

Switches Types

Ethernet network switches are broadly categorized into two main categories –

**Modular and
Fixed configuration.**

Modular switches

- **Modular switches let you add expansion modules into the switches as needed, giving you flexibility if your network needs change. Examples of expansion modules are application-specific (such as firewall, wireless, or network analysis) and modules for additional interfaces, power supplies, or cooling fans.**

Fixed configuration Ethernet switches

- Fixed configuration switches are switches with a fixed number of ports and are typically not expandable.
- The fixed configuration switch category is further broken down into

1. Unmanaged switches,

2. Smart switches,

3. Managed L2 and L3 switches

Unmanaged switches

- An unmanaged switch is designed so that you can simply plug them in and they work, no configuration required. Unmanaged switches are typically for basic connectivity. You'll often see them used in home networks or wherever a few more ports are needed, such as at your desk, in a lab, or in a conference room.

Example of Unmanaged Switch



Smart switches

- This category of switches is evolving. The general rule here is that these switches offer some management, QoS, and security, but they are “lighter” in capabilities and less scalable than managed switches. They can be a cost-effective alternative to managed switches. They can be deployed at the edge of a large network (with managed switches being used in the core), as the infrastructure for smaller networks, or for low complexity needs.

Smart Switch



- They also offer some levels of security, such as 802.1x endpoint authentication, and in some cases with limited numbers of ACLs (access control lists), though the levels of control and granularity would not be the same as a managed switch.

Fully managed L2 and L3 switches

- **Managed switches are designed to deliver the most comprehensive set of features to provide the best application experience, the highest levels of security, the most precise control and management of the network, and offer the greatest scalability in the fixed configuration category of switches. As a result, managed switches are usually deployed as aggregation/access switches in very large networks or as core switches in relatively smaller networks. Managed switches should support both L2 switching and L3 IP routing though you'll find some with only L2 switching support.**

Manageable Switch



Difference

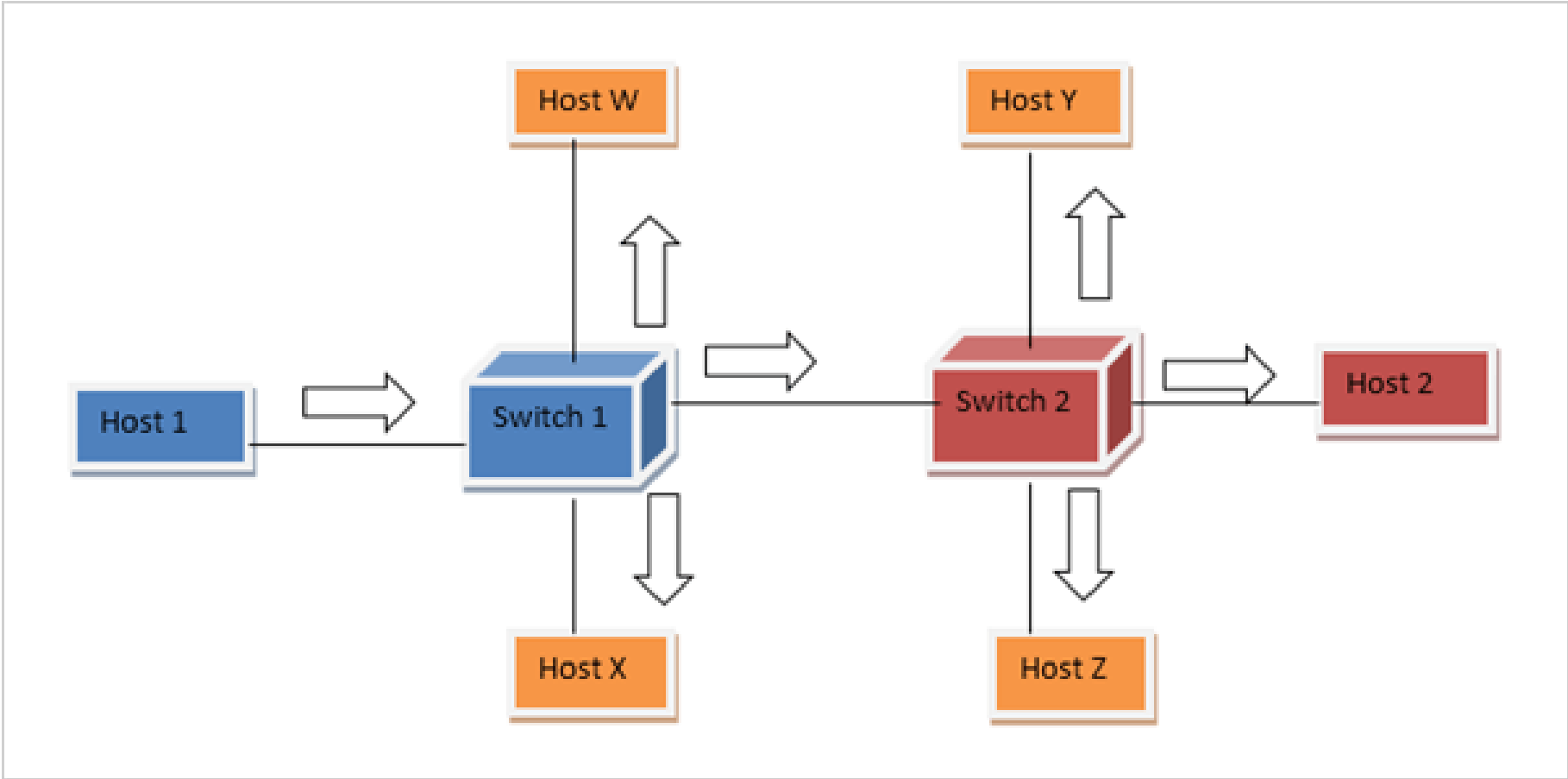
LAYER 2 SWITCH	LAYER 3 SWITCH
Operate on layer 2 (Data link) of OSI model.	Operate on layer 3 (Network Layer) of OSI model.
Send packet to destination on the basis of MAC address.	Route Packet with help of IP address
Work with MAC address only	Can perform functioning of both 2 layer and 3 layer switch
Used to reduce traffic on local network.	Mostly Used to implement VLAN (Virtual Local area network)
Quite fast as they do not look at the Layer 3 portion of the data packets.	Takes time to examine data packets before sending them to their destination
It has single broadcast domain	It has multiple broadcast domain.
Can communicate within a network only.	Can communicate within or outside network.

Collision and Broadcast Domain

- Collision can occur in Layer-2 switching where two or more hosts are trying to communicate at the same interval of time on the same network link.
- The network efficiency will get diminish here as the data frame will collide and we have to resend them. But every port in a switch generally lies in a dissimilar collision domain. The domain which is used to forward all type of broadcast messages is known as Broadcast domain.
- All layer-2 devices inclusive of Switches appear in the identical broadcast domain.

VLAN (Virtual Local Area Network)

- To overcome the issue of collision and broadcast domain, the VLAN technique is introduced in the computer networking system.
- Virtual Local area network commonly known as VLAN is a logical set of end devices lying in the identical group of the broadcast domain. VLAN configuration is done at the switch level by using different interfaces. Different switches can have different or same VLAN configuration and set up according to the need of a network.
- The hosts connected to two or more different switches can be connected within the same VLAN even if they are not connected physically as VLAN behave as virtual LAN network. Therefore, hosts, that are connected with different switches can share the same broadcast domain.



- Without VLAN, the broadcast message sent from host 1 will reach to all the network components of the network.
- But by using VLAN and configuring VLAN in both switches of the network by adding an interface card naming fast Ethernet 0 and fast Ethernet 1, generally notated as Fa0/0, in two different VLAN network, a broadcast message from Host 1 will deliver only to Host 2.
- This happens while doing the configuration, and only Host 1 and host 2 are defined under the same set of VLAN while the other components are a member of some other VLAN network
- It is important to note here that layer-2 switches can allow hosts devices to reach the host of the same VLAN only. To reach the host device of some another network the Layer-3 switch or router is required.