Study on VLAN in Wireless Networks

Rajul Chokshi and Dr. Chansu Yu
Department of Electrical and Computer Engineering
Cleveland State University
Cleveland, Ohio 44115

April 30, 2007

Abstract

This technical report is basically on how VLAN works in wireless networks and how its creates VLAN and also the deployment of VLAN in wireless environment. Its also includes some advantages and disadvantages of this technique. this technical report also includes how traffic is passing between VLAN at different layer switch and also its shows trunking of the VLAN. It includes basic security and enhanced security too.

1. Introduction

A virtual LAN is a broadcast domain created by one or more switches. The switch creates a VLAN simply by putting some interfaces in one VLAN and some in other. So basically using of all ports on a switch and forming a one broadcast domain, the switch separate them into many. Without VLAN a switch treats all interfaces on the switch as being in the same broadcast domain- it means all connected devices are in the same LAN. So we can say that switch creates multiple broadcast domains. Now here the basic idea has been shown in two figures. Fig1[4] show that there is no VLAN and two separate broadcast domains has been created by two switches. While Fig 2[4] shows multiple broadcast domain has created by single switch. So there are some useful motivations that motivates to use VLANs:

- To reduce overhead by limiting the size of each broadcast domain.
- Also making better security by putting sensitive devices on separate VLAN.
- Also making traffic special traffic separate than main

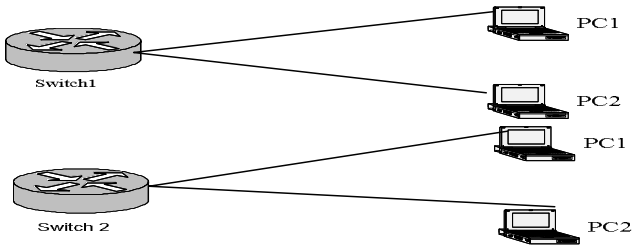

Fig1. Network with two broadcast domains and No VLAN [4]

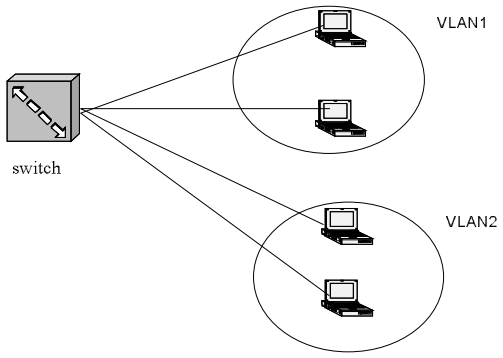

Fig2. Network with two VLANs using one switch [4]

2. Wireless Components:
The list of components needed for WLAN is short. Only wireless NIC(Network Interface Card) and Access Point(AP) are needed for communication to take place.

Wireless NIC: the hardware that allows a computer to be connected to a wired network is called network interface card. Also called a network adapter. A NIC is the device that connects the computer to the network so that it can send and receive the data. A wireless NIC performs the same functions as a wired NIC with one major exception. There is no port for wire connection to the network. In its place there is an antenna to send and receive RF signal. When wireless NIC transmit;

- **(i)** change the computers internal data from parallel to serial transmission.
- **(ii)** Divide the data into packets and attach the sending and receiving computer's address.
- **(iii)** Determine when to send the data.
- **(iv)** Transmit the packet.

Access Point: this device is consists of three major parts. First it contains an antenna and radio transmitter and receiver to send and receive signals. Second ot has an RJ-45 wired network interface that allows it to connect by cable to standard wired network. Third is special bridging software is installed.

An access point has two basic functions: first the access point acts as a base station for the wireless network. All of the devices that have a wireless NIC transmit to the AP; which in turn redirects the signal to the other wireless devices. The second function of an AP is to act as a bridge between the wireless and wired networks.

2.1 Quick Overview of 802.11 Protocol:
802.11 a standard has a maximum speed of 54 Mbps and also supports 48, 36, 24, 12 , 9 and 6 mbps. 802.11 a has achieves its higher speed and flexibility over 802.11b through high frequency, more transmission channels and new multiplexing techniques.

802.11b standard has added two more speed 5.5Mbps and 11 Mbps to the original standard. With faster data rates the 802.11b quickly became the standard of WLAN. The 802.11b standard uses the Industrial, Scientific and Medical band for transmission. IEEE developed 802.11g standard to preserve the stable and widely accepted features of 802.11b but increases the data transfer rates to those similar 802.11a. 802.11g specifies that it operates in the 2.4GHz ISM frequency band.

Traffic controlling is done by two methods. One is firewall which prevents unauthorized access to the network, connection for DSL and cable modems and other features. Another is DMZ which is basically non trusted zone in which user has given some more freedom to the users. As a practical matter, most wireless LANs have been built for coverage. Figure 3 [1] below illustrates the typical scenario. Although stations close-in connect at the maximum data rate, stations that are further away require much longer time intervals to transmit the same data. Figure is only a qualitative display of how the speed of a network changes with distance.

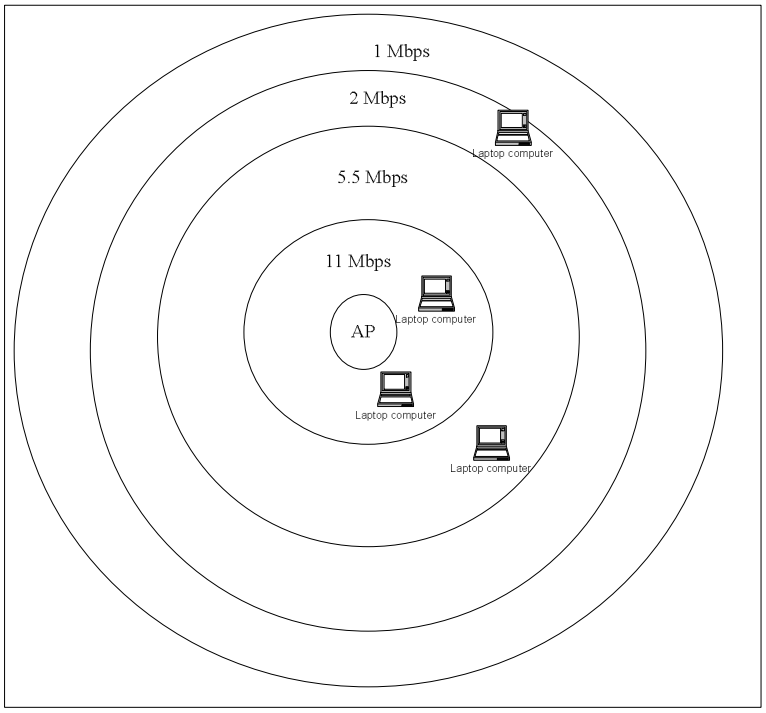

Fig 3. shows performance which depends on range [1]

2.2 Creating VLAN:
Switches normally define VLANs in terms of which ports are in each VLAN. Port based VLANs, the typical choice for configuring VLANs in a switch, can be done very easily, without needing to know the MAC address of the devices. A rarely used alternative for

creating VALNs is to group devices into VLAN based on MAC address. Practically what happen is networking engineer would discover all the MAC address of all the devices and then would configure the MAC address in the various switches, associating each MAC address with a VLAN. This allows device to moves around easily.

2.3 Configuration:
Now here how are the grouped into different VLANs? Stations are configured in one of three ways. (1) Manual (2) Semiautomatic. (3) Automatic.

(1) Manual: in this configuration the network administrator uses the VLAN software to manually assign the stations into different VLANs at setup. Later migration from one VLAN to another is also done manually. This is not a physical configuration but its logical configuration. So we can say that here administrator types the port numbers, the IP address or other characteristic using VLAN software.

(2) Semiautomatic: A semiautomatic is between manually and automatic. It means initializing is done manually and migration is done automatically.

(3)Automatic: In an automatic configuration, the stations are automatically connected or disconnected from a VLAN using criteria defined by administrator. For example administrator can assign a project number as criteria as a being a member of group. When user changes the project it automatically migrate to a new VLAN.

3.1 Trunking of VLAN:
When multiple switches can be connected together with traffic from multiple VLANs crossing the same Ethernet links using a feature trunking. Now lets see how trunking works in VLAN. When sending a frame to another switch, the switches need a way to identify the VLAN from which the frame was sent. With VLAN trunking the switches tag each frame sent between switches so that receiving switch knows which VLAN the frame belongs too.

With trunking we can support multiple VLANs that have members on more than one switch. For example, in fig.4 [4] when switch 1 receives a broadcast from a device in VLAN1, it needs to forward the broadcast to switch 2. before sending a frame to switch 2, switch 1 adds another header to the original Ethernet frame; that new header has the VLAN number in it. When switch 2 receives the frame, it sees that the frame was from a device in VLAN1. so switch 2 knows that it is forwarded broadcast.

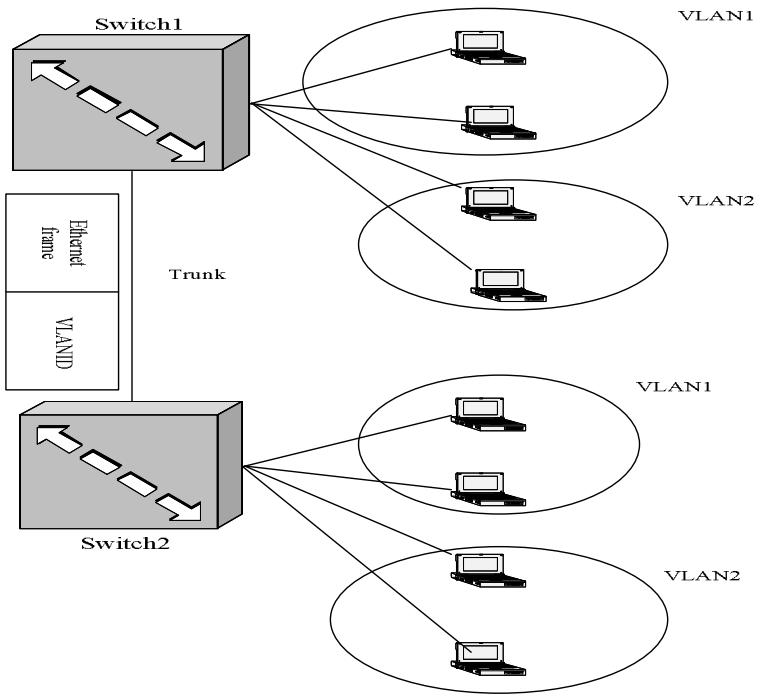

Fig4. VLAN Trunking between Two Switches

3.2 Traffic Passing between VLAN:

We have defined VLAN as broadcast domain. The same devices that comprise a VLAN are also in the same TCP/IP subnet. So we can say that the devices in the same VLAN are in the same subnet, and devices in different VLANs must be different IP subnets. Here the relationship between VLAN and subnet is one to one.

3.2.1 L2 Switching:

A L2 switching refers to the typical switch processing logic. A switch receives a frame and looks at the MAC address. If the MAC table ahs an entry for that destination, it forwards the frame but if not then it forwards the frame out all ports except the port in which the frame entered the switch. When VLANs are used an L2 switch uses the same logic but per VLAN. So we can say that there is a MAC address table for each VLAN because the MAC address tables are separate, unicasts sent inside one VLAN cannot forwarded out ports in another VLAN.

3.2.2 L3 forwarding using a router:

As we discussed L2 switching we can say that L2 do not forward frames between different VLAN but what if we want to do this function? Then we have to use router. The reason behind is that router needs an interface in each subnet to forward traffic between the subnets even though if we are not using VLANs. But using more interfaces seems wasteful. So we can use a router with fast Ethernet port that supports trunking and use a single physical connection from the router to use the switch. The below figure.5[4] shows example of L3 forwarding.

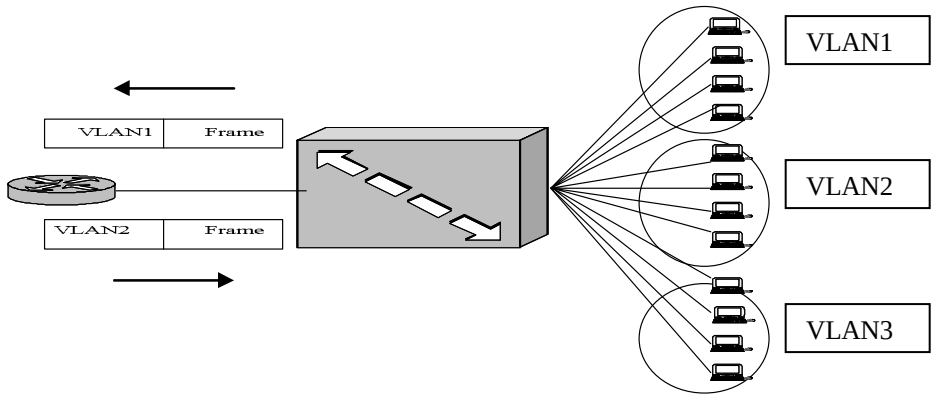

Fig 5.Router forwarding between VLANs over a Trunk [4]

3.3.3 L3 forwarding using a layer switch:

The term L3 switch refers to a switch that also has a routing features. So instead of requiring a router external to the switch, the router internal to the switch performs the same function. The only difference between routing using a router and using a L3 switch lies in the internal processing. There are basically two points that makes difference and explained what happen inside the L3 switch.

First is that L3 switches used specialized hardware to make the forwarding process runs very fast. The switch ASICs (Application Specific Integrated Circuits) on an L3 switch have been built so that the normal very fast L2 forwarding path can also be caused to perform the forwarding function for L3 switch. So we can say that the changing of headers and forwarding of the packets uses the same internal high speed of L2 switch. The routing protocols which are used in L3 switch are used to build the tables used by the specialized forwarding hardware.

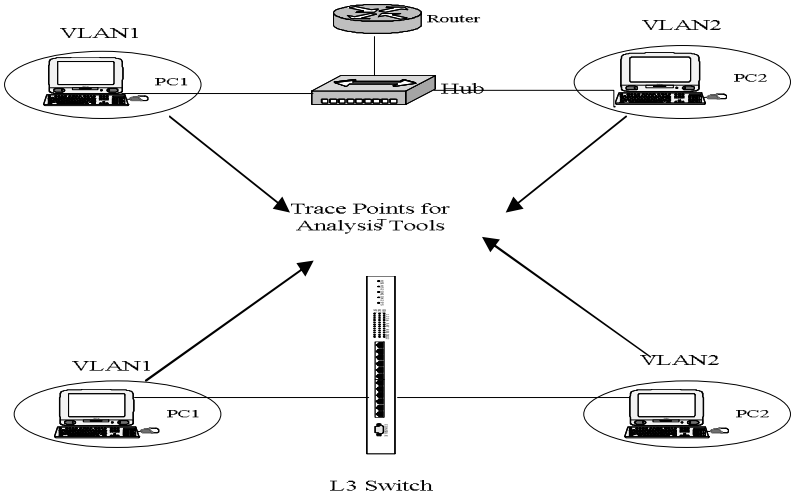

Fig 6: Analysis point shows no difference between L3 switching and routing [4]

Above figure6[4] shows routing and L3 switching between two interfaces in two different VLANs. If you were put a LAN analysis tool at the points shown each of the two topologies and compare the packets being forward between the two and we can see no difference. By tracing the two similar networks at the points shown we can confirm that there are no difference to the effect of the external router against L3 switch. The L3 switch runs routing protocols and builds an IP routing table and the switch makes the forwarding decision based on destination IP address. The L3 switch even discards the only Ethernet data link header and builds a new one.

3.2.4 Layer 4 Switching:

The L4 switches refers to a type of switching in which the switch considers the information in the layer 4 headers when forwarding the packets. Sometimes the forwarding decision is based on information inside the L4 headers. In some cases L3 forwarding is used but the switch does an accounting based on the L4 headers. In that sense both are considered as L4 switching. The key is to understand the L4 switch is the understanding of TCP and UDP port numbers. Port numbers identify the application process of the sender and the receiver of a packet. An L4 switch can make the decision of where to forward the packet based on the information in the TCP and UDP header, typically the port numbers. The other function is also simply keep track of the numbers of packets and bytes sent per TCP port number while still performing L3 forwarding.

The figure.7 [4] below shows an example with L4 switching which show L4 switch how it makes forwarding decisions based on the TCP port numbers. Now in this example there are two replicated server means either of the server can be used for any user and the last server is for FTP traffic. So when user wants anything related to FTP and then it comes form Server 3. now here all the request for web service or related to FTP services are directed through single IP address that represents all 3 servers. now for a new TCP connection which is going through port 80, the L4 switch will pick any of the server1 or server2. same way if TCP connection is requested from port 21 the switch will select server3.

To perform L4 switching the switch must keep track of every individual L4 flow. L4 switching does require more forwarding capacity than does the equivalent with L3 switching. A L4 switch can perform accounting the track to the volume of traffic per TCP and UDP port number but still the decisions based on L3 switching logic.

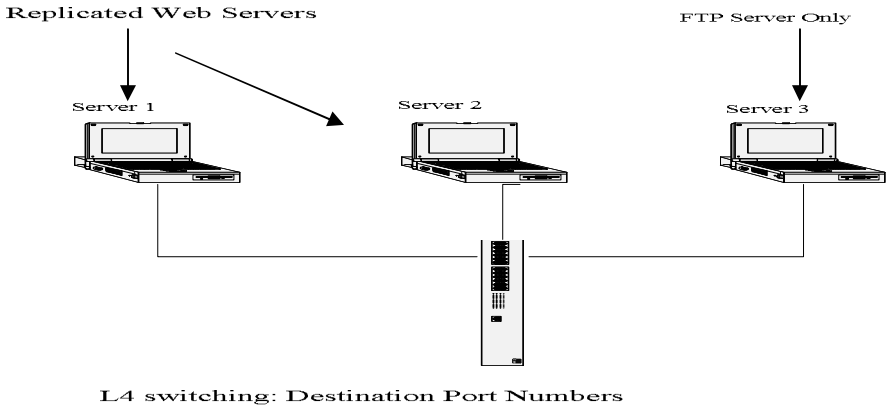

Fig7: L4 switching Based on TCP Port Numbers [4]

3.2.5 Layer 5-7 Switching:

Layer 5-7 switching typically falls into a category of features and products that calls Content Delivery Network.

Comparison of Multilayer Switching Options:

L2 switching is only the option that does not allow forwarding form one VLAN to another.

Type	Description
L2 Switching	The process of forwarding frames based on their MAC address.
External Router connected to L2 switch	Router forwards like always based on destination IP address.
L3 Switch	Switch's forwarding logic forwards based on destination IP address for traffic destined for another VLAN
L4 Switch	Can forward based on L4 information typically port numbers but can also just do accounting based o L4 information
L5-7 Switch	Forwards based on application layer information, typically considered a CDN (Content Delivery Network)feature.
Multilayer Switch	A switch that concurrently performs switching based on multiple layers. For example most L3 switches also perform L2 switching inside a VLAN and L3 switching for traffic between VLANs

Table 1 shows multilayer switching options.

4. Deployment Of WLAN using VLAN: In this part we will discuss the deployment of wireless LAN using virtual LAN. We have to decide what kind of architecture do we have to use at the best for security. In this section we will discuss some examples for wireless LAN

4.1 Single Subnet Network: for mobility an access point has connected to each other at layer 2 and to do this we have to build wired architecture in parallel to the wireless architecture. Fig 8.1(a)[1] shows wired architecture in which access points are supported by separate set of switches, links and cables. Virtual LANs can be implemented to cut down the required physical architecture, as in Fig8.1(b). Rather than acting as a simple layer-2 repeater, the switch in Figure8.1(b)[1] can logically divide its ports into multiple layer-2 networks. The access points can be placed on a separate VLAN from the existing wired stations, and the wireless VLAN will give its own IP subnet. Multiple subnets can be run over the same link because the VLAN tag allows frames to be separated. Incoming frames for the wired networks are tagged with one VLAN identifier, and frames for the wireless VLAN are tagged with a different VLAN identifier. Frames are sent only to ports on the switch that are part of the same VLAN, so incoming frames tagged with the wireless VLAN are delivered only to the access points.

Now in another figure 8.1(c)[1] where two switches are connected through the link and all access points are assigned to the same VLAN. Also this Access points are assigned to the same IP subnet. The link that which connects the switches also allow to separate them. If we use fiber optic link then we can extend the subnet across many buildings.

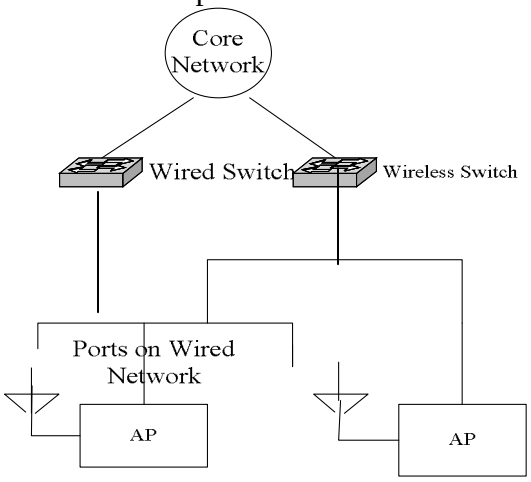

Fig 8.1(a) Non VLAN Deployment[1]

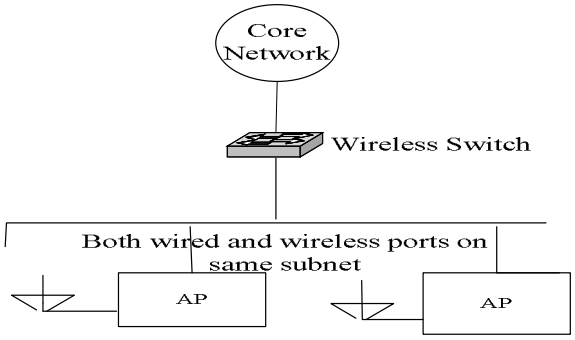

Fig 8.1(b) VLAN Deployment[1]

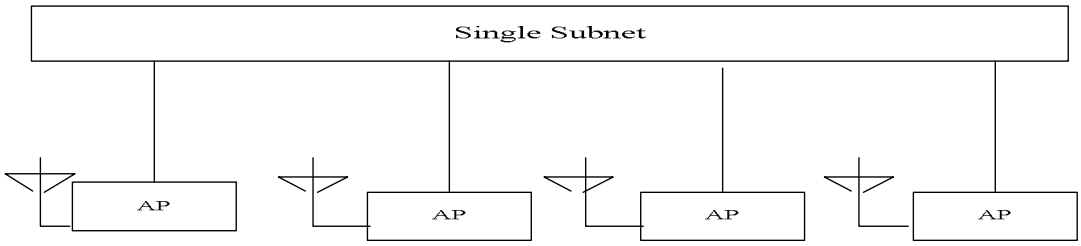

Fig:8.1(c) Logical Topology using VLAN to expand Multiple Switches [1]

Performance of this design is good because in this design there is only one choke point and the traffic that comes to this choke point is pushed through single network path.

4.2 Dynamic VLAN Deployment: basically dynamic VLAN deployment is instead of creating second parallel network, it is an extension of existing network with this feature we can add any security systems. 802.1X is the main part which joints wireless networks with existing authentication. The advantage of doing authentication at the link layer, rather than a higher layer, is that users can be placed on a particular network with the privileges associated with that network from the start.

Now in this technology the mobility quiet good. It means users User's are attached to a constant VLAN throughout the network, and thus can maintain the same IP address regardless of location. With the same IP address, any transport layer state or application state remains valid throughout the life of the connection. However, the underlying implementation of mobility offers several advantages over the single-subnet architecture. The first advantages is that it has to do with the use of authentication services. Attributes from the RADIUS server ensure that users are always attached to the same VLAN, and hence, they stay attached to the same logical point on the network. The other advantage is that the constant VLAN can make other services works better. IP security tunneling remains same because the IP address doesn't change.

Because the VLAN assignment is based on 802.1X and RADIUS, security in this Method is based on dynamically generated keys at the link layer, either through dynamic WEP or WPA. Dynamic key generation enables the second benefit of using authentication services. Once users have been identified, they can be separated into groups for different security treatment.

4.3 IEEE Standard:
IEEE committee has passed a standard called 802.1Q that defines the format for frame tagging. The standard also defines the format to be used in multi switched backbones and enables the use of multi vendor equipment in VLANs. IEEE 802.1Q has opened the way for further standardization in other issues related to VLANs. The below figure.9[4] shows trunking header.

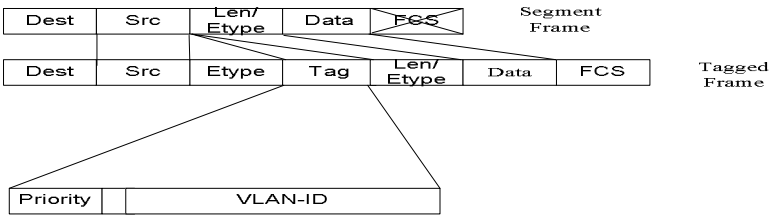

Fig 9: 802.1q Trunking Header [4]

802.1 Q uses a different style of header than does ISL(inter switch link). Basically what happens in 802.1 Q is that it doesn't actually encapsulate the original frame but it adds an extra 4 bytes header to the middle of the original Ethernet header. This additional field is useful to identify the number of VLAN. Because 802.1Q encapsulation forces a recalculation of the original FCS(frame check sequence) field in the Ethernet trailer because the FCS is based on the content of the entire frame. The basic function FCS is that it allows the receiving device to notice that errors occurred and then discard the data frame.

5. VLAN in WLAN System:
Sometimes operators share same physical Wireless architecture but those architecture gives different services to their clients. The traffic in WLAN can be identified by VLAN tag identifier. Basically there are three areas of this architecture.

(i) **The Service Network**: in this area the service provider provides their services.
(ii) **VLAN Switching Area:** this is basically backbone of WLAN. This consists of hubs and switches. In this area each VLAN is different.
(iii) **Interface of WLAN:** this area consists of wireless Access Point. As it is part of this architecture the different service provider shared it. The traffic in this area are separated by Extended Service Set Identifier which is 32 bit characters long. The different Extended service set identifier is used for each VLAN switching area.
The figure.10 [2] below shows shared wireless LAN architecture using VLANs and different Extended Service Set Identifier.

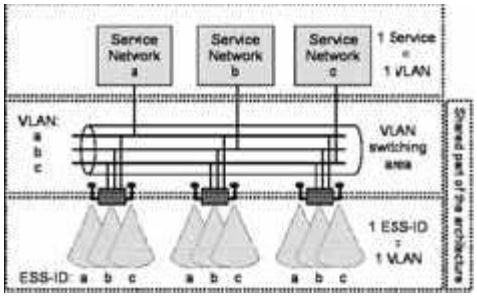

Fig 10: shared Wireless LAN Architecture [1]

VLAN over multi hop system in wireless LAN are facing two problems. First is that routing of the packet of the client and second one is the problem for access point to recognize the extended set service identifier of client. The solution of this problem is Tunneling. Figure.11 [5] describes that the routers which are enclosed in circles are capable of multicasting and without tunneling router are going to be isolated. A logical tunnel is established by encapsulating the multicast packet inside a unicast packet. So the multicast packet becomes the payload of the unicast packet. The intermediate routers route the packet as unicast routers and deliver the packet from one to another.

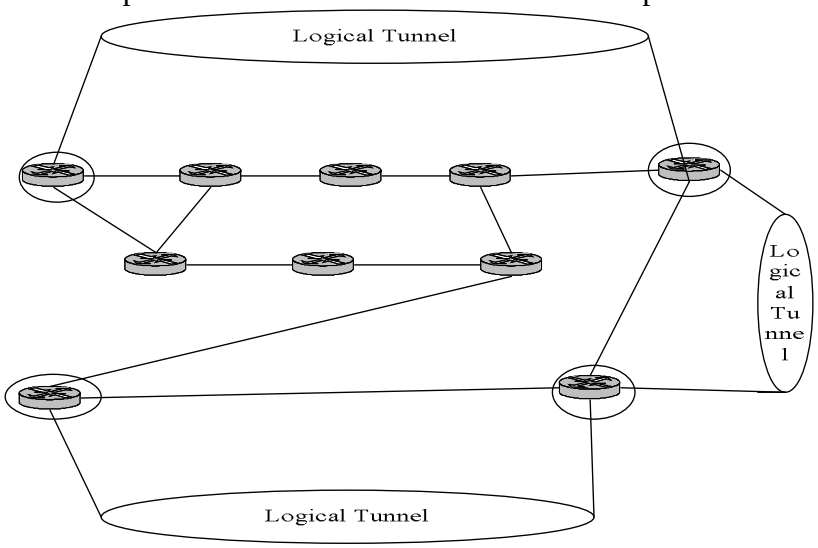

Fig 11: Logical Tunnel solution for multi hop system in WLAN [5]

5.1 VLAN Information Exchange Protocol:

This is the protocol that makes VLAN routing table update. The VLAN routing table must be updated regularly to give latest information about the location of the clients that are connected to multi hop wireless LAN. Every AP will tell which clients are connected to them by using flooding message. There are some features which are related to VLAN routing table:

- The table should be updated on the regular interval to give latest information of the client location which are connected to multi hop WLAN
- Every AP should have routing table.
- Every client should contain an information of VLAN and their IP address.

6. Security:

6.1 Basic Security:

Authentication is a process that verifies that the user has permission to access the network. It is critical with WLAN because of the open nature of a wireless network. Each WLAN client can be given service set identifier(SSID) of the network. This value is transmitted to the access point when the client is negotiating with it for permission to connect to the network. Only those clients that know the SSID are then authenticated as valid users and are allowed to connect to the network.

6.2 Enhanced Security:
Enhanced Security:

There are some methods that gives more efficient security to WLAN.

- **WEP:** Wired equivalent privacy specifications for data encryption between wireless devices to prevent eavesdropping. The strength of encryption rests not only on the keeping the keys secret but also on the length of the keys. The longer the key the stronger the encryption because a longer key is more difficult to break. IEEE WEP standard specifies data encryption using only 40-bit a shared key. But there is problem with the shared key cryptography, the key length is on 40 characters and the initialization vector can easily be broken. So its not that much reliable.

- **RADIUS:(Remote Authentication Dial-In User Service):** the 802.1x drafts uses a protocol known as extensible authentication protocol(EAP). EAP allows a client to negotiate authentication protocols with separate authentication server 802.1x also makes use of RADIUS. The 802.1x draft proposes the authentication would be performed as follows. The figure.12 [5] explain the example.
    1. A user on a wireless device connects to the access to the access point and enters a user name and password.

    2. The AP requests authentication of that user by sending the information to a RADIUS server on the wired network.

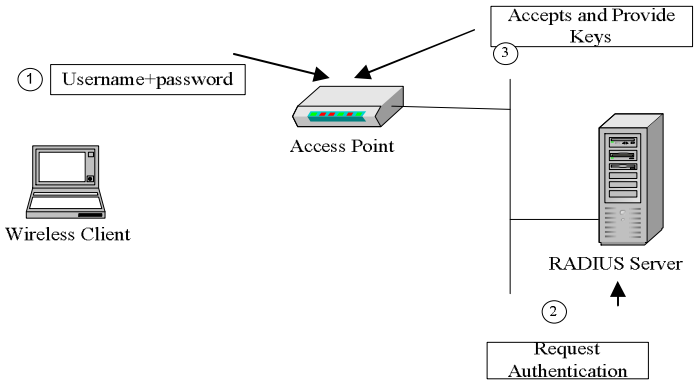

Fig 12: 802.1 x security [8]

    3. The RADIUS server reviews the request and can accept, reject or further challenge the request. If it accepts the requests the RADIUS server sends the security keys and other data for that wireless client to the AP so that it can establish secure connection with the client.

7. Advantages & Disadvantages:

Advantages:

There are several advantages to using VLANs.

1. **Cost and Time Reduction:** VLAN can reduce the migration costs of stations going from one group to another. Physical reconfiguration takes time and is costly. Instead of physically moving one station to another segment or even to another switch, it is much easier and quicker to move it using software.

2. **Creating Virtual Workgroups:** VLANs can be used to create virtual workgroups. For example, in a campus environment professors working on the same project can send broadcast message to one another without necessary of belonging to the same department. This can reduce the traffic if the multicasting capability of IP was previously used.

3. **Security:** VLANs provide an extra measure of security. People belonging to the same group send broadcast message with guaranteed assurance that users in another groups will not receive the messages.

Disadvantages:

1. **Communication Problem:** as we know VLAN is giving high security. But there is a communication problem. For example if any user in VLAN1 wants to communicate with another user in VLAN2 but they cant communicate. For the communication first they have to configure the data of the user in the switch. so we can say that for communication every time we have to do configuration.
2. **Complexity:** complexity in the sense of expansion of the network. It means if we expand the network and something goes wrong with that network then maintenance of the networks costs too much.
3. **Capacity:** routing of the VLAN does by router. If the network is too large then router cant be handle the load of the work by single router. So network should be small to handle the workload.
4. **Infection:** In VLAN network every user is connected with each other so if one user is infected by any virus or any worms then whole network will be affected by that viruses.

8. Conclusion:

Its hard to become network engineer and also hard to work with VLAN. Almost every campus LAN uses VLAN and almost every campus LAN with more than one switch uses trunking. We can say that VLAN allows switch to separate different physical port Into different groups so that traffic from devices in one group never gets forwarded to the other group. This allows network engineer to build the networks that meet their design requirements, without having to buy different switch for each group.

9. References:

[1] creating and administrating wireless network the definition guide by Matthew Gast
http://www.oreilly.com/catalog/802dot112/chapter/ch21.pdf

[2] VLAN over Multi-hop Wireless LAN System.
http://delivery.acm.org/10.1145/1190000/1189197/a8-matsui.pdf?key1=1189197&key2=7254872711&coll=&dl=GUIDE&CFID=15151515&CFTOKEN=6184618

[3] Mobile Ad-Hoc Wireless Access in Academia (MAWAA) Project.
http://www.jisc.ac.uk/uploaded_documents/mawaa-d1-v10.pdf

[4] CCNA INTRO Exam Certification Guide by Wendell Odom.

[5] Data Communication and Networking by Forouzan

[6] An Initial Security Analysis of the IEEE 802.1X standard
http://www.cs.umd.edu/~waa/1x.pdf

[7] GSM Association WLAN roaming Guidelines
http://www.gsmworld.com/documents/wlan/ir61.pdf

[8] Guide to Wireless Communication by Mark Ciampa.