Network Devices

Switch:

A switch, in the context of networking is a high-speed device that receives incoming data packets and redirects them to their destination on a local area network (LAN). A LAN switch operates at the data link layer (Layer 2) or the network layer of the OSI Model and, as such it can support all types of packet protocols.

A switch in an Ethernet-based LAN reads incoming TCP/IP data packets/frames containing destination information as they pass into one or more input ports. The destination information in the packets is used to determine which output ports will be used to send the data on to its intended destination.

Switches are similar to hubs, only smarter. A hub simply connects all the nodes on the network -- communication is essentially in a haphazard manner with any device trying to communicate at any time, resulting in many collisions. A switch, on the other hand, creates an electronic tunnel between source and destination ports for a split second that no other traffic can enter. This results in communication without collisions.

Hub:

A hub is a hardware device that relays communication data. A hub sends data packets (frames) to all devices on a network, regardless of any MAC addresses contained in the data packet. A data packet arriving at one hub’s port may be copied to other ports allowing all segments of the network to have access to the data packet.

A switch is different than a hub in that it keeps a record of all MAC addresses of all connected devices. Thus, it knows which device or system is connected to which port. When a data packet is received, the switch immediately knows which port to send it to.

Active Hub: This is a type of hub that monitors, amplifies, and regenerates signals. Signals are strengthened in active hubs.

Passive Hub: Passive hub serves only as a physical connection point for computer devices, it does not take an active role in maintaining, processing, or regenerating signals.

Wireless Access Point (WAP):

A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network. A WAP is also known as a hotspot.

Wireless access points (WAP) may be used to provide network connectivity in office environments, allowing employees to work anywhere in the office and remain connected to a network. In addition, WAPs provide wireless Internet in public places, like coffee shops, airports and train stations.

Wireless access points are most commonly thought of in the context of the 802 series of wireless standards, commonly known as Wi-Fi. While there are other wireless standards, the vast majority of the time the terms Wi-Fi hotspot and WAP are synonymous.

Network Interface Card (NIC):

A Network Interface Card (NIC) is a computer hardware component that allows a computer to connect to a network. NICs may be used for both wired and wireless connections.

A NIC is also known as a network interface controller (NIC), network interface controller card, expansion card, computer circuit board, network card, LAN card, network adapter or network adapter card (NAC).

Most new computers have either Ethernet capabilities integrated into the motherboard chipset or use an inexpensive dedicated Ethernet chip.

Wireless Network Interface Card (WNIC):

A wireless network interface controller (WNIC) is a network interface controller which connects to a wireless radio-based computer network, rather than a wired network. A WNIC, just like other NICs, works on the Layer 1 and Layer 2 of the OSI Model. This card uses an antenna to communicate via microwave radiation.

Router:

A Router is a device that transfers data from one network to another in an intelligent way. It has the task of forwarding data packets to their destination by the most efficient route.

In order to do this, the router has a micro computer inside it. This holds a table in memory that contains a list of all the networks it is connected to, along with the latest information on how busy each path in the network is, at that moment. This is called the 'routing table'.

When a data packet arrives, the router does the following:-

- Reads the data packet's destination address
- Looks up all the paths it has available to get to that address
- Checks on how busy each path is at the moment
- Sends the packet along the least congested (fastest) path

Other tasks the Router can perform:

- Exchange protocol information across networks
- Filter traffic - helps prevent unauthorised intrusion by malware

Routers are also needed to enable a computer to connect to the internet.

Repeater:

A repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than what would be capable with the original signal.

A repeater is implemented in computer networks to expand the coverage area of the network, repropagate a weak or broken signal and or service remote nodes. Repeaters amplify the received/input signal to a higher frequency domain so that it is reusable, scalable and available.

Repeaters were introduced in wired data communication networks due to the limitation of a signal in propagating over a longer distance and now are a common installation in wireless networks for expanding cell size.

Repeaters are also known as signal boosters.

Gateway:

A gateway is a data communication device that provides a remote network with connectivity to a host network.

A gateway device provides communication to a remote network or an autonomous system that is out of bounds for the host network nodes. Gateways serve as the entry and exit point of a network; all data routed inward or outward must first pass through and communicate with the gateway in order to use routing paths. Generally, a router is configured to work as a gateway device in computer networks.

Any network has a boundary or a limit, so all communication placed within that network is conducted using the devices attached to it, including switches and routers. If a network node wants to communicate with a node/network that resides outsides of that network or autonomous system, the network will require the services of a gateway, which is familiar with the routing path of other remote networks.

Bridge:

A bridge is a type of computer network device that provides interconnection with other bridge networks that use the same protocol.

Bridge devices work at the data link layer of the Open System Interconnect (OSI) model, connecting two different networks together and providing communication between them. Bridges are similar to repeaters and hubs in that they broadcast data to every node. However, bridges maintain the media access control (MAC) address table as soon as they discover new segments, so subsequent transmissions are sent to only to the desired recipient.

Firewall:

A firewall is designed to help protect a computer network from intruders. It does this by controlling what data can and cannot pass through it.

Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet. A firewall may be implemented using hardware, software, or a combination of both.

A firewall is recognized as the first line of defense in securing sensitive information. For better safety, the data can be encrypted.

A firewall can either be

- A piece of software e.g. Windows has a built in Firewall, Zone Alarm is a free firewall or you can purchase commercial software firewalls.
- A piece of hardware. These boxes are much faster than the software version but they are also much more expensive and tricky to set up.

You would expect home networks to be protected by a software firewall but a large corporation would have several layers of hardware firewalls protecting their networks as well as intruder detection software applications looking for odd behaviour on their networks. Basically, the more valuable or sensitive the information, the higher the level of protection expected.