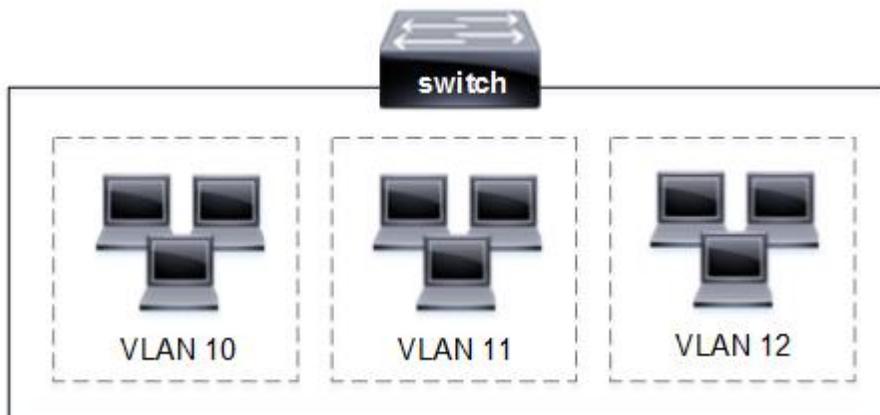


Virtual LAN (VLAN)

The primary purpose of a VLAN is to create a broadcast domain. All unicast, broadcast and multicast traffic is limited to each VLAN. It is a Layer 2 broadcast domain comprised of endpoints such as clients, servers, and/or network devices. In fact, each VLAN is the equivalent of an older bridge network device. One or more switch ports are assigned to a VLAN.

Any unassigned Cisco switch ports remain in the default VLAN 1. When a network endpoint connects to a switch port, the endpoint is placed in the VLAN assigned to that switch port. You can only create VLANs on Layer 2 or Layer 3 switches. Some typical network endpoints include desktop, mobile, IP phone and wireless access points.

Figure 1 Virtual LAN (VLAN) Logical Segments



Advantages of VLANs

VLANs enable segmentation or isolation of broadcast traffic. That prevents broadcasts from being advertised outside of the VLAN. That conserves bandwidth usage and improves performance. The level of complexity has increased significantly in recent years. Limiting the size of a broadcast domain improves both performance and security.

Consider that a broadcast domain is a logical network since VLANs can span multiple switches. VLANs do not prevent broadcast storms, they minimize the size and effect of the broadcast storm on neighbor switches and hosts. The following are advantages for deploying VLANs on a network switch.

1. Enable access to network services based on logical requirements such as company organization and department.
2. Network security is optimized with VLANs that enable managing and filtering sensitive traffic from other network traffic. Each VLAN is associated with a subnet for logical segmentation.
3. Bandwidth efficiency is accomplished through segmenting traffic into smaller broadcast domains. Unicasts, broadcasts and multicasts are not forwarded between VLANs minimizing bandwidth utilization.
4. Easier add/move/delete administration of endpoints on the network and scalability for larger enterprise deployments.

Table 1 Network Broadcasts

Broadcast Type	Destination Address	Examples
Layer 2	FFFF.FFFF.FFFF	MAC Learning, ARP, VLAN
Layer 3	255.255.255.255	DHCP, subnet only
Multicast	Reserved IP address	routing protocols

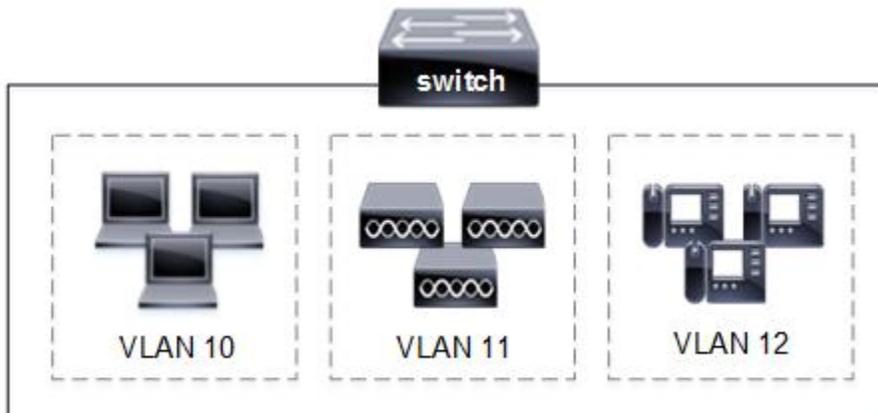
Normal/Extended VLANs

Cisco switch ports are all assigned to VLAN 1 as a default configuration. VLAN 1 is used for management traffic and cannot be deleted. The normal range VLAN 2 - 1001 can be added, modified or deleted from the switch. Cisco recommends assigning all data and voice traffic to a non-default VLAN. The following are guidelines for deploying VLANs to a Cisco switch.

Table 2 Normal/Extended VLANs

VLAN Range	Description
VLAN 1 – 1005	normal VLAN range
VLAN 1006 – 4094	extended VLAN range
VLAN 1, 1002 – 1005	auto-created and cannot be deleted
VLAN 1006 – 4094	cannot be pruned from a trunk

Figure 2 Multiple Endpoint Types



Access Ports (data and voice)

The switch access port provides connectivity for access devices such as a desktops, servers, IP phones, and wireless access points. The switch port can only be assigned one VLAN unless you are connecting an IP phone. The data VLAN 9 and voice VLAN 10 is permitted on an access port with the following configuration commands.

```
switch(config)# interface fastethernet0/1  
switch(config-if)# switchport mode access (access port mode)  
switch(config-if)# switchport access vlan 9 (assign data vlan)  
switch(config-if)# switchport voice vlan 10 (assign voice vlan)
```

VLANs are automatically created when assigned to a switch port interface, unless explicitly configured. For example, the switch would automatically create VLAN 9 and add it to the local VLAN database (vlan.dat) That is where the switch VLAN configuration is stored. The following global commands would also create VLAN 9 and assign a name. It is sometimes preferable to name VLANs for easier management and troubleshooting.

```
switch(config)# vlan 9  
switch(config-vlan)# name data
```

Cisco switch port interfaces support access mode or trunk mode. The default switch port mode is an access port. Switch access ports that receives an Ethernet frame with an 802.1q tag (trunk) in the header will discard the packet without learning the source MAC address.

Switch Port Interface Range

The following IOS commands create and assign VLAN 10 to a range of switch ports. There is no requirement to first create the VLAN in global configuration mode.

```
switch(config)# interface range gigabitethernet1/1 - 24  
switch(config-if)# switchport mode access  
switch(config-if)# switchport access vlan 10
```

Default VLAN

VLAN 1 is the default for any Cisco switch port interface. The primary purpose of VLAN 1 is to forward management frames between switches. The following are Cisco default switch configuration settings.

- single broadcast domain (VLAN 1)
- all switch ports are assigned to VLAN 1 as a default.
- VLAN 1 forwards management traffic and cannot be deleted.
- switch port default operational mode is access port

Operational Commands

The following commands list all VLANs configured on a switch. That includes VLAN number, VLAN name, status and port assigned.

```
switch# show vlan  
switch# show vlan brief
```

The following IOS show command only displays the switch port/s assigned to a single VLAN. It is handy when there is a complex switch configuration with multiple VLANs.

```
switch# show vlan id [vlan]
```

IP Default Gateway

Layer 2 switches do not support routing services. They can only read frames and make a forwarding decision based on MAC address table lookup. The default gateway is an upstream Layer 3 device that provides routing services. That is typically a router or Layer 3 switch that has an interface in the same subnet as an endpoint.

Data messages are forwarded to the default gateway when the destination subnet is on a different subnet than the endpoint. The default gateway could point to a physical interface or a VLAN interface. The Cisco default switch configuration does not have an IP default gateway.

The following IOS command configures an IP default gateway address on switch-1 for endpoint hosts on 192.168.1.0 subnet. The router has an interface (Gi1/1) that is assigned IP address 192.168.1.1 on the same subnet as VLAN 10. The IP default gateway also provides proxy ARP to host endpoints.

```
switch-1(config)# ip default-gateway 192.168.1.1
```

Figure 3 IP Default Gateway

