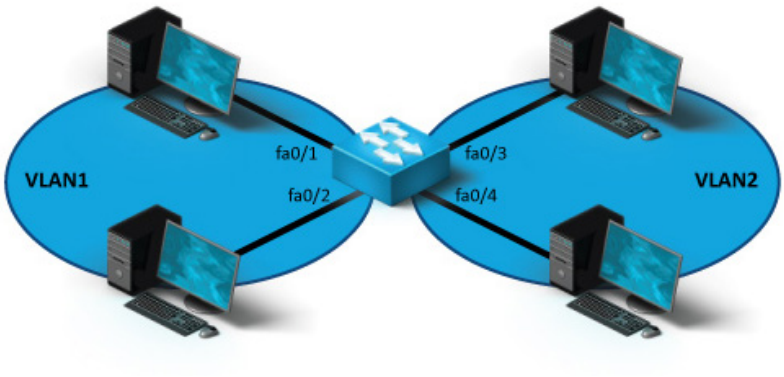
6.6.3 VLAN Facts

A virtual LAN (VLAN) can be defined as the following:

- A logical collection of devices that belong together and act as if they are connected to the same wire or physical switch.
- A grouping of devices based on service need, protocol, or other criteria, rather than physical proximity.

Using VLANs lets you assign devices on different switch ports to different logical (or virtual) LANs. Although each switch can be connected to multiple VLANs, each switch port can be assigned to only one VLAN at a time. The following graphic shows a single-switch VLAN configuration:



Be aware of the following facts about VLANs:

- In the graphic above, FastEthernet ports 0/1 and 0/2 are members of VLAN 1. FastEthernet ports 0/3 and 0/4 are members of VLAN 2.
- In the graphic above, workstations in VLAN 1 are not able to communicate with workstations in VLAN 2, even though they are connected to the same physical switch.
- Defining VLANs creates additional and separate broadcast domains. The above example has two broadcast domains, each of which corresponds to one of the VLANs.
- Switches are configured with the following default VLANs:
  - VLAN 1
  - VLAN 1002
  - VLAN 1003
  - VLAN 1004
  - VLAN 1005

  Default VLANs cannot be deleted or modified.

- By default, all ports are members of VLAN 1.
- Depending on the VLAN number, a VLAN is either normal or extended.
  - 1–1005 is the normal range for VLANs.
  - 1006–4094 is the extended range for VLANs.

VLANs with switches offer the following administrative benefits:

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

VLANs are commonly used with Voice over IP (VoIP) to distinguish voice traffic from data traffic. You can give traffic on the voice VLAN higher priority to ensure timely delivery.

Switches can be used to create voice VLANs as well as data VLANs. Voice VLANs are configured on access ports and are used to carry VoIP traffic from a Cisco IP phone. Voice VLANs send all VoIP traffic with a higher priority than data traffic to ensure timely delivery. Consider the following facts about voice VLANs:

- To create a voice VLAN, use the **switchport voice vlan *[number]*** command.
- By default, IP phone traffic on a voice VLAN is tagged with an 802.1Q priority of 5.
- When an interface is configured with a voice VLAN, the PortFast feature is automatically enabled on the interface.
- A Cisco IP phone automatically uses the VLAN ID of the port it is connected to. Non-Cisco IP phones require the VLAN ID to be manually configured on the IP phone.

Creating VLANs with switches offers the following benefits over using routers to create distinct networks:

- Switches are easier to administer than routers.
- Switches are less expensive than routers.
- Switches offer higher performance (they introduce less latency).

A disadvantage of using switches to create VLANs is that you might be tied to a specific vendor. How VLANs are created and identified can vary from vendor to vendor. Creating a VLAN might mean you must use only that vendor's switches throughout the network. When using multiple vendors in a switched network, be sure each switch supports the 802.1Q standards if you want to implement VLANs.

Despite advances in switch technology, routers are still typically used to:

- Filter WAN traffic
- Route traffic between separate networks
- Route packets between VLANs (though Layer 3 switches can also do this)
