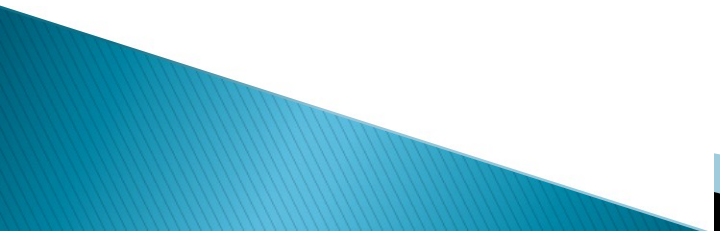
Virtual LANs

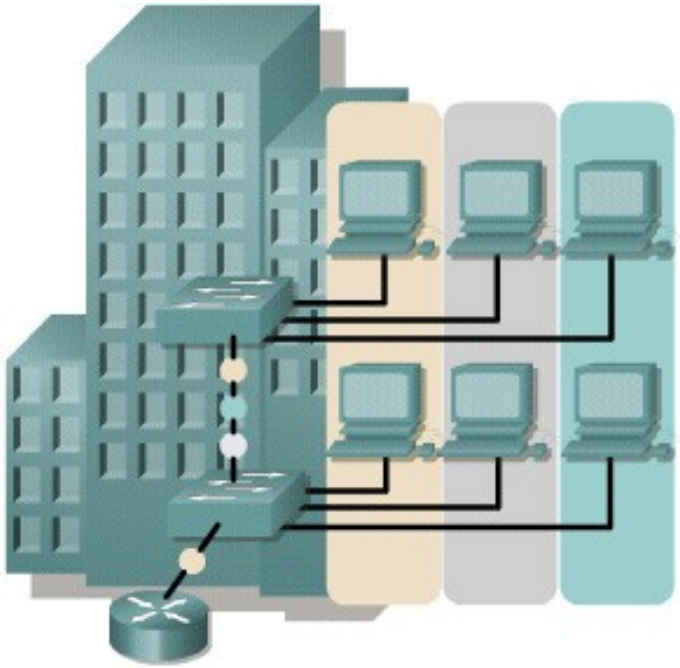


VLAN introduction

- VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.

VLAN introduction

- A workstation in a VLAN group is restricted to communicating with file servers in the same VLAN group.

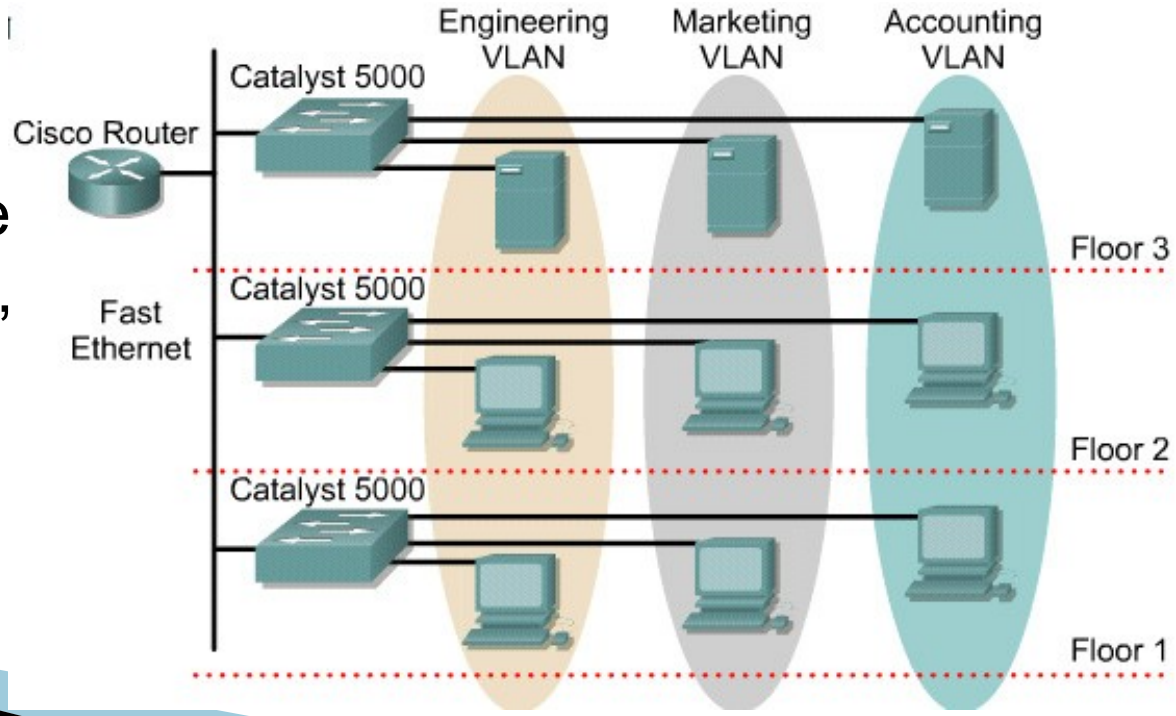


- A group of ports or users in same broadcast domain
- Can be based on port ID, MAC address, protocol, or application
- LAN switches and network management software provide a mechanism to create VLANs
- Frame tagged with VLAN ID

VLAN introduction

- VLANs function by logically segmenting the network into different broadcast domains so that packets are only switched between ports that are designated for the same VLAN.

- Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.

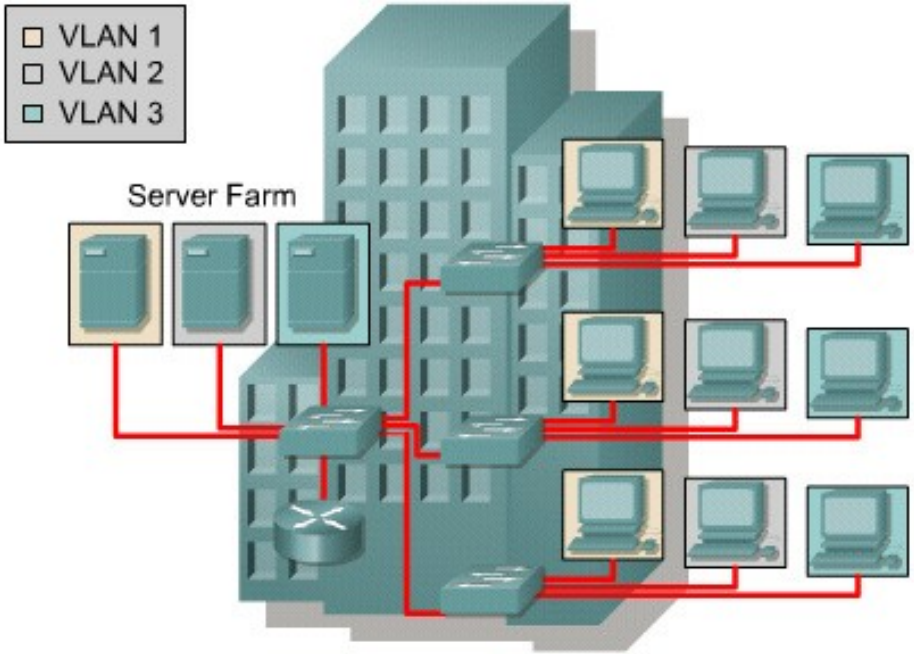


VLAN introduction

- VLANs address scalability, security, and network management.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain.
- Traffic should only be routed between VLANs.

Broadcast domains with VLANs and routers

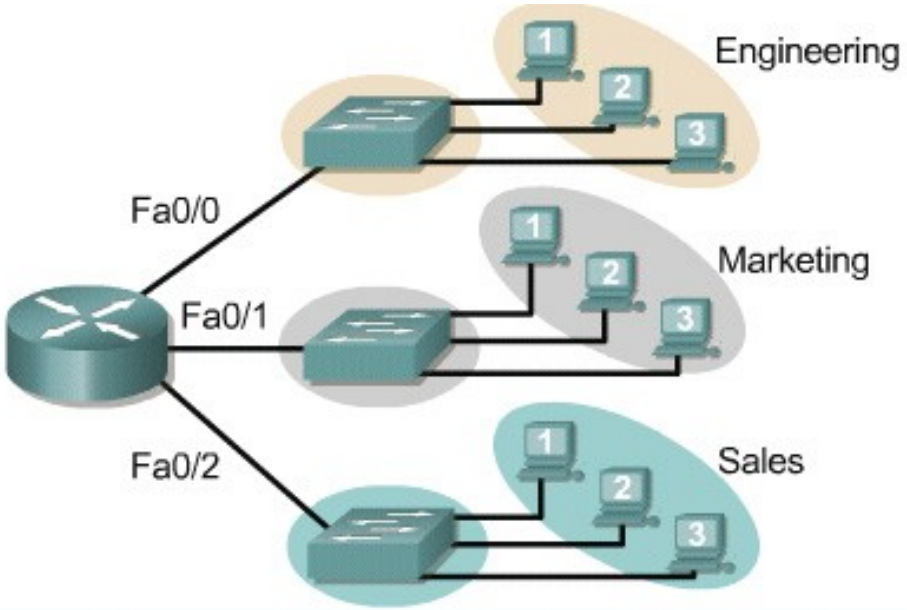
- A VLAN is a broadcast domain created by one or more switches.



- A switch creates a broadcast domain
- VLANs help manage broadcast domains
- VLANs can be defined on port groups, users, or protocols
- LAN switches and network management software provide a mechanism to create VLANs

Broadcast domains with VLANs and routers

- Layer 3 routing allows the router to send packets to the three different broadcast domains.



Three switches and one router could be used without VLANs:

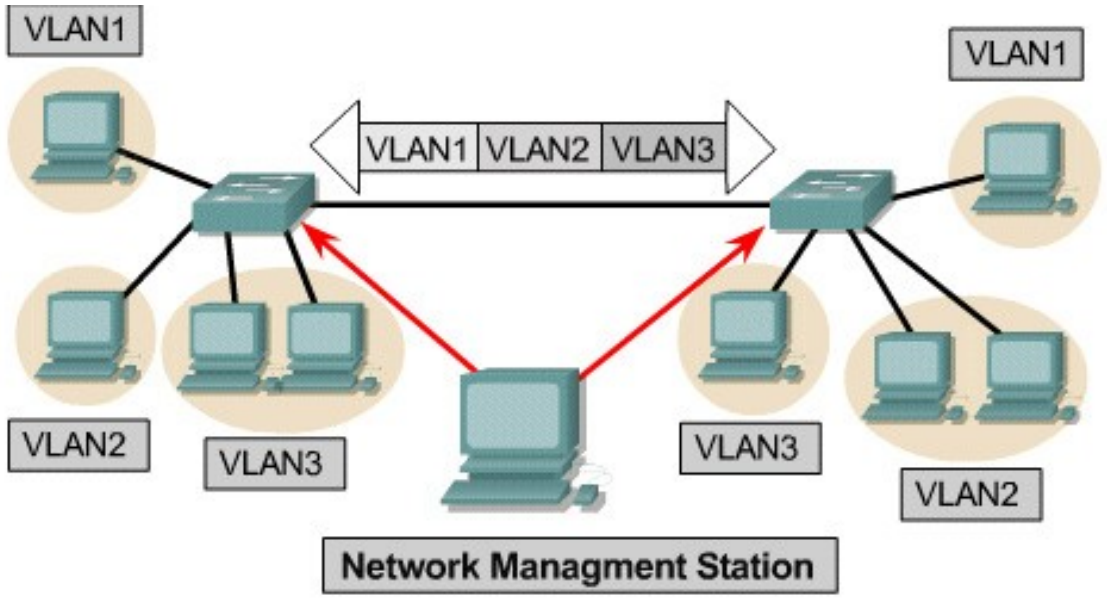
- Switch for Engineering
- Switch for Sales
- Switch for Marketing
- Each switch treats all ports as members of one broadcast domain
- Router is used to route packets among the three broadcast domains

Broadcast domains with VLANs and routers

- Implementing VLANs on a switch causes the following to occur:
  - The switch maintains a separate bridging table for each VLAN.
  - If the frame comes in on a port in VLAN 1, the switch searches the bridging table for VLAN 1.
  - When the frame is received, the switch adds the source address to the bridging table if it is currently unknown.
  - The destination is checked so a forwarding decision can be made.
  - For learning and forwarding the search is made against the address table for that VLAN only.

VLAN operation

- Each switch port could be assigned to a different VLAN.
- Ports assigned to the same VLAN share broadcasts
- Ports that c
these broa



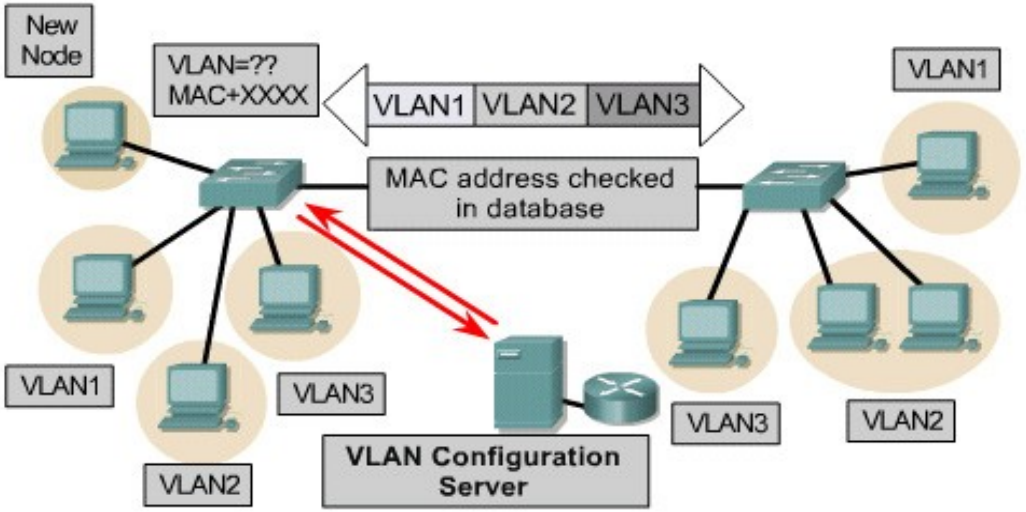
- Assign ports (port-centric)
- Static VLANs are secure, easy to configure and monitor

VLAN operation

- Users attached to the same shared segment, share the bandwidth of that segment.
- Each additional user attached to the shared medium means less bandwidth and deterioration of network performance.
- VLANs offer more bandwidth to users than a shared network.
- The default VLAN for every port in the switch is the management VLAN.
- The management VLAN is always VLAN 1 and may not be deleted. All other ports on the switch may be reassigned to alternate VLANs.

VLAN operation

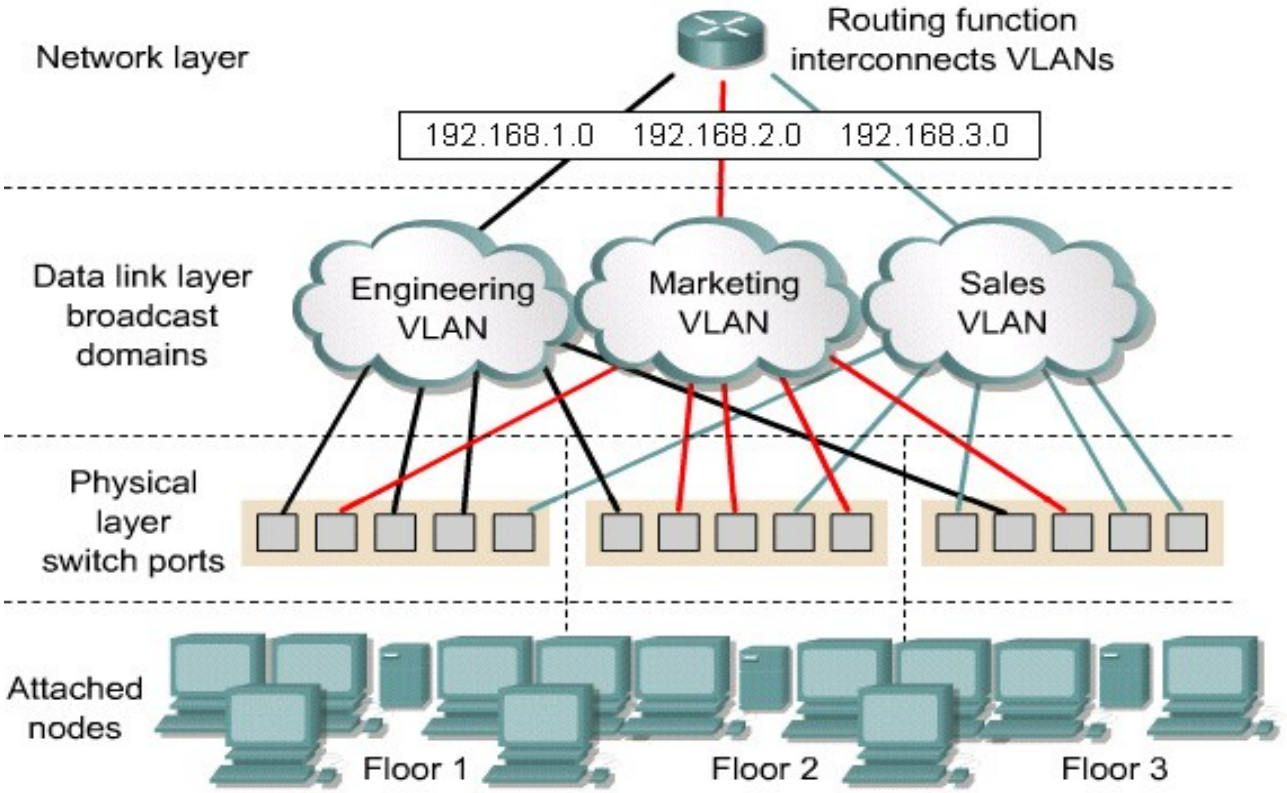
- Dynamic VLANs allow for membership based on the MAC address of the device connected to the switch port.
- As a device enters the network. it queries a data
men



- VLANs assigned using centralized VLAN management application
- VLANs based on MAC address, logical address, or protocol type
- Less administration in wiring closet
- Notification when unrecognized user is added to network

VLAN operation

- In port-based or port-centric VLAN membership, the port is assigned to a specific VLAN membership independent of the user or system attached to the port.
- All users of the same port must be in the same VLAN.



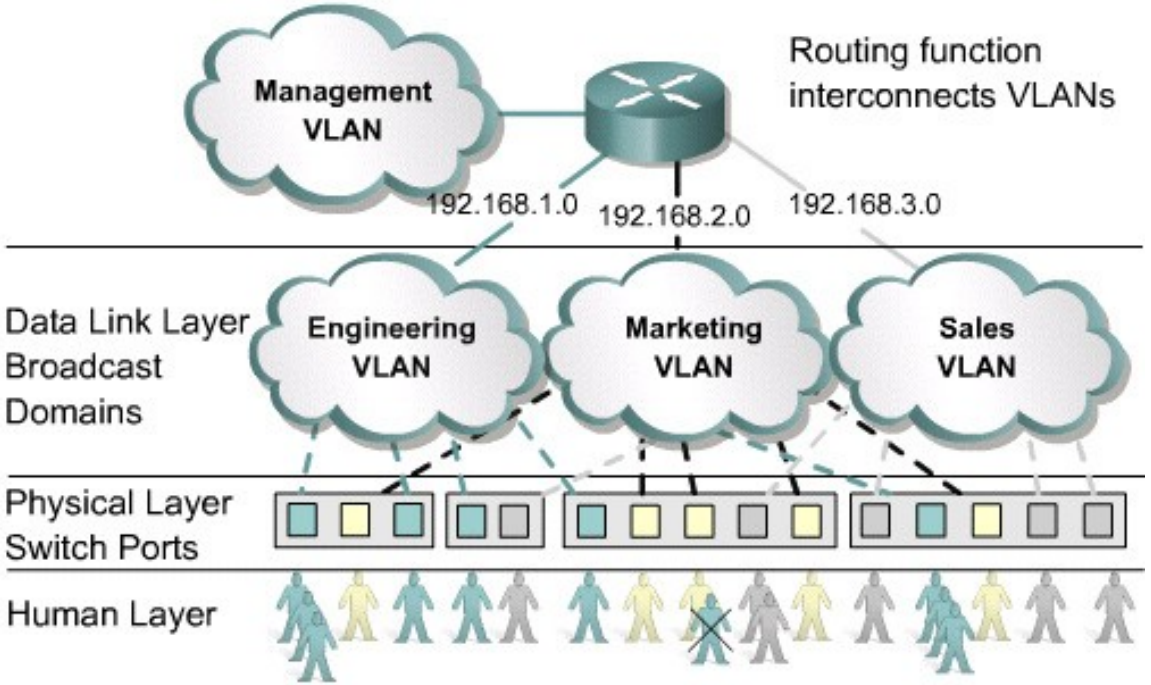
VLAN operation

- Network administrators are responsible for configuring VLANs both manually and statically.

Configuring VLANs	Description
Statically	Network administrators configure port-by-port. Each Port is associated with a specific VLAN. The network administrator is responsible for keying in the mappings between the ports and VLANs.
Dynamically	The ports are able to dynamically work out their VLAN configuration. Uses a software database of MAC address to VLAN mappings (which the network administrator must set up first).

Benefits of VLANs

- The key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically.



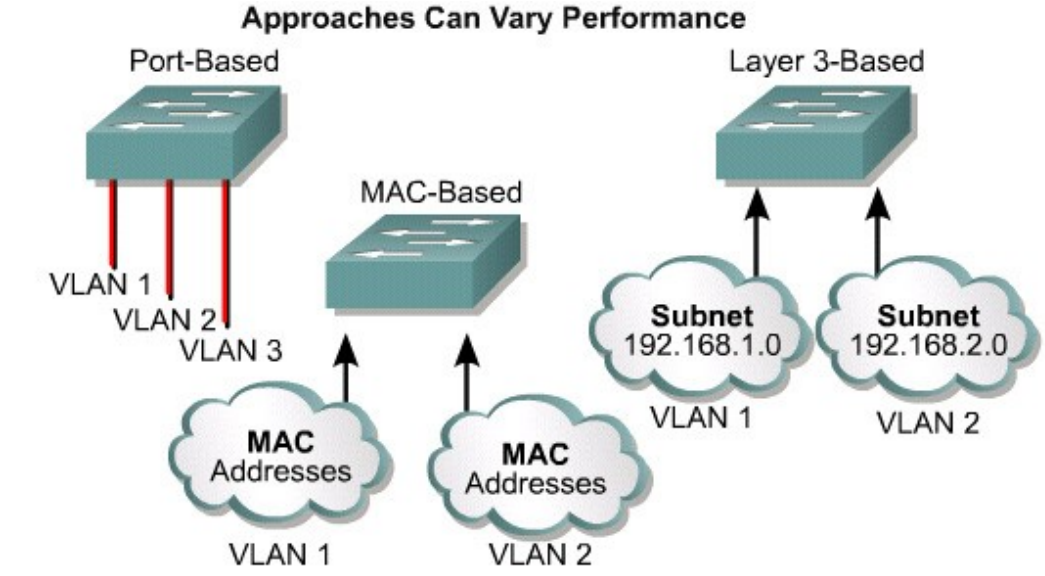
All users attached to the same switch port must be in the same VLAN.

VLAN types

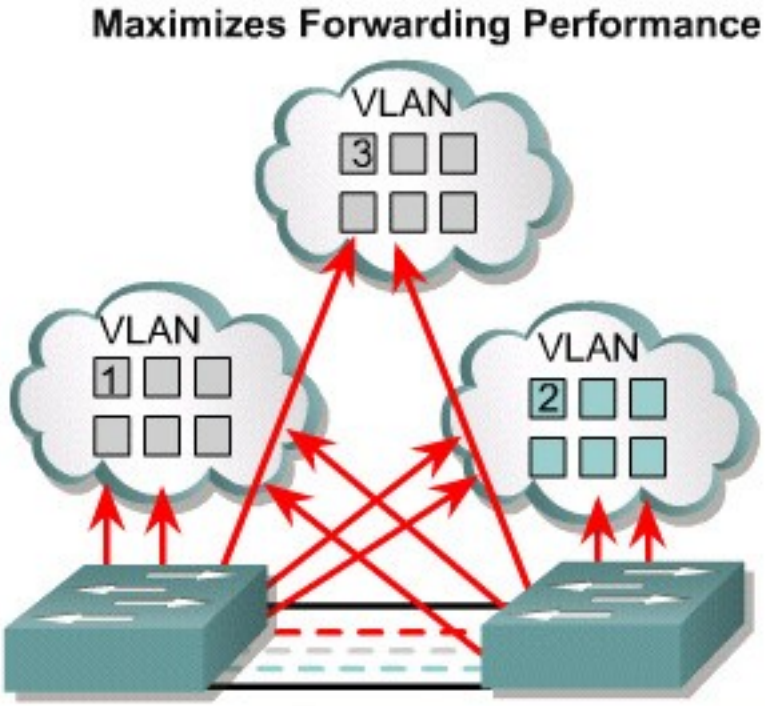
- There are three basic VLAN memberships for determining and controlling how a packet gets assigned: -
  - Port-based VLANs
  - MAC address based
  - Protocol based VLANs
- The frame headers are encapsulated or modified to reflect a VLAN ID before the frame is sent over the link between switches.
- Before forwarding to the destination device, the frame header is changed back to the original format.

VLAN types

- Port-based VLANs
- MAC address based VLANs
- Protocol based VLANs

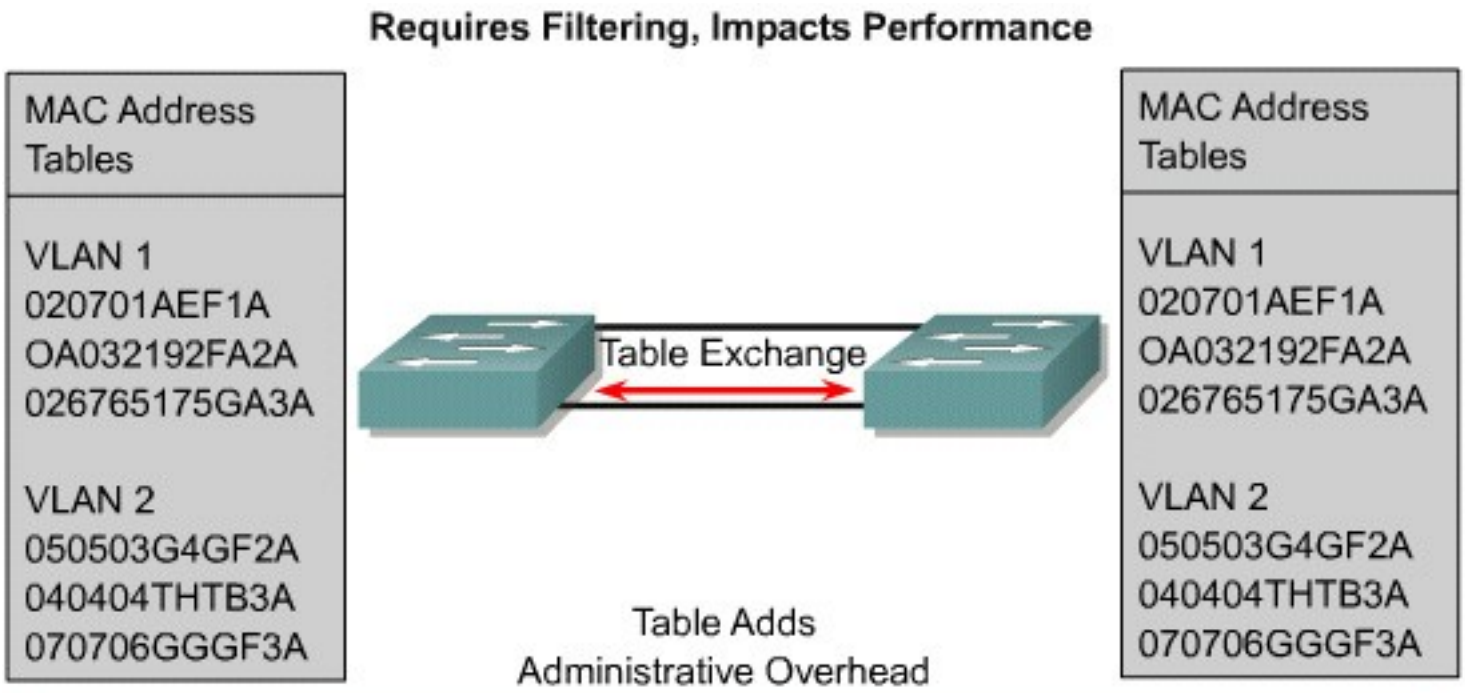


Membership by Port



- User assigned by port association
- Requires no lookup if done in ASICs
- Easily administered via GUIs
- Maximizes security between VLANs
- Packets do not "leak" into other domains
- Easily controlled across network

Membership by MAC-Addresses



- User assigned based on MAC addresses
- Offers flexibility, yet adds overhead
- Impacts performance, scalability, and administration
- Offers similar process for higher layers

VLAN types

- The number of VLANs in a switch vary depending on several factors:
  - Traffic patterns
  - Types of applications
  - Network management needs
  - Group commonality

VLAN types

- An important consideration in defining the size of the switch and the number of VLANs is the IP addressing scheme.
- Because a one-to-one correspondence between VLANs and IP subnets is strongly recommended, there can be no more than 254 devices in any one VLAN.
- It is further recommended that VLANs should not extend outside of the Layer 2 domain of the distribution switch.

VLAN types

- There are two major methods of frame tagging, Inter-Switch Link (ISL) and 802.1Q.
- ISL used to be the most common, but is now being replaced by 802.1Q frame tagging.

Tagging	Method	Media	Description
Inter-Switch Link (ISL)	Fast Ethernet	ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header	Frame is lengthened.
802.IQ	Fast Ethernet	IEEE defined Ethernet VLAN protocol	Header is modified.
802.IQ	FDDI	IEEE defined standard: The 802.10 protocol incorporates a mechanism whereby LAN traffic can carry a VLAN identifier	VLAN ID is the essential piece of required header information.
LAN Emulation (LANE)	ATM	No tagging	Virtual connection implies a VLAN ID.