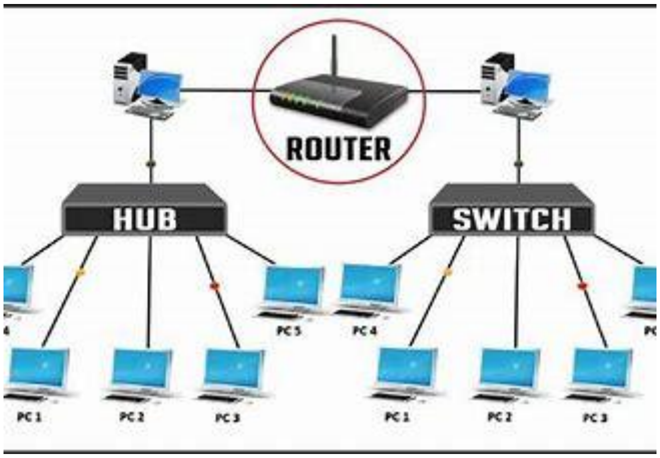
5)Wireless Access Point

- In computer networking, a wireless access point (WAP), or more generally just access point is a networking hardware device that allows other Wi-Fi devices to connect to a wired network. The AP usually connects to a router as a standalone device, but it can also be an integral component of the router itself. An AP is differentiated from a hotspot which is a physical location where Wi-Fi access is available.
- A wireless access point is a network device that transmits and receives data over a wireless local area network (WLAN)

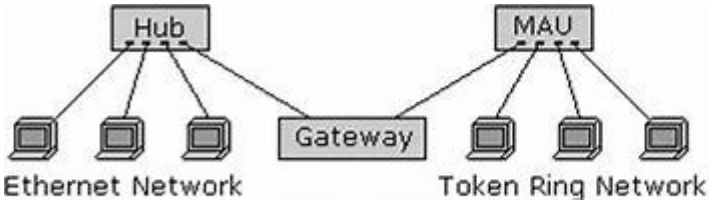


6)Router

- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a Layer 3 of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.



7)Gateway



- A gateway is a piece of networking hardware used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another.
- Gateways are distinct from routers or switches in that they communicate using more than one protocol to connect a bunch of networks and can operate at any of the seven layers of the open systems interconnection model.
- The term gateway can also loosely refer to a computer or computer program configured to perform the tasks of a gateway, such as a default gateway or router.

8)Modem

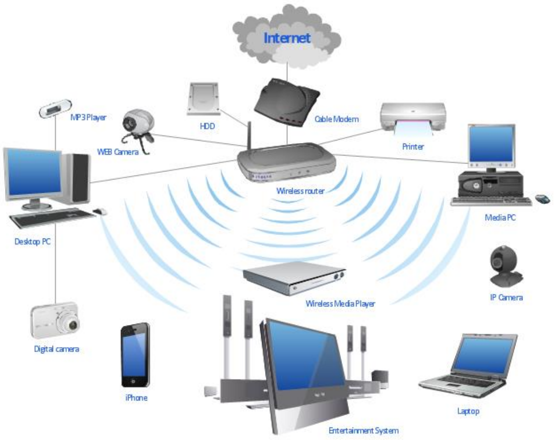
- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Based on the differences in speed and transmission rate, a modem can be classified in the following categories:

1)Standard PC modem or Dial-up modem

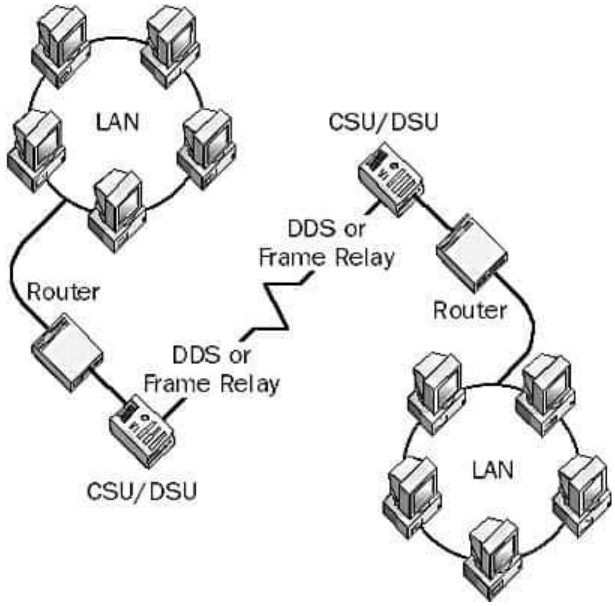
2)Cellular Modem

3)Cable Modem

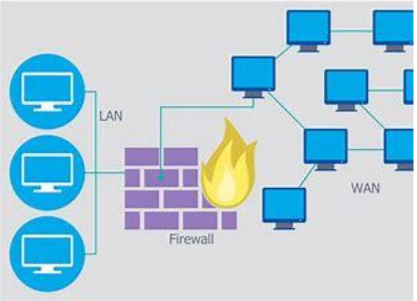


9)CSU/DSU

- CSU/DSUs essentially function as the digital counterpart to analog modems. They are typically external units that look similar to an external modem, but they can also come in sizes that can be mounted in a rack. Unlike analog modems, CSU/DSUs do not perform signal conversion because the signal at both ends is already digital. CSU/DSUs package digital data into a format suitable for the particular digital transmission line they are servicing, and buffer and rate-adapt digital signals going to and from the telephone company network. CSU/DSUs ensure that data frames are properly formed and timed for the telephone company network and provide a protective barrier to electrical disturbances that can harm customer premises equipment.



- Digital lines usually terminate at customer premises with four-wire connections having various connector types, including RJ-45, four-screw terminal blocks, and M-block connectors (used for V.35 interfaces). The four-wire connection is joined to the appropriate connector on the CSU/DSU. The CSU/DSU typically adjusts itself to the line speed of the digital data service (DDS) line using an autosensing feature.



- **10)Firewall**
- In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.
- Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.
- Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

  From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

  Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type *code* instead of port number which identifies purpose of that packet.