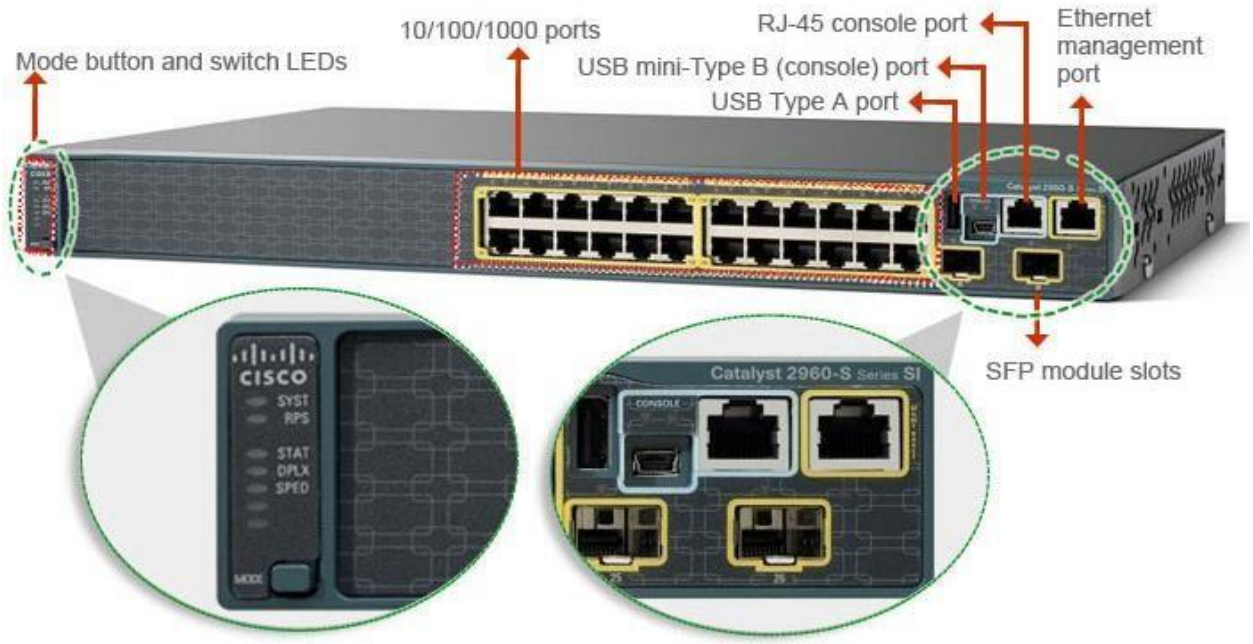
Cisco Router:

- Router is a hardware device work on Layer 3 or Network Layer of OSI Model.
- Router connects minimum of two networks generally find at the gateway.
- Router is used to interconnect two more different LANs with each other.
- Router is used to connect a LAN with WAN; Router is used to control broadcast.
- Router divide broadcast domains create routing table to store network information.
- Router is a device which select best path on the basis of routing protocol.
- Cisco Switches create a network and Cisco Routers connect different networks.
- Router uses a combination of hardware and software to "route" data.
- Routers segment large networks into logical segments called subnets.
- Router is networking device that forwards data packets between computer networks.
- Router is a layer 3 device used to forward packet from one network to another.
- Router perform various functions such as Static Routing and Dynamic Routing.
- Router also perform other various functions such as NAT, ACL, Inter VLAN Routing etc.

Cisco Switch:

- Switch is a device, which is used to connect multiple computers inside LAN.
- Switches are used to connect multiple devices on the same network.
- Switches which operate at Data Link Layer of OSI model called Layer 2 Switches.
- Switches which operate at Network Layer 3 called Layer 3 or multilayer switches.
- Basic Function of a Cisco Network Switch is to forward Layer 2 packets.
- Switch forward Ethernet Frames from source device to destination device.
- Switches are a key component of many business networks now a day.
- Switches connect multiple PCs, laptops, Printers, APs, Phones, Servers etc.
- Switches allow to send and receive information in the Computer Network.
- Switches access-shared resources in a smooth, efficient, highly secure manner.
- Cisco Layer 2 or Layer 3 switches can be managed both locally and remotely.
- Cisco IOS is proprietary Operating System that Cisco routers & switches run on.

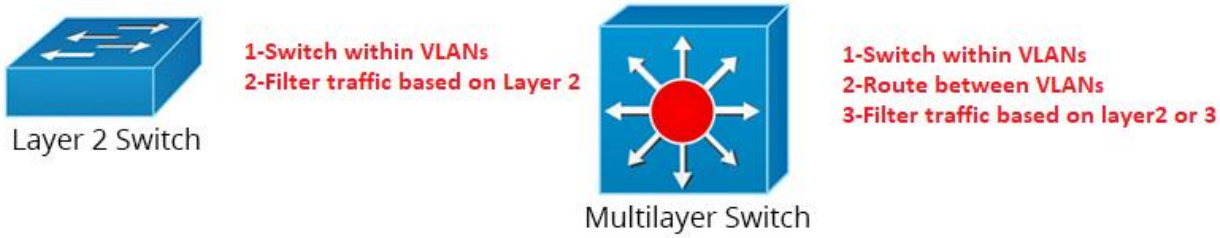


Layer 2 Switch:

- Terms Layers 2 & 3 are adopted from the Open System Interconnect (OSI) model.
- The Layer 2 provides direct data transfer between two devices within a LAN.
- Layer 2 switch functions by keeping a table of media access control (MAC) addresses.
- Switching operates at the Layer 2 of the OSI Reference Model.
- Uses MAC addresses to facilitate communication within devices from same network.
- Layer 2 Network devices can only communicate within the same network.
- Send packet to destination on the basis of MAC address, work with MAC address only.
- Switching at Layer 2 is quite fast as they do not look at the Layer 3 portion.
- Devices in the same layer 2 segment do not need routing to reach local peers.

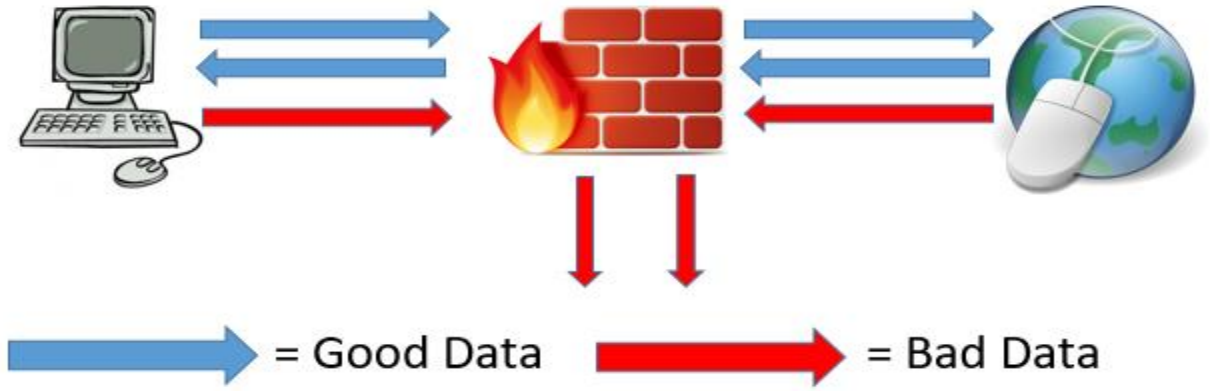
Layer 3 or Multilayer Switch:

- Operate on Layer 3 (Network Layer) of OSI model.
- Layer 3 switch also called Multilayer Switch as well.
- Can perform functioning of both 2 Layer and 3-Layer switch.
- Perform the routing of data packets using IP addresses.
- Layer 3 switches are the fast routers for Layer 3 forwarding in hardware.
- Layer 3 handles packet routing by logical addressing and subnet control.
- Layer 3 checks the source and destination IP addresses of every packet.
- Functions of Layer 3 switch combine some of a Layer 2 switch and some of a router.
- The main difference between Layer 2 and Layer 3 is the routing function.
- A Layer 3 or Multilayer switch can do all the job that a Layer 2 switch does.



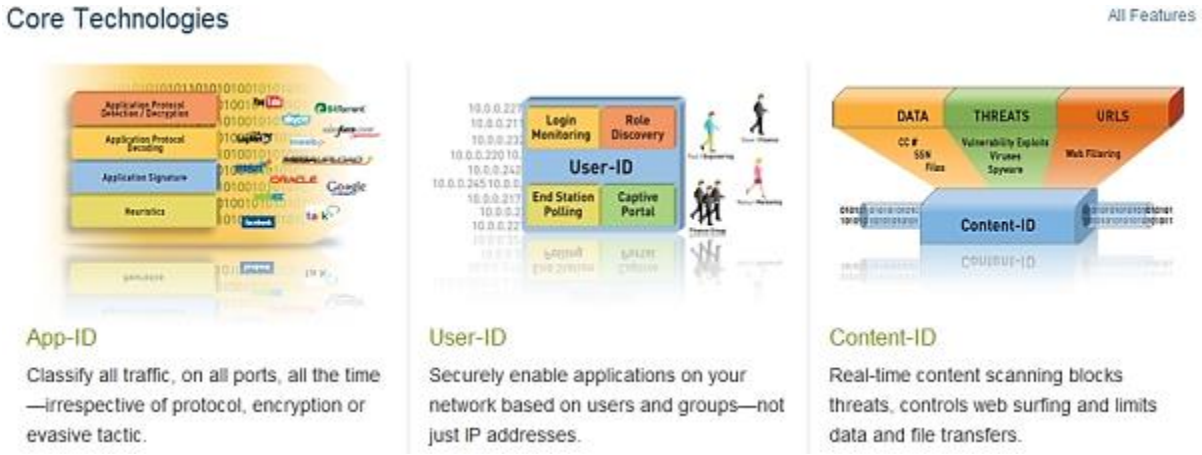
Firewall Technologies:

- The word firewall commonly describes a system or device.
- Firewall is placed between a trusted network and an untrusted network.
- A firewall is security devices used to stop or mitigate unauthorized access.
- The only traffic allowed on the network is defined via firewall policies.
- Firewall grants or rejects access to traffic flows between untrusted & trusted zone.
- A firewall monitors incoming and outgoing network related traffic.
- Firewall decides to allow or block specific traffic based on defined set of security rules.
- A firewall can be hardware, software, or both or can be Cloud-based firewall.
- The first generation of firewall technology consisted of packet filters.
- The second generation of firewall started with application layers.
- The third generation of firewall had “Stateful” filters inspection.
- Firewalls are relied upon to secure home and corporate networks from any attacks.



Next-Generation Firewall (NGFW):

- NGFW performs the role of a traditional firewall and adds NGIPS features.
- All NGFWs offer two key features App Awareness & Control & ID Awareness.
- Next-Generation Firewall provide deep-packet inspection.
- Next-Generation Firewall add application-level inspection & Intrusion Prevention.
- Next-Generation Firewall provides all traditional IPS features.
- Next-Generation Firewall allow/block traffic based on specific application.
- Next-Generation Firewall allow/block traffic based on user information.
- Next-Generation Firewall provide both IPS & application control functions.



IPS (Intrusion Prevention Systems):

Cisco Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are some of many systems used as part of a defense-in-depth approach to protect the network against malicious traffic. IDSs focus more on detection whereas IPSs focus on threat or unauthorized access prevention. The biggest difference between IDS and IPS is that an IPS responds immediately and does not allow any malicious traffic to pass, whereas an IDS, might allow malicious traffic to pass before responding.

Access Point:

- Access Point is a device that creates wireless local area network, or WLAN.
- Access Point is a device creates WLAN usually in an office or large building.
- AP is the device that allows multiple wireless devices to connect with each other.
- AP connects multiple wireless devices together in single or multiple wireless networks.
- AP is a networking device that is used to form wireless local area network in home.
- An access point connects to a wired router, switch, or hub via an Ethernet cable.
- AP is hardware device used to connect computer, laptops and mobile with each other.
- Wireless networks are suitable for those places where cables are difficult to install.
- An access point can also be used to extend the wired network to the wireless devices.

Wireless LAN Controller:

- WLAN controller manages wireless network access points that allow wireless devices.
- WLAN controller automatically handles the configuration of wireless access points.
- WLAN controller consolidated management for entire wireless network in one place.
- WLAN controllers automatically configure access points both locally and remotely.

Endpoint:

- Endpoint device is an Internet-capable computer hardware device on network.
- Endpoint refer to desktop computers, laptops, smart phones, tablets, printers etc.
- Endpoint device is LAN-connected hardware device that communicates across network.
- Endpoint are used by end users to access network and run network applications & other.
- On network with help of endpoints users can transmit and receive data across network.
- Endpoint or End Device is where a message originates from or where it is received.
- Data originates with end device, flows through the network, and arrives at end device.

Server:

- Server is software or hardware device that accepts & responds to requests over network.
- Server is system that provides resources, data, services, or programs to other computers.
- Server is computer which processes requests and delivers data over a network connection.
- Server is computer that provides data to other computers on a LAN or Wide Area Network.
- Server can provide various functionalities like centralized access to resources & stored data.
- Servers are computers that provide information to end devices such as web & FTP servers.