NETWORK PERFORMANCE DELAYS AND QU`ALITY OF SERVICES USING VIRTUAL LOCAL AREA NETWORK (VLAN) TECHNOLOGY

BY

ALI AHMED JAMA

ID: 193-25-846

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science and Engineering

Supervised By

Dr. Sheak Rashed Haidar Noori

Associate Professor and Associate Head

Department of CSE

Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

AUGUST 2020

APPROVAL

This Project titled “NETWORK PERFORMANCE DELAYS AND QUALITY OF SERVICES USING VIRTUAL LOCAL AREA NETWORK (VLAN) TECHNOLOGY”, submitted by ALI AHMED JAMA and ID No. 193-25-846 to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 29th August, 2020.

BOARD OF EXAMINERS

Prof. Dr. Syed Akhter Hossain **Chairman**
Head, Computer Science and Engineering
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Dr. Sheak Rashed Haider Noori **Internal Examiner**
Associate Professor and Associate Head
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Md. Zahid Hasan **Internal Examiner**
Assistant Professor
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Dr. Mohammad Shorif Uddin **External Examiner**
Professor
Department of CSE
Jahangirnagar University

DECLARATION

I hereby declare that, this thesis has been done by me under the supervision of **Dr. Sheak Rashed Haider Noori, Associate Professor and Associate Head, Department of CSE** Daffodil International University. I also declare that neither this thesis nor any part of this thesis has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Dr. Sheak Rashed Haider Noori
Associate Professor and Associate Head
Department of CSE
Daffodil International University

Submitted by:

Ali Ahmed Jama
ID: -193-25-846
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First i express my heartiest thanks and gratefulness to almighty God for His divine blessing makes me possible to complete the final year graduation thesis successfully.

I really grateful and wish my profound my indebtedness to **Supervisor Dr. Sheak Rashed Haider Noori**, **Associate Professor and Associate Head**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of my supervisor in the field of "NETWORK PERFORMANCE DELAYS AND QUALITY OF SERVICES USING VIRTUAL LOCAL AREA NETWORK (VLAN) TECHNOLOGY" to carry out this thesis. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this thesis.

I would like to express my heartiest gratitude to **Prof. Dr. Syed Akhter Hossain** Head of Department of CSE, for his kind help to finish my thesis and also to other faculty member and the staff of CSE department of Daffodil International University.

I would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, I must acknowledge with due respect the constant support and patients of my beloved parents.

ABSTRACT

In ordinary/traditional Local Area Network (LAN), all gadgets related/connected on switches have a spot with one transmission domain. Virtual Private Local Area Network (VLAN) innovation partitions a physical LAN into different gatherings called VLANs and allows only devices on the equal VLAN to talk with one another while confining devices on various VLANs from sending network traffic. This technological advancement remembers security for the LAN and controls system/network transmission domain. Virtual LANs (VLANs) offer a system for segregating one physical LAN into various correspondence domains. Regardless, VLAN-engaged switches can't, without any other person, forward traffic across VLAN cutoff points and limits. For interior VLAN correspondence, a Layer 3 switch is required. This investigation paper discusses the VLAN protocol and different ways and potential protocols related with making and completing Inter-VLAN routing for effective assignment of system/network benefits in our campus's four Virtual Local Area Networks.

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

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1 Introduction

Throughout the entire existence of ethernet, the VLAN is an ongoing expansion. The VLAN was acquainted with unravel various systems administration issues. In this section we will find out about the advancement of Ethernet, the reasons VLANs were presented, and the manners in which that VLANs can be utilized. we will likewise find out about the systems administration guidelines that address the VLAN usage.

As LAN protocol, an early ethernet was economical to introduce and work when contrasted with contending conventions, for example, Token Ring and Arc net. It worked as a straightforward transport design utilizing an entrance technique recognized as Carrier Sense Multiple Access CSMA with Collision Detection CD or CSAM/CD. A basic dispute protocol, CSMA/CD necessitated that stations "tune in" for broadcasting on the coaxial link-based system and possibly transmit if no different transmissions were heard. On the off chance that at least two devices transmitted simultaneously, a crash happened and the devices were required to transmit once more[1].

1.2 Statement of the Problem

Ethernet functioned admirably with a couple arranged devices however as networking systems developed, CSMA/CD ended up being a protocol with an issue regarding to traffic load and jams network performance delays. A lot of traffic caused such a large number of retransmissions, and the productivity of the system declined.

To make more simpler the establishment of ethernet networks, a change was made to the network system architecture. Network designs were changed over from coaxial link to turned pair cabling by presenting other devices into the network system. That desktop/device is known as a center point. The motivation behind the center was to rehash signals transmitted to it with the goal that all devices connected to the center point responded as though they were as yet joined to coaxial link. The center point or old hub never really evacuate the issues related with CSMA/CD and the network performance delays. On the off chance that anything, since it was anything but difficult to interconnect center points/hubs or add extra system devices to attach the network/hub, systems turned out to be increasingly packed. A swift response for the issue was important.
[2]

1.3 Goals and The Objectives of The Study

The fundamental goals of this study are to beaten the difficult coaxial cable and hub-based twisted pair cable network for the network trafficking and collision and the improvement of the Quality of Service QoS of network performance delays of the data through its journey from the sender to its destination and the followings are some tips which are the most accurate solutions for this manner.

1.3.1 Specific Objectives:

- To set a switch based ethernet peer to peer network for the solutions of the existing problem of the above scenario. “the reason we choose the switch is that the switch is more intelligent than the hub and it can be managed through different aspects same as the router”.
- Eliminate the conflict method of access initiate in the first CSMA/CD procedure that resulted data collision and traffic crowds and to improve the Quality of Services QoS of the network data/frame transmission delays with utilization of the vlan technology.
- Provide for a special pathway between each interface on the switch.
- To perform full duplex (2-way data transmission) or on the other hand synchronous transmission and gathering on each switch and system ports or network interface card.

1.4 Scope of The Study

The scope of this study will be shifting/evolving from the complex coaxial-based networks and un-intellectual hub-based networks to a better networking evolution with high quality of service QoS and lessen network performance delays which is the logically manageable switch-based network for implementing such VLANs and advanced networking implementations.

1.5 Significances of The Study

In this study the reason we choose for this study's scope to be implemented in virtual local area network vlan is the VLAN has more significances and they are as the followings

- It decreases the necessity to have switches put in placed on the network system to comprise communication traffic/jam.
- Flooding of a package is compelled to the switch ports that have a spot with a VLAN.
- Control of transmission areas on a network system in a general sense decreases traffic/jam.
- It permits numerous devices & devices to be related in every way that really matters to each other like they were in a LAN sharing a lonely transmission domain.
- It might support diminish IT cost, improve network security and execution, give less complex organizing, similarly as ensuring system flexibility [4].

1.6 Methodology and The Tools Required

In this study's methodology can sub divided into two parts which are a physical environment and virtual platforms to implement the scenario behind this study.

1.6.1 Physically

To set in to place a physical functional hub/switch devices and communication medium cables to implement the scenario as an actual data transmission between 4 or more computer devices and show the results for the above-mentioned problem statement and its solutions.

1.6.2 Virtually

In a virtual way it can be implemented in a virtual environment which means to implement this scenario on a Cisco-packet tracer or GNS3 platforms and other similar networking environments as well and also show the real configurations of this study and the connectivity ranges and data transmission among the connected devices.

1.7 Research Analysis and Results (Questionnaire)

In this research questionnaire later chapters we will focus the actual analysis and results of the network delay performance to improve the quality of the service QoS of the entire network and on this point while implementing on this network quality improvement we will also get out of the box the CSMA/CD issue that we mentioned in our problem statement during the VLAN concept inception by automatically.

In view of the above targets the examination is boarded to address the following research hypothesis:

i. How does the VLANs are configured?

ii. How does the network delay performance be improved?

iii. How can improve the QoS when using VLAN technology in the network?

iv. Does the switch apply internet protocol address for implementing the VLAN network?

ii. What are the difference between a Hub and Switch please specify how they operate?

iii. Distinguish between coaxial cable-based network and twisted pair cable-based network?

CHAPTER 2: VLAN BACKGROUND AND CONCEPTION

2.1 Introduction

Virtual Local Area Networks (VLANs) — a generally utilized innovation that is barely examined in network admins course books. VLANs originally proposed to permit network admins to relate a number of hosts in a comparable communication space, free from their physical area or location.

Be that as it may, the present companies or business managers utilize VLANs for decent assortment of different purposes, most particularly for better adaptability and flexible delineation of techniques. by the by, business heads have seen different issues of VLANs considering the way that VLANs are utilized for different purposes they were not proposed for. Reasonably, VLANs are, most perfect scenario a fragmented/incomplete reaction for a segment of these issues. Appropriately, regulating and supervising VLANs is one of the best testing exercises they face.

In this part and the entire investigation, we study four VLANS of containing three college sections and one academic division to a superior comprehend how VLANs are used for all intents and purposes speaking.

Through consultations with network admins, additionally, revolved around appraisal of switch config commands/orders, we have expanded further understandings into how the managers/supervisors use VLANs to achieve a gathering of plan targets, and the disarrays they experience through their journey. We show that VLANs are not particularly worked for enormous amounts of the tasks that they bolster today, and contend that future organizations or business network plans should decouple system depictions from adaptability issues with layer-2 protocols, network architecture, and tending to. After a concise survey of VLAN development, we describe how the four system/networks use VLANs to help resource division, get the opportunity to control, decentralize the board, and host adaptability.

However, VLANs were not planned in light of these objectives — network admins use VLANs for the nonattendance of a supervisor/manager substitute. We contend that VLANs are too head a section for demonstrating approaches, because of adaptability obstacles (on the number and size of VLANs) and the coarse-grained strategies for offering traffic to various VLANs. Further, VLAN config orders are irrationally stunning, in view of the tight associating with crossing/traversing tree creation, disillusionment recover, have address task, and Internet Protocol IP routing/directing.

[5]

2.2 Concept Inception

In this concept inception we will discuss about the entire four networks designed for the VLAN and how they are supported to each other with their main objective and adjacent of the different network classes of the entire network and how they understand each other.

The below diagram shows how does the four networks are connected and the switch device that support this network to be sustainable and scalable.

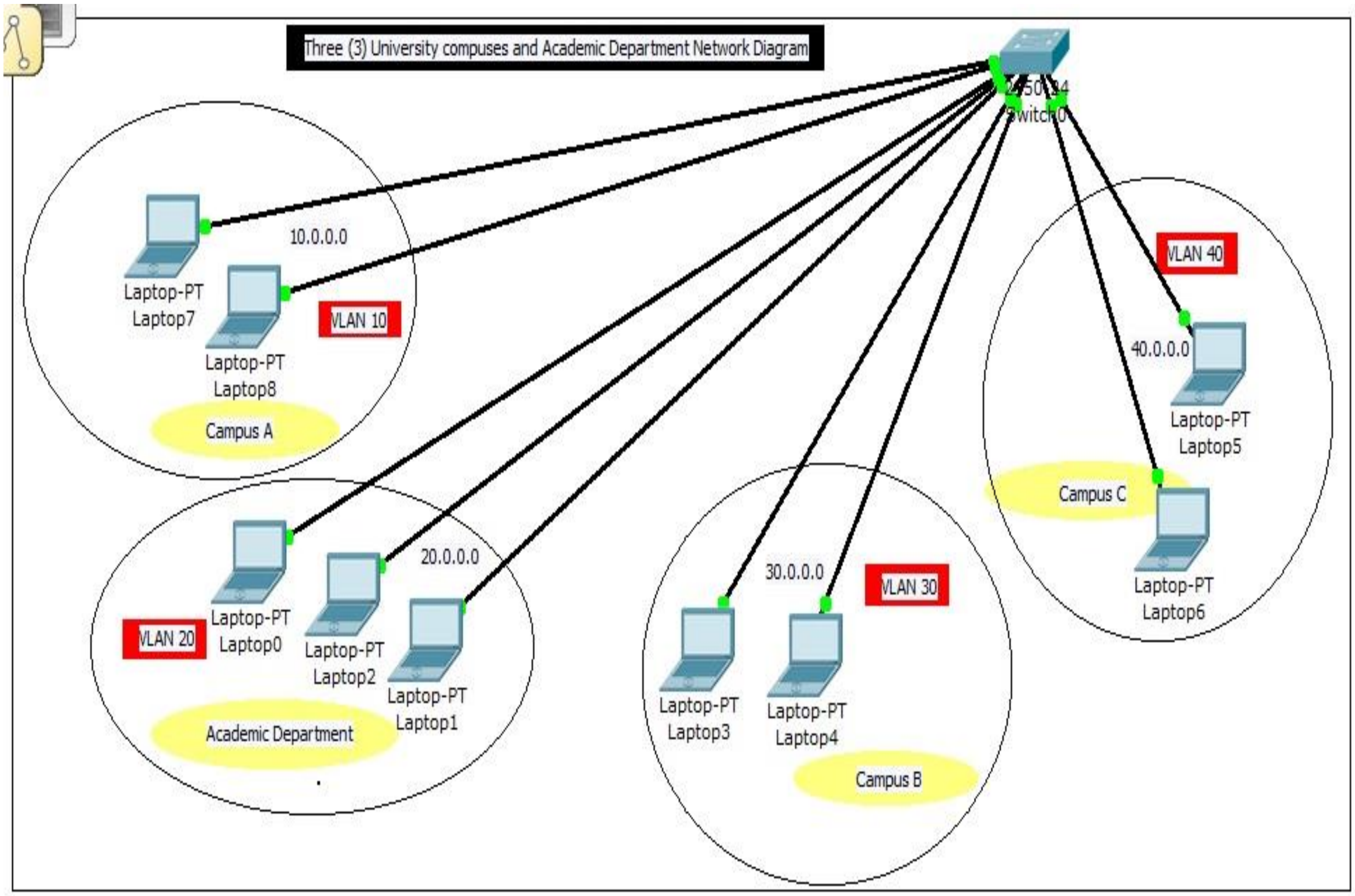


Figure 1. Network regions of the University campuses and academic department diagram using in Cisco packet tracer

2.3 Vlan Set Requirements

Before implementing up the VLANs, the best approach is to plan the entire network's physical and logical setup (in which means to plan for the network topology) carefully. VLAN configuration errors can cause serious connectivity and security problems on our network and having said on that we will consider for our network's topology to be as mesh network topology since we need that in all our computers can understand and communicate each other with in the entire network even if they have been assigned to have different network classes and routing protocols. [6]

In general, there are three or four things that should be configured on VLAN capable switches:

- Addition and defining the VLANs. Most of the switches have ways of defining a list of configured VLANs, and they should be added before they can be configured on any ports
- Construct the trunk port.
- Configure the access ports.
- Configure the Port VLAN ID (PVID).

[7]

2.4 Vlan Features and Significances

VLANs afford the following advanced features:

- VLANs grant ordinary partnerships or normal alliances of end-stations that are topographical remotely on a network.
- VLANs decrease/decline the necessity to have switches introduced on this network with contain communication/transmission traffics/jams.
- Detainment of transmission spaces on a network importantly diminishes traffic-streams.

[8]

2.5 Vlan Security Best Practices (For These Entire Four Networks Best Security)

A few other suggested best practices in regard to VLAN security includes the following:

- Shutting down unused ports and putting them in “a parking lot” VLAN. This is basically an unused VLAN where no other end-users or devices exist.
- Limit the VLANs enabled on trunk ports to only those that are compulsory.
- Physically configure access interfaces with the switchport mode access
- Inactivate Cisco Dynamic Trucking Protocol (DTP) in order to avoid illegal trunk link negotiation.

[9]

CHAPTER 3: VLAN SECURITY

In this part, we will experience how to ensure VLAN (tallying essential switch security), and how to control packages to improve the general quality of network and the desktops security. I will lean toward the term bundle rather than package/edge to refer to transmission units at both the entire system/network and the information/data interface layers. [6]

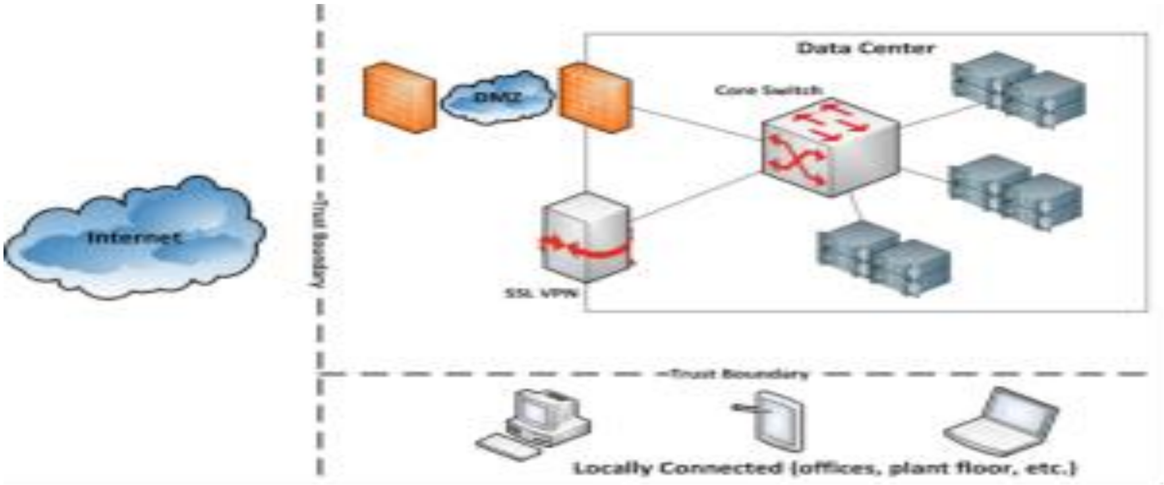


Figure 2. Network single broadcasting domain *[6]*

3.1 Why Information Division is Significant

Old styled system networks look like Figure 2. Border security controls the company's data hub from the external interferences with little shield against internal danger operators. When on the network cable or wire the programmer/hacker has free privilege or access to the network/system attack on overall the whole network. No framework assault surface barrier is great; destroying undesirable access reasonably declines danger of the systems and the network penetrations.

In our model, the trust constraints are set either on or outside to the organization's information center. Demilitarized zone (DMZ) and Secure Socket layer (SSL) VPN use give risk assurance from unapproved get to, yet they slight do once a danger operator enters the organization's information center network. Secretly associated pcs have full privilege to the organization's information center network once the customer enter in to the network. The desire now is that edge controls to stop unauthorized access to the network assault… an awful presumption.

In conclusion, the flat information/ data server network is one immense or huge transmission domain. Any device/desktop sending an ARP multi correspondence checking for an IP address in the data place/center will discover or bring up a solution if the zone is allocated to a working server or other machine/desktop. At the end of the day, an assailant can see all servers in the entire network. This offers a most amiable access to each network/device assault surface. With sufficient opportunity and the correct abilities, it is just a short time before any system/network gets penetrated.

Network division or segmentation with virtual LAN (VLANs) creates an assortment of difficult to reach systems inside the data ambarella. Each system/ network is an alternate transmission domain. By the time suitably commanded, VLAN division cautiously concedes access to system/network attack surfaces. It lessens bundle sniffing capacities and gives additional activities to the programmer effort. Finally, insisted customers simply "see" the servers and various devices critically to accomplish their day by day routine activities.

Another benefit of information/data division is a protocol command partition. System/Network designers may constrain certain protocols to specific divisions of the organization or the business. For instance, if IPX or AppleTalk systems exist on your cable link wire, they can each have their own VLAN where to work. This cutoff gridlocks/jams in each VLAN to applicable packages.

At long last, utilization of VLANs empowers secure, adaptable client/customer adaptability. For instance, a client dispersed to a particular VLAN will dependably interface with that VLAN paying little brain to zone. This is especially useful while structing or sorting out unwired network limitations.

[10]

3.2 Vlan Fundamentals

In our whole idea and four network/systems we instruct/command VLANs utilizing layer two technology (D-link layer) incorporated with switches. Notwithstanding network division/division, VLANs additionally utilize from switch security capacities. Switch producers base their VLAN usage on IEEE Std 802.1Q in which empowers vlan labeling for ethernet parcels/bundles to a particular client as their given or doled out address resolution protocol and it is related by methods to be utilized by extensions and switches in taking care of such bundles/parcels.

[11]

3.3 Address Resolution Protocol

At the point when a PC needs to move information/data with another system/network appended desktop, it broadcasts address resolution protocol (ARP) transmission. This expects the IP address, for instance, of the two devices has a similar system/network identifier. For instance, if the objective device and the source pc both have the ip address 192.168.10.0/24, the source device securely expect the objective device is on an equivalent network/system or system segmentation. The transmission bundle goes to all device on a comparable system/network partition requesting a reaction from the device with the objective IP address.

An 802.1D (D-switch) gets a transmission bundle & broadcasts to all ports/interfaces with the exception of that device which it is gotten. See Figure 4. The primary concern is parcel conveyance all the connected devices. This superfluously creates system/network jam and corrupts execution. The subsequent point or concern is perceivability. The desktop system in our model may locate to all associated device basically by broadcasting at least one ARP transmissions. A D-switch empowers most extreme perceivability since it can't decide if a mentioning device is approved to communicate the objective device. Further, all gadgets exist on a similar system/network fragment.

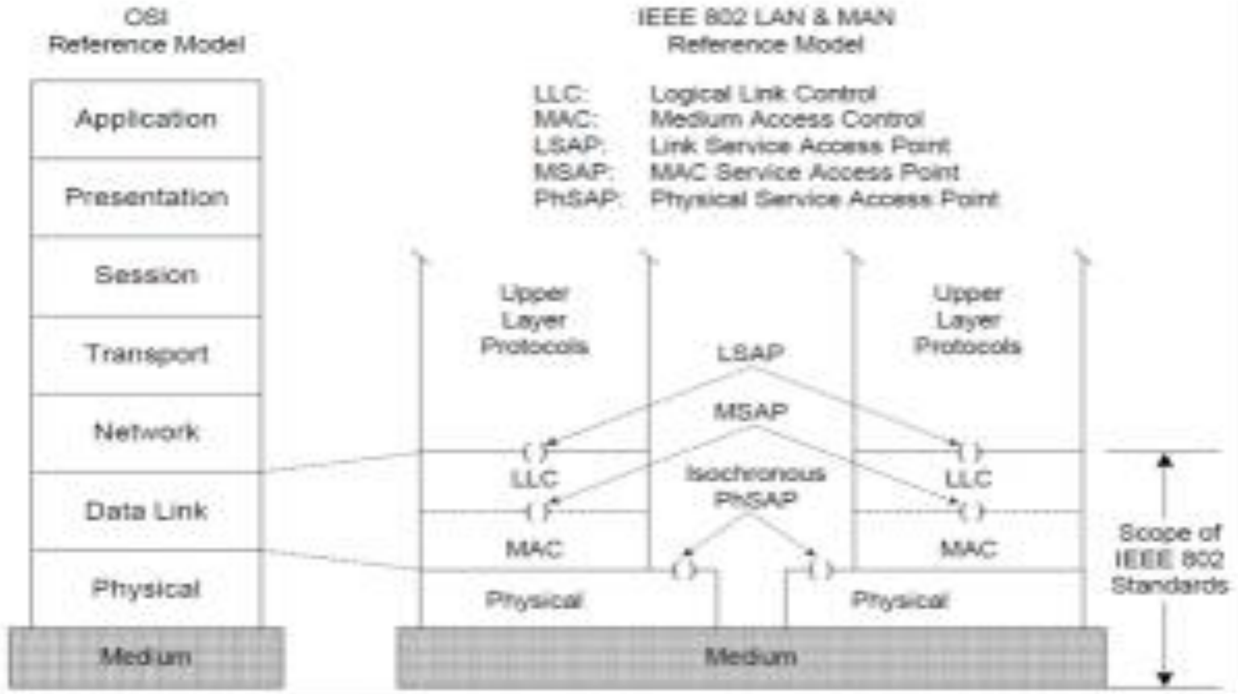


Figure 3. IEEE 802.2001 Data Link Mapping and scope *[12]*

In case a gadget with the objective IP address is on the system/network, it gets and forms the transmission bundle. Utilizing the source MAC address in the transmission bundle, it broadcasts a reaction to the referencing device that joins the objective's MAC address. Right when the source device gets the objective's MAC address, it begins the route toward setting up a communication path between the devices. [12]

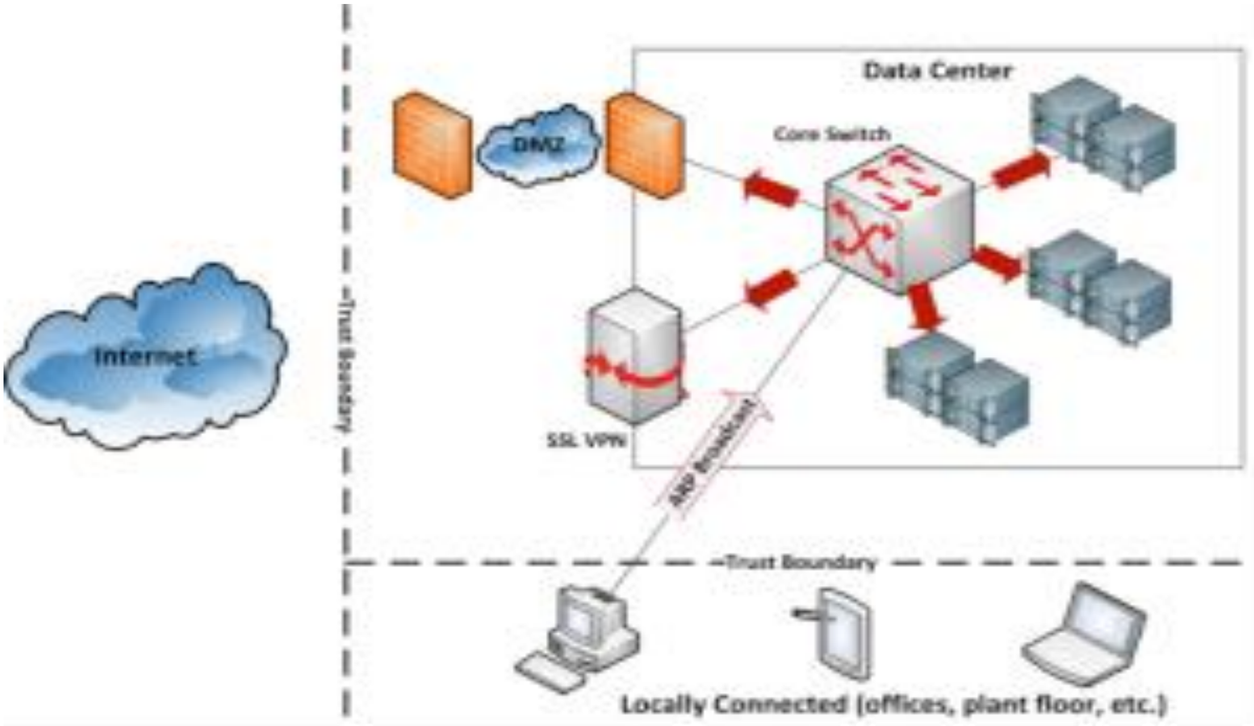


Figure 4. D-switch ARP Broadcast *[6]*

3.4 Content Address Memory

Switches utilize a substance/content addressable memory table to follow MAC address/port sets. For instance, when a device related with switch port 10 sends its first bundle, the switch revives the CAM table with the port and the MAC address. From the hour of the update through the entry's creating/maturing period, the switch drives all bundles with the device's MAC address as the objective/target through port 10. [12]

Creating/maturing is a system wherein a switch destroys address/port sets from its CAM table if certain conditions are met. For instance, an entry may be removed if the switch has not gotten bundles from a device for a predefined time span. Different switches are configurable so the CAM table port/address passages don't develop/age. This is a noteworthy security thought, as experienced many other scenarios and live routine activities within the interconnected devices.

[13]

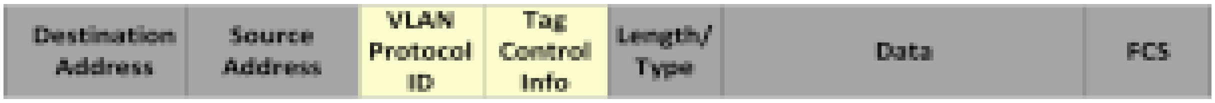
3.5 Medica Access Control Mac - Address

Network admins can develop a table of MAC address/VLAN sets inside the switch. Precisely when a bundle shows up, it is parsed to recover the source MAC address and named to the most ideal VLAN. While this can require basic sorting out effort, it is an approach to deal with keep up VLAN partnership and improving framework/network security for devices that routinely move; paying little regard to where they move or how they interface, each will dependably be transferred to the most ideal VLAN. A security weakness with this methodology is MAC address criticizing. It is basic for an assailant/software engineer to parody a genuine MAC address to get a access to the VLAN if the system/network admins don’t give a complete consideration and dependable to the MAC addresses. [12]

3.6 Vlan Tagging

The 802.1Q standard can besides be known as a naming explicit. Precisely when a VLAN partitioned/disconnected network contains just one switch, labeling/tagging isn't central. The single switch comprehends the port a bundle is jumped on; considering the switch's CAM, it moreover knows the VLAN to which the bundle has a spot and different ports related to it. In any case, things can get powerfully entangled if different switches exist, or if all packs, paying little notice to VLAN enlistment, must go more than in any event one collected ways (trunks).

802.1Q shows the configuration for a VLAN tag to guarantee bundles, paying little brain to where they travel, dependably make it to the right VLAN or trunk ports… and basically those ports. Figure 5 indicates the district of the tag in an Ethernet bundle. The name/tag contains four bytes segregated into two fields. VLAN Protocol ID contains the estimation of 0x8100 if Tag Control Info contains data about the VLAN to which the bundle has a spot. It looks just; However, it isn't regularly extraordinary or perfect with existing devices.



Destination Address	Source Address	VLAN Protocol ID	Tag Control Info	Length/ Type	Data	FCS

Figure 5. Ethernet Packet with VLAN Tag *[14]*

The 802.1Q data/information is embedded into the Ethernet bundle. This develops the bundle and makes extra data that VLAN-unaware devices can't process. Can't process comparable missteps and dropped bundles. Most D-switches offered today can process a labeled/named bundle whether it hasn't a hint how to process the tag. In any case, most by far of end-point devices won't. As we take a look at later in this part, tag/label ejection/expulsion is a bit of the package sending process.

[14]

3.7 Setting - Up Vlans

Bundles/Parcels have a place with VLANs, not devices. Every bundle showing up at a VLAN-designed/configured Q-switch is verified whether it meets the standards for having a place with any of the associated LANs. Network managers can utilize any of a few methodologies for VLAN setup:

Port undertaking/tasks

- MAC address
- IP Subnet
- Dynamic task/action
- Device task/action
- Protocols
- Applications

[14]

3.8 Port Assignment

The default strategy appeared in 802.1Q is to dispense ports expressly to VLANs inside the switch. In our past model (Figure 4), any bundle entering through port 2, 4, or 8 is in this manner relegated to VLAN 10. On the off chance that I need to grow the quantity of clients on the VLAN, I may add the Campus A desktops to an extension hub and the same way the hub to the switch for port extensions. Any extra PC that I partner with the hub is similarly part of VLAN 10.

[12]

3.9 Vlan Cable Trunking

Various companies/ organizations have more than one switch. Further, VLANs are not dependent or reliant on the genuine network zone of an end-point device or switches. Imply Figure 6. While utilizing two Q-changes to direct VLANs, a trunk is commanded/instructed between them utilizing a port on each switch: a trunk port. During a data/information transmission, all VLAN bundles entering either switch is sent through by the trunk to the next switch. This grants VLAN individuals to exist in various zones and still utilize all VLAN-committed resources. [12]

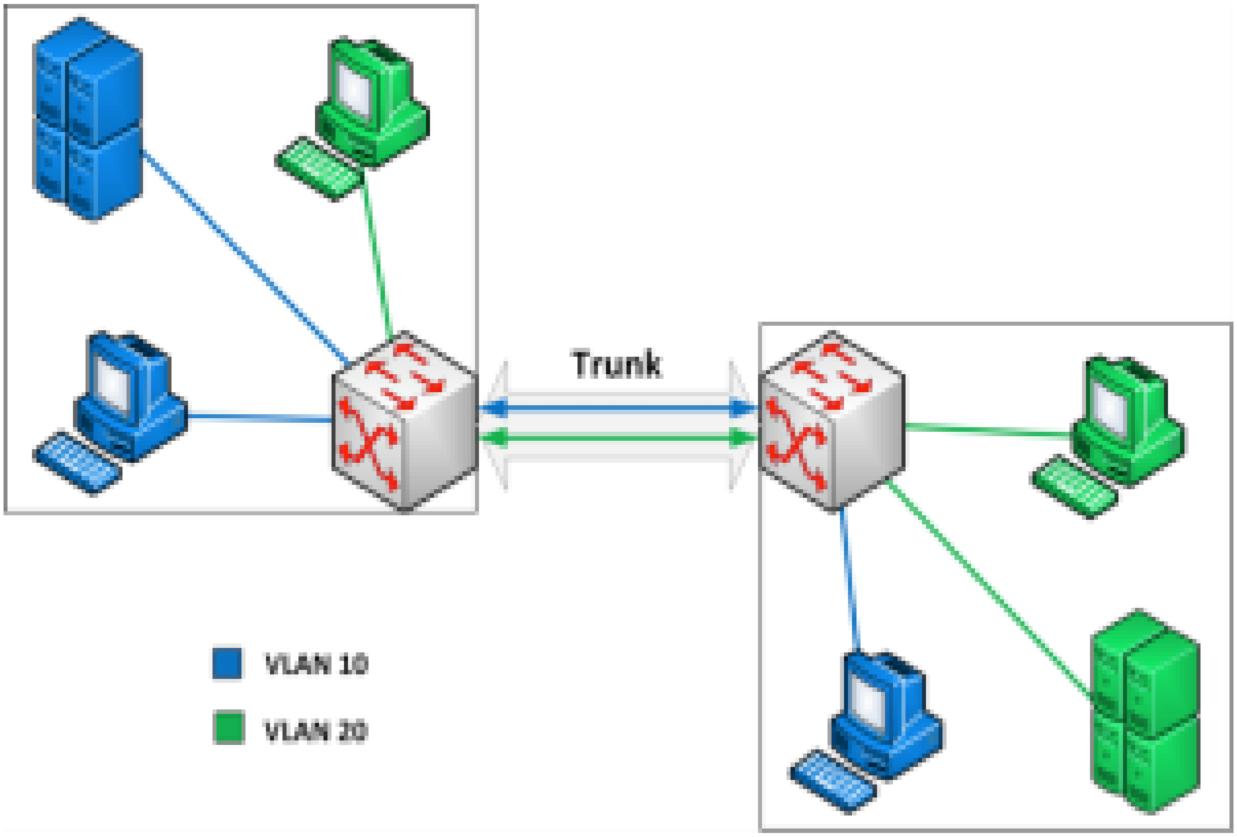


Figure 6. Trunking *[6]*

CHAPTER 4: VLAN CONFIGURATION

4.1 Introduction

This chapter describes VLANs on 2950/24 arrangement/series switches. It additionally gives rules, systems, and setup models. This part incorporates the accompanying significant segments:

- Overview of VLANs
- Current VLAN Configuration
- Configuring VLANs
- Required physical components and cables
  [15]

4.2 Overview of Vlans

A VLAN is gathering/group of devices on in any occasion one LANs that are planned to impart like they were joined to a near wire, when as reality they are organized on various indisputable LAN areas. Since VLANs depend upon reliable as opposed to physical affiliations, they are incredibly versatile/adaptable. VLANs portray transmission domains in a Layer 2 system/network. A transmission domain is the strategy of action of all devices that will get transmission bundles starting from any device/gadget inside the set. Transmission domains are normally obliged by switches/routers since router don't send mass data frames. Layer 2 switches make transmission of bulk frames relying upon the configuration of the switch. Switches are multiport spans/bridges that permits you to make distinctive or different transmission domains. Each transmission domain resembles a particular virtual expansion inside a switch. [12]

VLANs are routinely associated with IP subnetworks. For example, the entirety of the end stations in a specific IP subnet have a spot with the corresponding VLAN. Traffic between VLANs must be routed. You should give out LAN interface VLAN selection on an interface-by-interface premise (this is known as interface-based or static VLAN support).

[15]

4.3. Current Vlan Configuration

Table 1. Current vlan real configuration

Command		Purpose
Step 1	# vlan 10 #Name v10 Exit - # vlan 20 #Name v20 Exit - # vlan 30 #Name v30 Exit - # vlan 40 #Name v40 Exit	Declaration of VLAN ID and names
Step 2	#Int go fa 0/1-05 #switchport mode get to #switchport get to vlan 10	Assigning a specific switch-ports to vlan10 and also clarifying the switchport modes/status whether to be access or trunk. **NOTE:** In this case Vlan10 can only host 5 desktops starting from switchport 0/1 – 5.
Step 3	#Int go fa 0/5-10 #switchport mode get to #switchport get to vlan 20	Assigning a specific switch-ports to vlan20 and also clarifying the switchport modes/status whether to be access or trunk. **NOTE**:

		In this case Vlan20 can only host 5 desktops starting from switchport 0/5 –10.
Step 4	#Int go fa 0/10-15 #switchport mode get to #switchport get to vlan 30	Assigning a specific switch-ports to vlan30 and also clarifying the switchport modes/status whether to be access or trunk. **NOTE:** In this case Vlan20 can only host 5 desktops starting from switchport 0/10 –15.
Step 5	#Int range fa 0/15-20 #switchport mode get to #switchport get to vlan 40	Assigning a specific switch-ports to vlan40 and also clarifying the switchport modes/status whether to be access or trunk. **NOTE:** In this case Vlan40 can only host 5 desktops starting from switchport 0/15 –20.
Step 6	#int fa 0/21 #switchport mode trunk #switchport mode trunk permitted vlan10 #switchport trunk permitted vlan include 20 #switchport trunk permitted vlan include 30 #switchport trunk permitted vlan include 40 #exit	Switchport trunk configuration and adding all the VLANs in this trunk cable. **Note:** All the vlans can communicate if we put a router on the top but for our concept a router is excluded according to our study scope and specification, therefore each vlan desktops can communicate and thus provides highly network security.
Step 7	Exit	Terminates the process and everything is done

4.4. Configuring Vlans

Before you sort out VLANs, you should utilize VLAN Trunking Protocol (VTP) to keep up overall VLAN configuration for your system/network.

To make a VLAN, play out this undertaking:

Right when you make or adjust an Ethernet VLAN, note the followings:

Table 2 Vlan configuration steps

Command		Purpose
Step 1	Switch# design/command terminal	Enters worldwide design/command mode.
Step 2	Switch(config)# vlan vlan_ID Switch(config-vlan) #	Adds an Ethernet VLAN. Note You can't eradicate the default VLANs for these media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005. Right when you eradicate a VLAN, any LAN interfaces instructed as access ports consigned to that VLAN become an idle. They stay related with the VLAN (and subsequently dormant) until you designate them to another VLAN. You can use the no catchphrase to delete a VLAN. At the point when the brief peruses Switch(config-vlan) #, you are in vlans commanding mode. In case you wish to change

		any of the limits for the recent made VLAN, use this mode.
Step 3	Switch(config-vlan) # end	Comes back to empower mode from vlan-setup mode.
Step 4	Switch# show vlan [id | name] vlan_name	Confirms the VLAN setup.
Step 5	Exit	Terminates the process and everything is done

Exactly when you make or alter an Ethernet VLAN, think about the followings:

- Since Layer 3 ports and some item features require inner VLANs allocated from 1006 and up configuration extended go VLANs beginning with 4094 and work descending.
- You can design extended range VLANs just in overall arrangement mode. You can't mastermind expanded go VLANs in VLAN database mode.
- Layer 3 ports and some item features use expanded go VLANs. In case the VLAN you are endeavoring to make or change is being used by a Layer 3 port or an item feature, the switch shows a message and doesn't alter the VLAN setup.

This model tells the best way to make an Ethernet VLAN in worldwide design mode and confirm the setup:

```
Switch# arrange terminal
Switch(config)# vlan 10
Switch(config-vlan) # end
Switch# show vlan id 10
VLAN Name Status Ports
- - - - -
10 VLAN0010 dynamic
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
- - - - -
10 enet 100010 1500 - 0
Essential Secondary Type Interfaces
- - - - -
Switch#
```

[15]

4.5. Required Physical Components and Cables

4.5.1 General Objects

When vlans are planned to be implemented many essentials are required which are technological devices (desktops, switches and cables for this implementation) each of these has a separate function and role.

4.5.2 Cables

For this concept we will be using ethernet cat 5 or 6 cables for the switchports and the desktops as well so data can be transmitted through here very easy and no short outcomes if the cables are set regularly. If the machines are similar, we can set our cables in either type A on both ports of the cable color coding but if we are going to create a connection path between two different devices, we should make the vise-verse.

CHAPTER 5: METHODOLOGY AND RESEARCH ANALYSIS RESULTS

5.1 Introduction

Quality of Services is a proportion of system/network execution for all services which giving from the system/network. The Improving exhibition for the systems/network is the most significant objectives since it directly affects all the services, which giving by the system/network in this way, when constructing any system/network that imperative to building it in powerful manner to improve QOS for it by decreasing postpone Rate esteem and furthermore frame collision or jams through its excursion to the its endpoint.

There are numerous specialized strategies and innovations to build the capacity it and improve its presentation showing up high Quality of Services (QOS) level. The arriving at the ideal point of system/network performance implies taking care of a considerable lot of the issues and difficulties that confronting the systems/networks and creating exercises significant services in the significant number of fields in the life.

The utilization of the internet in a successful manner and deals with the system/networking to Invests all aspects of system/network assisting with improving QOS for the system/network in simple manner and not cost way. The deferral is framed an enormous scope from system/network issues which specific show up progressively application from video and voices. There is a huge pattern towards Real time services in nowadays, which prompted the development of a genuine issue around there.

The study keen on improve QOS for network in viable and simple manner utilizing VLAN innovation which spread LAN by conquer defer issue and the association of the system/network and improve the built.

The possibility of the project can be applied by building more than one system/network, studying and investigation of the exhibition of these systems/networks in information/data transmission, including the investigation of the quality of their exhibition, in certain services which choosing it, and note how the postpone affected in its exhibition.

The venture/project begins by investigating to apply the thought utilizing OPNET program, and improve the QOS when utilizing Vlans innovation in the system/network, indicating how the postpone impact on the quality of services which giving by the vlans organize.

The study inspired by examinations the exhibition a large number of services, which Affected by delays particularly voices, and recordings. Building and investigating the concept thought will be applied utilizing OPNET test system to show how choosing great route in planning system/network to lessen the worth deferral for improving the QOS. [16]

5.2 Procedures and Methodologies

The concept thought is applied by structuring LAN utilizing Vlan innovation. the system/network can be built utilizing numerous test systems, for example, OPNET test system, Cisco-parcel tracer, NS-3, GNS3, etc yet the OPNET test system is the best program to apply numerous thoughts in network world to investigation the exhibitions for any system/network. All instruments which requiring it for the plan are accessible in OPNET test system that permit to structure and configure in it. Furthermore, show the exhibition for all that in different types of curves gave by the Riverbed program. The fundamental thought in the concept regarded to design system/network with apply vlan innovation. The vlan innovation is utilized to improve the Quality of Service QoS for the system/network, it sorts out information/frame/data transmission in the network. It implies division a similar local system/network in to numerous little systems/networks called sections to give each part security and to ensure them to store every one of its information/data. To consider the exhibition the system/network will be utilized VLAN framework to test numerous parameters indicating the outcome to compare at performance between any chosen scenarios. In a basic manner, to apply the thought the system/network will be structured in two scenarios; the primary situation keen on utilizing vlan innovation and the second situation not utilizing vlan innovation. Every situation comprises or consists of two systems/networks to read the exhibition for data transferring between these networks. The exhibition will cover a few applications to consider the character and analysis it. That following numerous QOS parameters, contemplating the exhibition incorporate numerous Characteristics, for example, Packet Delay variety, Packet End-To-End Delay (sec),Traffic Received(byte/sec),Traffic Received(packet/sec),Traffic Sent(byte/sec) and Traffic Sent (parcel/sec) however the defer informed the principle Characteristic in the examination/study. The study inspired by application that affected by delay in plainly. The ongoing application is more affected in delay so there are more critical to concentrate genuine application, for example, voice (VoIP application) and (video conferencing) application. [16]

5.3 Comparative Analysis

The table give some specialized that inspired by improve the QOS in the system/network in numerous techniques and specialized. It demonstrating the significance in utilizing VLAN in light of the fact that its simple way and not cost in local networks.

Table 3 Similar examination of existing methods

Title study	**Specialized strategy**	**In comparison**
MPLS Network management. [17]	Multiprotocol Label Switching (MPLS) is an innovation that give instrument to improve QoS. It utilizes the data implanted in the labels appended to the IP Packets.	It gives great execution continuously application however it is significant expense.
"VPN: Virtual Private Network, tunnel, IPsec, layer 2 tunneling protocol, Mobile". [18]	Virtual private network provides security (VPN) for network in internet communication.	Improves QoS however it is a mind-boggling way.
"Analysis of VLAN Network Delay Performance to Improve Quality of Services".	VLAN is basic and successful specialized that giving the security to the system/network and deal with that into numerous sections to improve it by lessen the deferral in it.	Ideal approach to conquer postponement and frame crash as a rule for the system/network and improve QoS with low expenses.

5.4 Experimental Analysis

The possibility of the concept had been applied by plan straightforward system/network in two situations containing from two system university campuses: Campus A and Campus C. The system/network that utilizing VLAN innovation give results better than the system/network without utilizing VLAN innovation, for instance the postpone rate in first situation without utilizing VLAN practically equivalent from .0031 to .0036 second however in second situation with utilizing VLAN practically equivalent from .0026 to .0032 second, the details in fig 7. That demonstrating the role of utilizing VLAN innovation in Reducing delays and improving the exhibition for the system/network to improve network Quality of Service QoS. [16]

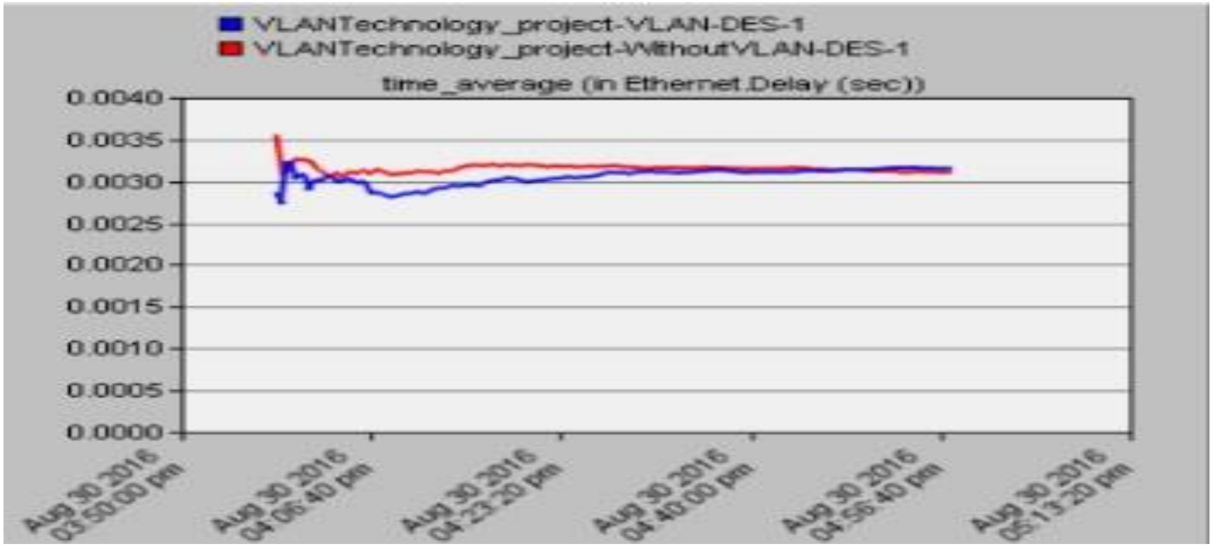


Figure 7. Time Average (in Ethernet Delay (Sec)) *[16]*

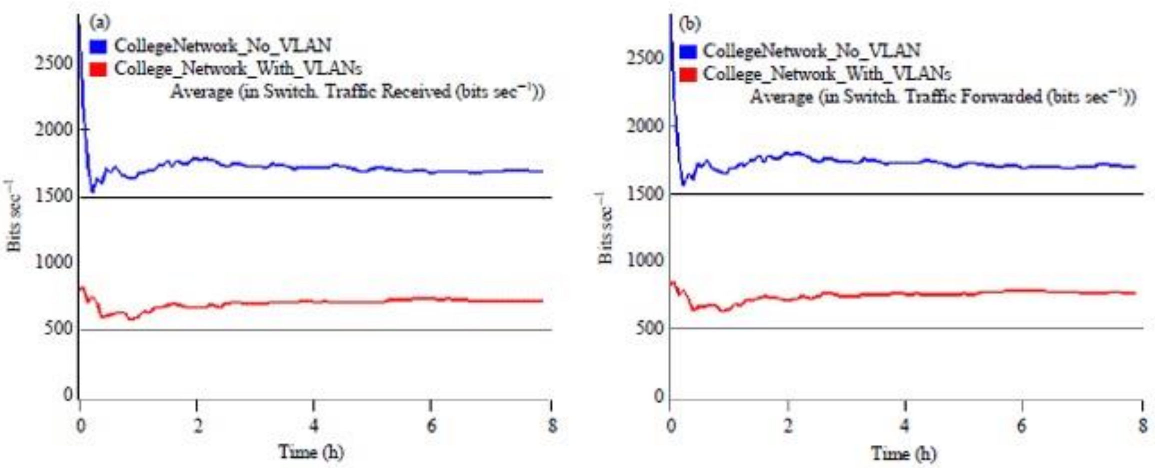


Figure 8. a) Traffic received b) Traffic forwarded *[19]*

Figure 8 a and b shows the traffic got and sent (bits sec–1) on Block_A (Switch 1). The diagram shows a huge contract difference in the traffic received and forwarded for the two situations. The X-axis speaks to the time, the situation in the Y-axis speaks to bits/sec. Average of 1,500 bits is gotten/received over a time of around 8 h on the system/network where VLAN isn't configured while an average of 500 bits is gotten/received simultaneously in the system/network where VLAN is being utilized or configured. The average traffic forwarded is found in Fig. 2 b which is a similar value as the traffic gotten/received. [19]

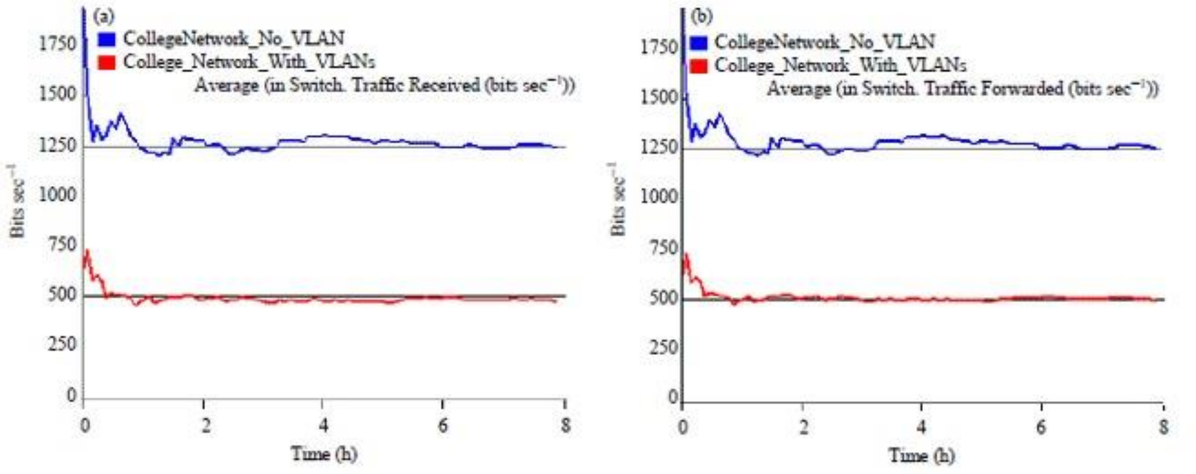


Figure 9. a) Traffic received b) Traffic forwarded *[19]*

Figure 9 a and b shows the traffic gotten/received and sent/forwarded on Block_B (Switch 2) in bits sec–1. The diagram shows a noteworthy difference in the traffic received and forwarded for the two situations. The traffic gotten/received and sent/forwarded in the scenario With VLAN is a lot lesser than that of No VLAN. This outcome agrees with the consequences of Block_A (Switch 1) further assisting with demonstrating that the system/network with VLAN is better than network with no VLAN as it decreases traffic. [19]

CHAPTER 6: CONCLUSSION AND RECOMMENDATIONS

6.1 Summary

A VLAN is a gathering of PCs, network printers, network servers, and other network gadgets that carry on as though they were in a solitary communication space/domain. To execute VLANs in a system/network domain, you need a Layer 2 switch that has VLAN ability. Practically all switches sold today that are portrayed as overseen/manageable switches give the ability to configure/command switch ports as individuals from various VLANs. In any case, switches that don't give any commanding/configurable work/functions, for example, many basic lower-end switches, don't give this capacity to configure VLANs. For instance, a switch you may purchase at your nearby PC store for a home system likely wouldn't have VLAN capacity.

VLANs characterize transmission domains without being obliged/constrained by the physical area of the system/network device, for example, a PC, server, or a network printer. For instance, rather than making all the clients on the VLAN10 in Campus A piece of a similar transmission domain paying little heed to their areas of expertise, you may utilize VLANs to make all the clients in the Campus A piece of a similar transmission domain, separate from the clients in the different campuses and sections.

Address-based VLANs are characterized by the Layer 2, or the MAC, address of each gadget. You config each VLAN inside the switch and a while later choose MAC conveys to the fitting VLAN. Address-based VLANs are port independent, which implies that it doesn't make a difference to which switch port the device is associated. Its VLAN enrollment is controlled by its MAC, or physical equipment, address.

The essential explanation behind VLAN execution/implementation is the cost decrease of taking care of client moves and changes. Any system/network desktop moved or included can be overseen from the system management console rather than the wiring closet. VLANs give an adaptable, simple, and less-expensive approach to alter and oversee coherent groups of PCs in evolving conditions and environment.

[20]

6.2 Challenges

1. VLANs are a generally unbendable approach to help strategies. In this area, we talk about three fundamental impediments VLANs force on the granularity of strategies — limits on the amount of VLANs, limits on the number of hosts per VLAN, and the difficulty of consigning an entrance port to various VLANs without end-host support. We in like manner talk about the lacking ways network admins endeavor to work around these containments. Unquestionably quantity of VLANs is obliged considering built in protocol constraints (i.e., VLAN ID space) and execution constraints (i.e., switch and switch resources/assets):
    - VLAN ID space: The VLAN ID is a 12-piece header field, constraining a system/network to 4096 VLANs.
    - Switch memory: Limited memory for putting away bridge tables frequently confines singular changes to supporting 300–500 VLANs.

2. In spite of the fact that Ethernet was intended with the goal of "zero configuration," VLAN config is trying/testing and error inclined, for two primary reasons. In the first place, each host's IP address must be unsurprising with the IP subnet of its VLAN. Second, the switches expects or asks for setup to ensure each VLAN has a successful spanning tree that remaining linked under general basic or simple situations and scenarios.

[20]

6.3 Conclusion

We have overviewed four of the University campuses (A, B, C and Academic department) networks/systems to all the more likely comprehend and illustrate how VLANs are utilized practical. Our investigation demonstrates that VLANs are utilized for many strategies and objectives that they were not initially planned for, and are frequently mismatched for the undertakings Further, the utilization of VLANs muddles network config management. We take into consideration that future business networks should see approaches to limit the utilization of VLANs and investigate more straightforward approaches to accomplish the network admin's targets with the objective to make the management simpler for the campuses and business operators. [12]

REFERENCES

[1] Misumi M, Yamaoka K., "Ethernet Bypass Nodes as Suspended Link Activators on Tagged-VLAN Disabled Ethernet Switches," *Ethernet Bypass Nodes,* vol. 4, no. 1, pp. 33-45, 2010.

[2] Fuchs Stefan, Schmidt Hans-Peter, "Real Time Ethernet and Synchronizing," *Real Time Ethernet and Synchronizing with Inhomogeneous Physical Layers: CAT5 and Unshielded Twisted Single Pair Cabling,* vol. 2, no. 8, pp. 10-28, 2015, SAE Technical Paper Series.

[3] Aweya James, "IEEE Standard for Information Technology - LAN/MAN," *IEEE Standard for Information Technology - LAN/MAN - Specific Requirements -Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications,* vol. 3, no. 2, pp. 123-137, 2009.

[4] "Data Communications Networking Devices," *CSMA/CD Network Performance,* vol. 2, no. 6, pp. 76-88, 2004.

[5] "Layer Management for 10 Mb/s Baseband Repeaters," *Layer Management for 10 Mb/s Baseband Repeaters (Section 19). Supplement to Carrier Sense Multiple Access With Collision Detection (CSMA/CD)Access Method and Physical Layer Specifications,* vol. 3, no. 1, pp. 54-79, 2009.

[6] "Network performance," *CSMA/CD Network Performance,* vol. 2, no. 1, pp. 33-68, 2008.

[7] "Application of Dynamic Port VLAN Membership," *Application of Dynamic Port VLAN Membership with Auxiliary VLAN in Campus Area Network,* vol. 3, no. 7, pp. 76-78, 2009· 2009 Ninth International Conference on Hybrid Intelligent Systems.

[8] John wiley and Sons Inc., "Switch/Router Architectures," *Introduction To Switch/Router Architectures,* vol. 2, no. 6, pp. 65-80, 2018 - Switch/Router Architectures.

[9] Foschiano M., "UniDirectional Link Detection (UDLD) Protocol," *Cisco Systems UniDirectional Link Detection (UDLD) Protocol,* vol. 4, no. 1, pp. 245-264, 2008.

[10] Watson R.W., "Modes of Access the Network Information Center," *An Interactive Network Experiment to Study Modes of Access the Network Information Center,* vol. 2, no. 1, pp. 76-79, 1971.

[11] Buchanan W. J., "Network design, switches and vLANs," *The Complete Handbook of the Internet,* vol. 2, no. 2, pp. 30-37, 2002.

[12] "Wireless network," *Wireless network device position location system,* vol. 2, no. 1, pp. 85-93, 2005.

[13] Seger Jon, "All for one," *Nature - all for one,* vol. 4, no. 1, pp. 104-118, 1989.

[14] Shimizu Hiroshi, "IEEJ Transactions on Electronics, Information and Systems," *Ring Network with VLAN Tag,* vol. 3, no. 2, pp. 234-235, 2005.

[15] John Wiley & Sons, Ltd, "Internetworking LANs and WANs," *vLANs and Virtual Networking,* vol. 3, no. 1, pp. 453-494, 2001.

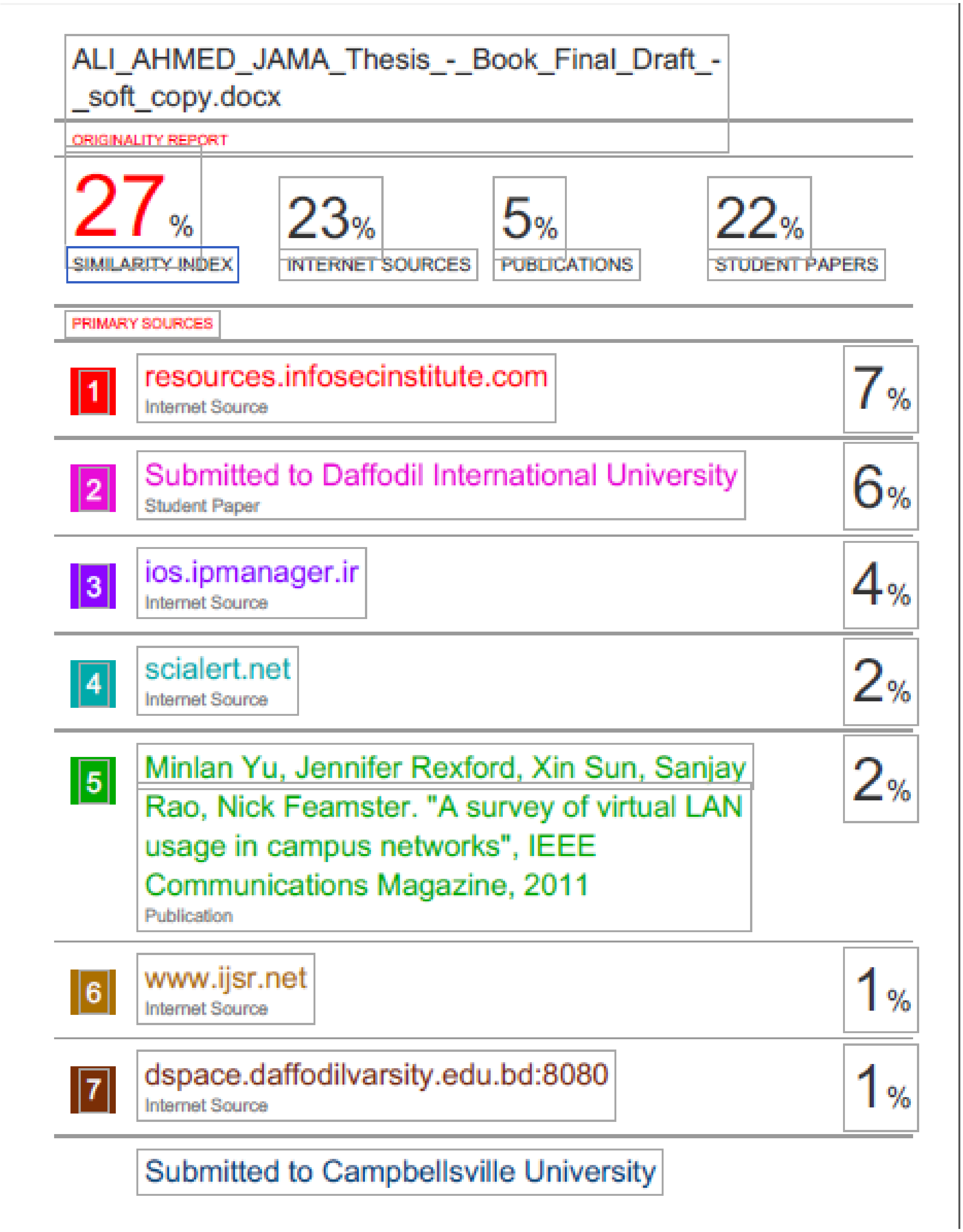
[16] Walaa Amayreh, Norah Alqahtani, "Analysis of Vlan network delay," *Analysis of Vlan network delay performances to improve quality of services,* vol. 1, no. 1, p. 51, 2016.

[17] Nadeau, T., "MPLS Network Managemen," *MPLS Network Management: MIBs, Tools and Techniques,* vol. 4, no. 2, pp. 51-53, 2003.

[18] Wikipedia , Q., "Virtual Private Network VPN," *Vpn: Virtual Private Network tunnel, ipsec, layer 2 tunneling protocol,* vol. 2, no. 1, pp. 52-57, 2013.

[19] Mohammed F. Alsharekh, "Analysis of Virtual Local Area Network (VLAN) with Physical Network," *Analysis of Virtual Local Area Network (VLAN) with Physical Network Security Implementation,* vol. 3, no. 2, pp. 52-55, 2016.

[20] HomChaudhuri S.Foschiano M., "Scalable Security in a Multi-Client Environment," *Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment,* vol. 3, no. 2, pp. 58-60, 2010.



ALI_AHMED_JAMA_Thesis_-_Book_Final_Draft_-_soft_copy.docx

ORIGINALITY REPORT

27%	23%	5%	22%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	resources.infosecinstitute.com Internet Source	7%
2	Submitted to Daffodil International University Student Paper	6%
3	ios.ipmanager.ir Internet Source	4%
4	scialert.net Internet Source	2%
5	Minlan Yu, Jennifer Rexford, Xin Sun, Sanjay Rao, Nick Feamster. "A survey of virtual LAN usage in campus networks", IEEE Communications Magazine, 2011 Publication	2%
6	www.ijsr.net Internet Source	1%
7	dspace.daffodilvarsity.edu.bd:8080 Internet Source	1%
	Submitted to Campbellsville University	