IMPROVING SECURITY IN A VIRTUAL LOCAL AREA NETWORK

OSAHON OKORO[1], EMMANUEL AZOM EDIM[2], OFEM AJAH OFEM[3], EYO ESSIEN[4], IWARA OFEM OBONO[5], BUKIE PAUL TAWO[6]

[1.2.3.4.5.6] Computer Science Department, University of Calabar, Nigeria

E-mail: [1]osahonokoro@gmail.com, [2]edimemma@gmail.com, [3]ofemofemajah@gmail.com, [4]essieneyo@unical.edu.ng, [5]ofemiwara@gmail.com, [6]bukiepaultawo@unical.edu.ng

ABSTRACT

Network services running in a native-VLAN infrastructure are vulnerable to security threats as a result of IP information exposure when connected with unmanageable switches. The aim of this study is to create VLANs with bounded network packets in order to reduce the security threats. The cisco hierarchical network design model was used to create separate VLANs, segment the network using IEEE 802.1q (dot1q) encapsulated sub-interfaces and assign ethernet ports (FastEthernet) to respective VLANs. Network packets and other data were captured and analyzed. The study found that on a flat-scale network infrastructure, broadcast packets destined for other vlans created in the switched network were visible to any terminal/node on the network infrastructure thereby exposing the classful IP information. In this study, system attack surface was reduced thereby protecting the VLAN-network. The study found that the 802.1q protocol added overhead to the vlan packets, reduced network efficiency and increased the network loss

Keywords: *IEEE 802.1q protocol, Network Performance, Network Security, VLAN Segmentation, Internet of Things(IoT)*

1. INTRODUCTION

The desire of every network administrator is to effectively manage and secure the network infrastructure with ease irrespective of its size. As the network connectivity continue to expand with the addition of devices and services, the management of dozens, hundreds, or even thousands of computers and other devices within the network become increasingly difficult to administer especially in a large, flat (native-vlan 1 network infrastructure) switched network. In such networks, unmanaged switches are connected together in a campus-wide network topology, the expansion in this context, usually relates to the technological network services introduced into the network with time within the learning environment. This increase in services affect the network Performance and raises security concerns [1]**.**

Sometimes, for its economic value, network developers may choose to deploy a flat-scale or native-vlan1 switched network to connect computer systems and other network devices for a single file sharing purpose service. Due to increase in demand for new services, there may arise a need to accommodate other services such as Voice over Internet Protocol (VoIP), Mailing and Multimedia Services etc. And as a result of the "scalability feature" of a switch network, seamless introduction of new services is possible. But a native vlan depicts a single broadcast domain were switches, by default, are responsible for forwarding all broadcast information from one network device (node) to all devices in the same broadcast domain through any of the ports to all clients. If there are several devices in the single broadcast network served by a single switch, the network is usually flooded with Address Resolution Protocol (ARP) packets' traffic requesting for the end-device mac-address. This in turn affects the performance of the network because, ARP is a protocol used for mapping an Internet Protocol address (IP address) to a physical machine address on the switch CAM table. And as the number of devices (ND) connected to the switch increases, the amount of bandwidth used by unnecessary broadcasts also increases [2].

This implies that there is a threshold in the number of devices a switch can accommodate and able to forward broadcast information. If this number is exceeded, there will be absolutely no communication on the network (downtime/broadcast storm). This is when all packet's Time-To-live (TTL) elapses for all unicast packets and a request-time-out is sent to end-devices. Most network engineers/designers avoid this problem by building a structured network [1]. One way to structure a growing network is to divide it into segments called Virtual Local Area Networks (VLANs). Computer users who work together (workgroups) can be grouped into the same VLANs, irrespective of their location within the building, complex or community.

VLANs are extensively used in Ethernet networks. They are widely deployed to reduce management complexity, to improve network performance and security in enterprise, campus and Data Centre Networks (DCNs) [3]. Traditionally, VLANs comprises of users belonging to the same category, permitting hosts connected to LAN switches to be grouped together into logical groups despite their physical location. Devices in the same logical group (for example, faculties or employees in the same department) are usually classified into a number of VLANs. Traffic loads are spread via a Spanning-Tree protocol, which spans all the switches in LAN and provides path redundancy while eliminating undesirable loops in the network. Traffic between different VLANs is routed through designated routers [4].

This study was an attempt to enhance the security and behavior of Transmission Control Protocol (TCP) used by most network services over a single and multiple broadcast domain in a campus-wide network. The network performance, efficiency and security were also improved by bounding each network service traffic thereby making the broadcast packets from its VLANs visible only to the target destination node. The study created a vlan on layer 2 and also created a virtual interface on a router as the vlan's gateway. The virtual interface was enhanced with an 802.1q tag enabling it to bound the vlan broadcast in a switched network. Thereafter, IP address were added to the enhanced interface for packet routing and switching.

2. REVIEW OF EXISTING INFRASTRUCTURE

VLAN technology has since grown to become one of the most widely used networking architecture today in designing an enterprise network. It is a technology that logically group devices in an Ethernet network together and tag each group as a virtual local area network. Ethernet is a combination of hardware (layer 1) and a specific data structure (layer 2) of the open system interconnection (OSI) reference model. While different "flavors" of Ethernet exist, both in hardware (10Base5, 100BaseT, etc.) and at layer 2 (Ethernet II, Ethernet 802.2, etc.) their principles of operations remain the same. Ethernet hardware consists of shared media (the network cable) connected to network interface cards (NICs) at each station. Stations on the shared media "listen" for it to be clear and transmit once it is clear. If multiple stations hear/sense a clear line and start transmitting at the same time, a "collision" occurs on the infrastructure and the stations involved wait a random amount of time to transmit again. This is the "Stop and Wait" protocol feature that limits signal propagation in a long-range wireless network [5].

In the transmission control protocol (TCP) stack, an address resolution protocol (ARP) message is always sent every time a network device intends to communicate within an internetwork. An important way in which a switch can improve the operation of a network system is simply by controlling this flow of traffic. This control is achieved by manageable switches that are able to logically create environments that their physical interface ports could be assigned to. The ability to intelligently broadcast network packets on only those ports assigned to specific groups makes the switches useful tools for any Ethernet designer faced with continually growing device populations and increasing traffic loads. The logically created environment is commonly referred to as the broadcast domain [6].

Poorly defined broadcast domains can also lead to a broadcast storm, occurring when one device sends a broadcast, and in response, all hosts receiving this broadcast answers with a broadcast of their own. The number of broadcasts continues to rise until these begin to block other network traffic. Collision domains are found on network segments shared by network devices sending unicast traffic. Any part of the network where there is a possibility that Unicast packets from two or more nodes will interfere with each other is considered to be part of the same collision domain. A network with a large number of nodes on the same segment will often have a lot of collision and therefore, large collision domain. Switches break up collision domain by logically placing hosts into their own, smaller collision domains [2].

The Open System Interconnection (OSI) reference model is a reference tool for designing a network of heterogeneous devices from different equipment vendors (i.e. IoT network). The OSI Model system architecture in [7] were categorized into three functional levels of abstraction layers. These are, OSI architecture comprising of OSI services specification and the OSI protocol specification; OSI service specifications which functions guarantee communication between the user and the system in each and every layer; and finally, the OSI protocol specification abstraction which detect and determines the protocol type to be used and run on a specific communication service.

2.1 Network Broadcast Domain

Each Ethernet packet starts with the destination address and thus enable the network interface on a particular workstation to rapidly 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 [8]. However, the Ethernet protocol itself and several higher-level protocols, such as NetWare's IPX/SPX 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 acts 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 corresponding greater use of CPU cycles. And this broadcast can extend from one switch to a switch-to-switch cable connection (aka trunk links) within an internetwork. A concatenation of switches in an internetwork is often referred to as a flat switch network and flat implying "one" broadcast domain. While the multiple broadcast domain is called the large-scale networks because of its scalability feature.

2.2 Broadcast vs Collision Domain

A broadcast domain is the set of hosts (i.e. hubs, switches, routers etc.) and networking devices (usually end-user devices) that are connected in such a way that they receive all broadcast sent on that segment. While a broadcast is a message that has no specific destination but to all, meaning that every single device on the network will receive it. If too many hosts exist in a flat-scale network infrastructure, congestion can occur [2]. A LAN includes all devices in the same broadcast domain. So, from one perspective, a LAN and a broadcast domain can be considered as being basically the same. Poorly defined broadcast domains can also lead to broadcast storm. This is a situation that occurs when one device sends a broadcast, and in response, all hosts receiving this broadcast answers with a broadcast of their own. The number of broadcasts continues to rise until the situation begins to block the network traffic [6].

Collision domains are found on network segments. Any part of the network where there is a possibility that packets from two or more nodes will interfere with each other is considered to be part of the same collision domain. A network with a large number of nodes on the same segment will often have a lot of collision and therefore a large collision domain. The vulnerability of such networks is exposed when a rogue/hacker gain access to such segments, they can easily sniff packets and open ports of all devices on that segment. Switches break up collision domain by logically placing hosts into their own, smaller collision domains [2].

The VLAN technology within switches has the ability to intelligently forward traffic to the specific ports needed to get the packet to its destination. This is what makes the switch a useful tool for the Ethernet implementation when devices and traffic load continue to increase. Switches are then used to manage the flow of packets round the network [6].

2.3 LAN/WAN Technologies in a Campus-Wide Network

Most enterprise computer network can be separated into two general types of technologies: Local-Area Networks (LAN) and Wide-Area Networks (WAN). LANs typically connect nearby devices such as devices in the same room, in the same building, or in buildings inside a campus. In contrast, WANs connect devices that are relatively far apart. Together, LANs and WANs create a complete enterprise computer network, working together to do the job of a computer network: delivering data from one device to another [6].

As the network grows, the traffic on it also grows as well. A network where all traffic flows around the entire network is quick become inefficient and overloaded with CPU cycles when a broadcast storm occurs. This also increases the vulnerability of the network. There is therefore the need for networks to be segmented into smaller, more manageable sections. Switches, routers and bridges can be applied in different ways to achieve this purpose [2]. Switches provide the basic traffic filtering functions which improves network bandwidth. Its internal switching circuits allow traffic flows to simultaneously occur between multiple ports. Supporting multiple simultaneous flows of traffic, or conversations between the ports is a major advantage of switches in network designs.

Several studies have been carried out in attempt to improve network security and performance. Some of these studies include [9] who suggested that Virtual Local area Networks and ACL (Access Control List) should be used to solve problems like low security and overhead management in organizations with large broadcast within their network. [9] Demonstrated that amongst other methods of measuring the performance and security index of a complex network, logical network segmentation has been seen to be the best and seamless method. [10] Proposed a criterion for optimizing network performance which is a trade-off between latency and bandwidth, by using simplified TCP model to show that, when content size is less than 10KB, the deployment should focus on optimizing latency, while for content sizes larger than 1MB, the deployment should focus on optimizing bandwidth. [12] describes an efficient routing algorithm that ensures higher degree of security by monitoring the TCP behavior of a complex network.

These studies have demonstrated that there are numerous ways of improving the performance of a network but there is a growing concern on the aspect of the security of these networks as it grows. However, this work presents an improved implementation of a switched network with VLAN. Because VLANs allows switches to CONTAIN/BOUND unnecessary broadcast traffic in the OSI layer two level, it therefore serves as an alternative solution to routers for broadcast containment. The containment of the unnecessary broadcast traffic improves the security and performance of the network as well.

3. RESEARCH METHOD

In order to achieve the aim of this study, the research process was divided and carried out in three phases. These include: Network analysis and design, Network implementation and Network Instrument/Data Collation matrix. The processes are presented next.

3.1. Network Analysis and Design

The study started with a survey of the available network facilities as well as the ones that were needed to achieve the research objectives. The network environment and other physical facilities within the environment were also examined. This survey provided the needed information that was used in the design of the network topology. The Cisco Three-Layer Hierarchical Model [13] was chosen for implementation of the campus-wide internetwork. Relating with the OSI reference model, the layer that handles more of routing is called the Core Layer, while the layer that covers switching of packets is referred to as the Distribution Layer and the layer that interfaces with the end-devices is known as the Access Layer. The study considered the Cisco 2800 series router for the core layer, the Cisco 2960 series switch for the distribution layer and the 3Com Ethernet switches for the Access layer (Figure 1). The Cisco Three-layer model distributes network devices into logical hierarchy of network responsibilities.

Table 1 presents infrastructures used for the network development of the Network. For a more sustainable network implementation and based on the environment the study applied cabling as a means of connectivity between the various components in the network. The network cable applied include the category-5e Ethernet cables.

Table 1. Network Infrastructures

Network Equipment	Implementation layer
Cisco 2800 series router	Core Layer
Cisco 2960 series switch	Distribution Layer
3Com Ethernet switches/End-devices	Access Layer

The network structure is presented in Figure 1. The design, consists of router, manageable switches and separate Ethernet switch/cable network connections to conform to the cisco hierarchical model specification standard. At the top of the design (Figure 1) is the core layer. In the core layer, the study applied the 2800 series router which is a layer three device as a suitable device for the setup of this network layer. The core layer's fast-Ethernet 0/0 physical interface was connected to the distribution layer. The 2960 series cisco switch is placed as the distribution unit/layer device in relation to the cisco model and 3Com switches are used to connect the end devices at the access unit/layer. The lines from the distribution layer shows the connection of the category-5e Ethernet cables from the manageable switch to the access layer. The access layer connects to the various user devices (e.g. desktop computers in the departments). The user devices in the departments are in separate VLANs.

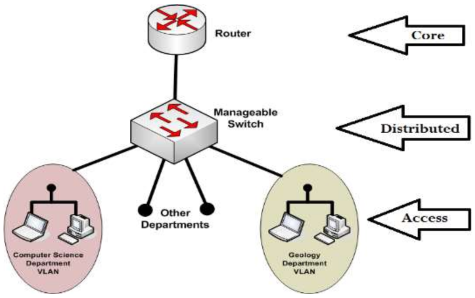


Figure 1. The Structure of the Campus-Wide Network

3.2. Network Implementation

Figure 2 represents the VLAN network connections consisting of the Comp LAN, the Geo LAN with a cisco 2960 switch and 2600 series routers for the different broadcast domains. The Comp_VLAN consists of a 3com switch that connects desktop/laptop and other user end devices in one broadcast domain (Computer Science Department), while Geo_VLAN (3com switch) connects computers and other user end devices in the second broadcast domain (Geology Department) within the campus-wide network. Ethernet cable was used to connect the cisco 2960 switch to all 3com switches. While the router (**Fa0/0 port**) was connected to the Switch (Fa0/24). The distribution and core layer devices were configured and network was fully implemented.

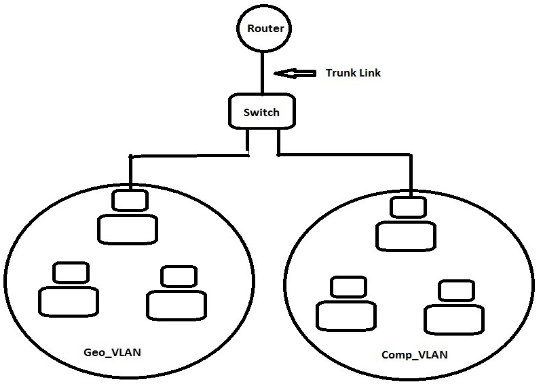


Figure 2. The Implemented VLAN Network Connection

3.2.1. The core layer implementation

Basically, the core of the network performs the function of transporting large volume of traffic both reliably and quickly. The main function of the network's core layer here is to switch traffic as fast as possible [13]. The core layer directly connects and communicate with the distribution layer. We have used the Cisco 2600 series router to implement the network core layer.

The function of this core layer router in this network include the following:

- ✓ Packet switching: it is responsible for moving packets from one broadcast domain to another broadcast domain.
- ✓ Packet filtering: It restricts packets from leaving a broadcast domain at a given time by placing priorities over packets from different devices
- ✓ Internetwork communication: It ensures seamless communication between devices in different broadcast domains
- ✓ Path Selection: It makes the "right" decision on the path a packet is to follow in getting to its destination.

The core router Ethernet interface (fast Ethernet 0/0) was implemented in the live environment. Every interface on the cisco router is on an administrative down state by default. After bringing up the physical interface, virtual interfaces were created using the interface fast Ethernet 0/0.100 command. Each interface was given an IP address using the IEEE 802.1q encapsulation VLAN trunking tag. Since each interface is locally resident on the router, their network addresses automatically appear on the router's routing table as directly connected interface, this is shown in Figure 3. The

IP address given to comp_VLAN network was 192.168.0.0/24 while that of Geo_VLAN, 192.168.1.0/24. Each VLAN has a VLAN ID of 100 and 200 for computer science and geology department respectively. In order not to interfere with the network configuration, it was necessary to introduce a test subnet and assigned IP-address of 19.1.1.0/24 with a VLAN tag of 300 to represent the other departments that are also covered in the network.

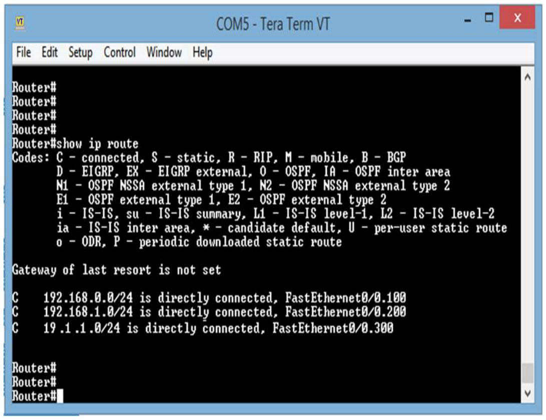
Network service segmentation through VLAN technology provides exclusion between logical network groups [11]. For scalability and security benefits, it is necessary to address some notable security concerns with VLANs switching network during development. For instance, as documented in, VLAN Hopping, MAC attacks, DHCP attacks, spoofing attacks and malicious insider attacks are common security issues [12, 13, 14] and need to be tackle during design and implementation of VLANs switching network. This study made efforts in order to reduce the system attack surface and protect the campus wide network.

Network segregation into VLANs create isolation networks by forming separate broadcast domain within each VLAN. To strengthen the security on the VLAN network against insider attacks, in the segmentation process, we isolated each group from traversing other network devices [15, 16]. The essence of taking this path is to avail the network administrator the flexibility to protect the network against unknown insider's attack. This scheme will also avert the possibility of malicious virtual machine plugged into the network port in order to exploit vulnerability to sniff packets, redirect or prevent traffic from going through virtual network switches. This according to [17], has the potentials to compromised the confidentiality, integrity, and availability of co-located clients on the Layer 2 network infrastructure.

On the design, the GEO_LAN and the COMP_LAN were segmented into Virtual organizational departments using segmentation approach [18]. Thereafter, all MAC addresses within the GEO_VLAN and the COMP_VLAN node were documented and added into the switches Media Access Control (MAC) table or VLAN database [11]. These designated Mac addresses on the switch were then configured as if they belong to either GEO_LAN or COMP_LAN. On testing the setup with Wireshark packet sniffer on a section of our device, we observed that only incoming Ethernet frames were captured which implies that, only frames based on the data residing within IEEE 802.1q frames where forwarded by the switch.

According to [17] vulnerability inherent in the 802.1q VLAN protocol could allow an attacker to evade network segmentation and spoof VLAN traffic by manipulating an Ethernet frame as if it contains two 802.1q VLAN tags. This is known as VLAN hopping. It is a malicious technique employed by an adversary in an attempt to gain access to network resources on a VLAN [14, 11]; or traffic on other VLANs, that in normal circumstance, will not be accessible [14]. The adversary attempts to create security vulnerabilities by sending malicious packets to a port on the switch that could be accessible from a given end. However, VLAN trunk lines configuration technique [13] applied as a countermeasure in mitigating attacks.
In addition, to mitigate CAM attack, MAC address flooding [14] and possibly DHCP starvation, this study enforced ports security restrictions and SNMP lock signal. Port security isolate MAC address flooding attack by allowing only one MAC address on the port interface [12].

Also, to avoid altering of VLAN ID on packets encapsulated for Trunking [19] and mitigate flooding out ports; this study created and use dedicated VLAN ID for all trunk port. This also include the use of 802.1q tags on all the trunk ports for VLAN Trunking, and auto-Trunking deactivation on user facing ports as suggested in [17]. That is, all switch connected ports were set not to negotiate trunk automatically and disabled the DTP. Ports that were not meant to be trunks were explicitly configured as access ports. In order to prevent double tagging attacks, we took all ports away from the native VLAN 1 and configured trunk ports for switch-router-switch connection, changed the native VLAN on all trunk ports to an unused VLAN ID.



```
Router#
Router#
Router#
Router#
Router#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.0.0/24 is directly connected, FastEthernet0/0.100
C    192.168.1.0/24 is directly connected, FastEthernet0/0.200
C    19 .1 .1.0/24 is directly connected, FastEthernet0/0.300


Router#
Router#
Router#
```

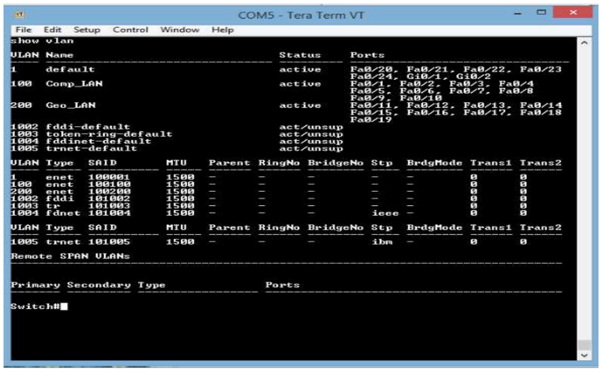
Figure 3. Core Router Routing Table

The codes section in Figure 3 presents how the route was learned by the router. The code “C” indicates that the route is a directly connected route. While “S” implies, the route was statically inputted by the network developer

3.2.2. The distribution layer implementation

The distribution layer links upward to the core layer switch and downwards to the access switches. It is also called aggregation switch which functions as a bridge between core layer switch and access layer switches. In addition, distribution switch ensures that the packets are appropriately routed between subnets and VLANs in enterprise network. The cisco catalyst 2960 switch was used for this implementation and two broadcast domains were created. The first is as the **Comp_VLAN** to cover one group/area and the second designated as Geo_VLAN to cover the other group/area within the campus-wide network.

Each VLAN is tagged with a numeric number called VLAN-ID. Comp_VLAN and Geo_VLAN and the corresponding ports assigned to each VLAN as present in the output of Figure 4. When each VLAN instance is running properly, the status section will indicate “active”.



```
show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
100  Comp_LAN                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
200  Geo_LAN                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
200  enet  100200     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Switch#
```

Figure 4. Distribution Switch VLAN Database

3.2.3. The access layer implementation

This is the lowest level of the Cisco three tier network model. It is often referred to as the desktop layer since it focuses on connecting client nodes to the network. The access layer ensures that packets are delivered to the users end devices. The user end devices used for this implementation include the HP pro desktop computers and other end-user devices. The Access layer setup was achieved through the use of a cross-over Ethernet cable to connect Ethernet interfaces assigned to Comp_VLAN and Geo-VLAN to the 3Com Ethernet switch which connects computing devices in computer science and geology departments respectively. After the implementation, a continuous ping test was conducted with two systems on the Comp_VLAN and a single continuous ping test with a computer system in the Geo_VLAN. During the ping tests, data was captured for analysis.

3.3. Network Output Data and Analysis

Wireshark is an open-source packet analyzer that was used for the data collection and analysis of the network output data and performance. This tool can also be used for network troubleshooting, analysis, software and communications protocol development, and education.

The statistical utility tool within the Wireshark software also collated the packets sequentially to produce Meta-data such as TCP Errors per unit time, Network Conversation, and Network Expert Information.

3.3.1. TCP errors per unit time

The meta-data represent the behavior of TCP packet in the network over a period of time. In this study, the time was set to 1minute and the graph of both existing campus-wide and VLAN TCP error were compared to determine the network performance.

3.3.2. Network conversation meta-data

Network conversation is the traffic negotiation between two specific endpoints in the network. The Wireshark statistical tool was used to capture each address, packet and byte counter, for each IP conversation including the duration of the conversation in seconds and average bits per second in each direction. The captured packets from the campus-wide network was analyzed in order to isolate packet loss via retransmission and duplicate ACKs (Acknowledgement Packet). This helped to determine the network efficiency.

3.3.3. Network expert information meta-data

During the study, the network expert information was also captured and analyzed to determine the network behavior. Expert information (Expert info) is another featured meta-data that groups the packets captured into severity, summary, protocol and count. It is this feature that produces the number of packets retransmitted and the number of packets transmitted per protocol. The TCP packet was used for computation in this study. Expert info is a log of all anomalies found the captured file. The general idea behind the "Expert Info" is to have a better display of "uncommon" or just notable network behavior. This way, both novice and expert users will hopefully find probable network problems a lot faster, compared to scanning the packet list "manually".

4. Results and Discussion

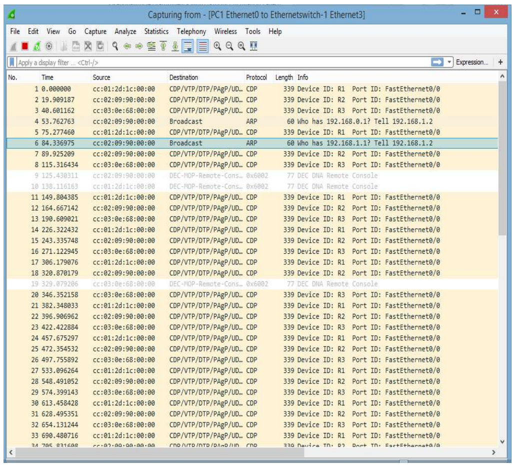
4.1 Results and Data Analysis

The ping command is a general-purpose network diagnostic command to check for network connectivity between two nodes in a network or internetwork. This command works by sending ICMP echo into the intended network requesting for the destination device's layer two (MAC) hardware address. A reply message is displayed on the screen if the sending host receives a reply from the destination, or else it returns a "destination host unreachable" returned by the router when the time to leave (TTL) assigned to each packet elapse. Packets generated by these ICMP echo request/reply were also captured in a flat-scale network infrastructure network and VLAN (multiple broadcast domain) respectively for analysis.

4.1.1 Data from the single (Flat-scale) broadcast domain

To capture data from the single-flat broadcast domain with multiple network services, a cross-over Ethernet cable was used to connect the 3Com switches which is a flat-scale flat-scale network infrastructure (VLAN1) in order to gain access into the Comp_VLAN. The connection merged both Comp_VLAN to Geo_VLAN and in turn flood both broadcast traffic to each subnet. This is possible due to the scalability qualities of switched Ethernet network. A Toshiba 64bit laptop was connected to one of the Computer Science LAN 3Com switch ports and a ping command (***ping 192.168.0.1 –t***) was issued in the command window. This command enabled the capturing of network packets from the flat-scale network infrastructure. The data is presented in Figure 5. The fourth (4th) and sixth (6th) rows (Figure 5) contains the captured packets data. The data showed that the broadcast information was meant for both 192.168.0.0/24 and 192.168.1.0/24 networks.

This shows the vulnerability of a single-flat broadcast domain. Since the Comp_VLAN can receive broadcast from Geo_VLAN. The information from the broadcast packet can be used to determine the classful IP address (192.168.1.0/24). With the classful address, an intruder can assign an address to his/her system. This is done with the intent that most network administrators hardly have that number of systems on the network. The intruder system can then post as a valid system and continue to gain unauthorized access into the network. A simple port scan of all the system in that network will further expose the open ports on the network devices. This points to the vulnerability of the single flat-scale broadcast domain that is very common in most organization network setup. Implementing VLAN and elevating the network layer 3 will further divide the broadcast domain into different bounded VLAN broadcast domains.

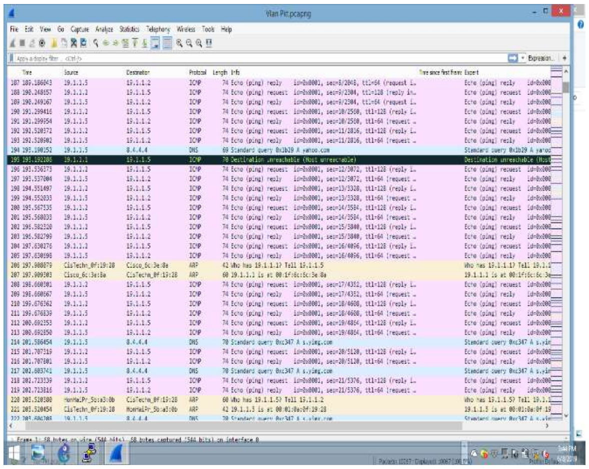

Capturing from - [PC1 Ethernet0 to Ethernetswitch-1 Ethernet3]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time        Source             Destination            Protocol Length Info
   1 0.000000    cc:01:2d:1c:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R1  Port ID: FastEthernet0/0
   2 19.909187   cc:02:09:90:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R2  Port ID: FastEthernet0/0
   3 40.601162   cc:03:0e:68:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R3  Port ID: FastEthernet0/0
   4 53.762763   cc:02:09:90:00:00  Broadcast            ARP       60 Who has 192.168.0.1? Tell 192.168.1.2
   5 75.277460   cc:01:2d:1c:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R1  Port ID: FastEthernet0/0
   6 84.336975   cc:02:09:90:00:00  Broadcast            ARP       60 Who has 192.168.1.1? Tell 192.168.1.2
   7 89.925209   cc:02:09:90:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R2  Port ID: FastEthernet0/0
   8 115.316434  cc:03:0e:68:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R3  Port ID: FastEthernet0/0
   9 125.430311  cc:02:09:90:00:00  DEC-MOP-Remote-Cons… 0x6002    77 DEC DNA Remote Console
  10 138.116163  cc:01:2d:1c:00:00  DEC-MOP-Remote-Cons… 0x6002    77 DEC DNA Remote Console
  11 149.804385  cc:01:2d:1c:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R1  Port ID: FastEthernet0/0
  12 164.667142  cc:02:09:90:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R2  Port ID: FastEthernet0/0
  13 190.609021  cc:03:0e:68:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R3  Port ID: FastEthernet0/0
  14 226.322432  cc:01:2d:1c:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R1  Port ID: FastEthernet0/0
  15 243.335748  cc:02:09:90:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R2  Port ID: FastEthernet0/0
  16 271.122945  cc:03:0e:68:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R3  Port ID: FastEthernet0/0
  17 306.179076  cc:01:2d:1c:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R1  Port ID: FastEthernet0/0
  18 320.870179  cc:02:09:90:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R2  Port ID: FastEthernet0/0
  19 329.079206  cc:03:0e:68:00:00  DEC-MOP-Remote-Cons… 0x6002    77 DEC DNA Remote Console
  20 346.352158  cc:03:0e:68:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R3  Port ID: FastEthernet0/0
  21 382.348033  cc:01:2d:1c:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R1  Port ID: FastEthernet0/0
  22 396.906962  cc:02:09:90:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R2  Port ID: FastEthernet0/0
  23 422.422884  cc:03:0e:68:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R3  Port ID: FastEthernet0/0
  24 457.675297  cc:01:2d:1c:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R1  Port ID: FastEthernet0/0
  25 472.354532  cc:02:09:90:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R2  Port ID: FastEthernet0/0
  26 497.755892  cc:03:0e:68:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R3  Port ID: FastEthernet0/0
  27 533.096264  cc:01:2d:1c:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R1  Port ID: FastEthernet0/0
  28 548.491052  cc:02:09:90:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R2  Port ID: FastEthernet0/0
  29 574.399143  cc:03:0e:68:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R3  Port ID: FastEthernet0/0
  30 613.458428  cc:01:2d:1c:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R1  Port ID: FastEthernet0/0
  31 628.495351  cc:02:09:90:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R2  Port ID: FastEthernet0/0
  32 654.131244  cc:03:0e:68:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R3  Port ID: FastEthernet0/0
  33 690.480716  cc:01:2d:1c:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R1  Port ID: FastEthernet0/0
  34 705.831608  cc:02:09:90:00:00  CDP/VTP/DTP/PAgP/UD… CDP      339 Device ID: R2  Port ID: FastEthernet0/0
```

Figure 5. Flat-Scale Broadcast Domain Packets

4.1.2 Data capture in multiple broadcast domain (VLAN) network

The test on the VLANs was conducted to gather data for analysis. The data represent the network traffic/packets transmitted in the network. These include packets captured packets in the different broadcast domain (The VLANs). The campus network contains different subnets where the tests were conducted. These include a ping test on 19.1.1.0/24 subnet alongside the ping test going on in the 192.168.0.0/24 and 192.168.1.0/24 subnets (the VLANS). The data captured contained packets that enter and leave the network. This is shown in Figure 6. The results show that no packet from 192.168.0.0/24 and 192.168.1.0/24 ARP (VLANs) was transmitted into other subnets within the campus network. Neither did the broadcast from the other subnets entered into the VLANs even though they were all connected to the same distribution layer. This means that the broadcast from other subnets ends within their subnets. The broadcast is all bounded to their subnets only. Hence when a network user or an intruder gain access into any of the subnets, broadcast packets from other subnets are not visible to the intruder and is unable to have access to the classful IP information of the VLANs. This feature will improve security in the VLAN.


Vlan Pit.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Time since first frame
Expert
Profile: Default

```
     Time        Source             Destination        Protocol Length Info
187 189.186043  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=8/2048, ttl=64 (request i…
188 190.248657  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=9/2304, ttl=128 (reply in…
189 190.249167  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=9/2304, ttl=64 (request i…
190 191.299416  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=10/2560, ttl=128 (reply i…
191 191.299954  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=10/2560, ttl=64 (request …
192 192.520372  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=11/2816, ttl=128 (reply i…
193 192.520902  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=11/2816, ttl=64 (request …
194 193.190152  19.1.1.5           8.4.4.4            DNS   69 Standard query 0x1b29 A yahoo.com
195 193.192286  19.1.1.1           19.1.1.5           ICMP  70 Destination unreachable (Host unreachable)
196 193.536373  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=12/3072, ttl=128 (reply i…
197 193.537004  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=12/3072, ttl=64 (request …
198 194.551497  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=128 (reply i…
199 194.552033  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=13/3328, ttl=64 (request …
200 195.567535  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=14/3584, ttl=128 (reply i…
201 195.568033  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=14/3584, ttl=64 (request …
202 196.582320  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=15/3840, ttl=128 (reply i…
203 196.582799  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=15/3840, ttl=64 (request …
204 197.630276  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=16/4096, ttl=128 (reply i…
205 197.630698  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=16/4096, ttl=64 (request …
206 197.908879  CisTechn_0f:19:28  Cisco_6c:3e:8a     ARP   42 Who has 19.1.1.1? Tell 19.1.1.5
207 197.909303  Cisco_6c:3e:8a     CisTechn_0f:19:28  ARP   60 19.1.1.1 is at 00:1f:6c:6c:3e:8a
208 198.660301  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=17/4352, ttl=128 (reply i…
209 198.660667  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=17/4352, ttl=64 (request …
210 199.676362  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=18/4608, ttl=128 (reply i…
211 199.676839  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=18/4608, ttl=64 (request …
212 200.692353  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=19/4864, ttl=128 (reply i…
213 200.692850  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=19/4864, ttl=64 (request …
214 201.586454  19.1.1.5           8.4.4.4            DNS   70 Standard query 0xc347 A s.yimg.com
215 201.707319  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=20/5120, ttl=128 (reply i…
216 201.707801  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=20/5120, ttl=64 (request …
217 202.603741  19.1.1.5           8.4.4.4            DNS   70 Standard query 0xc347 A s.yimg.com
218 202.723339  19.1.1.2           19.1.1.5           ICMP  74 Echo (ping) request  id=0x0001, seq=21/5376, ttl=128 (reply i…
219 202.723816  19.1.1.5           19.1.1.2           ICMP  74 Echo (ping) reply    id=0x0001, seq=21/5376, ttl=64 (request …
220 203.520380  HonHaiPr_5b:a3:0b  CisTechn_0f:19:28  ARP   60 Who has 19.1.1.5? Tell 19.1.1.2
221 203.520454  CisTechn_0f:19:28  HonHaiPr_5b:a3:0b  ARP   42 19.1.1.5 is at 00:01:0a:0f:19:28
222 203.604208  19.1.1.5           8.4.4.4            DNS   70 Standard query 0xc347 A s.yimg.com

Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Packets: 10067 · Displayed: 10067 (100.0%)
```

Figure 6. Multiple Broadcast Domain Packet Capture

4.2 Network Efficiency Analysis

The Transmission Control Protocol (TCP) is a complex protocol, relative to UDP, as it integrates a mechanism which checks that all packets are correctly delivered (i.e. acknowledgment). It consists of having the receiver transmit a specific packet or flag to the sender to confirm the proper reception of a packet. For efficiency purposes, not all packets will be acknowledged one by one; the sender does not wait for each acknowledgment before sending new packets. Indeed, the number of packets that may be sent before receiving the corresponding acknowledgement packet is managed by a value called TCP congestion window.
The TCP congestion window mechanism deals with missing acknowledgment packets as follows:

- ✓ If an acknowledgement packet is missing after a period of time, the packet is considered as lost and **retransmitted** which in turn will affect the speed of transmission.

- ✓ The TCP congestion window is reduced by half (hence, also the throughput – which corresponds to the perception of limited bandwidth capacity on the route by the sender); the TCP congestion window size can then restart increasing if acknowledgment packets are received properly.

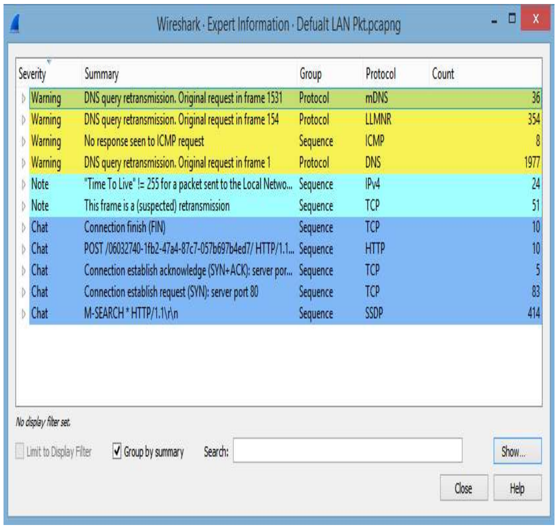
To measure the data transferred and retransmitted (packet loss), packets were sniff from the entire network including the VLANs. This was done in order to measure the efficiency of the network which is directly related to the performance of the network. To achieve this task, equation 1 below was used to calculate the efficiency of the network while Equation 2 was used to determine the network loss [14, 15].

$$\text{Efficiency}, \eta = 100 \text{ x } \frac{(Transferred - retransmitted)}{Transferred} \quad (1)$$

$$\text{Network Loss} = 100\% - \text{Efficiency} \quad (2)$$

The efficiency of the network is the percentage of data transmitted; and is derived by taking the difference between the amount of data transmitted and the packet loss divided by the amount of transmitted data multiplied by a hundred [9]. In order to determine the efficiency of the network, packets data were collected for analysis and to determine the network performance index.

The Expert Information pcapng metadata is displayed in Figure 7. different severity levels in the expert info window (Figure 7). It provides information or data about connection problems, successful workflow e.g. TCP packet with SYN flag set, and information about packet retransmission in the network.



Wireshark · Expert Information · Defualt LAN Pkt.pcapng

Severity	Summary	Group	Protocol	Count
Warning	DNS query retransmission. Original request in frame 1531	Protocol	mDNS	36
Warning	DNS query retransmission. Original request in frame 154	Protocol	LLMNR	354
Warning	No response seen to ICMP request	Sequence	ICMP	8
Warning	DNS query retransmission. Original request in frame 1	Protocol	DNS	1977
Note	"Time To Live" != 255 for a packet sent to the Local Netwo...	Sequence	IPv4	24
Note	This frame is a (suspected) retransmission	Sequence	TCP	51
Chat	Connection finish (FIN)	Sequence	TCP	10
Chat	POST /06032740-1fb2-47a4-87c7-057b697b4ed7/ HTTP/1.1...	Sequence	HTTP	10
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	5
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	83
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	414

No display filter set.

□ Limit to Display Filter ☑ Group by summary Search:

Figure 7. Default LAN Expert Information.

To calculate the network efficiency for flat-scale network infrastructure, the transmission control protocol (TCP) packets observed in Figure 9 are applied. The TCP protocol had three (3) set of transferred packets namely:

$$\text{Connection finish (FIN)} = 10 \text{ Packets}$$
$$\text{Connection establish acknowledge } (SYN - ACK) = 10 \text{ Packets}$$
$$= 5 \text{ Packets}$$
$$\text{Connection establish request (SYN)} = 83 \text{ Packets}$$

Therefore,

Total number of TCP transferred packets (X) = (PFIN +PSYN-ACK + PSYN)
= 10 + 5 + 83 = 98 Packets

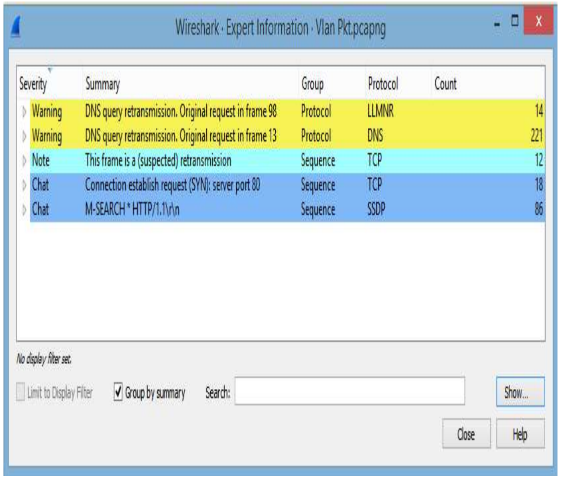
It also shows that number of TCP retransmission (Y) = 51 Packets

Thus:
The Efficiency of the network

$$= 100 * \frac{(X - Y)}{X}$$
$$= 100 * \frac{(98-51)}{98}$$
$$= 47.9\%$$

While the network loss = 100 – 47.9
= 52%

Figure 8 displays the transmission control protocol (TCP) packets from the VLAN. Warning (with yellow background) indicates applications returned an “unusual” error code like connection problem, Chat (with blue background) indicates information about successful workflow e.g. TCP packet with SYN flag set and established request and Note (with cyan background) displayed notable information about packet retransmission.



Wireshark · Expert Information · Vlan Pkt.pcapng

Severity	Summary	Group	Protocol	Count
Warning	DNS query retransmission. Original request in frame 98	Protocol	LLMNR	14
Warning	DNS query retransmission. Original request in frame 13	Protocol	DNS	221
Note	This frame is a (suspected) retransmission	Sequence	TCP	12
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	18
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	86

No display filter set.

□ Limit to Display Filter ☑ Group by summary Search:

Figure 8. VLAN Expert information

The data in Figure 8 was used to calculate the efficiency of the VLAN network. Unlike the default

LAN result, the TCP protocol in the VLAN had only one set of transferred packets namely:

$$\text{Connection establish request (SYN)}$$
$$= 18 \text{ Packets}$$

Therefore,

the Total number of TCP transferred packets (N) $= (P_{SYN})$

$= 18$ Packets

Number of TCP retransmission (M) $= 12$ Packets

Inserting the N and M into the efficiency equation (1),

The Efficiency of Comp_VLAN

$$= 100\ x\ \frac{(N-M)}{N}$$
$$= 100\ x\ \frac{(18-12)}{18}$$
$$= 33\%$$

Thus, the network loss $= 100 - 33$
$= 67\%$

The results imply that:

1. VLANs have a lower network efficiency when compared with the flat-scale network and
2. A relatively higher percentage in network loss, due to the overhead on the VLAN packets as a result of the sub-interfaces.

5. CONCLUSION

The issue of network security can never be over flogged. Setting up a flat-scale/single broadcast domain network is economically viable, but the security risk associated with it is relatively huge as the network increases in size. This study was an attempt to enhance the security in the Transmission Control Protocol (TCP) used by most network services over a single and multiple broadcast domain in a campus-wide network. The cisco hierarchical model was used to build a campus-wide network into the core, distribution and access layers and segment the network in VLANs. This bounded the broadcast of each network service to its subnet.

The open system interconnection (OSI) reference model addresses the concept of breaking or segmenting a broadcast domain at the network layer. Hence, this encourages the deployment of Classful IP address networks (i.e. /8, /16, /24) by network developers. But as the network expands with the addition of other network services that uses classless IP address scheme, each network broadcast information could be assessed by other networks in the same physical infrastructure. The situation creates security problems with serious implications. Hence the introduction of VLAN with multiple domains to enhance the security and performance in the network.

During this study, it was seen that VLAN (multiple broadcast domain) architecture produced a higher performance index compared to flat-scale network infrastructure, and Conserve bandwidth of the Links since lower TCP errors were recorded. also, it was showed that the VLANs have a lower network efficiency if compared to default-single broadcast network and a relatively higher percentage network loss. This was expected due to the additional overhead load that the encapsulation of VLAN tags introduced to the network.

REFERENCES

[1] A. Mohanned, &, S. S. Abubucker, "Managing Network Components using SNMP", *International Journal of Scientific Knowledge (IJSK)*, Vol 2, No. 3, 2012.

[2] Y. Bhaiji, Retrieved from Cisco.com: www.Cisco.com/c/dam/global/en_ae/assets/exposaud2009/assets/docs/layer2-attacks-and-mitigation-t.pdf, August 8, 2019

[3] R. L. Bull, J. N. Matthews, K. A. Trumbull, "VLAN hopping, ARP poisoning and Man-In-The-Middle Attacks in Virtualized Environments", *DEF CON*, 2016., p. 9.

[4] B. Chris, "Introduction to Cisco Networking Course Guide", The Bryant Advantage (pp. 1, 35, 37). San Diego: Lab Workbook

[5] cisco. (2006, August 25). Inter-Switch Link and IEEE 802.1Q Frame Format. (CISCO) Retrieved from www.cisco.com: https://www.cisco.com/c/en/us/support/docs/lan-switch/8021q/17056-741-4.html

[6] D. E. Comer, "Internetworking with TCP/IP" (3rd ed., Vol. 1). *New Jercey: Prentice Hall, Inc*.

[7] S. Deb, "Scaling your network with VLANs" Retrieved from www.techrepublic.com: http://www.techrepublic.com/article/scaling-your-network-with-vlans, 2015, March 4th

[8] Exinda, manuals.gfi.com. Retrieved 2019, from intronetworks.cs.luc.edu/current/html/packets.html: https://manuals.gfi.com/en/exinda/help/content/exos/how-stuff-works/packet-loss.htm, 2019

[9] B. M. Febrero, "TRAFFIC ANALYSIS WITH WIRESHARK" INTECO, Valencia.

[10] P. Garimella, Y. Sung, N. Zhang, and S. Rao, "Characterizing VLAN usage in an operational network" *2007 SIGCOMM workshop on Internet Network Managemen,t* (pp. 305-306). ACM.

[11] B. Genge, and C. Siaterlis, "An experimental study on the impact of network segmentation to the resilience of physical processes" *In International Conference on Research in Networking*, Berlin, Heidelberg: Springer, 2012, pp. 121-134.

[12] J. N. Guichard, W. S. Wainner, S. Adler, K. A. Jabr, and S. S. Van De Houten, Washington, DC Patent No. US 7,688,829 B2, 2010, March 30

[13] W. Krzysztof, "Introduction to Digital Communication Systems" *Poland: John Wiley & Sons Ltd*, 2009.

[14] G. Leischner , and C. Tews, "Security through VLAN Segmentation: Isolating and Securing Critical Assets without Loss of Usability" *9th Annual Western Power Delivery Automation Conference. Spokane, Washington,* 2007.

[15] P. Medagliani, G. Ferrari, G. Germi, and F. Cappelletti, "Simulation-assisted analysis and design of STP-based networks*" International Conference on Simulation Tools and Techniques,* Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST), 2, pp. 1-8.

[16] B. Murtha, E. P. Patrick, and U. B. Sheila "Introduction to Metadata". (Eds.) Paul, Getty, Vol 3.

[17] H. Ningning, S. Oliver, W. Jia, and S. Peter, "Optimizing Network Performance in Replicated Hosting" *Carnegie Mellon University, AT&T LABS, Pittsburgh,* 2007.

[18] T. Olzak, "VLAN Network Segmentation and Security" - *Chapter 5. Retrieved from INFOSEC: https://resources.infosecinstitute.com/vlan-network-chaper-5/#gret,* 2018, April 18

[19] Okoro Osahon, and Edim Azom Emmanuel, "A Wireless Network Infrastructure Architecture for Rural Communities" *International Journal of Computer Science and Information Technology,* Vol 9, No. 3, 2017 p. 43-62.

[20] K. S. Ramesh, "Network Performance: Does It Really Matter To Users And By How Much?" *University of Massachusetts. Amherst and Akamai Technologies Inc,* 2004.

[21] Stallings. (2003). "Network Security Essentials Applications and Standards" (2nd ed.)", New Jersey: Pearson Education. 2003.

[22] B. Suyadip, "Improving Network Performance with Affinity based Mobility Model in Opportunistic Network" *International Journal of Wireless & Mobile Networks*, 4(2), 189-202, 2012.

[23] S. Thakur, A. Khan, and J. Dave, "Three tier architecture with enhanced security at layer 2 and layer 3" *International Advanced Research Journal in Science, Engineering and Technology*, 5 (Special Issue 3), 12-17, 2018.

[24] L. Todd, *Cisco Certified Network Associate: Study Guide* (6th Ed.). (K. Jeff, Z. A. Toni, J. C. Patrick, G.-P. Sarah, & F. Judy, Eds.) Indiana, Indianapolis: Neil Edde, 2007.

[25] O. Wendell, *Cisco CCENT/CCNA ICND1 Official Cert Guide*, Cisco Press, 2003.