Understanding Virtual Local Area Networks

Surabhi Surendra Tambe

Final year Btech EXTC student, Electrical Engineering Department, VJTI, Matunga, Mumbai, India

Abstract: *The paper presents an overview for understanding Virtual Local Area Networks. It introduces the concept of VLANs, aims to discuss the purpose, main idea, design protocol, operation, benefits, applications and future scope of VLANs.*

Keywords: VLAN, IP, ISL, PC, IEEE 802.1Q.

I. Introduction

What is a VLAN?

In simple terms, a VLAN is a set of workstations within a LAN that can communicate with each other as though they were on a single, isolated LAN.The following points will clear the concept of VLANS further-

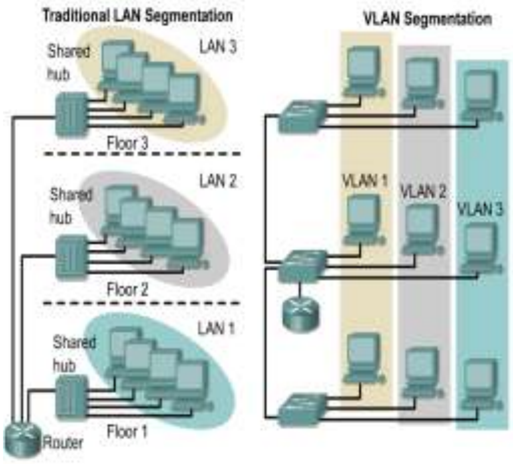
- broadcast packets sent by one of the workstations will reach all the others in the VLAN
- broadcasts sent by one of the workstations in the VLAN will not reach any workstations
- that are not in the VLAN
- broadcasts sent by workstations that are not in the VLAN will never reach workstations
- that are in the VLAN
- the workstations can all communicate with each other without needing to go through a
- gateway.
- IP and sending packets directly to the destination workstation—there would be no need
- to send packets to the IP gateway to be forwarded on.
- the workstations can communicate with each other using non-routable protocols.

II. PURPOSE OF VLANS

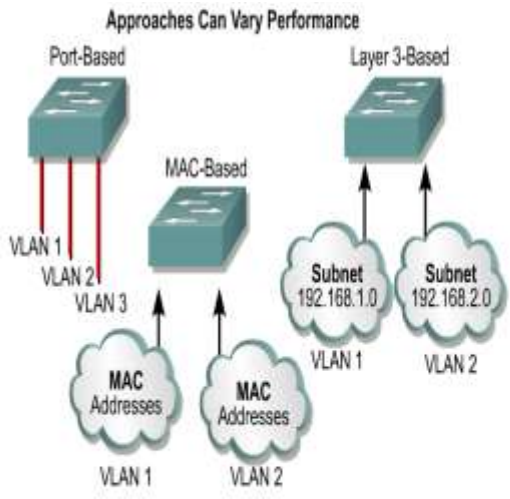
The basic reason for splitting a network into LANs is to reduce congestion on a large LAN. Initially LANs were very flat—all the workstations were connected to a single piece of coaxial cable, or to sets of chained hubs. In a flat LAN, every packet that any device puts onto the wire gets sent to every other device on the LAN. As the number of workstations on the typical LAN grew, they started to become hopelessly congested; there were just too many collisions, because most of the time when a workstation tried to send a packet it would find that the wire was already occupied by a packet sent by some other device.

VLANs can help reduce network traffic by forming multiple broadcast domains, to break up a large network into smaller independent segments with fewer broadcasts being sent to every device on the overall network.

III.MAIN IDEA

- **VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations.**
- VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain.
- Traffic should only be routed between VLANs.
- **VLANs provide segmentation based on broadcast domains.**
- VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.
- 

IV. TYPES OF VLAN



A. Protocol and Design

IEEE 802.1Q

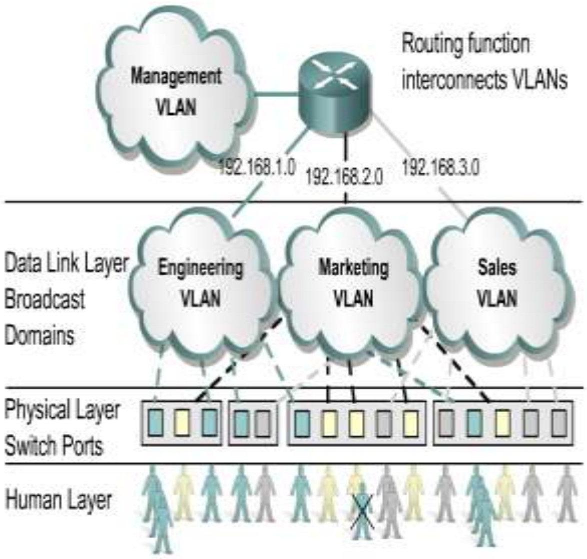
The protocol most commonly used today to configure VLANs is IEEE 802.1Q. The IEEE committee defined this method of multiplexing VLANs in an effort to provide multivendor VLAN support. Prior to the introduction of the 802.1Q standard, several proprietary protocols existed, such as Cisco's ISL (Inter-Switch Link) and 3Com's VLT (Virtual LAN Trunk).

B. VLAN Operation

Each switch port can be assigned to a different VLAN. Ports assigned to the same VLAN share broadcasts. **Static membership VLANs are called port-based and port-centric membership VLANs.** As a device enters the network, it automatically assumes the VLAN membership of the port to which it is attached. "The **default VLAN** for every port in the switch is the management VLAN. The management VLAN is always VLAN 1 **and may not be deleted."** All other ports on the switch may be reassigned to alternate VLAN.

VLAN Configuration involves the following:

- VLANs are assigned on the switch port. There is no "VLAN" assignment done on the host (usually).
- In order for a host to be a part of that VLAN, it must be assigned an IP address that belongs to the proper subnet.
- Assigning a host to the correct VLAN is a 2-step process:
- Connect the host to the correct port on the switch.
- Assign to the host the correct IP address depending on the VLAN memebership
- Tagging the data received on a LAN bridge from a workstation with a VLAN identifier provides information like the source of data,port at which data was received,the source MAC(Media Access control) field,source network address etc.



C. Benefits of using VLANs

The key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically.

This means that an administrator is able to do all of the following:

Easily move workstations on the LAN.
Easily add workstations to the LAN.
Easily change the LAN configuration.
Easily control network traffic.

VLANs provide **improved security by** addressing issues such as scalability and network management.

D. Applications of VLANs

1.Performance enhancement. Routers that forward data in software become a bottleneck as LAN data rates increase. Using switches and thus doing away with the routers removes this bottleneck.

2. **Implementation of virtual workgroups**. Because workstations can be moved from one VLAN to another just by changing the configuration on switches, it is relatively easy to put all the people working together on a particular project all into a single VLAN. They can then more easily share files and resources with each other.

3. **Greater flexibility.** If users move their desks, or just move around the place with their laptops, then, if the VLANs are set up the right way, they can plug their PC in at the new location, and still be within the same VLAN. This is much harder when a network is physically divided up by routers.

4. **Ease of partitioning off resources**: If there are servers or other equipment to which the network administrator wishes to limit access, then they can be put off into their own VLAN.

5.Reduced cost: Using switches on the VLAN to create broadcast domains,eliminates the need of expensive routers thereby reducing cost of the setup.

6. Security: When sensitive data is broadcasted on a network ,there are several risks and threats to the network. VLANs can minimize this threat by placing only those users on the network data on a VLAN with access and thus reducing chances of an intruder gaining access. Also control of broadcast domains, setting up firewalls, prohibition of access and alerting a network manager in case of an attack by an outsider can be achieved by implementation of VLANs.

E. Future Scope

- The future of VLANs is wide open to companies from 1000 plus employees to small businesses with 10 plus employees.
- VLANs will help reduce traffic ,increase security and make network management easier.
- Also there will be a reduction of cost to companies as employees will share the network data.

V. CONCLUSIONS

Thus, we can conclude that utilization of Virtual local area networks can surely simplify network management and also provide networks with improved security.

ACKNOWLEDGMENT

I would like to thank my college professor who taught me the TNM(Telecom Network Management) course as well as motivated me to select this topic .I would also like to thank my peers for constantly encouraging me and giving me critical reviews whenever needed.

REFERENCES

[1] 3GPP:Standards organization associated with ITU

[2] Mani Subramanium ,Network Management-Principles and Practices,2ndEdition,Pearson,2013

[3] www.cisco.com – Configuring VLANs from Catalyst 6500 12.2SX Software Configuration guide.

[4] VLAN –Sadhna Pal, Gyan Prakash Pal, IJSRET(International Journal of Scientific Research Engineering and Technology),Volume 1,Issue 10

[5] William Stallings ,Data and Computer Communications ,Prentice Hall,8th Edition,2006.