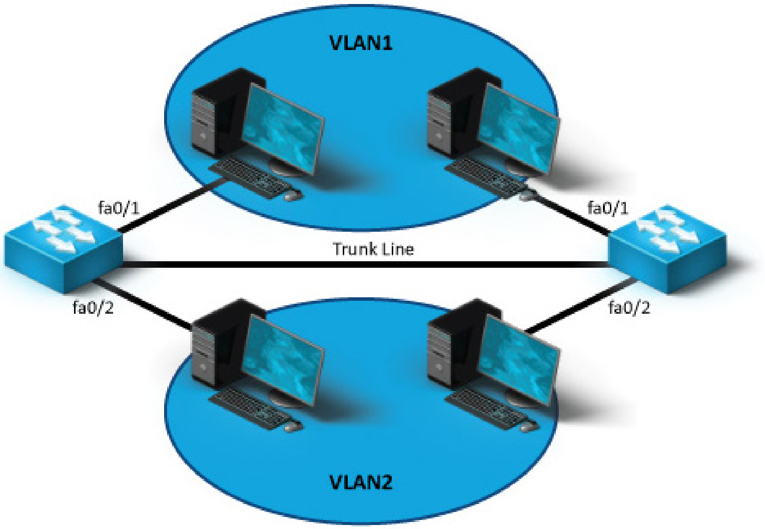
# 6.5.3 Trunking Facts

Trunking occurs when you configure VLANs that span multiple switches, as shown in the following diagram:



In this example, each switch has two VLANs configured with one port on each VLAN. Workstations in VLAN 1 can only communicate with other workstations in VLAN 1. This means that workstations connected to the same switch in this example cannot communicate directly with each other. Communications between workstations within each VLAN must pass through the trunk link to the other switch.

## Trunking Facts

Important facts regarding trunking and VLANs include the following:

- Access ports are connected to endpoint devices (such as workstations), while trunk ports are connected to other switches.
- An access port can be a member of only a single VLAN.
- Trunk ports are members of all VLANs on the switch by default.
- Any port on a switch can be configured as a trunk port.
- By default, trunk ports carry traffic for all VLANs between switches. However, you can reconfigure a trunk port so that it carries only specific VLANs on the trunk link.

When trunking is used, frames that are sent over a trunk port are tagged with the VLAN ID number so the receiving switch knows which VLAN the frame belongs to. In VLAN tagging:

- Tags are appended by the first switch in the path and removed by the last.
- Only VLAN-capable devices understand the frame tag.
- Tags must be removed before a frame is forwarded to a non-VLAN capable device.

A trunking protocol defines the process that switches use to tag frames with a VLAN ID. One widely implemented trunking protocol is the IEEE 802.1Q standard, which supports a wide range of switches from many device manufacturers. 802.1Q supports VLAN numbers 1 through 4094.

802.1Q trunking does not tag frames from the default VLAN, but does tag frames from all other VLANs. For example, suppose VLAN 1 is the default VLAN on a switch (the default setting on most Cisco switches). In this configuration, any frame on VLAN 1 that is placed on a trunk link is not assigned a VLAN tag. If a switch receives a frame on a trunk port that doesn't have a VLAN tag, the frame is automatically put on VLAN 1.

When using switches from multiple vendors in the same network, be sure that each device supports the 802.1Q standard.

The VLAN Trunking Protocol (VTP) simplifies VLAN configuration on a multi-switch network by propagating configuration changes between switches. For VTP to work, the switches must be connected by trunk links. With VTP, switches are configured in one of the following configuration modes:

- A switch in *server mode* is used to modify the VLAN configuration. The switch then advertises VTP information to other switches in the network.
- A switch in *client mode* receives changes from a VTP server switch and passes that information on to other switches. Changes cannot be made to the local VLAN configuration on a client switch.

- A switch in *transparent mode* allows local configuration of VLAN information, but it does not update its configuration with information from other switches. Likewise, local VLAN information is not advertised to other switches. However, VTP information received on the network is passed on to other switches.

By default, most managed switches are preconfigured to operate in server mode. If you do not intend to use VTP, configure your switches to use transparent mode.