What is a VLAN?

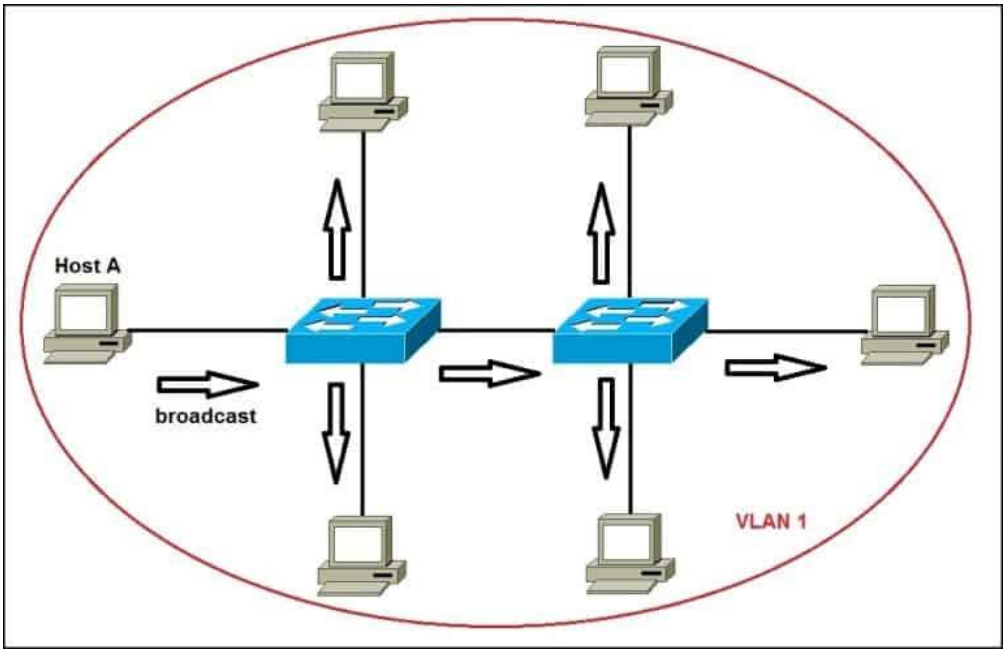
VLANs (Virtual LANs) are logical grouping of devices in the same broadcast domain. VLANs are usually configured on switches by placing some interfaces into one broadcast domain and some interfaces into another. Each VLAN acts as a subgroup of the switch ports in an Ethernet LAN.

VLANs can spread across multiple switches, with each VLAN being treated as its own subnet or broadcast domain. This means that frames broadcasted onto the network will be switched only between the ports within the same VLAN.

A VLAN acts like a physical LAN, but it allows hosts to be grouped together in the same broadcast domain even if they are not connected to the same switch. Here are the main reasons why VLANs are used:

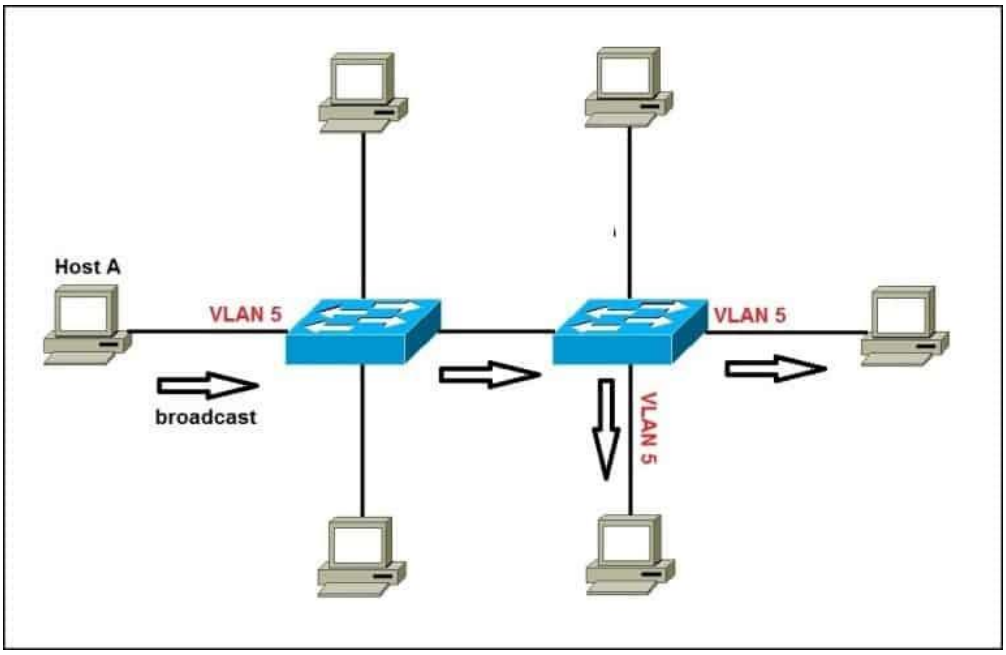
- VLANs increase the number of broadcast domains while decreasing their size.
- VLANs reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood.
- you can keep hosts that hold sensitive data on a separate VLAN to improve security.
- you can create more flexible network designs that group users by department instead of by physical location.
- network changes are achieved with ease by just configuring a port into the appropriate VLAN.

The following topology shows a network with all hosts inside the same VLAN:



Without VLANs, a broadcast sent from host A would reach all devices on the network. Each device will receive and process broadcast frames, increasing the CPU overhead on each device and reducing the overall security of the network.

By placing interfaces on both switches into a separate VLAN, a broadcast from host A would reach only devices inside the same VLAN, since each VLAN is a separate broadcast domain. Hosts in other VLANs will not even be aware that the communication took place. This is shown in the picture below:



How VLAN works

Here is step by step details of how VLAN works:

- VLANs in networking are identified by a number.
- A Valid range is 1-4094. On a VLAN switch, you assign ports with the proper VLAN number.
- The switch then allows data which needs to be sent between various ports having the same VLAN.
- Since almost all networks are larger than a single switch, there should be a way to send traffic between two switches.
- One simple and easy way to do this is to assign a port on each network switch with a VLAN and run a cable between them.

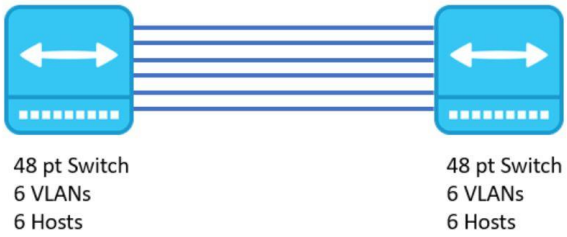
VLAN Ranges

Here are the important ranges of VLAN:

Range	Description
VLAN 0 & 4095:	Reserved VLAN, which cannot be seen or used.
VLAN 1:	This is a default VLAN of switches. You cannot delete or edit this VLAN, but it can be used.
VLAN 2-1001:	It is a normal VLAN range. You can create, edit, and delete it.
VLAN 1002-1005:	These ranges are CISCO defaults for token rings and FDDI. You cannot delete this VLAN.
VLAN 1006-4094:	It is an extended range of VLANs.

Example of VLAN

In the below example, there are 6 hosts on 6 switches having different VLANs. You need 6 ports to connect switches together. It means, if you have 24 various VLANs, you will have only 24 hosts on 45 port switches.



Example of VLAN

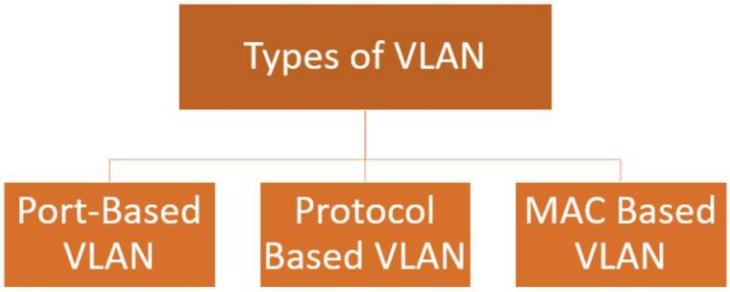
Characteristics of VLAN

- Here are the important characteristics of VLAN:
- Virtual LANs offer structure for making groups of devices, even if their networks are different.
- It increases the broadcast domains possible in a LAN.
- Implementing VLANs reduces the security risks as the number of hosts which are connected to the broadcast domain decreases.
- This is performed by configuring a separate virtual LAN for only the hosts having sensitive information.

- It has a flexible networking model that groups users depending on their departments instead of network location.
- Changing hosts/users on a VLAN is relatively easy. It just needs a new port-level configuration.
- It can reduce congestion by sharing traffic as individual VLAN works as a separate LAN.
- A workstation can be used with full bandwidth at each port.
- Terminal reallocations become easy.
- A VLAN can span multiple switches.
- The link of the trunk can carry traffic for multiple LANs.

Types of VLANs

Here are the important types of VLANs



Types of VLAN

Port-Based VLAN

Port-based VLANs groups virtual local area network by port. In this type of virtual LAN, a switch port can be configured manually to a member of VLAN.

Devices that are connected to this port will belong to the same broadcast domain that is because all other ports are configured with a similar VLAN number.

The challenge of this type of network is to know which ports are appropriate to each VLAN. The VLAN membership can't be known just by looking at the physical port of a switch. You can determine it by checking the configuration information.

Protocol Based VLAN

This type of VLAN processes traffic based on a protocol that can be used to define filtering criteria for tags, which are untagged packets.

In this Virtual Local Area Network, the layer-3 protocol is carried by the frame to determine VLAN membership. It works in multi-protocol environments. This method is not practical in a predominately IP based network.

MAC Based VLAN

MAC Based VLAN allows incoming untagged packets to be assigned virtual LAN and, thereby, classify traffic depending on the packet source address. You define a Mac address to VLAN mapping by configuring mapping the entry in MAC to the VLAN table.

This entry is specified using source Mac address proper VLAN ID. The configurations of tables are shared among all device ports.

Difference between LAN and VLAN

Here is an important difference between LAN and VLAN:

LAN	VLAN
LAN can be defined as a group of computer and peripheral devices which are connected in a limited area.	A VLAN can be defined as a custom network which is created from one or more local area networks.
The full form of LAN is Local Area Network	The full form of VLAN is Virtual Local Area Network.
The latency of LAN is high.	The latency of VLAN is less.
The cost of LAN is high.	The cost of a VLAN is less.
In LAN, the network packet is advertised to each and every device.	In VLAN, the network packet is sent to only a specific broadcast domain.
It uses a ring, and FDDI (Fiber Distributed Data Interface) is a protocol.	It uses ISP and VTP as a protocol.

Advantages of VLAN

- Here are the important pros/benefits of VLAN:
- It solves a broadcast problem.
- VLAN reduces the size of broadcast domains.
- VLAN allows you to add an additional layer of security.
- It can make device management simple and easier.

- You can make a logical grouping of devices by function rather than location.
- It allows you to create groups of logically connected devices that act like they are on their own network.
- You can logically segment networks based on departments, project teams, or functions.
- VLAN helps you to geographically structure your network to support the growing companies.
- Higher performance and reduced latency.
- VLANs provide increased performance.
- Users may work on sensitive information that must not be viewed by other users.
- VLAN removes the physical boundary.
- It lets you easily segment your network.
- It helps you to enhance network security.
- You can keep hosts separated by VLAN.
- You do not require additional hardware and cabling, which helps you to saves costs.
- It has operational advantages because of changing the IP subnet of the user is in software.
- It reduces the number of devices for particular network topology.
- VLAN makes managing physical devices less complex.

Disadvantages of VLAN

- Here are the important cons/ drawbacks of VLAN:
- A packet can leak from one VLAN to other.
- An injected packet may lead to a cyber-attack.
- Threat in a single system may spread a virus through a whole logical network.
- You require an additional router to control the workload in large networks.
- You can face problems in interoperability.
- A VLAN cannot forward network traffic to other VLANs.

Application/Purpose of VLAN

Here are the important uses of VLAN:

- VLAN is used when you have 200+ devices on your LAN.
- It is helpful when you have a lot of traffic on a LAN.
- VLAN is ideal when a group of users need more security or being slow down by many broadcasts.
- It is used when users are not on one broadcast domain.
- Make a single switch into multiple switches.

Summary:

- VLAN is defined as a custom network which is created from one or more local area networks.
- VLAN in networking are identified by a number.
- A Valid range is 1-4094. On a VLAN switch, you assign ports with the proper VLAN number.
- Virtual LANs offer structure for making groups of devices, even if their networks are different.
- The main difference between LAN and VLAN is that In LAN, the network packet is advertised to each and every device Whereas in VLAN, the network packet is sent to only a specific broadcast domain.
- The primary advantage of VLAN is that it reduces the size of broadcast domains.
- The drawback of VLAN is that an injected packet may lead to a cyber-attack.
- VLAN is used when you have 200+ devices on your LAN.