# - Virtual LANs (VLANs) and VTP -

## ***Collision vs. Broadcast Domains***

A **collision domain** is simply defined as any physical segment where a **collision** can occur. Hubs can only operate at half-duplex, and thus all ports on a hub belong to the same collision domain.

Layer-2 switches can operate at full duplex. *Each individual port* on a switch belongs to its *own collision domain*. Thus, Layer-2 switches create **more collision domains**, which results in **fewer collisions.**

Like hubs though, Layer-2 switches belong to only *one* **broadcast domain.** A Layer-2 switch will forward both broadcasts and multicasts out *every* port but the originating port.

Only Layer-3 devices separate broadcast domains. Because of this, Layer-2 switches are poorly suited for large, scalable networks. The Layer-2 header provides no mechanism to differentiate one *network* from another, only one *host* from another.

## ***Virtual LANs (VLANs)***

By default, a switch will forward both broadcasts and multicasts out *every* port but the originating port. However, a switch can be *logically* segmented into separate broadcast domains, using **Virtual LANs** (or **VLANs**).

Each VLAN represents a unique broadcast domain:

- Traffic between devices within the *same* VLAN is switched.
- Traffic between devices in *different* VLANs requires a Layer-3 device to communicate.

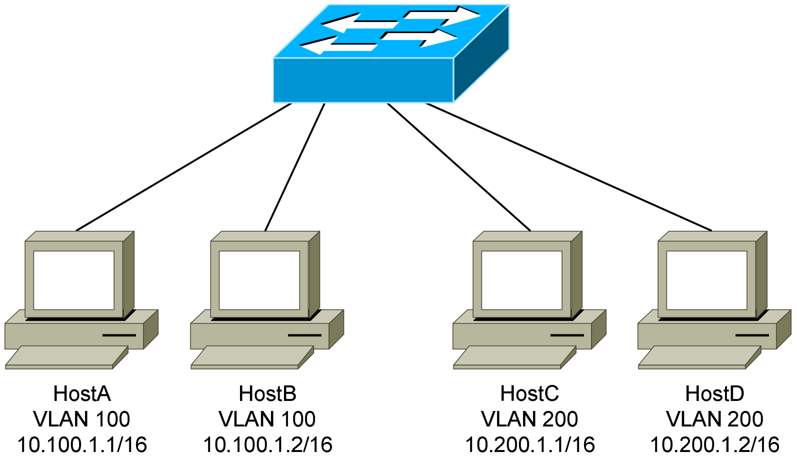
Broadcasts from one VLAN will not be forwarded to another VLAN. The logical separation provided by VLANs is **not a Layer-3 function.** VLAN tags are inserted into the **Layer-2 header**.

Thus, a switch that supports VLANs is not necessarily a Layer-3 switch. However, a purely Layer-2 switch cannot route between VLANs.

**Remember,** though VLANs provide separation for *Layer-3* broadcast domains, they are still a *Layer-2* function. A VLAN often has a direct relationship with an IP subnet, though this is not a requirement.

## ***VLAN Example***

Consider the following example:



Four hosts are connected to a Layer-2 switch that supports VLANs:

- HostA and HostB belong to VLAN 100
- HostC and HostD belong to VLAN 200

Because HostA and HostB belong to the *same* VLAN, they belong to the same broadcast domain as well. The switch will be able to forward frames between the two hosts without the need of a Layer-3 device, such as a router.

Likewise, HostC and HostD belong to the same VLAN, and thus the same broadcast domain. They also will be able to communicate without an intervening Layer-3 device.

However, HostA and HostB *will not* be able to communicate with HostC and HostD. They are members of separate VLANs, and belong in *different* broadcast domains. Thus, a Layer-3 device is required for those hosts to communicate.

A broadcast sent from a host in VLAN 100 will be received by all other hosts in that same VLAN. However, that broadcast will not be forwarded to any other VLAN, such as VLAN 200.

On Cisco switches, all interfaces belong to **VLAN 1** by default**.** VLAN 1 is also considered the **Management VLAN,** and should be dedicated for system traffic such as CDP, STP, VTP, and DTP.

## ***Advantages of VLANs***

VLANs provide the several benefits:

- **Broadcast Control –** eliminates unnecessary broadcast traffic, improving network performance and scalability.
- **Security –** logically separates users and departments, allowing administrators to implement access-lists to control traffic between VLANs.
- **Flexibility –** removes the physical boundaries of a network, allowing a user or device to exist anywhere.

VLANs are very common in LAN and campus networks. For example, user networks are often separated from server networks using VLANs.

VLANs can span across WANs as well, though there are only limited scenarios where this is necessary or recommended.

## ***VLAN Membership***

VLAN membership can be configured one of two ways:

- **Statically**
- **Dynamically**

**Statically** assigning a VLAN involves manually assigning an individual or group of ports to a VLAN. Any host connected to that port (or ports) immediately becomes a member of that VLAN. This is *transparent* to the host - it is unaware that it belongs to a VLAN.

VLANs can be assigned **dynamically** based on the MAC address of the host. This allows a host to remain in the same VLAN, regardless of which switch port it is connected to.

Dynamic VLAN assignment requires a separate database to maintain the MAC-address-to-VLAN relationship. Cisco developed the **VLAN Membership Policy Server (VMPS)** to provide this functionality.

In more sophisticated systems, a user's network account can be used to determine VLAN membership, instead of a host's MAC address.

Static VLAN assignment is far more common than dynamic, and will be the focus of this guide.

## ***Creating VLANs***

By default, all interfaces belong to **VLAN 1.** To assign an interface to a different VLAN, that VLAN must first be *created*:

```
Switch(config)#  vlan 100
Switch(config-vlan)#  name SERVERS
```

The first command creates VLAN 100, and enters VLAN configuration mode. The second command assigns the name *SERVERS* to this VLAN.

Note that naming a VLAN is *not* required.

The standard range of VLAN numbers is **1 – 1005,** with VLANs 1002-1005 reserved for legacy Token Ring and FDDI purposes.

A switch operating in VTP **transparent mode** can *additionally* use the VLAN range of **1006 – 4094.** These are known as extended-range VLANs. VTP is covered in great detail later in this guide.

To remove an individual VLAN:

```
Switch(config)#  no vlan 100
```

Note that VLAN 1 cannot be removed. To remove a group of VLANs:

```
Switch(config)#  no vlan 150-200
```

To view all created VLANs, including the interfaces assigned to each VLAN:

```
Switch# show vlan
```

```
VLAN Name                           Status    Ports
---- ------------------------------ --------- -----------
1    default                        active    gi1/1-24
100  SERVERS                        active
1002 fddi-default                   suspended
1003 token-ring-default             suspended
1004 fddinet-default                suspended
1005 trnet-default                  suspended
```

Note that no interfaces have been assigned to the newly created VLAN 100 yet.

## ***Statically Assigning VLANs***

To statically assign an interface into a specific VLAN:

```
Switch(config)#  interface gi1/10
Switch(config-if)#  switchport mode access
Switch(config-if)#  switchport access vlan 100
```

The first command enters interface configuration mode. The second command indicates that this is an *access* port, as opposed to a *trunk* port. This will be explained in detail shortly.

The third command assigns this access port to VLAN *100*. Note that the VLAN *number* is specified, and not the VLAN *name.*

The *show vlan* command should now reflect the new VLAN assignment:

```
Switch# show vlan
```

```
VLAN Name                          Status    Ports
---- -------------------------- --------- -----------
1    default                       active    gi1/1-9,11-24
100  SERVERS                       active    gi1/10
1002 fddi-default                  suspended
1003 token-ring-default            suspended
1004 fddinet-default               suspended
1005 trnet-default                 suspended
```

For switches running in VTP **server** or **client mode***,* the *list* of VLANs are stored in a database file named **vlan.dat.** The vlan.dat file is usually stored in **flash**, though on some switch models it is stored in NVRAM. The VLAN database will be maintained even if the switch is rebooted.

For switches running in VTP **transparent mode**, the list of VLANs is stored in the startup-config file in NVRAM. VTP is covered extensively later in this guide.

Regardless of VTP mode, the VLAN *assignment* for every switch interface is stored in the switch's **startup-config**.