

## BACKBONE NETWORK DEVICES

In today's networked backbone, there are certain hardware devices that connect other networks to the backbone. These are special purpose devices and computers that just transfer messages from one network to another. Before we look deep into the topic **Virtual LAN's**, let us see the basic devices used in the network backbone. They are

1. Bridges.
2. Switches.
3. Routers.
4. Gateways.
5. Hubs.

**BRIDGES**-Bridges operate at the data link layer. They connect two LAN segments that use the same data link and network protocol. They may use the same or different types of cables. Bridges "learn" whether to forward packets, and only forward those messages that need to go to other network segments.

If a bridge receives a packet with a destination address that is not in the address table, it forwards the packet to all networks or network segments except the one on which it was received. Bridges are a combination of both hardware and software, typically a "black box" that sits between the two networks, but can also be a computer with two NICs and special software.

**SWITCHES**-Like bridges, switches operate at the data link layer. Switches connect two or more computers or network segments that use the same data link and network protocol. They may connect the same or different types of cable. The switch is a device that connects a material coming in with an appropriate outlet. They require more processing power. Switches operate at the same layers as bridges but differ from them in two ways:

1. First, most switches enable all ports to be in use simultaneously, making them faster than bridges.
2. Second, unlike bridges, switches don't learn addresses, and need to have addresses defined.

There are two types of switches:

1. Cut-through switches examine the destination of the incoming packet and immediately connect the port with the incoming message to the correct outgoing port. It is hardware-based.
2. Store-and-forward switches copy the incoming packet into memory before processing the destination address.

**ROUTERS**-Routers operate at the network layer. Routers connect two or more LANs that use the same or different data link protocols, but the same

network protocol. Routers may be “black boxes,” computers with several NICs, or special network modules in computers.

In general they perform more processing on each message than bridges and therefore operate more slowly.

Routers can choose the best route when compared with bridges. They only process messages specifically addressed to it. Routers can connect networks using different data link layer protocols. Therefore, routers are able to change data link layer packets. Routers may split a message into several smaller messages for better transmission.

**GATEWAYS-**Gateways operate at the network layer and use network layer addresses in processing messages. Gateways connect two or more LANs that use the same or different (usually different) data link and network protocols. They may connect the same or different kinds of cable.

Gateways process only those messages explicitly addressed to them. Gateways translate one network protocol into another, translate data formats, and open sessions between application programs, thus overcoming both hardware and software incompatibilities.

A gateway may be a stand-alone microcomputer with several NICs and special software, a FEP connected to a mainframe computer, or even a special circuit card in the network server. One of the most common uses of gateways is to enable LANs that use TCP/IP and Ethernet to communicate with IBM mainframes that use SNA. The gateway provides

both the basic system interconnection and the necessary translation between the protocols in both directions.

**HUBS-** Physical layer devices that are really just multiple port repeaters. When an electronic digital signal is received on a port, the signal is reamplified or regenerated and forwarded out all segments except the segment from which the signal was received.

<b>Device</b>	<b>Operates at</b>	<b>Messages</b>	<b>Physical Layer</b>	<b>Data Link Layer</b>	<b>Network Layer</b>
Hub	Physical	All transferred	S/D	Same	Same
Bridge	Data Link	Filtered using Data link layer addressing	S/D	Same	Same
Switch	Data Link	Switched using Data link layer addressing	S/D	Same	Same
Router	Network	Routed using network layer addressing	S/D	S/D	Same
Gateway	Network	Routed using network layer addressing	S/D	S/D	S/D

## WHAT is VLAN?

In a broadcast environment, a broadcast is sent out by a host on a single segment would propagate to all segments, saturating the bandwidth of the entire network. Also, without forcing some method of checking at an upper layer, all devices in the broadcast domain would be able to communicate via Layer 2. This severely limits the amount of security that could be enforced on the network.

Before the introduction of switches and VLANs, networks were divided into multiple broadcast domains by connectivity through a router. Because routers do not forward broadcasts, each interface is in a different broadcast domain. Each segment is an individual IP subnet and regardless of a workstation's function, its subnet is defined by its physical location.

**Definition:** A group of devices on one or more logically segmented LANs (configured by use of software), enabling devices to communicate as if attached to the same physical medium, when they are actually located on numerous different LAN segments. VLANs are based on logical instead of physical connections and thus are tremendously flexible.

A **VLAN** is logical broadcast domain that can span multiple physical LAN segments. A VLAN can be designed to provide independent broadcast domains for station logically segmented by functions, project teams, or applications without regard to the physical location of users. Each switch port can only be assigned to only one VLAN. Ports in a VLAN share broadcasts. Ports that do not belong to the same VLAN do not share

broadcasts. This control of broadcast improves the network's overall performance.

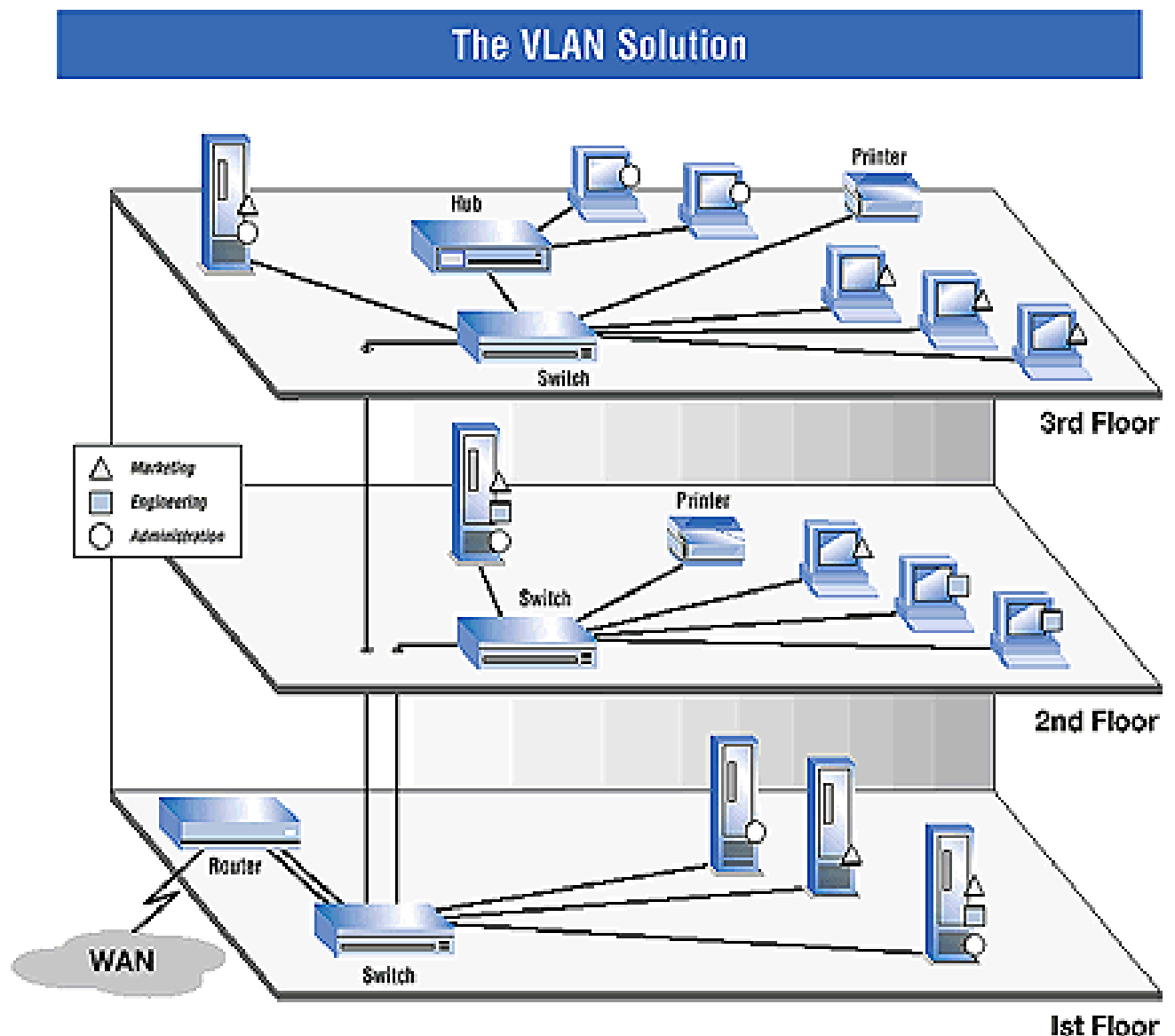
VLANs enable switches to create multiple broadcast domains within a switched network. Any user in this VLAN would receive a broadcast from any other member of the VLAN; users of other VLANs would not receive these broadcasts. Each of the users in a given VLAN would also be in the same IP subnet.

### **How VLANs Operate?**

A Catalyst Switch operates in your network like a traditional bridge. Each VLAN configured on the switch implements address learning, forwarding /filtering decisions and loop avoidance mechanisms as if it were a separate bridge. This VLAN might include several ports.

Internally, the catalyst switch implements VLANs by restricting data forwarding to destination ports in the same VLAN as originating ports. In other words, when a frame arrives on a switch port, the catalyst must retransmit the frame only to a port that belongs to the same VLAN. The implication is that a VLAN operating on a Catalyst switch limits transmission of unicast, multicast and broadcast traffic. Flooded traffic originating from a particular VLAN floods out only other ports belonging to that VLAN. This means that each VLAN is an individual broadcast domain.

Normally, a port carries traffic only for the single connection VLAN it belongs to. In order for a VLAN to span multiple switches on a single connection, a trunk is required to connect two switches. A trunk port can only be configured on the Fast Ethernet ports on the Catalyst 1900 switches.



Here we can see that each figure (triangle, circle, and square) represents a separate **VLAN**. These nodes do not communicate with each other but communication is between those represented by the same figure. For example here we can see that circle represents Administrative section. Therefore network can be divided into Administrative VLAN (circle), Engineering VLAN (square) and Marketing VLAN (triangle).

## The Need for VLANs.

By the 1980's, most networks consisted of a simple, hierarchical arrangement in which multiple, shared-media networks were connected by a router. With their sophisticated packet handling, routers allowed communication between networks when necessary, while effectively segmenting traffic so that large shared networks were not swamped by excessive traffic. Unfortunately, traditional routers were slow, complicated and expensive. As the need for faster networks emerged, a new solution was needed.

Switches spearheaded the next evolution of network structure. By segmenting the network and providing dedicated bandwidth where needed, they greatly increased performance, while reducing cost and complexity. However, traditional switches segment only unicast, or node-to-node, traffic. Unlike routers, they do not limit broadcast traffic (packets that are addressed to all the nodes within the network) or multicast traffic (packets that are distributed to a group of nodes).

As networks have grown and traffic has increased, IT managers have been forced to segment their networks into more and more switched subnets to meet increasing performance demands. With these changes, broadcast and multicast traffic have placed a greater burden on network bandwidth. In the worst case scenario, broadcast traffic can spiral out of control, creating broadcast storms that can bring down the network. As switched networks have become more common, routers have continued

to exist within the network. But they've been forced toward the periphery, where speed is generally less critical.

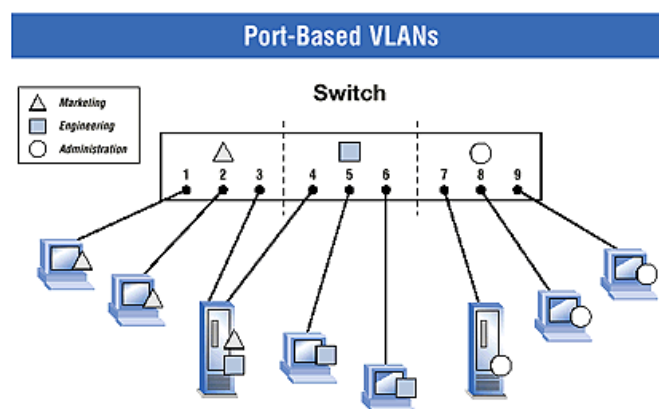
VLANs offer an effective solution to swamped routers and broadcast storms. By limiting the distribution of broadcast, multicast and unicast traffic, they can help free up bandwidth, reduce the need for expensive and complicated routing between switched networks, and eliminate the danger of broadcast storms. With these advantages, VLANs revive many of the key advantages of LAN routing, but with greater flexibility, performance, simplicity and affordability.

## VLANs: Different Models

In general there are three basic models for determining and controlling how a packet gets assigned to a VLAN. They are:

### ➤ Port-based VLANs-

In this implementation the administrator assigns each port of a switch to a VLAN. The switch determines the VLAN membership of each packet by noting For example, ports 1-3 might be assigned to the Sales VLAN, ports 4-6 to the Engineering VLAN and ports 7-9 to the Administrative VLAN (see Figure). The switch determines the VLAN membership of each packet by noting the port on which it arrives. When a user is moved to a different port of the switch, the administrator can simply reassign the new port to the user's old VLAN. The network change is then completely transparent to the user, and the administrator saves a trip to the wiring closet. However, this method has one significant drawback. If a repeater is attached to a port on the switch, all of the users connected to that repeater must be members of the same VLAN.



### ➤ MAC address-based VLANs-

The VLAN membership of a packet in this case is determined by its source or destination MAC address. Each switch maintains a table of MAC addresses and their corresponding VLAN memberships. A key advantage of this method is that the switch doesn't need to be reconfigured when a user moves to a different port.

However, assigning VLAN membership to each MAC address can be a time consuming task. Also, a single MAC address cannot easily be a member of multiple VLANs. This can be a significant limitation, making it difficult to share server resources between more than one VLAN. (Although a MAC address can theoretically be assigned to multiple VLANs, this can cause serious problems with existing bridging and routing, producing confusion in switch forwarding tables.)

### ➤ Layer 3 (or protocol)-based VLANs-

With this method, the VLAN membership of a packet is based on protocols (IP, IPX, NetBIOS, etc.) and Layer 3 addresses. This is the most flexible method and provides the most logical grouping of users. An IP subnet or an IPX network, for example, can each be assigned their own VLAN. Additionally, protocol-based membership allows the administrator to assign non-routable protocols, such as NetBIOS or DECnet, to larger VLANs than routable protocols like IPX or IP. This maximizes the efficiency gains that are possible with VLANs.

Another important distinction between VLAN implementations is the method used to indicate membership when a packet travels between switches. Two methods exist:

### 1. Implicit —

VLAN membership is indicated by the MAC address. In this case, all switches that support a particular VLAN must share a table of member MAC addresses.

### 2. Explicit —

A tag is added to the packet to indicate VLAN membership. Cisco ISL and the IEEE 802.1q VLAN specifications both use this method.

To summarize, when a packet enters its local switch, the determination of its VLAN membership can be port-based, MAC-based or protocol-based. When the packet travels to other switches, the determination of VLAN membership for that packet can be either implicit (using the MAC address) or explicit (using a tag that was added by the first switch). Port-based and protocol-based VLANs use explicit tagging as their preferred indication method. MAC-based VLANs are almost always implicit.

The bottom line is that the IEEE 802.1q specification is going to support port-based membership and explicit tagging, so these will be the default VLAN model in the future.

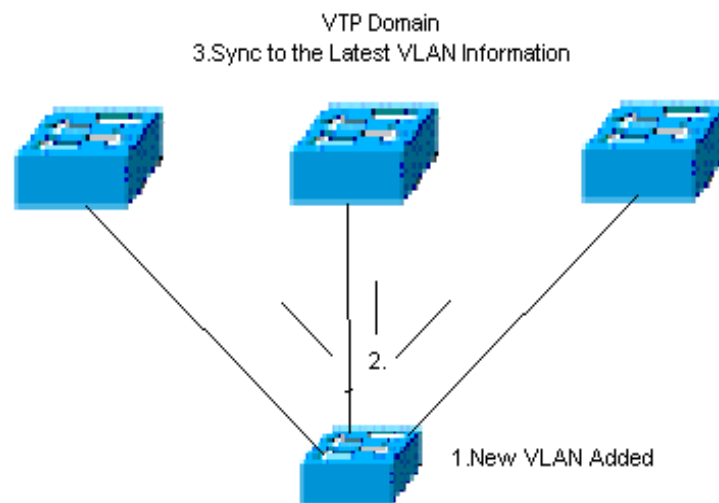
**PROTOCOL USED**

In order to provide VLAN connectivity throughout the switch fabric, VLANs must be configured on each switch. Cisco's **VLAN Trunking Protocol (VTP)** provides easier method for maintaining consistent VLAN configuration throughout the switched network.

VTP is a protocol used to distribute and synchronize identifying information about VLANs configured throughout a switched network. Configurations made to single VTP server are propagated across trunk links to all connected switches in the network. VTP enables switched network solutions to scale to large sizes by reducing the network's manual configuration needs.

VTP is a layer 2 messaging protocol that maintains VLAN configuration consistency throughout a common administration domain by managing the additions, deletions and name changes of VLANs across networks. VTP minimizes misconfigurations and configuration inconsistencies that can cause problems, such as duplicate VLAN names or incorrect VLAN- type specifications.

A VTP domain is one switch or several interconnected switches sharing the same VTP environment. A switch is configured to be in only one VTP domain.



**Step 1:** A new VLAN is added. At this point, VTP makes your job easier.

**Step 2:** The VTP advertisement is sent to other switches in the VTP domain.

**Step 3:** The new VLAN is added to other switch configurations. The result is consistent VLAN configuration.

By default, a catalyst switch is in the no-management-domain state until it receives an advertisement for a domain over a trunk link, or until you configure a management domain.

## BENEFITS OF VLAN

### **Flexible Network Segmentation**

Users and resources that communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is largely contained within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.

### **Simple Management**

The addition of nodes, as well as moves and other changes can be dealt with quickly and conveniently from the management console rather than the wiring closet.

### **Increased Performance**

VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network. In many network environments, an increasing number of routers are deployed to segment traffic into additional broadcast domains. However, as the router population grows, latency increasingly degrades network performance. This causes problems not only for legacy applications, but also for newer multimedia applications. It's also harder to assign network resources by groups unless each group is physically on the same LAN, so users can experience poor performance due to a number of causes. VLANs solve these issues by creating broadcast domains on their switches that ensure traffic from one user group doesn't impact the traffic from another. Plus, as network resources can be assigned by user groups, groups get what they need based on business requirements, and not according to how the users drive the network at any particular moment. Transferring high priority financial documents needn't be impacted by lower

priority graphic arts file transfers. Moreover, performance is generally much greater using switches than it is using routers, so these switches forward traffic at higher rates as well.

### **Better use of Server Resources**

With a VLAN-enabled adapter, a server can be a member of multiple VLANs. This reduces the need to route traffic to and from the server.

### **Reduced Costs**

Switches, not routers, typically implement VLANs. By reducing the dependency on routers, which are much more costly to deploy, organizations can reduce costs. In addition, the reduction in overhead costs associated with automated and simplified moves, additions and changes cuts costs even further.

### **Network Resource Assignment**

VLAN tagging provides a new and effective method for grouping users by function, and defining the bandwidth and network resources that can be used by them. This allows administrators to dedicate network resources by business need rather than by some floating, arbitrary means. So, network resources, like bandwidth, can both be assigned and managed on a very granular level, ensuring that each group or department gets what they need or pay for.

### **Enhanced Network Security**

VLANs create virtual boundaries that can only be crossed through a router. So standard, router-based security measures can be used to restrict access to each VLAN as required.