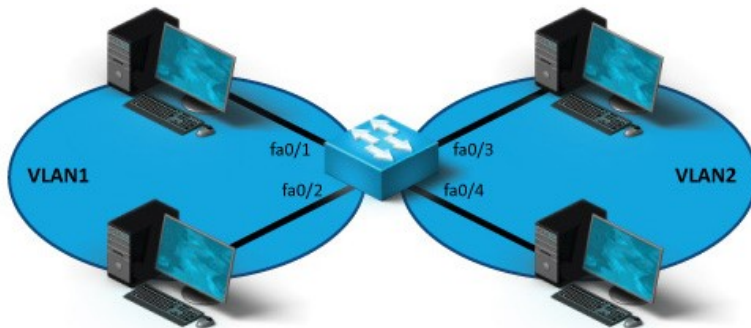# 6.4.2 VLAN Facts

A virtual LAN (VLAN) uses switch ports to define a broadcast domain. When you define a VLAN, you assign devices on different switch ports to a separate logical (or virtual) LAN. Although a switch can support multiple VLANs, each switch port can be assigned to only one VLAN at a time. The following graphic shows a single-switch VLAN configuration:

In the single-switch VLAN configuration above, the following is true:

- FastEthernet ports 0/1 and 0/2 are members of VLAN 1.
- FastEthernet ports 0/3 and 0/4 are members of VLAN 2.
- Workstations in VLAN 1 will not be able to communicate with workstations in VLAN 2, even though they are connected to the same physical switch. Communications between VLANs requires a router, just as with physical LANs.
- Defining VLANs creates multiple broadcast domains. The above example has two broadcast domains defined, each of which corresponds to one of the VLANs.
- On Cisco switches, all ports are members of VLAN 1 by default.

Switches use VLAN IDs to route VLAN traffic. VLAN IDs:

- Are appended to the header of each frame.
- Allow switches to identify which VLAN the frame belongs to.
- Are used for inter-switch traffic.

VLAN IDs are only understood by switches. VLAN IDs are added and removed by switches, not the clients.

Creating VLANs with switches offers many administrative benefits. You can:

- Create virtual LANs based on criteria other than physical location (such as workgroup, protocol, or service).
- Simplify device moves (devices are moved to new VLANs by modifying the port assignment).
- Control broadcast traffic and create collision domains based on logical criteria.
- Control security (isolate traffic within a VLAN).
- Load-balance network traffic (divide traffic logically rather than physically).

VLANs are commonly used with Voice over IP (VoIP) to separate voice traffic from data traffic. Traffic on the voice VLAN can be given a higher priority to ensure timely delivery.