Printer Friendly Version
WEB LINK - http://www.networkmagazineindia.com/200205/primer.shtml

Virtually yours: VLAN

*Want more control on your data packets. Check out how VLANs can help you achieve this. by **Mahesh Rathod***

VLAN is a group of PCs, servers and other network resources that behave as if they were connected to a single, network segment

The IEEE has defined the 802.1q standard for VLAN, to ensure the interoperability of VLAN implementations between switches and NICs from different vendors

The rapid pace at which Information Technology changes has compelled many an IT manager to upgrade his/her knowledge on an ongoing basis. The new technologies and tools that emerge every now and then demand more network bandwidth, better workstations and faster applications. Network managers are under a lot of pressure to upgrade networks. Virtual LANs (VLANs) might be the very solution to these pressures and these networks can also improve over-all efficiency. Read on to find out how all this is possible.

What are VLANs?

VLANs can be defined as a group of devices on different physical LAN sections or on a single LAN section, which can interact with each other as if they were all on the same physical LAN segment. In other words, a VLAN is a group of PCs, servers and other network resources that behave as if they were connected to a single, network segment even though they are not, physically. To understand VLANs better, let's take an example of a two-floor network (Figure - 1), each floor having both the marketing and the accounts people.

If we assign all the account people (that is port 1,2 of switch #1, and port 4,5,6,7 of switch #2) to a single VLAN A, they will be able to share resources and bandwidth as if they were connected to the same section. Similarly we can form a VLAN B (port 3,4,5,6,7,8 of switch #1, and port 1,2,3,8 of switch #2) for the marketing people. A member of VLAN A may not be able to share resources of VLAN B and vice-versa.

Switches with VLAN capability can create the same division of the network into separate LANs or broadcast domains. It is similar to "color coding" your ports. In the figure-1, red ports can communicate with other red ports, and green ports can communicate with the other green ports.

VLAN memberships

Normally there are three ways of assigning a member to a VLAN. In a port based VLAN, the administrator assigns each port of a switch to a VLAN. For example, ports 6-10 might be assigned to the Manufacturing VLAN, ports 1-4 to the Sales VLAN and ports 4-6 to the Accounts VLAN. The main drawback of VLANs defined by port is that the systems manager must reconfigure VLAN membership when a user moves from one port to another.
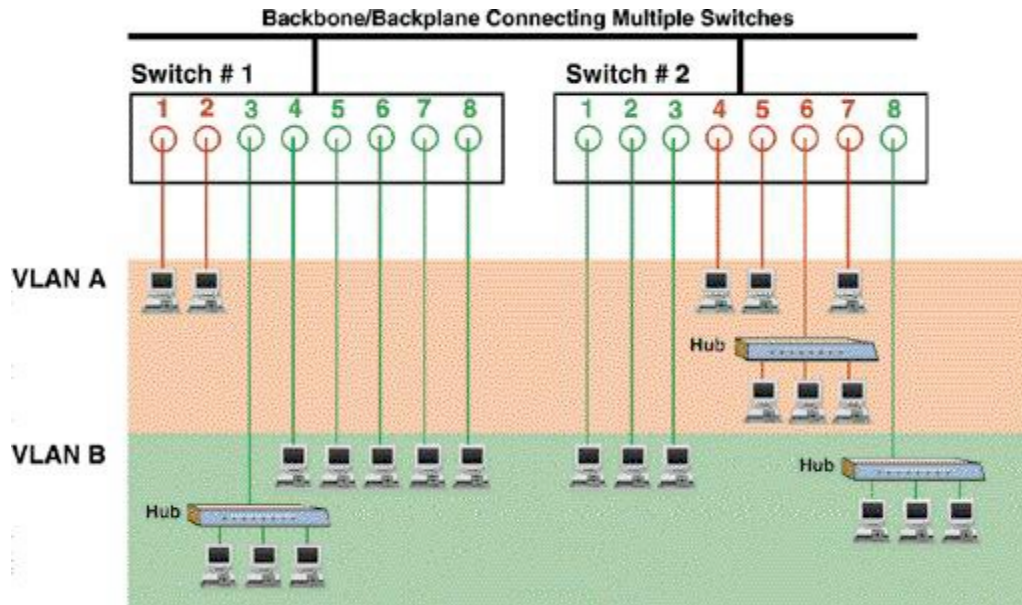
In MAC address-based VLANs, membership is defined by the source or destination MAC. The main advantage of this model is that the switch doesn't need to be reconfigured when a user makes a move to a different port. The main problem with MAC address-based VLANs is that a single MAC address cannot easily be a member of multiple VLANs.

VLANs based on Layer 3 information take into account protocol type (IP, NetBIOS) and Layer 3 addresses in determining VLAN membership. One of the main benefits of this method is that users can physically move their workstation without having to reconfigure their workstation's network address. The shortcoming of VLANs based on Layer 3 is the slow performance.

Yields from VLANs
There are significant benefits of using VLANs. The main reason for VLAN implementation is a reduction in the cost of handling user moves and changes. Any node moved or added, can be dealt with quickly and conveniently from the management console rather than the wiring closet. VLANs provide a flexible, easy and less costly way to modify logical groups in changing environments.

Forming 'virtual workgroups' is another compelling advantage of VLAN. VLANs provide independence from the physical topology of the network by allowing physically diverse workgroups to be logically connected within a single broadcast domain. It now becomes easier to add ports in new locations to existing VLANs if a department expands or relocates.

VLANs can increase performance of switched networks over shared media devices, by reducing the number of collision domains. Forming logical networks will improve performance by limiting broadcast traffic to users performing similar functions or within individual workgroups.

VLANs can enhance network security in a shared media network environment. In a switched network, frames are delivered only to the intended recipients, and broadcast

frames only to other members of the VLAN. This enables network managers to segment users requiring access to sensitive information into separate VLANs from the general user community regardless of physical distance.

What about VLAN standards?
Due to various types of VLAN definitions, each vendor has developed its own unique and proprietary VLAN solution and product. Hence switches from one vendor will not interoperate entirely with VLANs from other vendors.

The IEEE has defined 802.1q standard for VLAN, to ensure the interoperability of VLAN implementations between switches and NICs from different vendors. A second IEEE specification, 802.1p, defines the use of priority bits, which are part of the explicit VLAN tag as defined in 802.1q. There are two different VLAN models specified in the 802.1q specification: the shared model and the independent model.

Usage of VLANs
One of the main application areas for VLANs these days is Hosting Centers. Customers of hosting centers often avoid routes through the Internet (ISP networks) to access the hosting centers, because they want to minimize exposure to hackers. Data centers can reduce their investments by using VLANs to create a separate dedicated LAN to each customer's server with the same physical LAN infrastructure. Because each VLAN uses its own IP subnet, the customer's private address spaces can also be preserved.

Another application of VLAN is in Ethernet Metropolitan Area Network (MAN). Service providers use VLANs to provide logical segregation of the traffic from different customers within a metro area, thus creating the equivalent of an X.25 "closed user group."

Mahesh Rathod can be reached at rathodmp@hotmail.com