Implementation of Virtual Local Area Network using network simulator

Sarah Yahia Ali
Department of Computer Engineering Techniques, Dijlah University College, Iraq

ABSTRACT
Large corporate environments, and for that matter healthcare sites, comprise multiple departments which can be segmented into separate layer-2 LANs. An efficient and cost effective means of accomplishing this is through the use of inter-connected VLANs. A virtual local area network (VLAN) is defined as a local area network configured by software, not by physical wiring.

VLANs 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. VLANs represent an alternative solution to routers for broadcast containment, since VLANs allow switches to also contain broadcast traffic. With the implementation of switches in conjunction with VLANs, each network segment can contain as few as one user (approaching private port LAN switching), while broadcast domains can be as large as 1,000 users or perhaps even more. This paper present, in details, exactly what a VLAN is and how VLAN memberships are used in a switched network.

Keywords - VLAN, Router, Switch, Network, Routing, Hosts.

1. INTRODUCTION
By default, switches break up collision domains and routers break up broadcast domains. By creating virtual local area network (VLAN), broadcast domains break up in a pure switched internetwork. A VLAN is a logical group of network users and resources connected administratively defined ports on a switch. When VLANs created, it will be the ability to create smaller broadcast domains within layer 2 switched internetworks by assigning different ports on the switch to different sub networks. A VLAN is treated like its own subnet or broadcast domain, meaning that frames broadcast onto the network are only switched between the ports logically grouped within the same VLAN. By default, hosts in a specific VLAN cannot communicate with hosts that are members of another VLAN, so for inter-VLAN communication router is needed [1].

In Figure (1) we see Host A sending out a broadcast and all ports on all switches forwarding it all except the port that originally received it.

Now check out Figure (2). It pictures a switched network and shows Host A sending a frame with Host D as its destination. What’s important is that, as you can see, that frame is only forwarded out the port where Host D is located. This is a huge improvement over the old hub networks, unless having one collision domain by default is what you really want.

Now you already know that the largest benefit you gain by having a layer 2 switched networks is that it creates individual collision domain segments for each device plugged into each port on the switch. This scenario frees us from the Ethernet distance constraints, so now larger networks can be built. But often, each new advance comes with new issues. For instance, the larger the number of users and devices, the more broadcasts and packets each switch must handle [2].

VLAN implementation combines Layer 2 switching and Layer 3 routing technologies to limit both collision domains and broadcast domains, and can also be used to provide security by creating the VLAN groups according to function and by using routers to communicate between VLANs.

A physical port association is used to implement VLAN assignment. And the communication between VLANs can occur only through the router. This limits the size of the broadcast domains and uses the router to
determine whether one VLAN can talk to another VLAN [3].

If create a virtual LAN (VLAN), then can solve many of the problems associated with layer 2 switching with VLANs [4]. VLANs simplify network management:

- Network adds, moves, and changes are achieved with ease by just configuring a port into the appropriate VLAN.
- A group of users that need high level of security can be put into its own VLAN so that users outside of the VLAN cannot communicate with them.
- As a logical grouping of users by function, VLANs can be considered independent from their physical or geographic locations.
- VLANs greatly enhance network security.
- VLANs increase the number of broadcast domains while decreasing their size [1].

II. DEFINITION OF VLAN

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 that shown in Figure (3) [5].

VLAN's also allow a network manager to logically segment a LAN into different broadcast domains, see Figure (4). 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 [5].
III. TYPES OF VLAN'S

♦ Port-based VLAN

VLAN membership can be defined in several different ways, which is one of the reasons they can be confusing. The simplest way is to assign specific ports on a switch to VLANs. For example, ports 1, 2, 7, and 8 on an 8-port switch make up VLAN A, while ports 3, 4, 5, and 6 make up VLAN B. If an assigned switch port is connected to a shared segment - one with multiple nodes - all those nodes will be part of the VLAN, along with the nodes on other ports assigned to that VLAN. This VLAN segmentation is basically a matter of electronically isolating the ports of each VLAN.

Port grouping is the most popular method of defining VLAN membership, and configuration is fairly straightforward. However, the primary limitation of defining VLANs by port is that the network manager may have to reconfigure VLAN membership when a user moves from one port to another [6].

♦ MAC Address-based VLAN

MAC address-based VLAN has a different set of advantages and disadvantages. In this method, switches maintain tables of MAC addresses with their VLAN membership. With this form of membership, the nodes on a shared segment need not belong to the same VLAN. Because MAC addresses are hardwired into the Network Information Cards (NICs), this Layer 2 VLAN definition has the advantage of portability. Wherever a workstation or laptop is plugged in across the switched network, the switches will recognize it as a member of the assigned VLAN. This is especially useful for a WIFI connected switch port.

The disadvantage of MAC address-based VLAN solutions is the requirement that all users must initially be configured to be in at least one VLAN. Only after that initial manual configuration, the automatic VLAN grouping of users is possible. The manual VLAN configuration has to be repeated, if more than one switch is used. The disadvantage of having to configure VLAN membership becomes apparent in very large networks where thousands of users must each be explicitly assigned to a particular VLAN [6].

♦ Layer 3-based VLANs

VLANs can also be defined by their network or Layer 3 addresses. Many network managers, frustrated by the administrative overhead that comes with highly changeable networks configured with IP, could happily replace their existing subnet structure with VLANs. Once the node's VLAN membership is defined, the VLAN handles everything, even if the node is moved to a port connected to a different subnet or if the IP addresses need to be reassigned.

Layer 3-based VLANs take into account protocol type (if multiple protocols are supported) or network-layer address (for example, subnet address for TCP/IP networks) in determining VLAN membership. There are several advantages to defining VLANs at Layer 3. First, it enables partitioning by protocol type. This may be an attractive option for network managers who are dedicated to a service - or application-based VLAN strategy. Second, users can physically move their workstations without having to reconfigure each workstation’s network address a benefit primarily for TCP/IP users. Third, defining VLANs at Layer 3 can eliminate the need for frame-tagging in order to communicate VLAN membership between switches, reducing transport overhead [6].

IV. BENEFITS OF VLANS

* Performance

In networks where traffic consists of a high percentage of broadcasts and multicasts, VLAN's can reduce the need to send such traffic to unnecessary destinations.

* Formation of Virtual Workgroups

It is common to find cross-functional product development teams with members from different departments such as marketing, sales, accounting, and research. These workgroups are usually formed for a short period of time. With VLAN's it is easier to place members of a workgroup together. Without VLAN's, the only way this would be possible is to
physically move all the members of the workgroup closer together.

* Simplified Administration

Seventy percent of network costs are a result of adds, moves, and changes of users in the network. Every time a user is moved in a LAN, recabling, new station addressing, and reconfiguration of hubs and routers becomes necessary.

Some of these tasks can be simplified with the use of VLAN's. If a user is moved within a VLAN, reconfiguration of routers is unnecessary. In addition, depending on the type of VLAN, other administrative work can be reduced or eliminated.

* Reduced Cost

VLAN's can be used to create broadcast domains which eliminate the need for expensive routers.

* Security

Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data, on a VLAN can reduce the chances of an outsider gaining access to the data. VLAN's can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion [5].

V. VLAN TRUNKING PROTOCOL (VTP)

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain (also called a VLAN management domain) is made up of one or more network devices that share the same VTP domain name and that are interconnected with trunks [7].

The basic goals of VLAN Trunking Protocol (VTP) are to manage all configured VLANs across a switched internetwork and to maintain consistency throughout that network VTP allows you to add, delete, and rename VLANs information that is then propagated to all other switches in the VTP domain. Here’s a list of some of the cool features VTP has to offer:

- Accurate tracking and monitoring of VLANs
- Dynamic reporting of added VLANs to all switches in the VTP domain
- Plug and Play VLAN adding.

Before can get VTP to manage VLANs across the network, must have to create a VTP server. All servers that need to share VLAN information must use the same domain name, and a switch can be in only one domain at a time. So basically, this means that a switch can only share VTP domain information with other switches if they’re configured into the same VTP domain. By use a VTP domain if have more than one switch connected in a network, but if have got all switches in only one VLAN, just don’t need to use VTP. Do keep in mind that VTP information is sent between switches only via a trunk port [2].

Before create VLANs, you must decide whether to use VTP in your network. With VTP, you can make configuration changes centrally on one or more network devices and have those changes automatically communicated to all the other network devices in the network [7].

VI. DESIGN AND IMPLEMENTATION OF VLAN

The designed network is the model of the college consists of several sections. Each section represents VLAN, where engineering department represents VLAN4 with IP address 192.168.10.0 255.255.255.0 (Eng.) and the department of Law represents VLAN5 have IP address 172.16.1.0 255.0.0.0 (law) while the department of Business Administration represents VLAN6 with IP address 10.0.0.0 255.0.0.0 (manage.) and finally the department of Science represents VLAN 7 with IP address 192.168.20.0 255.255.255.0 (snc.).

This network is shown in the Figure (5) consist of four switches whereas the connector line among them called trunk. The trunk which is located between switch 1 and switch 2 have VLAN 1 with IP address 192.1.100.0 255.255.255.0 , while the trunk which is located between switch 2 and switch 3 have VLAN 2 with IP address 192.30.100.0 255.255.255.0 and the trunk which is located between switch 2 and switch 4 that have VLAN 3 with IP address 172.16.100.0 255.255.0.0
VII. DISTRIBUTING OF VLANS

Where it is selected each node of the switch to configure VLAN as shown in the groups below:

- **Department of Engineering VLAN 4**
  - PC1: 192.168.10.1 Subnet 255.255.255.0
  - PC4: 192.168.10.2 Subnet 255.255.255.0
  - PC8: 192.168.10.3 Subnet 255.255.255.0
  - PC12: 192.168.10.4 Subnet 255.255.255.0

- **Department of Law VLAN 5**
  - PC0: 172.16.1.1 Subnet 255.255.0.0
  - PC5: 172.16.1.2 Subnet 255.255.0.0
  - PC9: 172.16.1.3 Subnet 255.255.0.0
  - PC13: 172.16.1.4 Subnet 255.255.0.0

- **Department of Science VLAN 7**
  - PC3: 192.168.20.1 Subnet 255.255.255.0
  - PC7: 192.168.20.2 Subnet 255.255.255.0
  - PC11: 192.168.20.3 Subnet 255.255.255.0
  - PC15: 192.168.20.4 Subnet 255.255.255.0

VIII. RESULTS

When we send a message from computer 1 to computer 0 led to a failure because the two on the same switch but the difference VLANs that shown in the following Figure (6).

While we send a message from computer 1 to computer 8 appears success of the transmitter with the process different switches but the same VLAN, and transfer the message between 2 to 14 in the same case.

![Figure (6) result of sending messages](image-url)

When ping PC10 in PC6 appearing successful the ping without lost because PC10 and PC6 in the same VLAN that shown in the Figure (7).

![Figure (7) successful ping](image-url)

While the ping PC4 with PC6 that is failure ping lets to all message is lost that shown in the Figure (8).
IX. CONCLUSION

VLANs are in affective means of portioning a larger LAN into manageable subsets. VLANs restrict the broadcast domain improve performance and security and are ideal for isolating industrial automation systems from IT systems while retaining the plants structural wiring. The simplest of VLANs to implement are port VLANs but the most effective VLAN scheme is the IEEE 802.1Q VLAN tagging standard that improves mobility by allowing a user to potentially access any VLAN from any point on the LAN.

X. REFERENCES


