Novateur Publication's
International Journal of Innovation in Engineering, Research and Technology [IJIERT]
ICITDCEME'15 Conference Proceedings
ISSN No - 2394-3696

EVOLUTION OF VLAN

Manisha Barse
Department of E&TC, D. Y. Patil College of Engineering, Akurdi, Pune, India.

Rodney Manuel
Department of E&TC, D.Y.Patil College of Engineering, Akurdi, Pune, India.

ABSTRACT
Enterprise networks are large and complex and their designs must be frequently altered to adapt to changing organizational needs. The process of redesigning and reconfiguring enterprise networks is ad-hoc and error-prone, and configuration errors could cause serious issues such as network outages. Earlier, a Local Area Network (LAN) was defined as a network of computers located within the same area. Today, they are defined as a single broadcast domain. In this paper, we take a step towards systematic evolution of network designs in the context of virtual local area networks (VLANs).We focus on VLANs giving their importance and prevalence, the frequent need to change LAN designs, and the time-consuming and error-prone process of making changes. A virtual LAN, commonly known as VLAN, is a group of networking devices in the same broadcast domain logically. A VLAN is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same LAN segment. Network reconfiguration can be done through software instead of physically relocating devices. Network Resource is opened for every user in LAN. Considering administration and security, we must restrict them to some degree. Whatever the rank of LAN member is, most of them should be free of route when access to network. Virtual Local Area Network, being a new technique to settle broadcast containment and network security, has already become an important strategy in LAN solution. [3][4][5]

KEYWORDS: VLAN, broadcast domain

INTRODUCTION

A VLAN is a switched network that is logically segmented on an organizational basis, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they might be intermingled with other teams. Reconfiguration of the network can be done through software rather than by physically unplugging and moving devices or wires.
A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment; for example, LAN switches that operate bridging protocols between them with a separate bridge group for each VLAN.

The basic reason for splitting a network into VLANs is to reduce congestion on a large LAN. To understand this problem, we need to look briefly at how LANs have developed over the years. 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.
The LAN itself is referred to as a broadcast domain, because if any device within the LAN sends out a broadcast packet, it will be transmitted to all devices in that LAN, but not to devices beyond the LAN.As the number of workstations on the typical LAN grew, they started to become 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.[1][2][5]

ADVANTAGES

VLAN is the logical division of broadcast domain. It breaks down the broadcast domain, where one VLAN corresponds to one broadcast domain which in turn represents one network. VLAN has the following benefits:

1) Cost effective: The cost of user's moving and changing can be reduced as VLAN makes use of logical switches, thus making it cost effective.

2) Broadcast storm mitigation: Broadcasting traffic can be controlled effectively, and routed traffic can also be controlled. This can be achieved as VLAN reduces flooding of frames, due to which other domains bandwidth remains unaffected. This in turn improves the bandwidth usage.

3) Network administration: It is simplified and administration cost can also be cut down. As the interfaces are grouped in smaller broadcast domains, making project management and troubleshooting easier.

4) Security: It is improved because VLAN can limit the number of members under the same broadcast domain. VLAN reduces the interference and interaction between the broadcast domains, enhancing security.

5) Greater flexibility: If the user move the desk or just move around the place with the laptops, then if the VLAN's are setup the right way they can plug their laptop at the new location, and still be within the same VLAN. This is much harder when a network is physically divided up by the routers.

BACKGROUND:

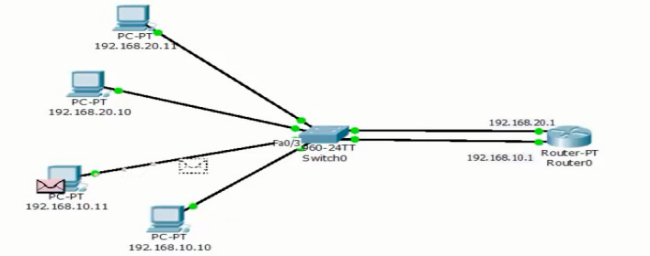
A Local Area Network (LAN) was originally defined as a network of computers located within the same area. Today, Local Area Networks are defined as a single broadcast domain. This means that if a user broadcasts information on his/her LAN, the broadcast will be received by every other user on the LAN. Broadcasts are prevented from leaving a LAN by using a router. The disadvantage of this method is routers usually take more time to process incoming data compared to a bridge or a switch. More importantly, the formation of broadcast domains depends on the physical connection of the devices in the network.

For sending a packet from one LAN network to the other, we need to make use of a router. A default Gateway needs to be set in order to transfer the packet between multiple LAN's. When a message is broadcasted from a PC, it gets delivered to all the other PC's in the same network. For instance, if a source wants to send a packet to the destination, it would require its MAC address. An ARP (Address Resolution Protocol) request is broadcasted to all the PC's in the same network to obtain the MAC address of destination PC, and only the destination PC sends back an ARP response to the source along with its MAC address.

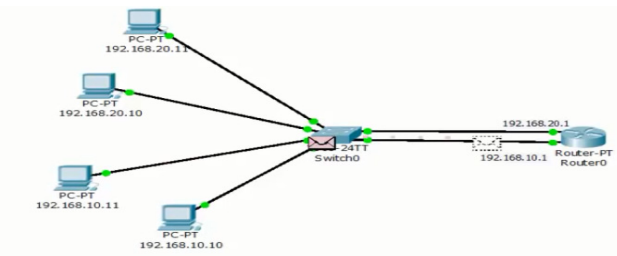
Let us have a look at the communication which takes place through LAN

The steps involved are as shown below:

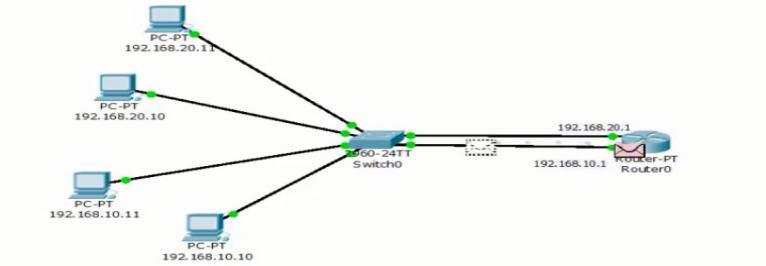
A PC having IP address 192.168.10.11 (source) located in LAN 1, wants to send a packet to another PC having IP address 192.168.20.11(destination) present in LAN 2.



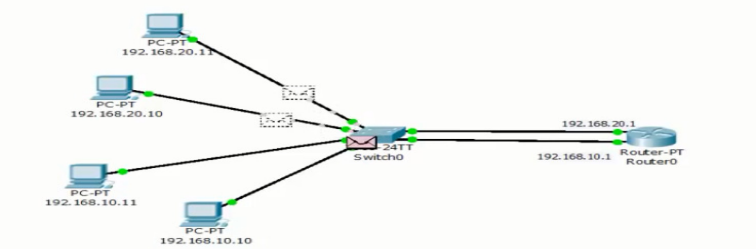
Step 1: An ARP request is first sent from source PC to the switch.



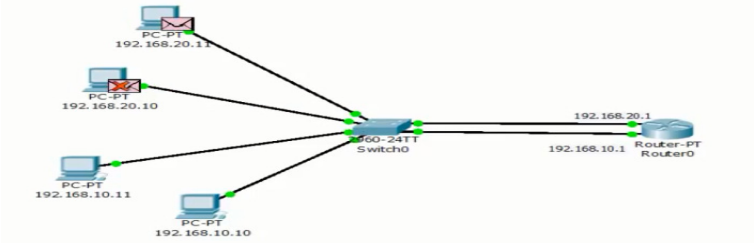
Step 2: The Switch then forwards the packet through the default gateway of 192.168.10.1 to the router.



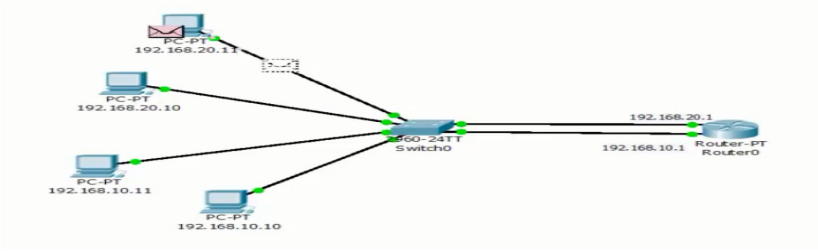
Step 3: The Router then sends the ARP request back to the switch.



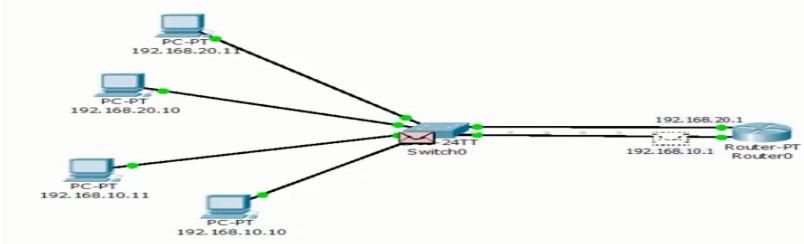
Step 4: The Switch broadcasts the ARP request to all the PC's present in LAN 2.



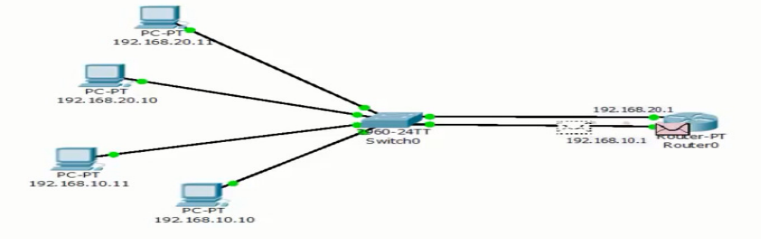
Step 5: After receiving the packages, only the destination PC recognizes the ARP and sends an ARP response back to the source.



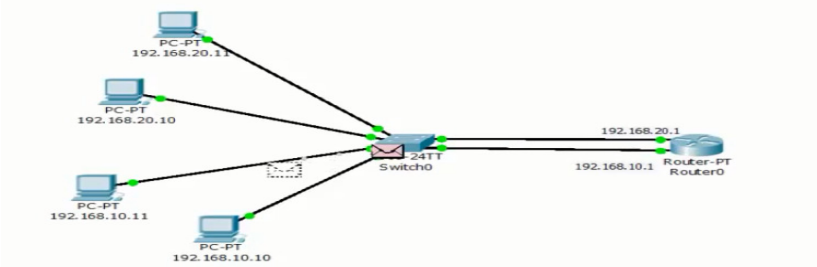
Step 6: The ARP response contains the MAC address of destination PC; it is send from the destination PC towards the Switch.



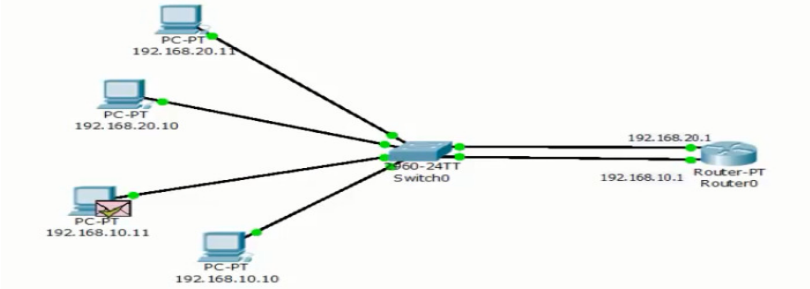
Step 7:The Switch then forwards the packet through the default gateway of the 192.168.20.11 to router.



Step 8: The router then sends back the ARP response to Switch.



Step 9: The ARP response is then sent from the Switch to the Source PC (192.168.10.11).



Step 10. The ARP response is then received by the source PC, it thus acquires the MAC address of the destination PC i.e. 192.168.20.11, and further transfer of data can take place.

Virtual Local Area Networks (VLAN's) were developed as an alternative solution to using routers to contain broadcast traffic.

In a traditional LAN, workstations are connected to each other by means of a hub or a repeater. These devices propagate any incoming data throughout the network. However, if two people attempt to send information at the same time, a collision will occur and all the transmitted data will be lost. Once the collision has occurred, it will continue to be propagated throughout the network by hubs and repeaters. The original information will therefore need to be resent after waiting for the collision to be resolved, thereby incurring a significant wastage of time and resources. To prevent collisions from traveling through all the workstations in the network, a bridge or a switch can be used. These devices will not forward collisions, but will allow broadcasts (to every user in the network) and multicasts (to a pre-specified group of users) to pass through. A router may be used to prevent broadcasts and multicasts from traveling through the network.

The workstations, hubs, and repeaters together form a LAN segment. A LAN segment is also known as a collision domain since collisions remain within the segment. The area within which broadcasts and multicasts are confined is called a broadcast domain or LAN. Thus a LAN can consist of one or more LAN segments. Defining broadcast and collision domains in a LAN depends on how the workstations, hubs, switches, and routers are physically connected together. This means that everyone on a LAN must be located in the same area

VLAN's allow a network manager to logically segment a LAN into different broadcast domain. Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together. Users on different floors of the same building, or even in different buildings can now belong to the same LAN.

VLAN's also allow broadcast domains to be defined without using routers. Bridging software is used instead to define which workstations are to be included in the broadcast domain. Routers would only have to be used to communicate between two VLAN's.

VLANs allow logical network topologies to overlay the physical switched infrastructure such that any arbitrary collection of LAN ports can be combined into an autonomous user group or community of interest. The technology logically segments the network into separate Layer 2 broadcast domains whereby packets are switched between ports designated to be within the same VLAN. By containing traffic originating on a particular LAN only to other LANs in the same VLAN, switched virtual networks avoid wasting bandwidth, a drawback inherent to traditional bridged and switched networks in which packets are often forwarded to LANs with no need for them. Implementation of VLANs also improves scalability, particularly in LAN environments that support broadcast- or multicast-intensive protocols and applications that flood packets throughout the network.[1][2][3][4][5]
The following figure illustrates the difference between traditional physical LAN segmentation and logical VLAN segmentation.

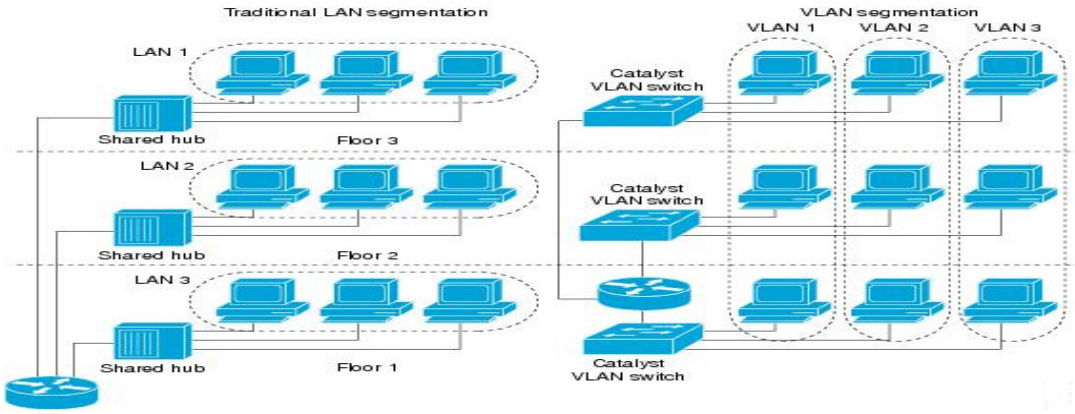


Figure1:LAN Segmentation and VLAN Segmentation

HOW A VLAN WORKS?

When a LAN bridge receives data from a workstation, it tags the data with a VLAN identifier indicating the VLAN from which the data came. This is called explicit tagging. It is also possible to determine to which VLAN the data received belongs using implicit tagging. In implicit tagging the data is not tagged, but the VLAN from which the data came is determined based on other information like the port on which the data arrived. Tagging can be based on the port from which it came, the source Media Access Control (MAC) field, the source network address, or some other field or combination of fields. VLAN's are classified based on the method used. To be able to do the tagging of data using any of the methods, the bridge would have to keep an updated database containing a mapping between VLAN's and whichever field is used for tagging. For example, if tagging is by port, the database should indicate which ports belong to which VLAN. This database is called a filtering database. Bridges would have to be able to maintain this database and also to make sure that all the bridges on the LAN have the same information in each of their databases. The bridge determines where the data is to go next based on normal LAN operations. Once the bridge determines where the data is to go, it now needs to determine whether the VLAN identifier should be added to the data and sent. If the data is to go to a device that knows about VLAN implementation (VLAN-aware), the VLAN identifier is added to the data. If it is to go to a device that has no knowledge of VLAN implementation (VLAN-unaware), the bridge sends the data without the VLAN identifier.
To understand VLAN more clearly let's take an example.

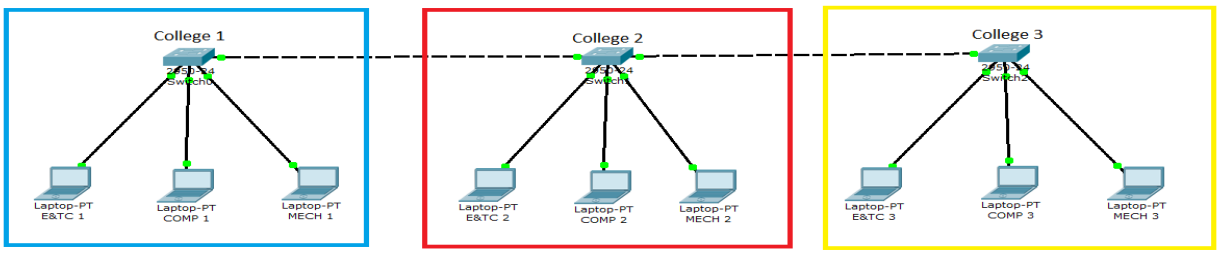


Figure2: LAN

- Our University has three colleges.
- All colleges are connected with black dotted links.

- College has three departments E&TC, Computer and Mechanical..
- E&TC department has three computers.
- Computer department has three computers.
- Mechanical department also has three computers.
- Each college has one PC from E&TC, Computer and Mechanical department.
- Each department has sensitive information and need to be separate from each other.

With default configuration, all computers share same broadcast domain.
With VLAN we could create logical boundaries over the physical network. Assume that we created three VLANs for our network and assigned them to the related computers.

- VLAN E&TC for E&TC department
- VLAN Comp for Computer department
- VLAN Mech for Mechanical department

Physically we changed nothing but logically we grouped devices according to their function. These groups [VLANs] need router to communicate with each other. Logically our network look likes following diagram.

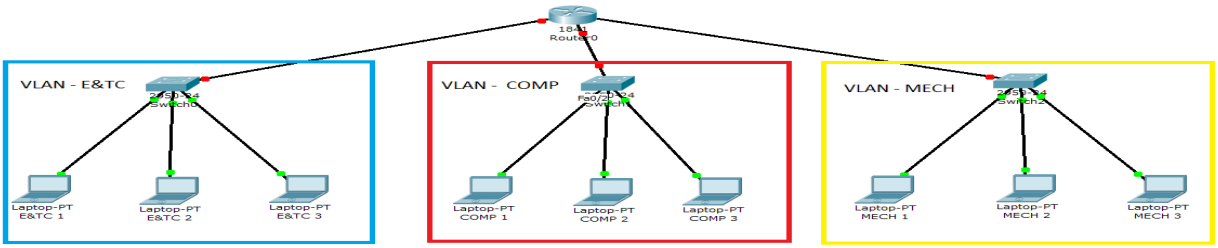


Figure3: VLAN

With the help of VLAN, we have separated our single network in three small networks. These networks do not share broadcast with each other improving network performance. VLAN also enhances the security. No department can access the other department directly. Different VLAN can communicate only via Router where we can configure wild range of security options.

VLAN MEMBERSHIP
VLAN membership can be assigned to a device by one of two methods. These methods decide how a switch will associate its ports with VLANs.
1) STATIC
Assigning VLANs statically is the most common and secure method. It is pretty easy to set up and supervise. In this method we manually assign VLAN to switch port. VLANs configured in this way are usually known as port-based VLANs.
Static method is the most secure method also. As any switch port that we have assigned a VLAN will keep this association always unless we manually change it. It works really well in a networking environment where any user movement within the network needs to be controlled.

2) DYNAMIC
In dynamic method, VLANs are assigned to port automatically depending on the connected device. In this method we have configure one switch from network as a server. Server contains device specific information like MAC address, IP address etc. This information is mapped with VLAN. Switch acting as server is known as VMPS (VLAN Membership Policy Server). Only high end switch can configured as VMPS. Low end switch works as client and retrieve VLAN information from VMPS.
Dynamic VLANs supports plug and play movability. For example if we move a PC from one port to another port, new switch port will automatically be configured to the VLAN which the user belongs. In static method we have to do this process manually

VLAN CONNECTIONS

During the configuration of VLAN on port, we need to know what type of connection it has. Switch supports two types of VLAN connection.

1) ACCESS LINK

Access link connection is the connection where switch port is connected with a device that has a standardized Ethernet NIC. Standard NIC only understand IEEE 802.3 or Ethernet II frames. Access link connection can only be assigned with single VLAN. That means all devices connected to this port will be in same broadcast domain.

For example, twenty users are connected to a hub, and we connect that hub with an access link port on switch, then all of these users belong to same VLAN. If we want to keep ten users in another VLAN, then we have to purchase another hub. We need to plug in those ten users in that hub and then connect it with another access link port on switch.

2) TRUNK LINK

Trunk link connection is the connection where switch port is connected with a device that is capable to understand multiple VLANs. Usually trunk link connection is used to connect two switches or switch to router. VLAN can span anywhere in network, which happens due to trunk link connection. Trunking allows us to send or receive VLAN information across the network. To support trunking, original Ethernet frame is modified to carry VLAN information.

Figure: Access Link and Trunk Link

IMPLEMENTING VLANS

At present, there are four general methods to group VLAN:

1) Grouping by port: Port grouping is the most common method in defining VLAN membership and its configuration is fairly straightforward. The primary limitation of defining VLAN by port is that network manager must reconfigure VLAN membership when a user moves from one port to another. For example, in a bridge with four ports, ports 1, 2, and 4 belong to VLAN 1 and port 3 belongs to VLAN 2

Table1: Assignment of ports to different VLAN'S

PORT	VLAN
1	1
2	2
3	2
4	1

2) Grouping by MAC address: VLAN based on MAC addresses enable network manager to move a workstation to a different physical location and have that workstation automatically retaining its VLAN membership. The main drawback is that every user must initially manually be configured to be in at least one VLAN, especially in a very large network where thousands of users must each be explicitly assigned to a particular VLAN.

Table2: Assignment of MAC addresses to different VLAN'S

MAC Address	VLAN
64-5A-04-A3-7C-7F	1
16-5A-04-B5-6D-7E	1
48-4B-06-E4-79-3E	2
56-6A-05-E2-42-2D	2

3) Grouping by network layer: VLAN based on network layer takes into account protocol type. It is particularly effective for TCP/IP networks. Since it doesn't need additional frame tagging to communicate VLAN membership information, it reduced regular transport overhead. But inspecting network addresses is more time consuming than looking at MAC addresses in frames.

Table3: Assignment of protocols to different VLAN'S

Protocol	VLAN
IP	1
IPX	2

4) Grouping by IP multicast: VLAN defined by IP multicast groups consider that all workstations that join an IP multicast group can be seen as members of the same VLAN. It has a high degree flexibility and can span routers and WAN. But it doesn't fit LAN because of its low efficiency.[3][4]

DISCUSSIONS

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.

What does it mean to say that they "communicate with each other as though they were on a single, isolated LAN"?

AMONG OTHER THINGS, IT MEANS THAT:

- 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 agate way. For example, IP connections would be established by ARPing for the destination 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.

Although VLAN is an emerging solution for the problems faced by the LAN, yet it is facing some problems like:

1) Ignored member individuality: Every member has his own characteristic and requirement for network resources although they are in the same workgroup. The behavior of each member is diversified especially in campus, research institute networks and so on.

2) Hard to obey 80/20 rule: In general, network traffic is reasonable when 80% traffic is local while 20% is remote or outside the workgroup. However, many requirements are crossed because of various and diversified work characters, such as hourly real time discussion among design department and factory, videoconference amid department leaders. The rule can be broken up too easily.

3) The concept of virtual workgroup may encounter some problems. For example, a user belongs to the VLAN of finance department, but in fact he is physically located in VLAN of market department. When he want to print some document locally, the print demand should traverse the routers connected the two VLAN. Although it can be avoided through reconfigure membership, this kind of trifles will torture administrator frequently.

4) Dynamic Communication: And their domain and lasting time are uncertain too. VLAN solutions in couldn't create and cancel VLAN according to application.[4]

The future work involves focusing on these issues and finding ways to implement VLAN in a much better and efficient way and expand the horizons for communication.

CONCLUSION

From the above analysis, we have studied various techniques by which VLAN can be implemented. Furthermore, we found out that VLAN based on service cannot only timely dynamically configure VLAN but distribute administration right to owners of network resources. VLAN based on service still leave much to be desired. We also came across various advantages of using VLAN's like reduction in the cost, controlling broadcast traffic, flexibility and security. In this paper, our primary contribution is to show thefeasibility and importance of a systematic approach to evolving VLAN designs in operational enterprise networks, consider issues at the design level. There are mainly two parts we need to do in near future. The first one is that let hardware to complete the function of VLAN schedule client program based on service, for it will be more transparent for users. We can choose embedded system or improved network card as our solutions. The second is to make Manager Server run more active and initiative. In this paper we studied characterization of VLAN related change activities of a large-scale operational campus network, and explanation of causes behind the need of switching to use of VLAN.
Future work also considers the techniques to redesign (not just evolve) VLANs, considering costs of reconfiguration in doing so. We shall also be exploring and extending our research to other domains such as evolution of routing designs.

REFERENCES

[1]http://computernetworkingnotes.com/switching-vlan-stp-vtp-dtp-ether-channels/vlan.html
[2] http://www.9tut.com/virtual-local-area-network-vlan-tutorial
[3]Overview of VLAN's (Virtual LANS), Allied Telesis, USA (2008)
[4] Xiaoying Wang, Hai Zhao, Mo Guan, Chengguang Guo, Jiyong Wang (2003). Research and Implementation of VLAN Based on Service, IEEE (2932-2936).
[5]Xin Sun, Yu-Wei E. Sung, Sunil D. Krothapalli, and Sanjay G. Rao(2010). A Systematic Approach for Evolving VLANDesigns, IEEE.