

VIRTUAL LOCAL AREA NETWORKS TECHNOLOGIES IMPLEMENTATION AND DEVELOPMENTS IN LAST FEW YEARS CLASSIFIED BY PORT, MAC ADDRESS AND LAN BASED PROTOCOL

^[1]Dr. UmeshSehgal, ^[2] Ms. Anu, ^[3]Ms.Prity

Asso. Prof. Arni University
M.Tech student Arni University

ABSTRACT

A virtual area network (VAN) is a network on which users are enabled to share a more visual sense of community through high band-width connections. As conceived by Pennell Media Online, an online directory for specialized networking products, a virtual area network is something like a metropolitan area network (MAN) or extended local area network (LAN) in which all users can meet over high- bandwidth connections, enabling "face-to-face" online "coffeehouses," remote medical diagnosis and legal consultation, and online corporate or extra corporate workgroups, focus groups, and conferences. A VAN requires multi-megabyte data flow and can be implemented through the use of Asymmetric Digital Subscriber Line but more likely through the installation of cable modem. Since the high-bandwidth connections imply a common infrastructure, the first VANs are likely to be local or regional. However, a VAN can also be national or international in geographic scope, assuming all users share similar capabilities. Virtual Local Area Networks or VLANs are one of the latest and coolest network technologies developed in the past few years, though have only recently started to gain recognition. The non-stop growth of Local Area Networks (LANs) and the need to minimize the cost for this expensive equipment, without sacrificing network performance and security, created the necessary soil for the VLAN seed to surface and grow into most modern networks. The truth is that VLANs are not as simple as most people perceive it to be. Instead they cover extensive material to be a whole study in itself as they contain a mixture of protocols, rules, and guidelines that a network administrator should be well aware of. Unfortunately, most documentation provided by vendors and other sites is inadequate or very shallow. They lightly touch upon the VLAN topic and fail to give the reader a good understanding on how VLANs really work and the wonderful things one can do when implementing them.

Keywords: - VLAN Software

INTRODUCTION TO VLANs

A Local Area Network (LAN) [2] 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. Virtual

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

Types of VLAN's

VLAN membership can be classified by port, MAC address, and protocol type.

1) Layer 1 VLAN: Membership by Port

Membership in a VLAN can be defined based on the ports that belong to the VLAN. For example, in a bridge with four ports, ports 1, 2, and 4 belong to VLAN 1 and port 3 belongs to VLAN 2 (see Figure 3).

Port	VLAN
1	1
2	1
3	2
4	1

The main disadvantage of this method is that it does not allow for user mobility. If a user moves to a different location away from the assigned bridge, the network manager must reconfigure the VLAN.

2) Layer 2 VLAN: Membership by MAC Address

Here, [1] membership in a VLAN is based on the MAC address of the workstation. The switch tracks the MAC addresses which belong to each VLAN (see Figure 4). Since MAC addresses form a part of the workstation's network interface card, when a workstation is moved, no reconfiguration is needed to allow the workstation to remain in the same VLAN. This is unlike Layer 1 VLAN's where membership tables must be reconfigured.

MAC Address	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1

Figure 1: Assignment of MAC addresses to different VLAN's.

The main problem with this method is that VLAN membership must be assigned initially. In networks with thousands of users, this is no easy task. Also, in environments where notebook PC's are used, the MAC address is associated with the docking station and not with the

notebook PC. Consequently, when a notebook PC is moved to a different docking station, its VLAN membership must be reconfigured.

3) Layer 3 VLAN: Membership by Protocol Type

VLAN membership for Layer 2 VLAN's can also be based on the protocol type field found in the Layer 2 header (see Figure5).

Protocol	VLAN
IP	1
IPX	2

Figure 2: Assignment of protocols to different VLAN's.

4) Layer 4 VLAN: Membership by IP SubnetAddress

Membership is based on the Layer 3 header. The network IP subnet address can be used to classify VLAN membership (see Figure 6)

IP Subnet	VLAN
23.2.24	1
26.21.35	2

Figure 3: Assignment of IP subnet addresses to different VLAN's

Although VLAN membership is based on Layer 3 information, this has nothing to do with network routing and should not be confused with router functions. In this method, IP addresses are used only as a mapping to determine membership in VLAN's. No other processing of IP addresses is done.

5) Higher LayerVLAN's

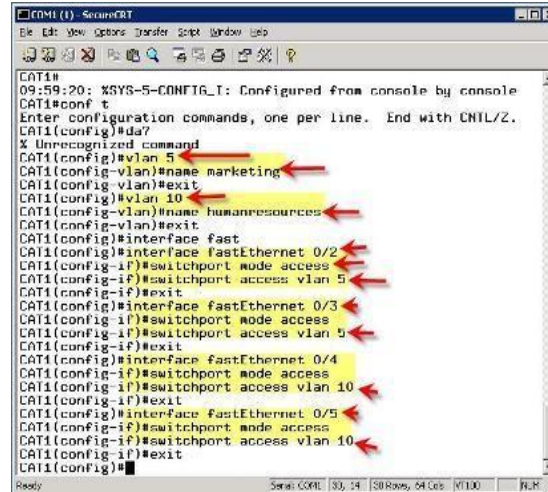
It is also possible to define VLAN membership based on applications or service, or any combination thereof. For example, file transfer protocol (FTP) applications can be executed on one [1] VLAN and telnet applications on another VLAN.

How do I create a VLAN?

Configuring VLAN's can vary even between different models of Cisco switches. Your goals, no matter what the commands are, are to:

- Create the newVLAN's
- Put each port in the properVLAN

Let's say we wanted to create VLAN's 5 and 10. We want to put ports 2 & 3 in VLAN 5 (Marketing) and ports 4 and 5 in VLAN 10 (Human Resources). On a Cisco 2950 switch, here is how you would do it:



```

COM1 (1) - SecureCRT
File Edit View Options Transfer Script Window Help
09:59:20: %SYS-5-CONFIG_I: Configured from console by console
CAT1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CAT1(config)#da?
% Unrecognized command
CAT1(config)#vlan 5
CAT1(config-vlan)#name marketing
CAT1(config-vlan)#exit
CAT1(config)#vlan 10
CAT1(config-vlan)#name humanresources
CAT1(config-vlan)#exit
CAT1(config)#interface fast
CAT1(config)#interface fastEthernet 0/2
CAT1(config-if)#switchport mode access
CAT1(config-if)#switchport access vlan 5
CAT1(config-if)#exit
CAT1(config)#interface fastEthernet 0/3
CAT1(config-if)#switchport mode access
CAT1(config-if)#switchport access vlan 5
CAT1(config-if)#exit
CAT1(config)#interface fastEthernet 0/4
CAT1(config-if)#switchport mode access
CAT1(config-if)#switchport access vlan 10
CAT1(config-if)#exit
CAT1(config)#interface fastEthernet 0/5
CAT1(config-if)#switchport mode access
CAT1(config-if)#switchport access vlan 10
CAT1(config-if)#exit
CAT1(config)#
  
```

At this point, only ports 2 and 3 should be able to communicate with each other and ports 4 & 5 should be able to communicate. That is because each of these is in its own VLAN. For the device on port 2 to communicate with the device on port 4,[2] you would have to configure a trunk port to a router so that it can strip off the VLAN information, route the packet, and add back the VLAN information.

VLAN SECURITY - MAKING THE MOST OF VLANS

When deploying VLANs, here are five key considerations to address:

1. Links on VLAN Switches

VLAN switches have two main types of links: access links and trunk links.

Access Links are the most common type of links on any VLAN capable switch. All network hosts connect to the switch's Access Links to gain access to the local network. These links are the ordinary ports found on every switch, but configured to access a particular VLAN.

Trunk Links are the links that connect two VLAN capable switches together. While an Access Link is configured to access a specific VLAN, a Trunk Link is almost always configured to carry data from all available VLANs.

2. Native VLAN, ISL and 802.1q

When a port on a switch is configured as an access link, it has access to one specific VLAN. Any network device connecting to it will become part of that VLAN.

Ethernet frames entering or exiting the port are standard Ethernet II type frames which are understood by the network device connected to the port. Because these frames belong only to one network, they are said to be “untagged” — meaning that they do not contain any information as to which VLAN they are assigned.

Trunk links on the other hand are a bit more complicated. Because they carry frames from all VLANs, it's necessary to somehow identify the frames as they traverse switches. This is called VLANtagging.

Two methods known for this job are ISL (Inter-Switch Link, a proprietary Cisco protocol) and IEEE 802.1q. Of the two, 802.1q is the most popular VLAN tagging method and is compatible among all vendors supporting VLANtrunking.

What might come as a surprise is that a trunk link can also be configured to act as an access link when a device (computer or switch) that does not support VLAN trunking connects to it. This means that if you have a trunk link on a switch and connect a computer, the port will automatically provide access to a specific VLAN. The VLAN in this case is known as the “native VLAN,” a common term that refers to the VLAN a trunk port is configured for when acting as an access link.

3. Virtual Trunk Protocol and VTPPruning

VTP is Cisco proprietary protocol that ensures all VLAN information held by the VTP Server, usually the core switch, is propagated to all network switches within the VTPdomain.

During initial network configuration, all switches are configured members of the same VTP domain. With the use of VTP, an IT administrator can create, delete or rename VLANs on the core switch. All information is then automatically sent to all members of the VTP domain. The VTP equivalent for other vendors, such as HP and Juniper, is the Garp VLAN Registration Protocol (GVRP), which has been fine-tuned in the recent years and includes many features implemented previously only in Cisco's VTP Protocol.

, ensures that unnecessary network traffic is not sent over trunk links. This is done by forwarding broadcasts and unknown unicast frames on a VLAN, over trunk links, only if the receiving end of the trunk has ports assigned to that VLAN.

In practice, this means that if a network broadcast occurred on VLAN5 for instance, and a particular switch did not have any ports assigned to VLAN5, it would never receive the broadcast traffic through its trunk link. This translates to a major discount in broadcast or multicast traffic received by end switches in a VLAN network.

5. Inter-VLAN Routing

Inter-VLAN routing, as the term implies, is all about routing packets between VLANs. This is perhaps one of the most important features found on advanced switches. Because inter-VLAN routing directs packets based on their Layer 3 information (the IP address), switches that perform this function are known as Layer 3 switches and, of course, are the most expensive. The core switch is commonly a Layer 3 switch. In cases where a Layer 3 switch is not available, this function can also be performed by a server with two or more network cards or a router, a method often referred to as “router on a stick.”

Because this is one of the most important aspects of a VLAN network, the Layer 3 switch must have a fast switching fabric (measured in Gbps) and provide advanced capabilities such as support for routing protocols, advanced access-lists and firewall. The Layer 3 switch can offer outstanding protection for a VLAN network but can also be a network administrator’s worst nightmare if not properly configured.

6. Securing VLAN Devices

Even though many administrators and IT managers are aware of VLAN technologies and concepts, that doesn't necessarily hold true when it comes to VLAN security.

The first principle in securing a VLAN network is physical security. If an organization does not want its devices tampered with, physical access must be strictly controlled. Core switches are usually safely located in a data centre with restricted access, but edge switches are often located in exposed areas.

Just as physical security guidelines require equipment to be in a controlled space, VLAN-based security requires the use of special tools and following a few best security practices to achieve the desired result.

CONCLUSION

As we have seen there are significant advances in the field of networks in the form of VLAN's which allow the formation of virtual workgroups, better security, improved performance, simplified administration, and reduced costs. VLAN's are formed by the logical segmentation of a network and can be classified into Layer1, 2, 3 and higher layers. Only Layer 1 and 2 are specified in the draft standard 802.1Q. Tagging and the filtering database allow a bridge to determine the source and destination VLAN for received data. VLAN's if implemented effectively, show considerable promise in future networking solutions.

REFERENCES

- 1) IEEE, ``Draft Standard for Virtual Bridge Local Area Networks," P802.1Q/D1, May 16, 1997, This is the draft standard for VLAN's which covers implementation issues of Layer 1 and 2VLAN's.
- 2) IEEE, ``Traffic Class Expediting and Dynamic Multicast Filtering," 802.1p/D6, April 1997,This is the standard for implementing priority and dynamic multicasts. Implementation of priority in VLAN's is based on thisstandard.

IJAER