

**Hub**– connects multiple network devices together on an internal network. It has multiple ports that accepts ethernet connections from network devices, hub receives data and copies to all its other posts, so it duplicates the package and broadcasts to all other devices. Hubs causes unnecessary traffic and only suitable for small businesses.

Example:

* When a device connected to one of the ports sends data, the hub broadcasts that data to all other ports, regardless of the intended recipient.
* All devices connected to the hub receive the broadcasted data, but only the device with the correct destination address processes and uses the data.
* Unlike switches, hubs do not intelligently forward data based on MAC addresses, making them less efficient in managing network traffic.

**Bridge**- is a networking device or Components of computer network that connects two or more network segments together. It allows devices on different segments to communicate with each other. A bridge operates at the Data Link layer of the OSI model and uses MAC addresses to forward data packets between network segments. A bridge can be used to segment a network, improve network performance, and improve network security. Bridge connects hubs but stops data flow to the other hub unless requested There are different types of bridges, including local bridges, remote bridges, and wireless bridges. A local bridge connects two network segments within the same physical location, while a remote bridge connects two network segments in different physical locations. A wireless bridge is a type of bridge that uses Wi-Fi technology to connect two wireless networks together.

Example:

* The IT department installs a network bridge on each floor, connecting it to the existing switches on both Floor 1 and Floor 2.
* The network bridge acts as a link between the two LANs, operating at the data link layer (Layer 2) of the OSI model.
* When a computer on Floor 1 wants to communicate with a computer on Floor 2, the network bridge facilitates the communication by forwarding data between the two LANs.
* The network bridge intelligently filters and forwards traffic based on MAC addresses. It learns the MAC addresses of devices on both LANs, creating a table to efficiently forward data to the correct destination.
* Computers on Floor 1 and Floor 2 can now communicate seamlessly as if they were on the same LAN, even though they are physically on different floors.

**Switch**– this is responsible for connecting multiple computers within a network. Usually found in large network environments.

Switch facilitates communication within a network by connecting multiple computers within a network. It connects networking components (hub used to connect simple components) uses physical(mac address) table, operates at layer 2

Switch is a combination of hubs and bridges. It works with ports. When a switch is used, only relevant devices receive the data so reduces unnecessary traffic and broadband usage.

Example:

* Two devices within the same LAN need to communicate.
* The devices communicate through a switch. When Device A sends data to Device B, the switch uses MAC addresses to forward the data only to the port where Device B is connected, reducing unnecessary network traffic.

**Router** facilitates communication between networks by allowing connection between the home network or internet and devices. It usually functions at the edge of the networks, connects two network segments together, operates between two subnets. Router routs or forwards data from one network to another based on their IP address, it looks at the packet and destination and makes decision where to send, operates in layer 3

Example:

* The family sets up the router in their home and connects it to the cable modem. The router is configured with the necessary settings provided by the ISP.
* Devices within the home, such as laptops, smartphones, and smart TVs, can now connect to the router either wirelessly or through Ethernet cables.
* When a device requests internet access, the router acts as a gateway, forwarding the data between the home network and the internet. It uses Network Address Translation (NAT) to map multiple private IP addresses in the home network to a single public IP address provided by the ISP.
* The router manages the flow of data, directing incoming data to the appropriate device within the home network based on the destination IP address and port number.
* If a family member is streaming a video on their tablet, another member can simultaneously browse the internet on a laptop. The router efficiently manages the traffic, ensuring that each device receives the data it requests.

**WAP** A wireless access point is a networking device that allows wireless-capable devices to connect to a wired network. It is simpler and easier to install WAPs to connect all the computers or devices in your network than to use wires and cables.

Example:

* A laptop connects to a Wi-Fi network.
* The laptop communicates with the access point (AP) over a wireless connection. The AP relays the data to the router or switch, which then routes the data to its destination. The access point manages the wireless communication within its coverage area.

**Firewall-** A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. Functions at layer3.

Example:

* Incoming data to a network is checked for security.
* The firewall examines incoming data packets based on predefined security rules. If the data meets the criteria, it is allowed to pass through to the intended destination. If the data is suspicious or violates security policies, the firewall blocks or filters it.

**Proxy server-** A proxy server is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network. It is a server, referred to as an “intermediary” because it goes between end-users and the web pages they visit online.

Example:

* When a user within the company opens a web browser and attempts to access a website, the request is first sent to the proxy server.
* The proxy server evaluates the request and, if allowed, forwards the request to the internet. If the content is already in the proxy's cache from a previous request, it may serve the content directly from the cache, reducing bandwidth usage and speeding up access.
* The proxy server acts as a gateway between the corporate network and the internet, making requests on behalf of the local devices. This allows the proxy server to enforce access policies and filter content based on company policies.
* The Cisco ASA firewall ensures that only the proxy server has direct access to the internet. This setup enhances security by limiting direct internet access for individual devices within the corporate network.
* The proxy server logs internet usage, providing administrators with detailed information on which websites users are visiting. This helps in monitoring and enforcing acceptable use policies.