International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

The Proposed Roles of VLAN and Inter-VLAN Routing in Effective Distribution of Network Services in Ebonyi State University

Agwu Chukwuemeka Odi[1], Nweso Emmanuel Nwogbaga[2], Ojiugwo Chukwuka N. [3]

[1]Lecturer 1, Department of Computer Science, Ebonyi State University – Abakaliki, Nigeria

[2]Lecturer 11, Department of Computer Science, Ebonyi State University – Abakaliki, Nigeria

[3]Undergraduate Student, Department of Computer Science, Ebonyi State University – Abakaliki, Nigeria

Abstract: ***In traditional Local Area Network (LAN), all devices connected on switches belong to one broadcast domain. Virtual Private Local Area Network (VLAN) technology segments a physical LAN into different groups called VALNs and allows only devices on the same VLAN to communicate with one another while restricting devices on other VLANs from sending network traffic. This technology adds security in the LAN and controls network broadcast domain. Virtual LANs (VLANs) offer a method of dividing one physical LAN into multiple broadcast domains. However, VLAN-enabled switches cannot, by themselves, forward traffic across VLAN boundaries. For inter-VLAN communication, a Layer 3 router is required. This research paper discusses the VLAN protocol and different ways and possible protocols involved in creating and implementing Inter-VLAN routing for effective distribution of network services in Ebonyi State University.***

Keywords: Virtual LAN (VLAN), Inter-VLAN, Local Area Network (LAN), Routing, Inter-Routing, Network Services.

1. Introduction

Local Area Network (LAN) is built with the help of network switches which by default creates a single flat network with large broadcast domain. The increase in the number of devices on LAN become paramount as we populate the network with more switches and workstations. Since most workstations tend to be loaded with existing operating system, it results in unavoidable broadcasts being sent occasionally on the network. Unfortunately, each host on such network cannot escape from the effects generated by such uncontrollable broadcast which decreases network performance.

Security is never guaranteed in the above network infrastructure since all users are able to see all devices on local area network. In the case of Ebonyi University network having critical file servers, organisational databases and other confidential information, this would mean that everyone would have network access to these resources and naturally, they are prone to different attacks. To effectively prevent such situations from operational network we need to restrict access by implementing Virtual Private Network (VLAN) which segments the existing network into different work groups.

A VLAN is a logical grouping of network users and resources connected to administratively defined ports on a switch. When you create VLANs, you're given the ability to create smaller broadcast domains within a layer 2 switched internetwork by assigning different ports on the switch to service different sub-networks. A VLAN is treated as its own subnet or broadcast domain, meaning that any frames broadcast from Ebonyi State University Database Admin can only be switched between the ports logically grouped within the same Admin VLAN thereby restricting access from any other network groups within the University. By default, hosts in a specific VLAN can't communicate with hosts that are members of another VLAN. This concept of grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design and increase performance. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections. Most enterprise-level networks today use the concept of virtual LANs. Therefore, in the absence of VLANs technology, a switch considers every its LAN ports to be in the same broadcast domain.

VLAN design and implementation in Ebonyi State University can create lots of benefits. Here's a short list of ways VLANs simplify network management:

2. Benefits of VLAN and Inter-Routing

- **Scalability**: Network adds, moves, and changes are achieved with ease by just configuring a port into the appropriate VLAN and assigning hosts to the same VLAN
- **Security:** VLANs provide enhanced network security. In a VLAN network environment, with multiple broadcast domains, network administrators have control over each port and user. A malicious user can no longer just plug their workstation into any switch port and sniff the network traffic using a packet sniffer. The network administrator controls each port and whatever resources it is allowed to use. VLANs help to restrict sensitive traffic originating from an enterprise department within itself.
- **Creating Workgroups:** A group of users that need an unusually high level of security can be put into its own

Licensed Under Creative Commons Attribution CC BY

VLAN so that users outside of that VLAN can't communicate with it. This implies that in an organisation each department can be made independent from other departments.

- **Cost effective**: Cost savings can be seen by eliminating the need for additional expensive network equipment like routers. VLANs will also allow the network to work more efficiently and command better use of bandwidth and resources.
- **Easy Troubleshooting:** By grouping our network users and resources into different VLANs, problems emanating in the network can easily be identified and fixed by mere tracing group such hosts belong to.
- **Integrity:** As a logical grouping of users by function, VLANs can be considered independent from their physical or geographic locations. Therefore, our University data can be handled without comprise.
- **Broadcast Control:** The broadcast of the network can be managed and controlled by creating many VLANs which invariably increases the number of broadcast domains while decreasing their size.

3. Literature Review

A comprehensive discussion of networking is beyond the scope of this work. However, Derfler and Freed (1996);[4] usefully define many of the terms used in discussing networks. A local area network (LAN) is "a group of computers typically connected by no more than 1,000 feet of cable, which interoperate and allow people to share resources." A network interface card (or LAN adapter) is the device which packages data for transmission and acts as "a gatekeeper to control access to the shared network cable." Network interface cards break data streams into packets, which are reassembled at the destination. Bridges segment LANs or join LANs together; they act to control traffic by learning the "station address" of each machine on the networks in question, and only send a packet across the bridge if the destination of the packet is a station on the other side. Routers function similarly to bridges, but look at the network address of packets and use different routing protocols to send the packet to its destination efficiently.

[5] Henry and De Libero (1996) describe the use of switching to divide the network into smaller segments. Switching helps to reduce the number of nodes trying to use the same network segment, resulting in lower congestion on each segment. In switched hubs or bridges, each node can have its own network segment, and therefore have access to all of the network bandwidth of the segment. Switching bridges can look deep into a packet and use protocol information and the like to provide a level of filtering and prioritization (Henry and De Libero, 1996);[5].

The evolution of the local area network (LAN) has followed a logical progression of improvements to tackle one problem at a time. LAN switches have essentially replaced repeating hubs in business environments. A conceptual software-driven special application of LAN switches, called Virtual LANs (VLANs), was introduced in the mid-nineties with a lot of hype. They promised cost effective router-like benefits with the added advantage of reduced system administration costs. As we approached and then entered into the 21st century, other technological advances challenged the VLAN, and ultimately displaced it. This paper builds the case for VLANs and then examines some of these alternate technologies. Since VLAN technology is relatively new, and is different from vendor to vendor, it is not surprising that there is sparse mention of the technology in the literature.

Virtual local area networks address and attempt to solve many of the issues and problems facing network administrators, particularly on large, enterprise-wide networks. Some common issues include network utilization, particularly collisions and broadcasts, and network security. In addition, administrators want to reduce the amount of time and resources required to perform "moves, adds, and changes" to the workstations on a network; such activities often take up a disproportionate amount of an administrator's time and resources. VLANs offer additional advantages besides breaking up the broadcast domain. One widely touted advantage is simplified system administration functions, particularly related to office moves and employee relocations. Take the simple example of a four-story office building, where each floor is segregated into a traditional LAN and isolated by routers. If an employee is reassigned to another floor, then the system administrator has to change the IP number of the employee's relocated computer to correspond to the new subnet. A VLAN could save the system administrator a trip to the employee's new office, because VLAN membership could be reallocated at the main control console. Other situations where VLANs come in particularly useful are those requiring the quick segmentation of LAN membership, like the formation of a proposal team working on a highly proprietary bid.

Of particular interest to network administrators is the area of network utilization. Network utilization describes the percentage of available network resources that are being used by end stations on the network. [6] Martin, Chapman, and Leben (1994) and Tittel and Robbins (1994);[11] provide a great deal of information on general networking theory, including the issue of network utilization. The most common type of network, Ethernet, allows any station to transmit information on the network as long as no other station is currently transmitting. However, it is possible for two or more stations to simultaneously "sense" that the network is clear and transmit at the same time, causing a collision. While Ethernet and other network protocols include methods for dealing with collisions, the larger the network (i.e. the more users it supports), the higher the frequency of collisions (Martin et al., 1994);[6]. As network activity increases, the frequency of collisions can severely degrade network speeds, to the point that the network may seem to have stopped working. [3] Comer (1995) and Chappell and Hakes (1994);[2] describe a feature of local area networks that is related to the problem of collision frequency and its impact on network utilization: the propagation of "useless" network traffic. All signals from a station on a given network are sent to all other stations on the network, regardless of whether they are intended for a station or whether that station can even interpret those signals (Comer, 1995);[5]. The designers of Ethernet had the foresight to place the destination address at the beginning of each Ethernet packet (Comer, 1995);[5], and thus the network interface on a particular workstation can rapidly

Licensed Under Creative Commons Attribution CC BY

determine whether or not a packet is addressed to it. Packets addressed to other stations can be examined and discarded with minimal use of system resources. However, the Ethernet protocol itself (Comer, 1995);[5] and several higher-level protocols, such as NetWare's IPX/SPX (Chappell & Hakes, 1994);[2] utilize packets that are designed to be received and processed by all interfaces on a network. These packets have a special "broadcast address" instead of the destination address of a single station. When a workstation's network interface receives such a packet, it does not discard the packet based on its destination address; it examines it further to determine what action should be taken. If the interface "speaks" the protocol for which the packet is used, it takes action on the packet's contents; otherwise, the packet is discarded. Determining whether or not a broadcast packet should be discarded requires that the receiver look many bytes deeper into the packet, with a correspondingly greater use of CPU cycles. Roese (1998);[8] discusses the particular problems associated with a "flat," switched network. Unlike large-scale networks consisting of sub-networks connected through a series of routers, a flat network is essentially one large broadcast domain. While this does have some advantages over traditional, routed networks, namely higher-speed connections between segments, lower cost of networking equipment, and lower administrative overhead, flat networks do have disadvantages as compared to routed networks. According to Roese, connecting switches as routers are connected, with multiple possible paths from one point to another, can lead to "loops" in the network, wherein broadcast packets propagate infinitely, creating "broadcast storms" that can severely degrade network performance.

[1] Baker (1995) discusses a broad range of topics related to network security. He provides a good summary of the network security problem. "Good" networks should operate smoothly with other networks, be transparently to users, provide remote access, and maintain peak performance. On the other hand, "secure" networks protect confidential information, keep network performance reliable, and emphasize data integrity. The two dimensions are often at odds (Baker, 1995);[1].

Most of what Baker terms "network security" would be more precisely called "server security." He is more concerned with securing machines on a network than the network itself. Such a focus is appropriate, since common sense tells us that the targets of most malicious attacks are end stations and the data that reside in them, rather than the network itself. However, network abuses (and misuses) do occur, and in any event the means of accessing a server for purposes of breaching security is often a network (Baker, 1995);[1]. Network hardware, such as switches and routers, can implement some kinds of security, such as routing traffic in such a way that it travels by the most direct path, thereby minimizing the chance of interception. They can also implement security-oriented functions such as authentication and encryption (Baker, 1995);[1].

Most literature on VLANs available today comes from vendors who are supplying VLAN technologies. As mentioned earlier, no fully qualified standards exist for defining VLAN implementation; thus definitions are often different from vendor to vendor. One third-party source for VLAN information is the UC-Davis Network 21 initiative (1998);[12]. It defines much of the terminology involved in discussing VLANs, and includes a discussion of the uses of VLANs, especially with regard to an academic network. Henry and De Libero (1996);[5] define a VLAN as the construction of logical LANs across a switched network using "virtual circuits or connections (p. 75)." They further defines virtual circuits as

. . .the pathways created between two devices communicating with each other in a switched network or communications environment. These circuits are active only for the duration of the originating data packet. Even though an exclusive connection is established between two devices, it's only temporary and is closed, or taken down, when the communications session is completed (p. 75).

The only VLAN-related standard currently under development comes from the Institute of Electrical and Electronics Engineers (IEEE). Their standard, "IEEE P8021.Q, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Networks" (Institute of Electrical and Electronics Engineers, 1998);[14], describes enhancements to the 802.x LAN/MAN standards for packet structure. The standard (from here on abbreviated to "802.1Q") complements the 802.1p standard for inter-bridge/switch communication, which includes the "Spanning Tree" algorithm used to eliminate network loops and broadcast storms. The packet structure of the major IEEE-defined network architectures (Ethernet, Token Ring, etc.) are redefined by 802.1Q to include "tags" that further describe the contents of the packet (IEEE, 1998.) The 802.1Q standard dos not, however, define the actual content of these tags under the current draft; rather, it simply "makes room" for the tags in the existing packet structure.

A relatively unbiased overview of VLAN technology comes from Passmore and Freeman (1998);[7], writing a white paper for 3Com, Inc. VLANs, they say, "represent an alternative solution to routers for broadcast containment, since VLANs allow switches to also contain broadcast traffic (p. 2)." While many enterprises have used switches to segment their networks, standard switches do not stop broadcast traffic. VLAN technology allows broadcast containment without the high cost and speed penalty of routers. Passmore and White also discuss the typical reasons enterprises do not readily adopt VLAN technology: They are proprietary solutions, which are "anathema" (p. 2) to the networking market, which emphasizes open systems and interconnectivity. VLANs add additional cost, both visible and hidden, to the administration of a network. VLANs can impede full-speed access to centralized servers.

Passmore and White divide VLANs into four categories, based on the means by which they assign stations to a given VLAN: port grouping, MAC-layer grouping, network-layer grouping, and multicast grouping.

[15] Cisco Systems (Virtual LAN communications, 1996) views VLAN technology (at least, their version of it) as providing flexibility in organization and greater segmentation of an enterprise's network. Cisco concentrates on port grouping, in which the port to which a user connects

Licensed Under Creative Commons Attribution CC BY

her or his workstation is grouped together with the ports of other users in her or his workgroup. Thus members of the same workgroup (the example in the text is the Accounting department) can work in different locations throughout the organizations, be it different floors, offices, buildings, or even campuses, and still connect to each other as if on the same physical network.

Now that you have a network with many different VLANs, the next question is, "How do you permit devices on separate VLANs to communicate?" This reviews the concepts of inter-VLAN routing and how it is used to permit devices on separate VLANs to communicate.

Another common addition to the Inter-VLAN routing service is the application of Access Lists (packet filtering) on the routing switch, to restrict access to services or hosts as required. In modern implementations, central file servers and services are usually placed in their own isolated VLAN, securing them from possible network attacks while controlling access to them. When you take into consideration that most Trojans and viruses perform an initial scan of the network before attacking, an administrator can intelligently disable ICMP echoes and other protocols used to detect a live host, avoiding possible detection by an attacker host located on a different VLAN.

Finally, Cabletron Systems (1998), in a series of white papers and technical documentation, and Roese and Knapp (1997);[9] describe Cabletron's proprietary VLAN system, SecureFast Virtual Networking. SecureFast implements a tagging system similar to that proposed by the IEEE's 802.1Q standard, but with some enhancements, such as utilizing both the source and the destination address in determining packet routing (Roese & Knapp, 1997);[9].

4. Discussion

A flat network is a computer network design approach that aims to reduce cost in terms of maintenance and administration. Flat networks are designed to reduce the number of routers and switches on a computer network by connecting the devices to a single switch instead of separate switches, or by using network hubs rather than switches to connect devices to each other. The topology of a flat network is not segmented or separated into different broadcast areas by using routers and switches. Unlike Virtual Local Area Network design, the network is not logically separated into different broadcast domains. Generally, all devices on the flat network belong to the same broadcast area.

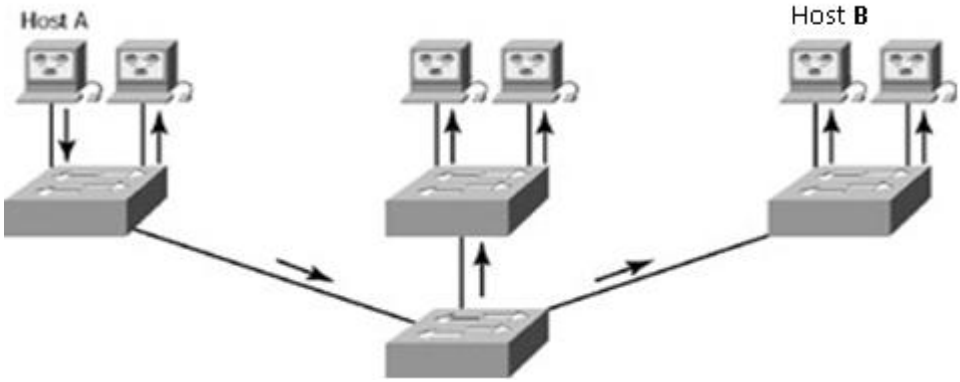

Figure 1: Broadcast Flow on Flat Network structure (Source: Mega Guide, CCNA 640-802, www.preplogic.com)

Considering figure 1 above where Host A sends a traffic to Host B. Unfortunately as Host A sends out the broadcast all ports on all switches forward the same broadcast except the port that originally received the frame. This random broadcasts forwarding occurred because there is no logical segmentation restricting such traffic to none designated hosts. Therefore, Ebonyi State University as a case study currently faces the following problems as a result none VLAN implement in her network.

- **Poor security**: Because traffic travels through one switch, it is not possible to segment the networks into sections and prevent users from accessing certain parts of the network. It is easier for unauthorised persons to intercept data on the network.
- **No redundancy**: Since there is usually one switch, or a few devices, it is possible for the switch to fail. Since there is no alternative path, the network will become inaccessible and computers may lose connectivity.
- **Scalability and speed:** Connecting all the devices to one central switch, either directly or through hubs, increases the potential for collisions (due to hubs), reduced speed at which the data can be transmitted and additional time for the central switch to process the data. It also scales badly and increases the chance of the network failure.

5. VLAN Architecture

All the above problems, and a lot more, can be forgotten with the creation of VLANs. As we know in order to create VLANs, you need a layer 2 switch that supports such protocol. A lot of people new to the networking field bring the misconception that it's a matter of simply installing additional software on the clients or switch, in order to "enable" VLANs throughout the network - this is totally incorrect. It is never true, rather we have VLAN enabled switches like cisco catalysts switches for the cisco system.

VLANs involve millions of mathematical calculations, they require special hardware which is built into the switch and your switch must therefore support VLANs at the time of purchase, otherwise you can't create VLANs on it. Each VLAN created on a switch is a separate network. This means that a separate broadcast domain is created for each VLAN. Network broadcasts, by default, are filtered from all

Licensed Under Creative Commons Attribution CC BY

ports on a switch that are not members of the same VLAN and this is why VLANs are very important in today's large network like Ebonyi State University network as they help isolate network segments between each section. Figure 2 below shows four VLANs created from switches.

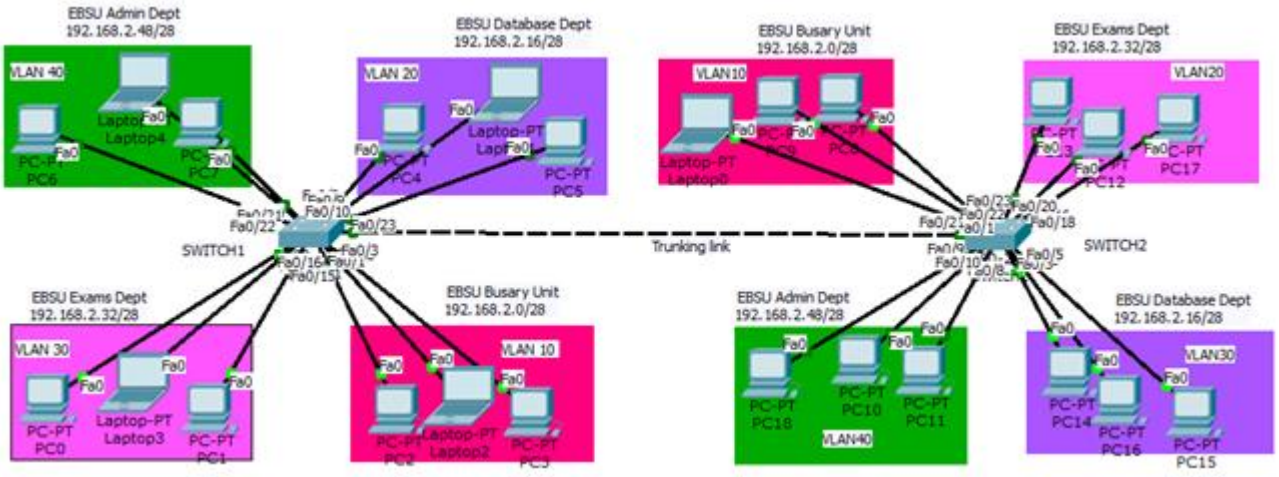

Figure 2: An Imagine of the proposed Ebonyi State University (EBSU) VLAN Infrastructure

6. Broadcast Control

Broadcasts occur in all protocol, but how often they occur depends on the type of protocol, the application(s) running on the internetwork, and how these services are used. Some older applications have been rewritten to reduce their bandwidth consumption, but there's a new generation of applications that are so bandwidth greedy which consume every bandwidth they see like multimedia applications. As if they weren't enough trouble, factors like faulty equipment, inadequate segmentation, and poorly designed firewalls can seriously compound the problems already caused by these broadcast-intensive applications.

All of this has new dimension to network design and presents a bunch of new challenges for an administrator. Positively making sure that network is properly segmented as shown in *figure 2* above controls network broadcast from propagating throughout the entire network. Therefore, a broadcast from EBSU Database Dept VLAN in *figure 2* cannot be seen by EBSU Admin Dept, EBSU Bursary Unit and EBSU Exams Dept VLANs. And the most effective way to do that is through strategic switching and routing. Since switches have become more affordable, most people had replaced their flat hub networks with pure switched network and VLAN environments. All devices within a VLAN are members of the same broadcast domain and receive all broadcasts relevant to it. By default, these broadcasts are filtered from all ports on a switch that aren't members of the same VLAN. Hence, with VLAN implementation broadcast is controlled on switched network.

7. Network Security

Security issues are always the major challenges we face in data communication. A flat internetwork's security used to be tackled by connecting hubs and switches together with routers. So it was basically the router's job to maintain security. This arrangement was pretty ineffective for several reasons. First, anyone connecting to the physical network could access the network resources located on that particular physical LAN. Secondly, for anyone to observe any and all traffic traversing that network is to simply plug a network analyser into the hub. And similar to the last, a scary fact, is that users could easily join a workgroup by just plugging their workstations into the existing hub.

But that's exactly what makes VLANs a better technology. If you build and create multiple broadcast groups, you can still have total control over each port and user thereby restricting people from unauthorized access by plugging workstations into any switch port. VLANs can be created in harmony with a specific user's need for the network resources. In *figure 2, SWITCH1 and SWITCH 2* can be configured to inform a network management station about unauthorized access to those vital network resources. And if you need inter-VLAN communication, you can implement restrictions on a router to ensure access of level of users and place restrictions on hardware addresses, protocols, and applications that traverse the network.

8. Flexibility and Scalability

From OSI reference model, we learnt that layer 2 switches only read frames for filtering because they don't look at the Network layer protocol. Likewise we also know that by default, switches forward broadcasts to all ports except the port that received the broadcast to be forwarded. But if you create and implement VLANs, you're essentially creating smaller broadcast domains at layer 2. As a result, broadcasts sent out from a node in one VLAN won't be forwarded to ports configured to belong to a different VLAN. But if we assign switch ports or users to VLAN groups on a switch or on a group of connected switches, we gain the flexibility to exclusively add only the users we want to let into that broadcast domain regardless of their physical location. This setup can also work to block broadcast storms caused by a faulty network interface card (NIC) as well as preventing an intermediate device from propagating broadcast storms throughout the entire internetwork. Another great advantage is that as VLAN gets too big, you can simply create more VLANs to keep the broadcasts from consuming too much bandwidth. The less users in a VLAN, the fewer users

Licensed Under Creative Commons Attribution CC BY

affected by broadcasts evil and less bandwidth consumed. This is all good, but you seriously need to keep network services in mind and understand how the users connect to these services when creating a VLAN. A good strategy is to try to keep all services, except for the email and Internet access that everyone needs, local to all users whenever possible.

9. Enabling VLAN Technologies And Protocols

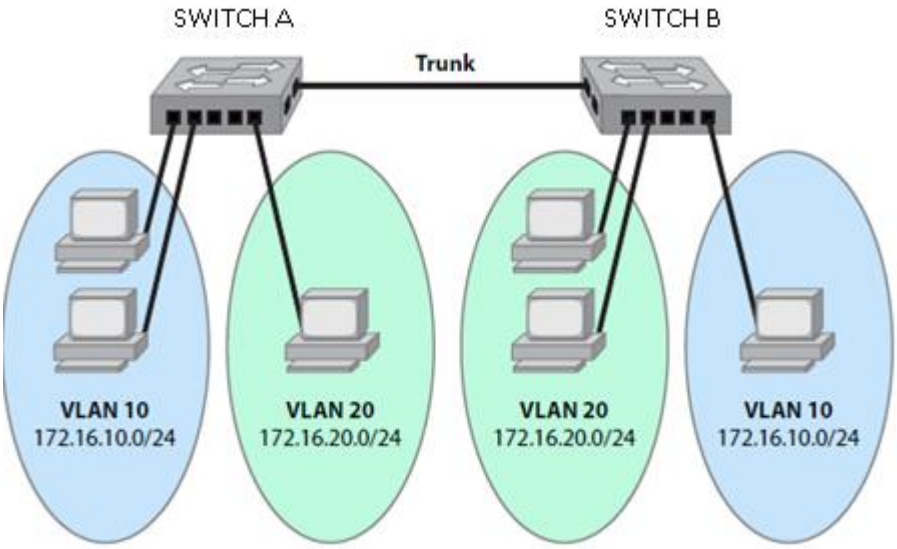

Figure 3: Trunking protocol between switches (Source: Mega Guide, CCNA 640-802, www.preplogic.com)

VLAN identification is what switches use to keep track of all those frames as they're traversing a switch fabric. It's how switches identify which frames belong to which VLANs, and there's more than one trunking method. As we can see in *figure 3* above that each port on both switches that connect both switch A and switch B together indicate a trunk link. VLANs divides a large network into separate broadcast domains. A broadcast within a particular VLAN 10 stays in that VLAN 10 and can never be felt by VLAN 20 no matter the location.

- **Frame Tagging Technique and VLAN Identification Methods**

A Network Engineer can set up VLANs to span more than one connected switches as shown in *figure3* above. This flexible and robust nature is probably the main advantage to implementing VLANs, and we can do this with up to a thousand VLANs and thousands upon thousands of hosts. The frame identification method uniquely assigns a user-defined VLAN ID to each frame. Here's how it works: Once within the switch fabric, each switch that the frame reaches must first identify the VLAN ID from the frame tag. It then finds out what to do with the frame by looking at the information in what's known as the filter table. If the frame reaches a switch that has another trunked link, the frame will be forwarded out of the trunk-link port. Once the frame reaches an exit that's determined by the forward/filter table to be an access link matching the frame's VLAN ID, the switch will remove the VLAN identifier. This is to enable destination device receive the frames without being required to understand their VLAN identification information.

The great thing about trunk ports is that they'll support tagged and untagged traffic simultaneously. Example, if you're using 802.1q trunking, the trunk port is assigned a default port VLAN ID (PVID) for a VLAN upon which all untagged traffic will travel. This VLAN is also called the native VLAN and is always VLAN 1 by default, but it can be changed to any VLAN number. Similarly, any untagged or tagged traffic with a NULL (unassigned) VLAN ID is assumed to belong to the VLAN with the port default PVID. Again, this would be VLAN 1 by default. A packet with a VLAN ID equal to the outgoing port native VLAN is sent untagged and can communicate to only hosts or devices in that same VLAN. All other VLAN traffic has to be sent with a VLAN tag to communicate within a particular VLAN that corresponds with that tag. VLAN identification is what switches use to keep track of all those frames as they're traversing a switch fabric. It's how switches identify which frames belong to which VLANs, and trunking methods discussed are of two types namely:

- **Inter-Switch Link (ISL) Identification Method**

Inter-Switch Link (ISL) is a way of explicitly tagging VLAN information onto an Ethernet frame. This tagging information allows VLANs to be multiplexed over a trunk link through an external encapsulation method. This allows the switch to identify the VLAN membership of a frame received over the trunked link. By running ISL, you can interconnect multiple switches and still maintain VLAN information as traffic travels between switches on trunk links. ISL functions at layer 2 by encapsulating a data frame with a new header and by performing a new cyclic redundancy check (CRC). Of note is that ISL is proprietary to Cisco switches and it's used for Fast Ethernet and Gigabit Ethernet links only. ISL routing is pretty versatile and can be used on a switch port, router interfaces, and server interface cards to trunk a server. Although some Cisco switches still support ISL frame tagging, Cisco is moving toward using only 802.1q.

Licensed Under Creative Commons Attribution CC BY

- **EEE 802.1q Identification Method**

Created by the IEEE as a standard method of frame tagging and vendor independent. IEEE 802.1q actually inserts a field into the frame to identify the VLAN. If you're trunking between a Cisco switched link and a different vendor switch, you've got to use 802.1q for the trunk to work. Unlike ISL, which encapsulates the frame with control information, 802.1q inserts an 802.1q field along with tag control information, as shown in Figure 3.5 below.

For the Cisco exam objectives, it's only the 12-bit VLAN ID that matters. This field identifies the VLAN and can be 212, minus 2 for the 0 and 4,095 reserved VLANs, which means an 802.1q tagged frame can carry information for 4,094 VLANs. It works like this: You first designate each port that's going to be a trunk with 802.1q encapsulation. The other ports must be assigned a specific VLAN ID in order for them to communicate. VLAN 1 is the default native VLAN, and when using 802.1q, all traffic for a native VLAN is untagged. The ports that populate the same trunk create a group with this native VLAN and each port gets tagged with an identification number reflecting that. Again the default is VLAN 1. The native VLAN allows the trunks to accept information that was received without any VLAN identification or frame tag

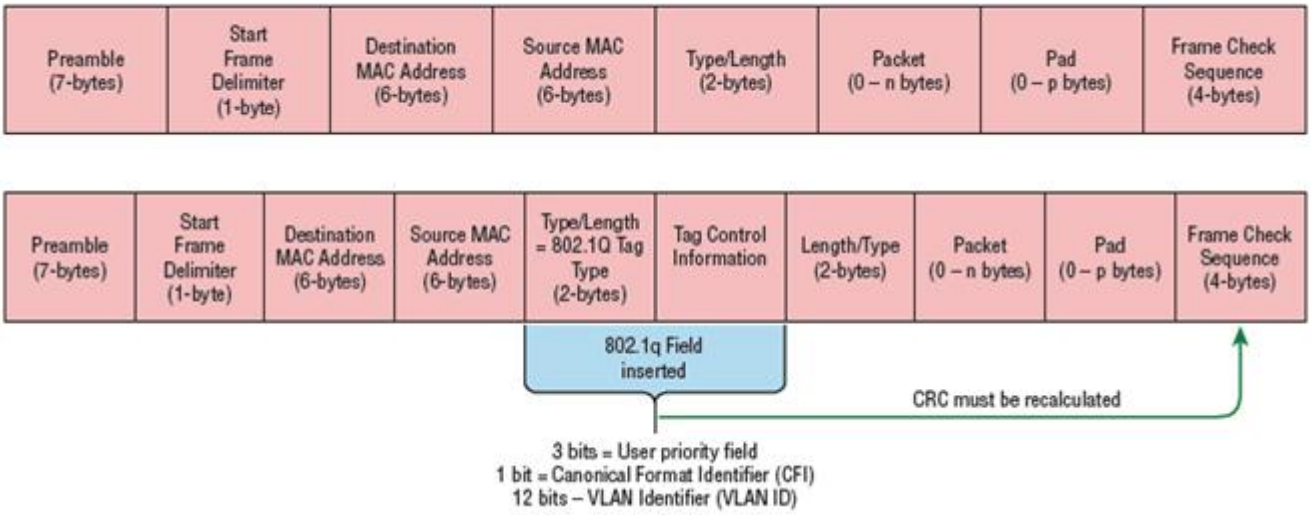

Figure 4: IEEE 802.1q encapsulation with and without the 802.1q tag (**source:** CCNA Routing and Switching, 2013)
Most 2960 model switches only support the IEEE 802.1q trunking protocol, but the 3560 will support both the ISL and IEEE methods

10. Creating And Configuring Vlans

It is easy to create and configure VLAN. One has to decide on the number of VLANs you want to create and establish which users you want in each VLAN, by that one brings an idea of VLAN models into the real world. To configure VLANs on a Cisco Catalyst switch via the Cisco IOS Command Line Interface (CLI), use the *global config vlan command.* Below is an example demonstrating how to configure VLANs on the S1 switch by creating three VLANs for three different departments—Sales, Marketing and Accounting again. Remember that VLAN 1 is the native and management VLAN by default:

```
S1(config)#vlan ?
  WORD        ISL VLAN IDs 1-4094
  access-map  Create vlan access-map or enter vlan access-map command mode
  dot1q       dot1q parameters
  filter      Apply a VLAN Map
  group       Create a vlan group
  internal    internal VLAN
S1(config)#vlan 2
S1(config-vlan)#name Sales
S1(config-vlan)#vlan 3
S1(config-vlan)#name Marketing
S1(config-vlan)#vlan 4
S1(config-vlan)#name Accounting
S1(config-vlan)#^Z
S1#
```

Figure 5: Creating VLAN in CLI (**source:** CCNA Routing and Switching, 2013)

From the output of *figure 5* above, we saw up to 1 to 4094 VLANs. But invariably only 1001 VLANs can be created, and you can't use, change, rename, or delete VLANs 1 or 1002 through 1005 because they're reserved. The VLAN numbers above 1005 are called extended VLANs and won't be saved in the database unless your switch is set to what is called VLAN Trunk Protocol (VTP) transparent mode. You won't see these VLAN numbers used too often in production. After you create the VLANs that you want, you can use the "*show vlan command*" to check them out. By default, all ports on the switch are in VLAN 1. To change the VLAN associated with a port, you need to go to each interface and specifically tell it which VLAN to be a part of. Once the VLANs are created, one can verify it with the show "*vlan command."*

11. Inter-VLAN Routing

The major problem in VLAN is; how can users from one VLAN (broadcast domain), use services offered by another VLAN. Each network has its own needs, though whether it's a large or small network, internal routing, in most cases, is essential. The ability to segment your network by creating VLANs, thus reducing network broadcasts and enhancing security is a technique used by most engineers. Popular setups include a separate broadcast domain for critical

Licensed Under Creative Commons Attribution CC BY

services such as File Servers, Print servers, Domain Controllers and other servers.

Inter-VLAN routing is process of forwarding network traffic from one VLAN to another VLAN using a router. In the previous pages, we learned about how to configure VLANs on a network switch(s). To allow devices connected to the various VLANs to communicate with each other, you need to connect a router. In figure 2, for any host from EBSU Admin VLAN to send traffic to EBSU Database VLAN we deploy Inter-VLAN routing. Hosts in a VLAN live in their own broadcast domain and can communicate freely. VLANs create network partitioning and traffic separation at layer 2 of the OSI. Therefore, if you want hosts or any other IP-addressable device to communicate between VLANs, you must have a layer 3 device to provide routing services.

- **Inter-VLAN routing Implementation**

Using VLANs technology and protocols to segment a network can be useful to control broadcast traffic and implement security boundaries. However, allowing absolutely NO access between VLANs is never very beneficial. To fix this, we suppose to implement inter-VLAN routing. At the CCNA level, there are two ways we can make this happen namely:

a) Attach a unique router port to each VLAN
b) Implement a router on a stick.

12. Conclusion

Though there are some many problems facing network and data communication today but security has always been the most paramount challenge. Every efforts is always how to mitigate insecurity issues and ensure that information is communicated to appropriate destinations without compromise. This paper had adequately discussed the need of implementing Virtual Local Area Network (VLAN) and Inter-VLAN Routing technologies in Ebonyi State University Network. Going by the usual flat Local Area Network infrastructure where every users belong to one broadcast domain different series of network insecurities exist. In the case of an enterprise network having critical file servers, application servers, organisational databases and other confidential information, this would mean that all users would have equal access privileges to these resources. To effectively prevent such situations from operational network we need to restrict access at the network level by segmenting the existing network into different broadcast domains, hence, the need of Virtual Local Area Network (VLAN). In contrast to normally flat LAN architecture where every hosts are connected without segmentation; we break a large broadcast domain into different sizes of broadcast domains by creating Virtual Local Area Networks (VLANs). This VLAN architecture which is a logical grouping of network users and resources connected to administratively defined ports on a switch when deployed in Ebonyi State University Network would be of immense benefit as outlined in the work. In all, this work exhaustively x-rayed the benefits of VLAN and Inter-VLAN routing in managing and maintaining of Ebonyi State University Networks.

References

[1] Baker, R. H. (1995). *Network security*: How to plan for it and achieve it. New York: McGraw Hill, Inc.
[2] Chappell, L. A. and Hakes, D. E. (1994). *Novell's guide to NetWare LAN analysis*. 2nd ed. Alameda, CA: SYBEX Inc.
[3] Comer, D. E. (1995). *Internetworking with TCP/IP*, volume I: Principles, protocols, and architecture. 3rd ed. Upper Saddle River, NJ: Prentice Hall, Inc.
[4] Derfler, F. J. and Freed, L. (1996). *How Networks Work*. 2nd ed. Emeryville.
[5] Henry, P. D. and De Libero, G. (1996) *Strategic networking*: From LAN and WAN to Information superhighways. London: International Thomson Computer Press.
[6] Martin, J., Chapman, K. K., & Leben, J. (1994). *Local area networks: Architectures and implementations*. 2nd ed. New Jersey: P T R Prentice Hall, Inc.
[7] Passmore, D. and Freeman, J. (1998). *The virtual LAN technology report*. [online]. Available: http://www.3com.com/nsc/200374.html. (October 2, 1998)
[8] Roese, J. (1998) *Switched LANs: Implementation, operation, maintenance.* New York: McGraw-Hill, Inc.
[9] Roese, J. and Knapp, E. (1997). *SecureFast:* A comparative analysis of SecureFast and 802.1Q. Rochester, NH: Cabletron Systems, Inc.
[10] SecureFast services overview. (1998). Cabletron Systems product marketing white papers. Rochester, NH: Cabletron Systems, Inc.
[11] Tittel, E. and Robbins, M. (1994). *Network design essentials*. Cambridge, MA: AP Professional
[12] Virtual LAN communications. (1996). [online]. Available: http://cio.cisco.com/warp/public/614/13.html. (October 22, 1998)
[13] VLAN information. UC Davis Network 21. (1998). [online]. Available: http://net21.ucdavis.edu/newvlan.htm. (October 21, 1998)
[14] Institute of Electrical and Electronics Engineers (1998). IEEE P8021.Q, IEEE standards for local and metropolitan area networks: Virtual bridged networks. New York: Institute of Electrical and Electronics Engineers.
[15] CCNA Routing and Switching, 2013 cisco systems *Mega Guide, CCNA 640-802, www.preplogic.com*

Licensed Under Creative Commons Attribution CC BY