ISSN No:-2456-2165

An Improvement of Performance in Virtual Local Area Network or Virtual LAN using Software Defined Network

Fatima Laassiri
IR2M Laboratory, FST, Univ Hassan UH1- Settat, Morocco

Mohamed Moughit
IR2M Laboratory, FST, Univ Hassan 1 UH1-
Settat, Morocco
EEA&TI Laboratory, FST, Univ Hassan
Mohammedia, Morocco
National Schools of Applied Sciences Khouribga,
Univ Hassan 1, UH1- Settat, Morocco

Noureddine Idboufker
National School of Applied
Sciences, Univ Cadi Ayyad
Marrakech, Morocco

Abstract:- **This article is an improvement of the performance in Virtual Local Area Network or Virtual LAN using Software Defined Network via the development of a new application for the creation of VLANs with and without SDN in a dynamic way with their scalability under OMNeT 4.6 ++. VLANs are defined by the IEEE 802.1D, 802.1p, 802.1Q and 802.10 standards. A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes.**

Keywords:- *Dynamic SDN; VLAN; QoS; OpenFlow.*

I. INTRODUCTION

A Virtual Local Area Network (VLAN) [1] is a distributed LAN on devices operating at Level 2 of the OSI model [2]. It allows isolating the traffic within the same switch. Each VLAN has own broadcast domain.

VLAN is distributed on different devices via dedicated links between two switches called trunk. It has long been used in campus and enterprise networks as the most popular network virtualization solution. Because of the disadvantages and benefits of using the VLAN, operators and network administrators have used it so far to build their networks. However, their configuration is a complex, tedious process with high percentage errors. Because.

SDN [3] has centralized network management and network programmability; it is a promising solution for managing the aforementioned challenges in managing VLANs. This part first introduces a new architecture for VLANs using SDN and Open Flow. Via, an implement to easily manage the configuration of VLANs dynamically with and without SDN. By the use of the dynamic configuration protocol of VLANs and that, it allows to update the VLAN association table, called Generic Attribute Registration Protocol (GVRP) [4]. For distribution the broadcast messages in the network, to dynamically configure VLANs in all devices on the network.

II. PROBLEM AND SOLUTION

In today's enterprise networks, LAN switching scenarios are implemented in large scale domains. For example, communication within hosts in a single architecture is established via LANs (Layer 2 Switching). That it is based on the use of the MAC addresses for the communication between the final hosts. For such switching scenarios, this concept is derived because manual configuration of VLANs is very complex in the enterprise network architecture currently. VLANs are configured throughout the architecture by network administrators. If there is a small change in the network topology, the manager must reconfigure the entire topology. In today's businesses, host behavior patterns connecting to the network are changing rapidly, making it impossible to manually reconfigure the network.

Over the many years of development, new architectures have emerged, giving a programmable capacity to manage the

ISSN No:-2456-2165

networks. This is achieved by developing a network operating system. Many attempts have been made to make the network more manageable and secure. To meet this requirement, an application has been developed for creating dynamic VLANs with centralization by an SDN controller. SDN allows separation of the network control plan and the SDN routing plan via a secure channel. It's called the Open Flow protocol.

Open Flow is a protocol that offers the possibility to the administrator to program the dashboards of the different switches. It virtualizes the network into delegation channels of the network segments. What it implements is network virtualization.

III. PROBLEMS OF LOCAL NETWORKS

- Limit the propagation of level 2 or 3 problems on the network.
- Limit broadcast domains.
- Contain the multicast frames, that they are propagated on all the ports of the switch.
- Difficulty administering a poorly organized network.
- Borner any security issues.

IV. THE SOLUTION: VIRTUAL LOCAL NETWORKS

- Have layer 3 functions with the speed of layer 2.
- Facilitate the management of job mobility.
- Remove the possibility of communication between certain parts of the network, secure domains.
- It can easily assign different permissions, depending on the rights and roles of each group of people.

V. BENEFITS OF VLANS

Among the advantages related to the implementation of a VLAN, we note in particular:

- *Network Segmentation Flexibility*

The users and resources between which communications are common, and they can be grouped without having to consider their physical location. It is also conceivable that a station belongs to several VLANs at the same time.[5]

- *Simplification of management*

Adding new elements or moving existing elements can be done quickly and easily without having to manipulate physical connections in a technical room.

- *Increasing Network Performance*

As network traffic in a user group is confined within a VLAN, it increases network performance.

- *Better use of network servers*

When a server has a network interface that is compatible with the VLAN, the administrator has the opportunity to make this server belong to several VLANs at the same time. This membership allows to reduce the traffic, which it must be routed (Process at higher level protocol level, eg IP) "from" and "to" this server; and therefore to optimize this traffic. Just like splitting a hard drive into multiple partitions to increase performance (fragmentation can be decreased) of one's computer.

- *Strengthening network security*

As virtual boundaries created by VLANs can only be crossed through routing capabilities, communication security is enhanced.

- *Scalable technology*

It is low cost, the simplicity of the method of access and ease of interconnection with other technologies; it is a scalable Ethernet technology at low cost, regardless of users.

- *The regulation of bandwidth*

One of the most basic concepts of Ethernet networks is the notion of sending a network message to all (broadcast or multicast) of the elements connected to the same switch (hub / switch). Unfortunately, this type of broadcast seriously increases the network traffic within the connection component. Although transmission speeds are increasing, it is important to control this waste of traffic capacity, again, VLAN provides the administrator with the means to regulate the use of traffic volume available within infrastructure.

VI. VLAN MODEL

This model was invented and distributed by Cisco, (Figure 1)
It contains three layers each having a specific role.

- The core layer, "Core layer" network layer; (CL).[6]
- The distribution layer, "Distribution layer" (DL).[6]
- The access layer, "Access layer"; (G). [6]

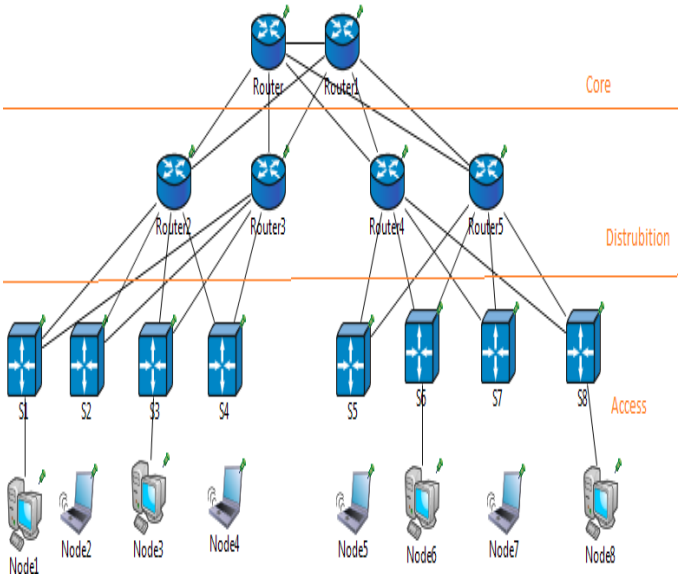

Fig 1:- Three switching layers

ISSN No:-2456-2165

A. *Core layer* CL

This is the layer 3 or the upper layer, its role is to link between different segments of the network, for example remote sites, LANs or floors of a company. We usually find routers at this level. It is essential to the interconnectivity between the devices of the distribution layer, via this layer the switch makes it possible to communicate with the outside world.

B. *Distribution Layer DL Layer 2*

This layer is used to filter, route, and allow packets. It acts as a link between the Core layer and the Access layer.

C. Access Layer AL Layer1

which is the interfaces to the terminal (The user). It includes routers, switches, bridges, hubs and dots. Wireless access. It provides a means of connection to the network, and it controls the communication on the network.

VII. ASSOCIATION THE PORTS WITH A VLAN

A. VLAN per port (VLAN level 1)

Each switch port is assigned to a VLAN. The membership of a frame in a VLAN is determined by the connection of the network adapter to a switch port. The ports are statically assigned to a VLAN.

If you physically move a station, you must unassigned, its VLAN port and assign the new one to the correct VLAN. If you move a station logically (Change VLAN), you must change the port assignment to the VLAN. There is the possibility of configuring the ports dynamically (Auto, desirable, access) through the DTP protocol.[7]

B. VLAN per MAC (Level 2 VLAN)

We assign each MAC address to a VLAN. The membership of a frame to a VLAN is determined by its MAC address, it is the association of the Mac / VLAN address. The ports of the switches are dynamically assigned to each of the VLANs according to the MAC address. of the host, which he emits on this port.

The main interest of this type of VLANs is independence with respect to geographical location. If a station is moved on the physical network, its physical address does not change, it continues to belong to the same VLAN (This operation is well adapted to the use of machines). If we want to change the VLAN, we must change the association MAC / VLAN.

C. VLAN per Level 3 Address (Level 3 VLAN)

We assign a level 3 address to a VLAN. The membership of a frame to a VLAN is then determined by the address of level 3 or higher, which it contains (the switch must therefore have access to this information). This is the level 3 / VLAN address association to dynamically assign the switch ports to each of the VLANs.

In this type of VLANs, the switches automatically learn the configuration of the VLANs, accessing the Layer 3 information. This is a fast operation as the VLAN Level 2.

VIII. FRAME TYPES

There are three types of frames

- *Tagged Frame*

This is a frame, it contains an additional header (Label), it includes information about membership in a VLAN.
This tag is removed when the frame leaves a port belonging to this VLAN.

- *Untagged frames*

This is a frame that contains no information about its membership in a VLAN.

- *Priority tagged frame*

This allows the transmission of "tagged with priority" frames and also deals with other types of frames.

➢ *Method of transmitting a packet or Mode of transmission the frames*

There are different switching modes. These modes will influence two parameters:

1- Store-and-Forward Switching

Delayed Mode switch waits until it receives 100% of the frame; it makes sure the frame is good after it starts sending. [8]

✓ *The* advantage

The most reliable method, the frame is transmitted if the checks (Checksum) are good, it detects errors before sending. (FCS fields)

✓ *The disadvantage:* The height, (It takes time)

2- Cut Trough (1-Fast Forward

Direct mode: The switch just checks the hardware address of the destination and transmits it as is. No error detection is performed with this method.

✓ *The advantage:* The fastest method.

✓ *The disadvantage*

This method is not reliable, it is possible that the sent frame has a size <64 bytes (So it is an incomplete frame)

3- Cut Trough (2- Fragment Free):

It allows analyzing only the first 64 bytes of the frame. (Minimum of an Ethernet frame). The packets are switched to a fixed rate, making it possible to perform simplified error detection. (Data fields).

✓ *The advantage:* It ensures that the frame is correct, and then it sends.

✓ *The disadvantage:* Slower than Fast Forward, Error detection.

ISSN No:-2456-2165

4- Adaptive Switching: Is an automatic mode. Depending on the errors found, the switch uses one of the three modes.

➢ *Trunk*

A trunk is a single physical connection on which the traffic of several virtual networks is transmitted.

This mechanism is used to insert the identifier of the VLAN on a user frame. The entire frame propagates over multiple switches, and will always retain the information of its membership in a VLAN. A Trunk link is configured between switches, often called uplinks. [9]

IX. METHODS AND IMPLEMENTATION OF DYNAMIC VLANS APPLICATION USING OMNET 4.6 ++

This part consists of the development of a new application with C ++, using OMNeT 4.6 for the dynamic creation of VLANs with and without SDN, via the choice of Generic Attribute Registration Protocol (GVRP). For distribution the broadcast messages in the network, to dynamically configure VLANs in all devices on the network.

The SDN controller must contain a group of six packets, for it to work properly (Open Flow, Controller Apps, Host Apps, Hyper Flow, Kandoo, and Utility).

➢ *Step 1:*

A window (Figure 2) appears inviting the user to specify the number of VLANs desired.

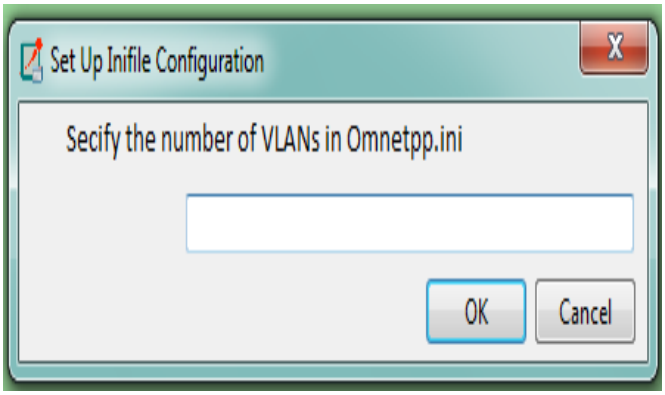

Fig 2:- Specification the number of VLANs

➢ *2nd step:*

After having specified the number of VLANs desired, a window (Figure 3) is automatically displayed, it consists of two parts for the creation of a dynamic VLAN architecture: Part Switch and Part Machines.

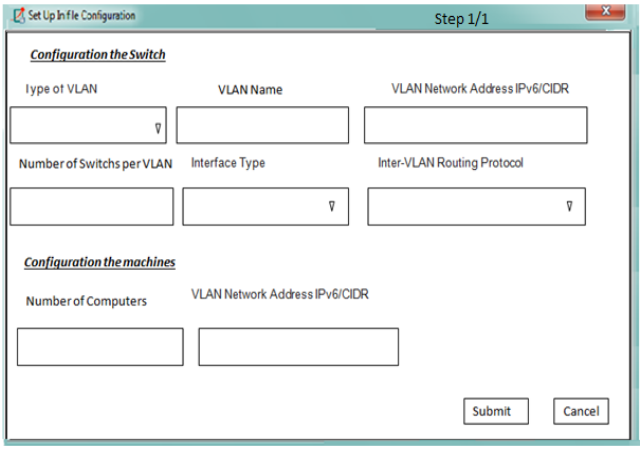

Fig 3:- Creating a dynamic VLAN.

➢ *Switch Party:*

The user must indicate for each VLAN:

- *Type of VLAN:* Define The Appropriate VLAN Type, That Is To Say VLAN Level 1 (VLAN Per Port), Or VLAN Level 2 (VLAN Per MAC Address), Or VLAN Level 3 (VLAN Per IP Address).
- *VLAN Name:* Specify A Name For The VLAN.
- *VLAN Network Address Ipv6 / CIDR:* Enter The Ipv6 Network Address For The VLAN With Its CIDR.

➢ *Interface Type*

It allows us to determine the type of the interface by other term the choice between the interface in Trunk mode or in Access mode.

Number of Switch per VLAN: Designate the number of switches per VLAN.

➢ *Machine part*

- *Number of Computers:* Enter the total number of machines for all networks in the architecture.
- *VLAN Network IPv6 / CIDR Address:* Enter the IPv6 network address with CIDR or VLAN.
- *Number of Computers per VLAN:* Present the number of machines for each VLAN.

➢ *Step 3:*

This step allows Access Control List (ACLs) [10] as shown in the figure 4 to be activated on the SDN controller, either for authorizing or prohibiting machines or networks to connect to other machines or networks.

Type of ACL: It allows determining the type of ACL, there are just two:

- *Deny*: To prohibit access to a machine or network.
- *Permit*: To allow access to a machine or network.

Layer 4 Protocol: It specifies the basic protocol for layer 4 of the OSI reference model. There are just 2 User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

ISSN No:-2456-2165

VLAN Address: It specializes the VLAN address to prohibit or allow with its CIDR.

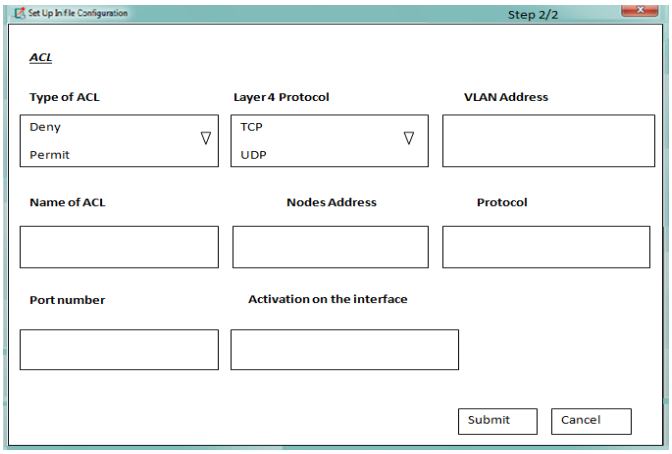

Fig 4:- Activating ACLs on VLANs

- *Name of ACL* It gives the possibility to create the name of the ACL.
- *Nodes Address* It specifies the machine (s) to allow or prohibit.
- *Protocol / Service* This is used to determine the protocol or service to allow or prevent.
- *Port number* It grants the port number to allow or prevent.
- Activation on the interface: It declares the name of the interface on which ACL will be applied.

Example of creating a dynamic VLAN:

➢ *Step 1*

This step allows the creation of 3 VLANs dynamically, as it is illustrated in the figure 5.

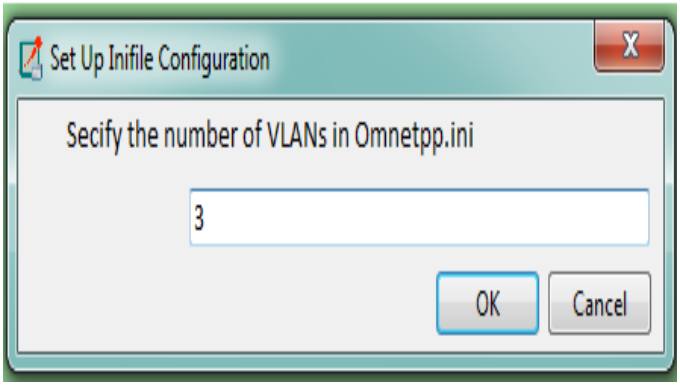

Fig 5:- Specification of number of VLANs

➢ *Step 2:*

This step specifies information about creating a VLAN, like that in figure 6.

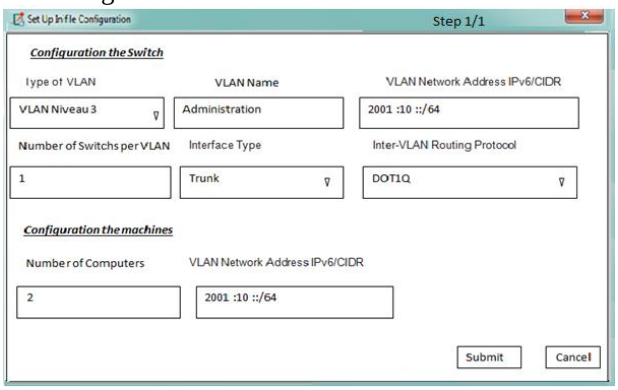

Fig 6:- Example of creating a dynamic VLAN

➢ *Step 3:*

This phase provides the ability to determine users as the figure 7, whether they are allowing or preventing access to a network or machine.

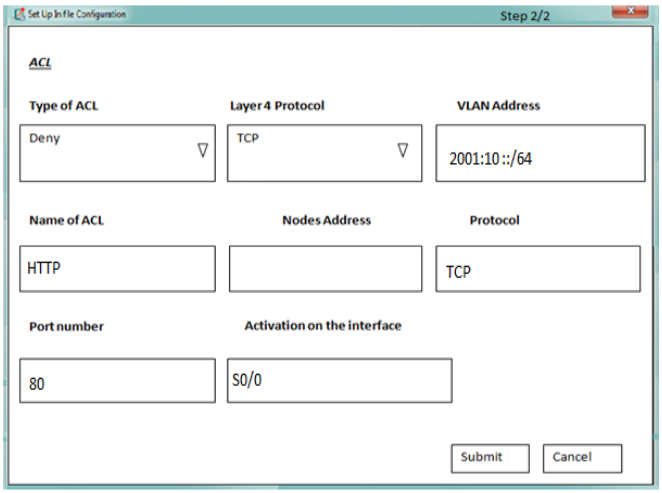

Fig 7:- Example of activating ACLs

X. RESULTS AND DISCUSSION OF SIMULATION IN QUALITY OF SERVICE CRITERIA (QOS)

A. VLANs without Scalability

The figures illustrate a network composed of 2 scenarios (Figure 8 and 9) for VLANs with and without SDN, the purpose of which is to centralize all traffic exchanged between VLANs.

Scenario 1: Figure 8: VALN without SDN.
Scenario 2: Figure 9: VALN with SDN.

ISSN No:-2456-2165

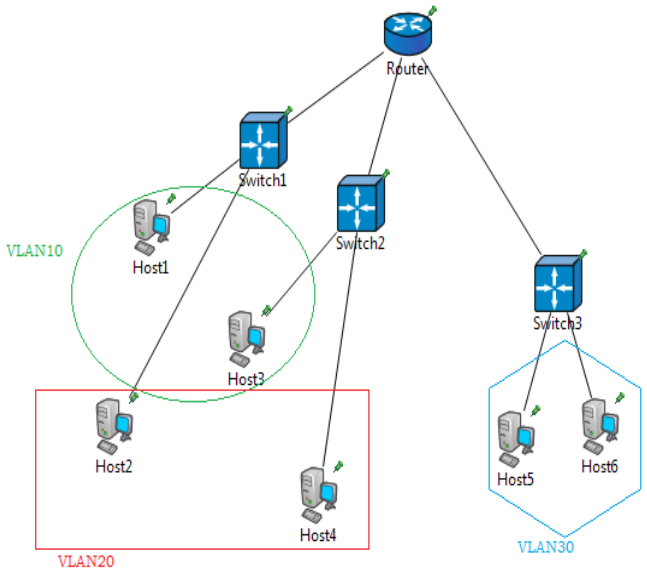

Fig 8:- VALN without SDN.

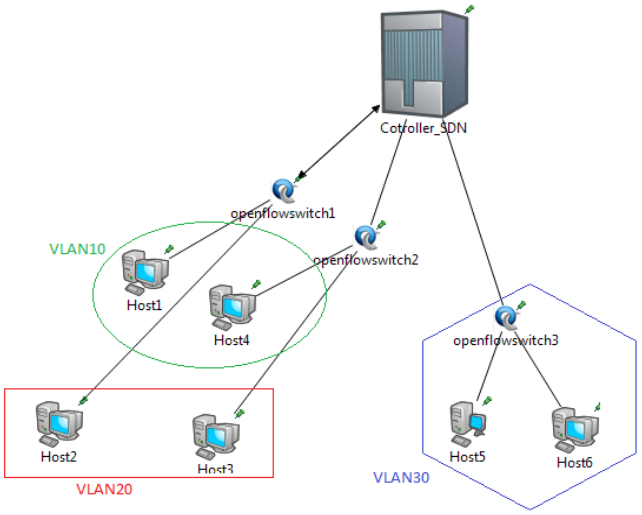

Fig 9:- VALN with SDN.

B. Scalability under VLANs

In order to study scalability under VLANs, the following architectures (Figure 10 and figure 11) is created with a high number of VLANs with and without.

Scenario 3: Figure 10: Scalability under VALN without SDN.
Scenario 4: Figure 11: Scalability under VALN with SDN.

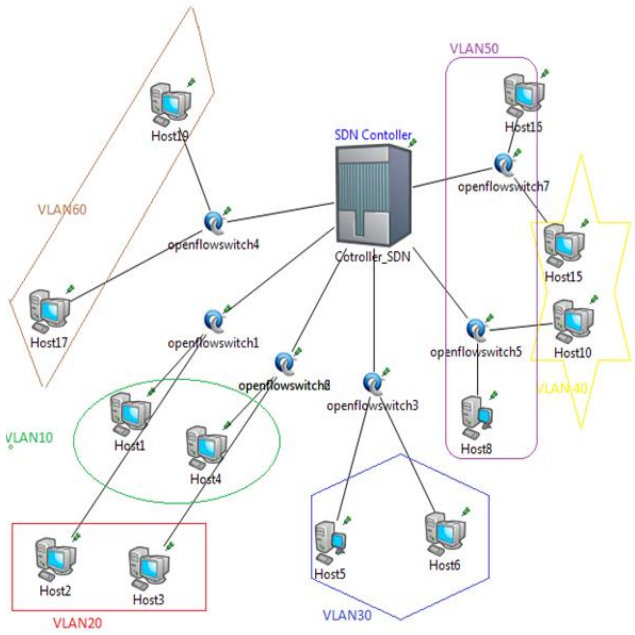

Fig 10:- Scalability under VALN with SDN

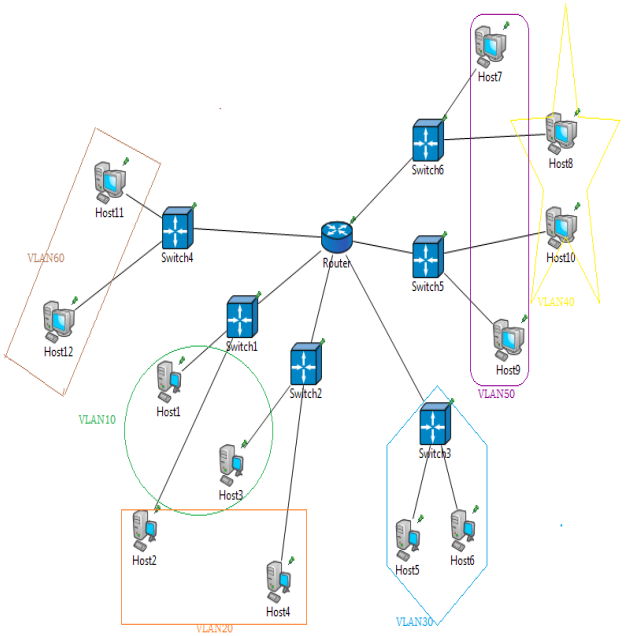

Fig 11:- VALN without SDN

C. SDN and Ethernet Scalability Simulation Results in Quality of Service (QOS) Criteria

This part offers each of the QoS parameters [11] (end-to-end delay, latency, jitter, lost packets, MOS) to show that VLANs with SDN is a powerful architecture, and it does not influence scalability.

D. End-to-end delay under VLANs with and without SDN with scalability

The results founding figure 12 show that the end-to-end delay for VLANs without SDN (10, 20, 30, 40, 50, and 60)

ISSN No:-2456-2165

takes more time in comparison with both SDN and the same as with scalability

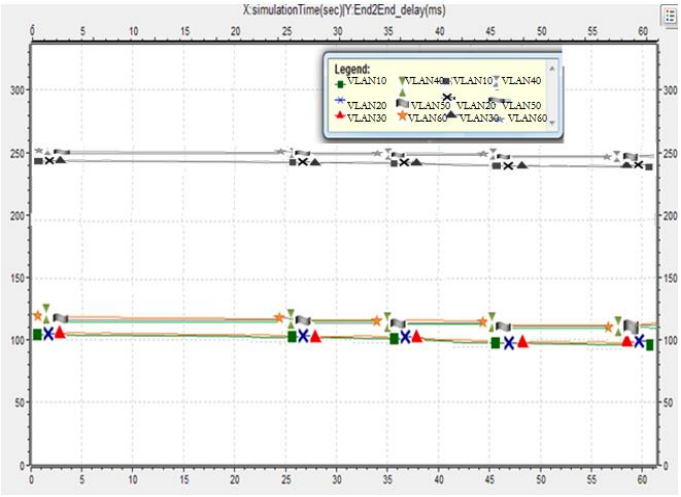

Fig 12:- End to end delay under VLANs with scalability.

E. Latency under VLANs with and without SDN with scalability

Figure 13 shows that the latency for VLANs (10, 20, 30, 40, 50, 60) without SDN has no relation with the addition of SDN with scalability, of which the addition of SDN is beneficial, which reduces latency time.

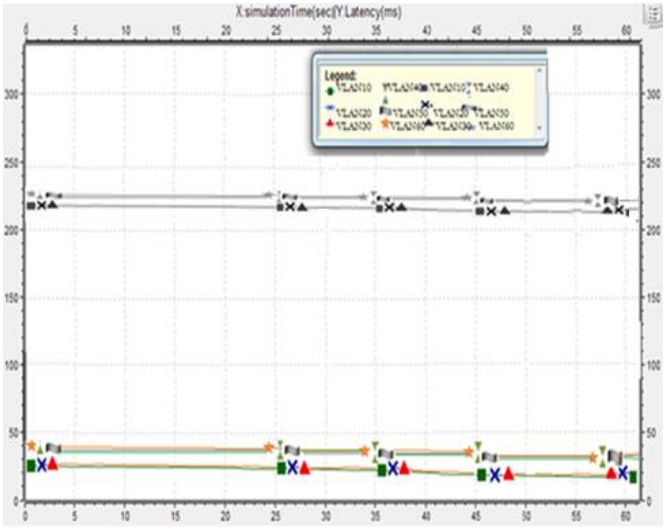

Fig 13:- Latency under VLANs with scalability.

F. Jitter under VLANs with and without SDN with scalability

Figure 14 shows that the Jitter for VLAN (10, 20, 30, 40, 50 60) with SDN does not exert upward scalability, which reduces the transmission time and that, thanks to the controller, SDN simplifies sending packages as well as the same thing with scalability.

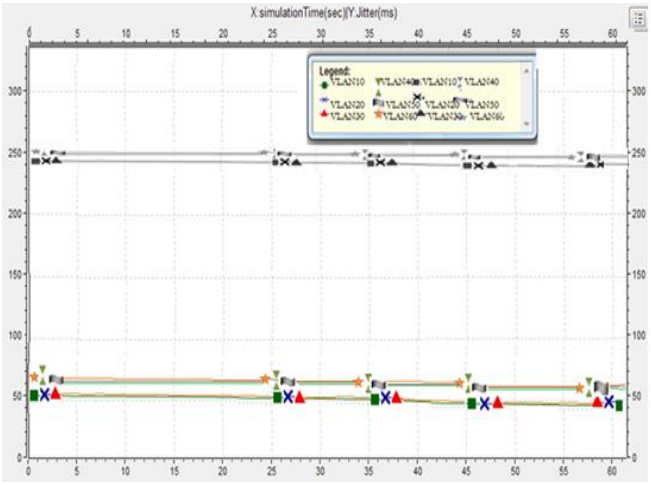

Fig 14:- Jitter under VLANs with scalability.

G. Packets lost under VLANs with and without SDN with scalability

The results show in figure 15 that the number of packets lost under the VLANs, even with their scalability, is almost zero, which justifies the main role of the SDN. On the other hand without SDN is very high.

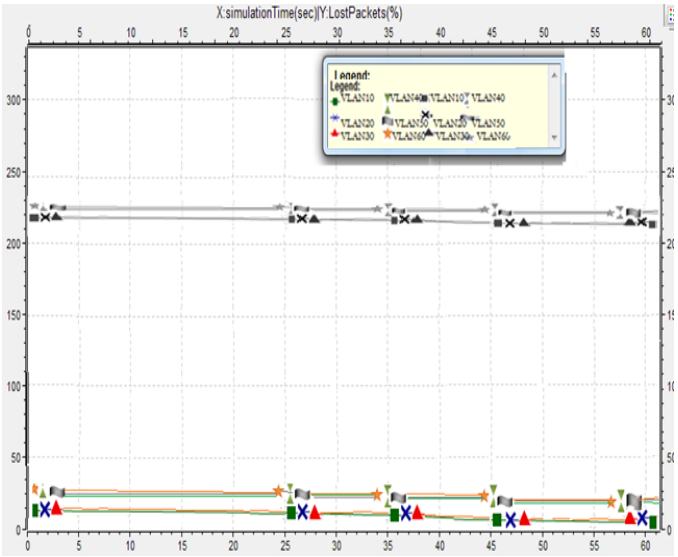

Fig 15:- Packets lost in VLANs with scalability.

H. MOS under VLANs with and without SDN with scalability

This figure 16 shows that the MOS offered by VLANs with SDN with their scalability is better because it exceeds 4, which demonstrates the impact of SDN integration with VLANs. but without SDN has a low level.

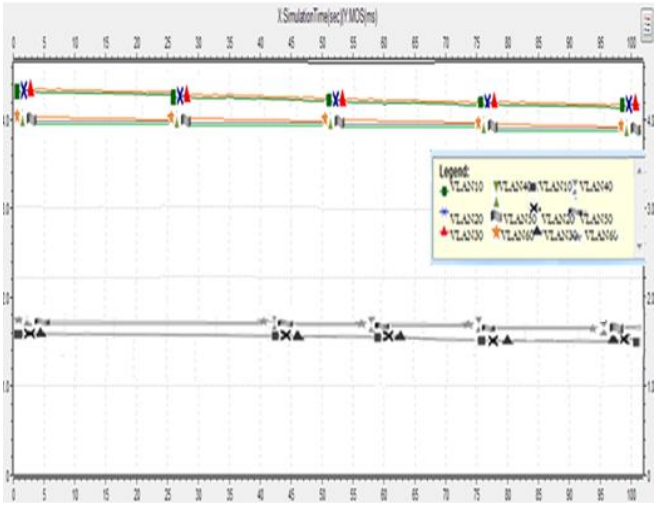

Fig 16:- MOS under VLANs with scalability.

XI. CONCLUSION

This article presents the performance of VLANs with and without SDN, their scalability in terms of QOS parameters (end-to-end delay, jitter, latency, number of lost packets and MOS), by creating a new application with C ++ using OMNET4.6 ++ for development in a dynamic way, the result is that VLAN union with SDN improves QOS.

REFERENCES

[1]. Yasuhiro Yamasaki, Yoshinori Miyamoto, Junichi Yamato, 2011, ‘‘Flexible Access Management System for Campus VLAN Based on OpenFlow’’IEEE/IPSJ International Symposium on Applications and the Internet, 30 August 2011.

[2]. Patrick T. Crinion, Vickie Pagnon, ‘‘Apparatus and method of assigning VLAN tags’’, 2001.

[3]. Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, Jonathan Turner, ‘‘OpenFlow: enabling ennovation in campus networks’’, ACM SIGCOMM Computer Communication Review archive, Volume 38 Issue 2, April 2008.

[4]. P. VenkaraMuthyalu, K. Ramu and G.V.R. Prasada Raju, ‘‘Study on performance of chemically stabilized expansive soil’’, ©IJAET, ISSN: 2231-1963, 2012.

[5]. Surabhi Surendra Tambe, ‘‘Understanding Virtual Local Area Networks ’’,(IJETT) –ISSN: 2231-5381, Volume 25 Number 4- July 2015.

[6]. Salah A. Jaro Alabady, ‘‘Design and Implementation of a Network Security Model using Static VLAN and AAA Server’’, IEEE, May 2008.

[7]. Trystan Johnson, Michael Pothier, Turnbull, Kenjin Huang, ‘‘Method and apparatus for VLAN ID discovery’’, 2008.

[8]. Haitao Wu, Yong Peng, Keping Long, ‘‘Performance of reliable transport protocol over IEEE 802.11 wireless LAN: Analyses and enhancement’’, IEEE, November 2002.

[9]. Jenq-Shiou Leu, Rong-Horng Lai, Hsin-I Lin ‘‘Running cellular/PWLAN services: practical considerations for cellular/PWLAN architecture supporting interoperator roaming’’, IEEE, February 2006.

[10]. Kimberly K.Smith, Darlene Gilcreast, KarenPierce, ‘‘Evaluation of staff’s retention of ACLs and BLS Skills’’, ScienceDirect, Volume 78, Issue 1, 2009.

[11]. Fatima LAASSIRI, Mohamed MOUGHIT, Noureddine IDBOUFKER, ‘‘Evaluation of the QoS Parameters in Different SDN Architecture Using Omnet 4.6++’’, IEEE, March 2018.