CHAPTER 1

Understanding VLANs

This chapter provides an introduction to VLANs and switched internetworking, compares traditional shared LAN configurations with switched LAN configurations, and discusses the benefits of using a switched virtual LAN architecture. It also explains how VlanDirector simplifies the management and configuration of the virtual LAN.

To install the VlanDirector software and start using the product immediately, proceed to "Installing VlanDirector."

Existing Shared LAN Configurations

A typical LAN configuration is configured according to the physical infrastructure it is connecting. Users are grouped based on their location in relation to the hub they are plugged into and how the cable is run to the wiring closet. Segmentation is typically provided by the router interconnecting each shared hub.

This type of segmentation does not group users according to their workgroup association or need for bandwidth. Engineering users can be plugged into the same hub as accounting and administration users because of their respective physical locations. They share the same segment and contend for the same bandwidth, although the bandwidth requirements may vary greatly according to workgroup or department.

Additionally, this segmentation requires that each hub connected to a router port have a unique subnet address. This prevents a logical assignment of network addresses across the network campus resulting in security issues.

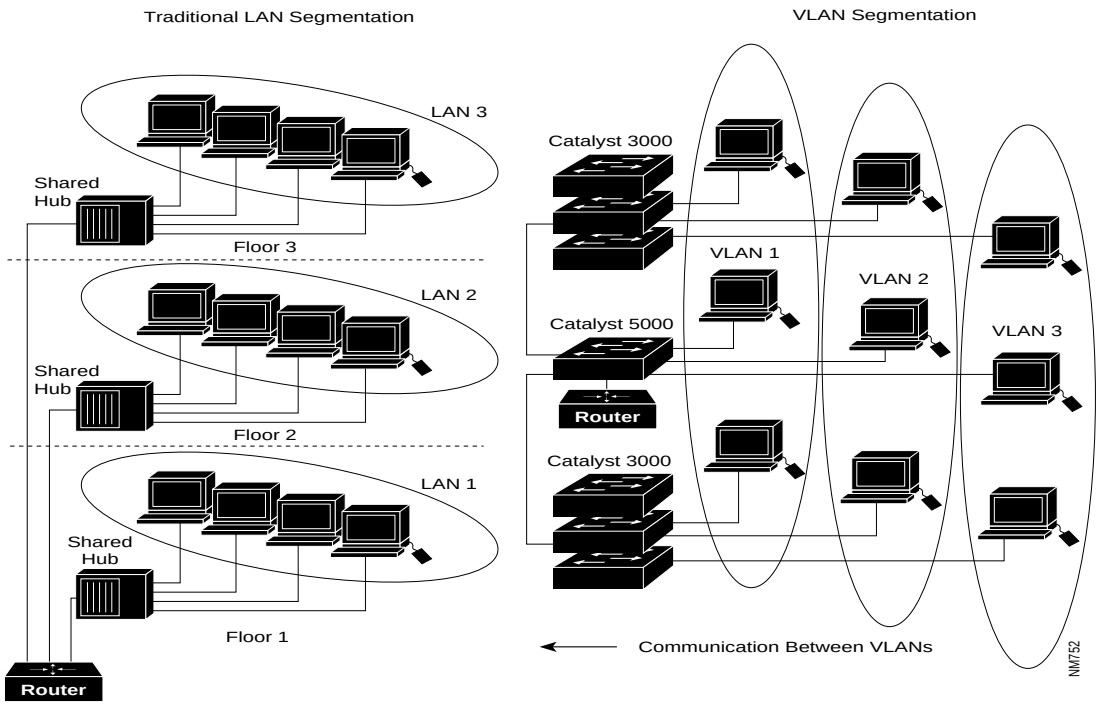
Switched Internetworking Configuration

The problems associated with shared LANs and the emergence of switches are causing traditional LAN configurations to be replaced with switched VLAN internetworking configurations. Switched VLAN configurations vary from LAN configurations in the following ways:

- Switches replace front-end hubs in the wiring closet. Switches are easily installed with little or no cabling changes, and can completely replace a shared hub with per port service to each user.
- VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. A VLAN is a switched network that is logically segmented by functions, project teams, or applications without regard to the physical location of users. Each switch port can be assigned to a VLAN. Ports in a VLAN share broadcasts. Ports that do not belong to that VLAN do not share these broadcasts. This improves the overall performance of the network.
- Communication between VLANs is provided by layer 3 routing.

Figure 1-1 shows the difference between LAN and VLAN segmentation.

Figure 1-1 LAN Segmentation and VLAN Segmentation



Segmenting with Switching Architectures

VLAN configurations group users by logical association rather than physical location. A majority of networks currently installed provide very limited logical segmentation. Users are commonly grouped based on connections to the shared hub and the router ports between the hubs. This topology provides segmentation only between the hubs, which are typically located on separate floors, and not between users connected to the same hub. This imposes physical constraints on the network and limits how users can be grouped. While a few shared-hub architectures have some grouping capability, they restrict how you can configure logically defined workgroups.

Switches remove the physical constraints imposed by a shared-hub architecture because they logically group users and ports across the enterprise. As a replacement for shared hubs, switches remove the physical barriers imposed in each wiring closet.

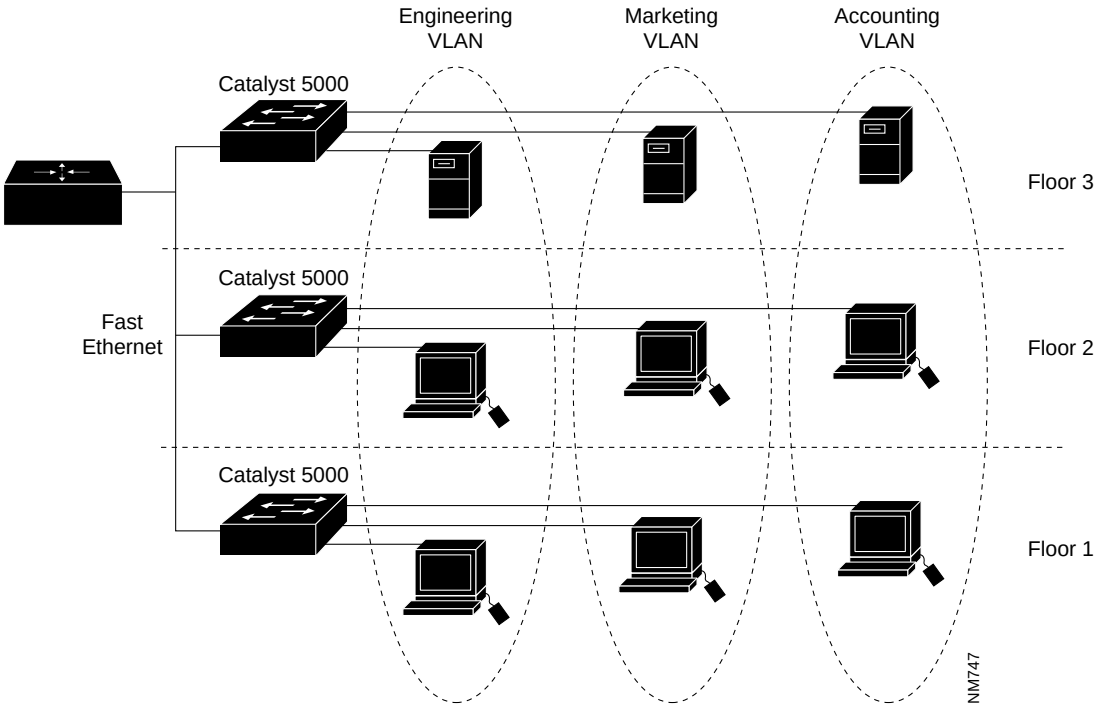
VLAN Solutions that Remove Physical Boundaries

Within the switched internetwork, VLANs provide segmentation and organizational flexibility. Using VLAN technology, you can group switch ports and their connected users into logically defined *communities of interest* such as the following:

- Coworkers in the same department
- A cross-functional product team
- Diverse user groups sharing the same network application or software (such as Lotus Notes users)

You can group these ports and users into *communities of interest* in a single switch or on connected switches. By grouping ports and users together across multiple switches, VLANs can span single-building infrastructures, interconnected buildings, or even wide-area networks (WANs). VLANs remove the physical constraints of workgroup communications. (See Figure 1-2.)

Figure 1-2 Logically Defined Networks (VLANs)



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 following:

- The intelligence to make filtering and forwarding decisions by packet, based on VLAN metrics that you define

- The ability to communicate this information to other switches and routers in the network

At present, LAN switches are installed between shared segment hubs and routers located in the backbone. In the future, they will play a larger role in VLAN segmentation and low-latency forwarding. LAN switches offer a significant increase in performance and dedicated bandwidth on the network. They also provide the intelligence for VLAN segmentation.

The Role of the Router

The role of the router changes from the traditional role of providing firewalls and broadcast suppression to policy-based control, broadcast management, and route processing and distribution. Routers remain vital for switched architectures configured as VLANs because they provide the communication between logically defined workgroups. Routers provide VLAN access to shared resources such as servers and hosts. They also connect to other parts of the network that are either logically segmented with the more traditional subnet approach or require access to remote sites across wide-area links.

Layer 3 communication, either embedded in the switch or provided externally, is an integral part of any high-performance switching architecture.

You can cost-effectively integrate external routers into the switching architecture with one or multiple high-speed backbone connections. These are typically FDDI, Fast Ethernet, or ATM connections. These connections provide the following benefits:

- Increased throughput between switches and routers
- Consolidation of overall number of physical router ports required for communication between VLANs

This architecture not only provides logical segmentation, it greatly enhances the efficiency of the network.

Benefits of VLANs

VLANs provide the following benefits:

- Reduced administration costs from solving problems associated with moves, adds, and changes

- Workgroup and network security
- Controlled broadcast activity
- Leveraging of existing hub investments
- Centralized administration control

Reduced Administration Costs

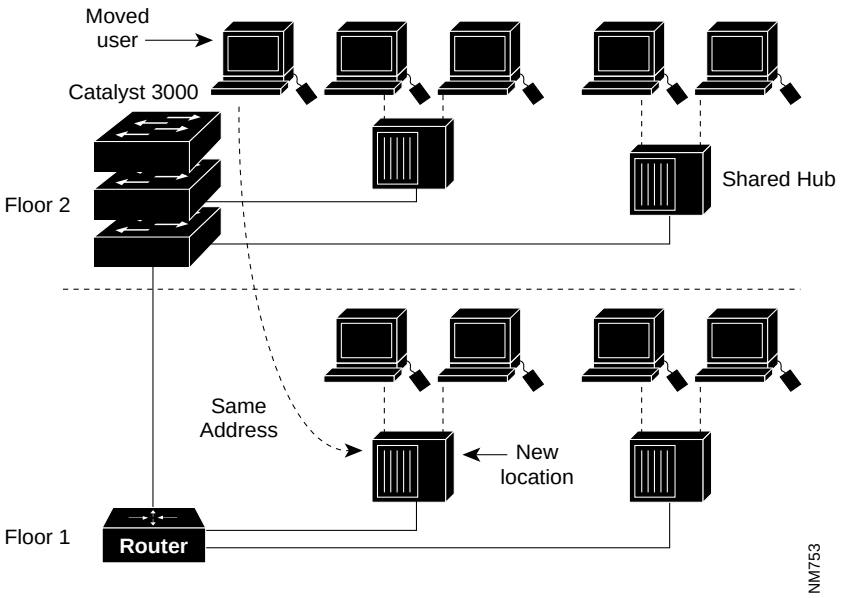
Companies continuously reorganize as they try to improve productivity. Each year 20 to 40 percent of the workforce is physically moved. These moves, adds, and changes are one of the greatest expenses in managing a network. Many moves require recabling. Almost all moves require new station addressing and hub and router reconfiguration. Invariably, as soon as managers stabilize their networks, more changes are requested.

VLANs provide an effective mechanism to control these changes and reduce much of the cost of hub and router reconfiguration. VLAN users can share the same network *address space* regardless of location. If a group of VLAN users move but remain in the same VLAN connected to a switch port, their network address does not change.

Location changes can be accomplished by

- Plugging a user into a port on a VLAN-capable switch, or
- Configuring the port on the switch to that VLAN, as shown in Figure 1-3.

Figure 1-3 Simplification of Moves with VLANs



This greatly simplifies the rewiring, configuration, and debugging required to get a user back on line. VLANs are a significant improvement over the techniques used in the wiring closet today. Router configuration is left intact; a simple move for a user from one location to another does not create any configuration modifications in the router if the user stays in the same VLAN.

Controlling Broadcast Activity

Broadcast traffic occurs in every network, whether controlled by effective network segmentation or by modifying an application's behavior. Broadcast traffic depends on the following:

- Types of applications
- Types of servers
- Amount of logical segmentation
- Use of network resources

Though applications have been fine-tuned to reduce the number of broadcasts, there are now multimedia applications that are both broadcast- and multicast-intensive. Broadcasts can also occur as a result of faulty network interface cards and communication devices. If incorrectly managed, they can seriously degrade network performance or even bring down an entire network.

You can take measures to prevent broadcast-related problems. One of the most effective measures is to properly segment the network with protective firewalls. Firewalls minimize problems in one area so they cannot damage other parts of the network. Thus, while one segment may show excessive broadcast conditions resulting from a faulty network device or a mismanaged application, the rest of the network is protected with the firewall, commonly provided by a router.

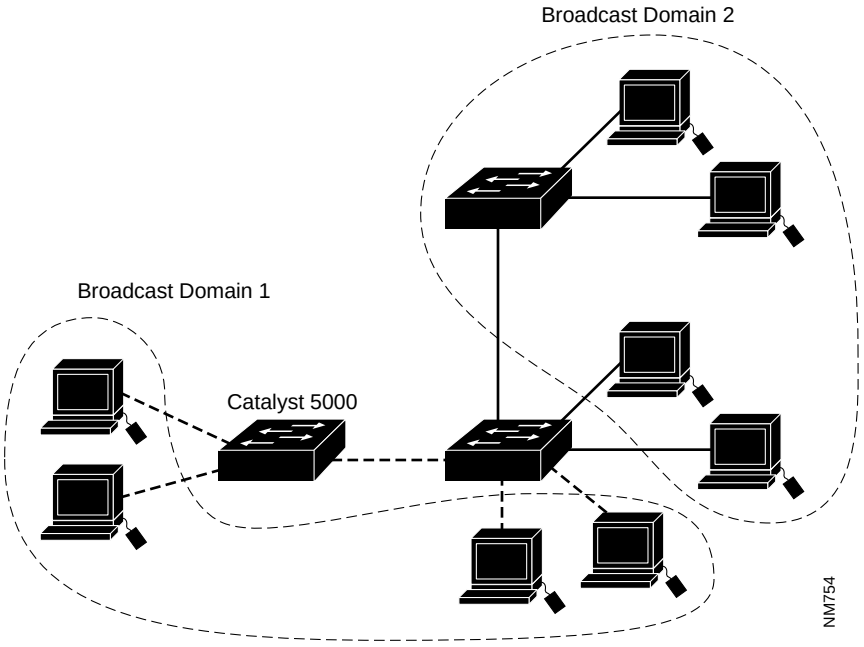
Firewall segmentation provides reliability, safeguards the network from inefficient bandwidth use, minimizes broadcast traffic overhead, and enables greater application traffic throughput.

As many designers migrate their networks toward switching architectures, they begin to lose the firewalls and safeguards that routers provide. By not placing routers between the switches, broadcasts are sent to every switched port. This is commonly called a *flat* network—one broadcast domain across the entire network. The advantage of a flat network is that it can provide both low latency and high throughput performance, and is much easier to administer. The disadvantage is that it increases vulnerability to broadcast traffic across all switches, ports, backbone links, and users.

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. 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. (See Figure 1-4.)

Figure 1-4 Managing Broadcast Activity



You can control the size of the broadcast domains by regulating the overall size of their associated VLANs and by restricting both the number of switch ports in a VLAN and the number of people using these ports.

You can also assign VLANs based on the application type and the amount of applications broadcasts. You can place users sharing a broadcast-intensive application in the same VLAN group and distribute the application across the campus.

Better Network Security

LAN use has increased exponentially in the past five years. As a result, LANs often carry confidential, mission-critical data. This data requires security through restricted access. An inherent shortcoming of shared LANs is that they can be easily penetrated. By plugging in to a live port, an unauthorized user can access all segment broadcasts. The larger the broadcast group, the greater the access (unless the hub has security control functions).

You can increase security easily and inexpensively by segmenting the network into distinct broadcast groups. Then you can also do the following:

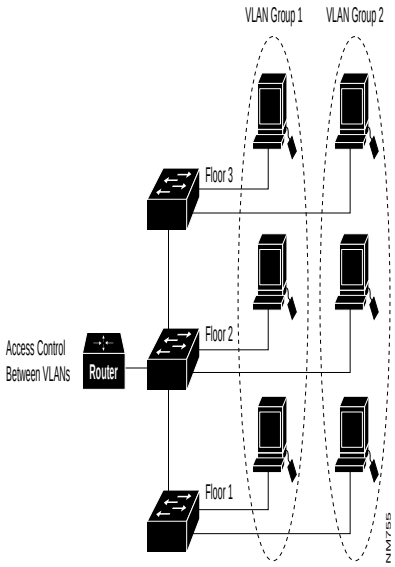
- Restrict the number of users in a VLAN
- Prevent another user from joining a VLAN without first receiving approval from the VLAN network management application
- Configure all unused ports to a default low-service VLAN

VLANs therefore can be used to provide security firewalls, restrict individual user access, flag any unwanted intrusion to the network, and control the size and composition of the broadcast domain.

To implement this type of segmentation, you can group switch ports based on the type of applications and access privilege, or place restricted applications and resources in a secured VLAN.

You can add more security enhancements by using router access lists. These are especially useful when communicating between VLANs. On the secured VLAN, the router restricts access to the VLAN as configured on both switches and routers. You can place restrictions on station addresses, application types, protocol types, or even by time of day. (See Figure 1-5.)

Figure 1-5 Enhancing Network Security with VLANs



Leveraging Existing LAN Hub Investments

Organizations have installed many shared hub chassis, modules, and stackable devices in the past three to five years. They replace many of these devices with newer switching technologies because network applications require more dedicated bandwidth and performance at the desktop. These concentrators still perform useful functions in many existing installations. You can leverage this investment by using backplane hub connections.

A backplane hub connection defines any shared-media hub connection to a network backbone. Stackable hubs, hub chassis, and even hub modules provide some form of this connection. It is the connections between shared hubs and switches that provide opportunities for VLAN segmentation.

You can assign 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.

The more the shared hub can be broken into smaller groups, the greater is the microsegmentation and the VLAN flexibility for assigning individual users to VLAN groups.

This furthers the migration to a high-performance switching architecture with enterprise LANs. With this approach, you can configure shared hubs as part of the VLAN architecture. You can also share traffic and network resources directly attached to switching ports with VLAN designations.

Managing VLANs with VlanDirector

VlanDirector simplifies the creation and management of VLANs, enabling you to easily perform configuration operations with simple “drag-and-drop” mouse clicks. You can create, modify, and delete VLANs and VLAN assignments. This enables you to centrally and simply plan and manage moves and changes.

VlanDirector reduces the amount of time required to set up and maintain VLANs. You can easily create VLAN names that directly correspond to the workgroups within your network. Multiple windows enable you to select between various views of the network.

When you first launch VlanDirector, it performs a discovery of your network. You can easily view existing VLANs and determine any changes you want to make or new VLANs you want to assign. VlanDirector also includes CiscoView. It uses the CiscoView application to drag and drop ports into a new or existing VLAN.

These capabilities help reduce the cost of switch management and increase overall services from centralized management operations.

VlanDirector Features

VlanDirector provides the following features:

- A network discovery feature that enables network managers to discover the Cisco switches and routers in a campus

  You can see an accurate representation of the network's physical connectivity to verify its design and configuration. This reduces operator configuration errors and ensures connectivity.

- Comprehensive switch support for Catalyst products

  You can integrate system-level VLANs for department and organization-wide switches.

- Software that operates with the CiscoView application to provide drag and drop port configuration functions

  You can reduce both the training effort and the skill level required for configuring VLANs.

- A simplified VLAN naming and assignment window with Expand, Collapse, and Name Search functions

  You can easily add, delete, and modify VLAN names in the network or configuration. The Expand and Name Search functions easily locate VLANs in networks that contain many VLANs.

- Application operation with HP OpenView and SunNet Manager.

  You can leverage existing hardware, software, and training investment in installed base network management applications and platforms.

- Logical VLAN views that show switches, links, and port memberships

  Using a simplified graphical method, you can see the configured VLANs in the network. Using a series of simple mouse clicks, you can quickly see individual ports, identified by their VLAN membership.

- Active switch and link screen icons

  By clicking on the representative screen icon, you can easily obtain VLAN configuration information for a specific device or link interface.

- Discrepancy reporting of anomalous device configurations

You can quickly troubleshoot and pinpoint individual device configurations that are incorrect in VLANs created at the system level.

- Graphical representation of the configured VLAN links between switches

  You can trace VLANs across the networks for monitoring. This eliminates much of the guesswork usually associated with VLAN configuration and management.

- Different VLANs represented by different colors for simplified viewing

  At a glance, network operators can detect the VLAN membership of switch ports by color association. They can then take configuration action based on the colors.

- Drag and drop addition and deletion of ports and VLANs

  You can quickly modify VLANs with simple mouse operations. It takes much less time to set up, modify, and administer VLANs.

- User authentication and write protection security

  You can prevent illegal network entry and configuration change from an unauthorized user.

- Online hypertext documentation and help system

  You have step-by-step online instructions to learn and operate the application. It takes less time to locate information about specific functions.

- Reliance on Cisco Discovery Protocol (CDP)

  VlanDirector uses CDP to discover the physical connectivity of the devices in the known network. VlanDirector cannot manage any devices that do not run CDP.