

# How Virtual LANs (VLANs) Work

## Introduction

A VLAN is a grouping of computers that is logically segmented by functions, project teams, or applications without regard to the physical location of users. For example, several end stations might be grouped as a department, such as Engineering or Accounting, having the same attributes as a LAN even though they are not all on the same physical LAN segment. To accomplish this logical grouping, a VLAN-capable switching device must be used. Each switch port can be assigned to a VLAN. Ports in a VLAN share broadcast traffic and belong to the same broadcast domain. Broadcast traffic in one VLAN is not transmitted outside that VLAN. This segmentation improves the overall performance of the network.

## Benefits

VLANs provide the following benefits:

- Reduced administration costs associated with moves, adds, and changes
- Controlled broadcast activity and better network security
- Leveraging existing investments
- Flexible and scalable segmentation

Companies continuously reorganize as they try to improve productivity. These moves, adds, and changes are one of the greatest expenses in managing a network. VLANs provide an effective mechanism to control these changes and reduce much of the cost of hub and router reconfiguration. If a group of VLAN users move but remain in the same VLAN connected to a switch port, their network addresses do not change. Router configuration is left intact; a simple move for a user from one location to another does not create any configuration changes in the router if the user stays in the same VLAN. Similar to routers, VLANs offer an effective mechanism for setting up firewalls in a switch fabric, protecting the network against broadcast problems that are potentially dangerous, and maintaining all the performance benefits of switching. You can create these firewalls by assigning switch ports or users to specific VLAN groups in single switches and across multiple connected switches, which will increase security easily and inexpensively by segmenting the network into distinct broadcast groups. Broadcast traffic in one VLAN is not transmitted outside that VLAN. This type of configuration substantially

reduces overall broadcast traffic, frees bandwidth for real user traffic, and lowers the overall vulnerability of the network to broadcast storms.

You can leverage existing hub investments by assigning each hub segment connected to a switch port to a VLAN. All the stations that share a hub segment are assigned to the same VLAN. If an individual station must be reassigned to another VLAN, the station is relocated to the appropriate corresponding hub module. The interconnected switch fabric handles communication between the switching ports and automatically determines the appropriate receiving segments.

You can also assign VLANs based on the application type and the amount of applications broadcasts.

## **VLAN Operation**

### Switches? the Core of VLANs

Switches are a primary component of VLAN communication. They perform critical VLAN functions by acting as the entry point for end-station devices into the switched fabric, facilitating communication across the organization, and providing the intelligence to group users, ports, or logical addresses into common communities of interest. Each switch has the intelligence to make filtering and forwarding decisions by frame, based on VLAN metrics defined by network managers, and to communicate this information to other switches and routers within the network. The criteria used to define the logical grouping of nodes into a VLAN is based on a technique known as frame tagging. There are two types of frame tagging?implicit and explicit. Implicit tagging enables a packet to belong to a VLAN based on the Media Access Control (MAC) address, protocol, the receiving port of a switch, or another parameter into which nodes can be logically grouped. Explicit tagging requires the addition of a field into a frame or packet header that serves to classify the VLAN association of the frame. Frame tagging functions at Layer 2 and requires little processing or administrative overhead.

### Routers

For inter-VLAN communication, you must use routers that extend VLAN communications between workgroups. Routers provide policy-based control,

broadcast management, and route processing and distribution. They also provide the communication between VLANs and VLAN access to shared resources such as servers and hosts. Routers connect to other parts of the network that are either logically segmented into subnets or require access to remote sites across wide-area links. Consolidating the overall number of physical router ports required for communication between VLANs, routers use high-speed backbone connections over Fast Ethernet, Fiber Distributed Data Interface (FDDI), or Asynchronous Transfer Mode (ATM) for higher throughput between switches and routers.

## **Types of VLANs**

Each VLAN is of a particular type, and has its own maximum transmission unit (MTU) size. Two types of VLANs are defined:

- Ethernet/802.3 VLANs
- Token Ring/802.5 VLANs

Switches will allow a VLAN of one of these types to be assigned to a static/dynamic port for which the physical MAC layer is of the corresponding type; for example, allow a VLAN of type Ethernet/802.3 to be assigned to a physical 10BaseT port.

## **Inter VLAN Communication**

By definition, Virtual LANs perform traffic separation within a shared network environment. Communication between VLANs is performed through routing functionality and, for non routable protocols, switching. This integrated solution of high-speed, scalable VLAN switching of local traffic and efficient routing and switching of inter-VLAN traffic is becoming increasingly attractive in large networks. Cisco routers address this requirement with their ability to connect 802.10, ISL, and ATM LANE-based VLANs.

## **VLAN Standardization**

IEEE 802.1q provides for the standardization of VLANs based on a three-layer approach. The IEEE 802.1q draft is expected to be approved as a standard in 1998. Currently, several different transport mechanisms are used for communicating VLAN information across high-performance backbones. Among them are the LANE standard that has been approved by the ATM Forum, Cisco's Inter-Switch Link (ISL)

for Fast Ethernet, and the IEEE 802.10 protocol, which provides VLAN communication across shared FDDI backbones.

**Source:** <http://www.go4expert.com/articles/virtual-lans-vlans-t534/>