www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-1, Issue-4, Oct- 2013
Review Paper

Int. J. Sci. Res. in
Network Security
and Communication

ISSN: 2321-3256

Virtual Local Area Network Technology

Shivappa M Metagar[1*] R.G.Hiregouder [2] and Hare Ram Sing[3]

[1]Department of CSE, W.I.T Solapur*
[2] Department of CSE,T.K.I.E.T Warana Nagar
[3] Raju Gandhi Institute of Technology Bangalore

Received: 12 September 2013 Revised: 26 September 2013 Accepted: 15 October 2013 Published: 30 October 2013

Abstract- VLANs are one of the important technologies is widely used in enterprise networks to improve Ethernet capability and support network policies. However, manuals and textbooks, offer very little information about how VLANs are actually used in practice in different fields. Through discussions with network administrators and analysis of configuration data, we describe how three university campuses and one academic department use VLANs to achieve a variety of goals. We argue that VLANs are ill-suited to some of these goals (e.g., VLANs are often used to realize access control policies, but constrain the types of policies that can be expressed). Furthermore, the use of VLANs leads to significant complexity in the configuration of network devices.

Key Words- Computer, Virtual Devices, LAN, End users

I. INTRODUCTION

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. Virtual Local Area Networks (VLAN's) [1]were developed as an alternative solution to using routers to contain broadcast traffic.

What are VLAN's? 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 (see *Figure*1).

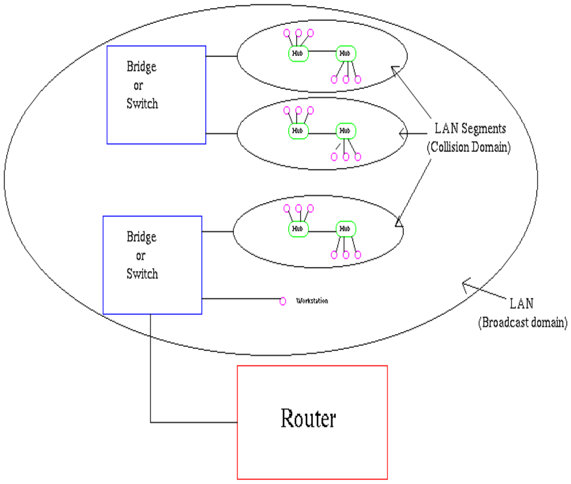

Figure:1 Physical view of a LAN.

VLAN's allow a network manager to logically segment a LAN into different broadcast domains (see *Figure*2). 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.

Corresponding Author: Shivappa M Metagar

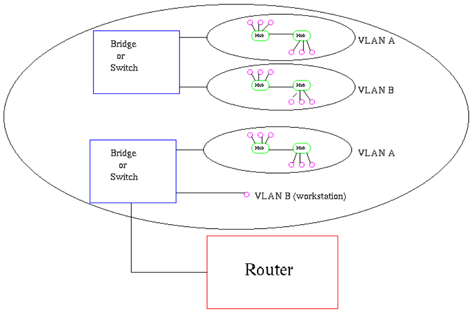

Figure:2 physical view

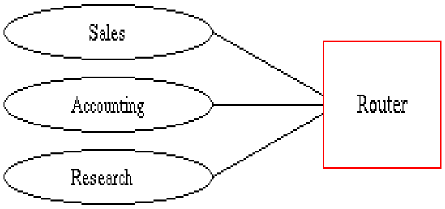

Figure:3 Logical view.

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 .

II. RELATED WORK

Why use VLAN's? VLAN's offer a number of advantages over traditional LAN's. They are:

1) 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. For example, in a broadcast domain consisting of 10 users, if the broadcast traffic is intended only for 5 of the users, then placing those 5 users on a separate VLAN can reduce traffic

Compared to switches, routers require more processing of incoming traffic. As the volume of traffic passing through the routers increases, so does the latency in the routers, which results in reduced performance. The use of VLAN's reduces the number of routers needed, since VLAN's create broadcast domains using switches [3] instead of routers.

2) Formation of Virtual Workgroups

Nowadays, 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. During this period, communication between members of the workgroup will be high. To contain broadcasts and multicasts within the workgroup, a VLAN can be set up for them. 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.

However, virtual workgroups do not come without problems. Consider the situation where one user of the workgroup is on the fourth floor of a building, and the other workgroup members are on the second floor. Resources such as a printer would be located on the second floor, which would be inconvenient for the lone fourth floor user.

Another problem with setting up virtual workgroups is the implementation of centralized server farms, which are essentially collections of servers and major resources for operating a network at a central location. The advantages here are numerous, since it is more efficient and cost-effective to provide better security, uninterrupted power supply, consolidated backup, and a proper operating environment in a single area than if the major resources were scattered in a building. Centralized server farms can cause problems when setting up virtual workgroups if servers cannot be placed on more than one VLAN. In such a case, the server would be placed on a single VLAN and all other VLAN's trying to access the server would have to go through a router; this can reduce performance.

3) 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. However the full power of VLAN's will only really be felt when good management tools are created which can allow network managers to drag and drop users into different VLAN's or to set up aliases.

Despite this saving, VLAN's add a layer of administrative complexity, since it now becomes necessary to manage virtual workgroups.

4) Reduced Cost

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

5) 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.

III. WORKING OF VLAN

When a LAN bridge[2] 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.

In order to understand how VLAN's work, we need to look at the types of VLAN's, the types of connections between devices on VLAN's, the filtering database which is used to send traffic to the correct VLAN, and tagging, a process used to identify the VLAN originating the data[5].

VLAN Standard: IEEE 802.1Q Draft Standard

There has been a recent move towards building a set of standards for VLAN products. The Institute of Electrical and Electronic Engineers (IEEE) is currently working on a draft standard 802.1Q for VLAN's[5]. Up to this point, products have been proprietary, implying that anyone wanting to install VLAN's would have to purchase all products from the same vendor. Once the standards have been written and vendors create products based on these standards, users will no longer be confined to purchasing products from a single vendor. The major vendors have supported these standards and are planning on releasing products based on them. It is anticipated that these standards will be ratified later this year.

IV. ANLYSIS STEPS

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

1) Layer 1 VLAN: Membership by Port

Port	VLAN
1	1
2	1
3	2
4	1

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).

The main disadvantage[4] 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, 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*4: 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 2 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 *Figure*5).

Protocol	VLAN
IP	1
IPX	2

*Figure*5: Assignment of protocols to different VLAN's.

4) Layer 3 VLAN: Membership by IP Subnet Address

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*6: 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.

In Layer 3 VLAN's, users can move their workstations without reconfiguring their network addresses. The only problem is that it generally takes longer to forward packets using Layer 3 information than using MAC addresses.

5) Higher Layer VLAN'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 VLAN and telnet applications on another VLAN.

The 802.1Q draft standard defines Layer 1 and Layer 2 VLAN's only. Protocol type based VLAN's and higher layer VLAN's have been allowed for, but are not defined in this standard. As a result, these VLAN's will remain proprietary.

V. TYPES OF CONNECTIONS & DATA FLOW DIAGRAMS:

Devices on a VLAN can be connected in three ways based on whether the connected devices are VLAN-aware or VLAN-unaware. Recall that a VLAN-aware device is one which understands VLAN memberships (i.e. which users belong to a VLAN) and VLAN formats.

1) Trunk Link

All the devices connected to a trunk link, including workstations, must be VLAN-aware. All frames on a trunk link must have a special header attached. These special frames are called tagged frames (see *Figure*7).

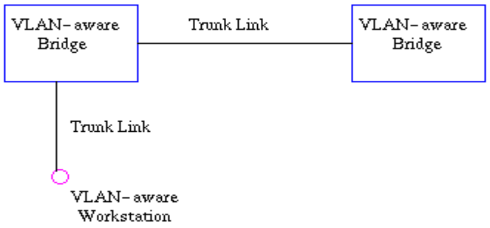

*Figure*7: Trunk link between two VLAN-aware bridges.

2) Access Link

An access link connects a VLAN-unaware device to the port of a VLAN-aware bridge. All frames on access links must be implicitly tagged (untagged) (see *Figure*8). The VLAN-unaware device can be a LAN segment with VLAN-unaware workstations or it can be a number of LAN segments containing VLAN-unaware devices (legacy LAN).

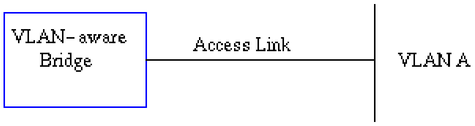

Figure 8: Access link between a VLAN-aware bridge and a VLAN-unaware device.

3) Hybrid Link

This is a combination of the previous two links. This is a link where both VLAN-aware and VLAN-unaware devices are attached (see *Figure*9). A hybrid link can have both tagged and untagged frames, but *all*the frames for a specific VLAN must be either tagged or untagged.

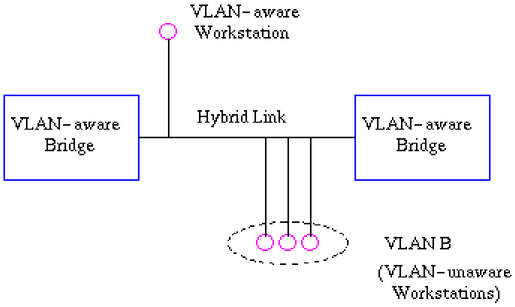

*Figure*9: Hybrid link containing both VLAN-aware and VLAN-unaware devices.

It must also be noted that the network can have a combination of all three types of links

.

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]. Umesh Kumar Singh, ShivlalMewada, Lokesh Laddhani & Kamal Bunkar, "An Overview & Study of Security Issues in Mobile Ado Networks", International Journal of Computer Science and Information Security (IJCSIS) USA, Volume-9, No.4, pp (106-111), April 2011.

[2]. 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 2 VLAN's.

[3]. Mathias Hein, David Griffiths, Orna Berry, ``Switching Technology in the Local Network: From LAN to Switched LAN to Virtual LAN," February 1997,Textbook explanation of what VLAN's are and their types.

[4]. Susan Biagi, "Virtual LANs," Network VAR v4 n1 p. 10- 12, January 1996, An Overview of VLAN's, advantages, and disadvantages.

[5]. David J. Buerger, ``Virtual LAN cost savings will stay virtual untilnetworking's next era," Network World, March 1995, A short summary on VLAN's.

[6]. 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 this standard.

BIBILOGRAPHY

SHIVAPPA M METAGAR received B.E. degree (Computer Science & Engineering) in 2010 from KBNCE, Gulbarga and M.Tech (Digital Communication and Networking) in 2012 from BTLIT, Bangalore. He is presently Working as Assistant Professor in the department of CSE, W.I.T Solapur, Maharastra. His research interests are in the area of Networks, Network Security, Data Mining, Web Technology and Image Processing.

R. G. HIREGOUDAR received B.E. degree (Computer Science & Engineering) in 2008 from BEC, Bagalkot and M.Tech (Computer Network Engineering) in 2012 from BITM, Bellary. He is presently Working as Assistant Professor in the department of CSE, T.K.I.E.T Warana nagar, Maharastra. His research interests are in the area of Networks, Network Security, Wireless sensor network, Web Technology and Image Processing.

HARE RAM SING received B.E. degree (Computer Science & Engineering) in 2008 from JSSATE, Bangalore.and M.Tech (Computer Science & Engineering) in 2012 from BTLIT, Bangalore. He is presently working as Lecturer in the department of ISE, RGIT, Bangalore. His research interests are in the area of Networks, Network Security, Natural Language Processing,, Data Mining, Operating System, Web Technology and Image Processing.