The Importance of VLANs and Trunk Links in Network Communication Areas

Dlnya Abdulahad Aziz
Computer Technical Engineering, AL-KITAB University, Iraq
dilnea89@gmail.com

Abstract— In this paper a new modern network design based on VLAN implementation was presented. The network was separated in to different VLANs to represent the performance of three departments in a university building. In addition, the paper discusses the impact of VLAN implementation on network performance and shows the security satisfaction approach in any filed. Furthermore, three different VLAN types identified by default, native, and management VLANs were presented. The results of the packet tracer software confirms that network separation based on VLAN methodology isolates the broadcast traffics of the devices regardless their existence in the same region with different network classification, even though all the devices of the regions can share the same cable and switch. As a final result, the creation of VLANs is important for data and traffic management in order to keep the broadcast frequency valid as long as the LAN increases and more network devices are added.

Index Terms— Local Area Network LAN, Virtual Local Area Network VLAN, Native VLAN, Default VLAN, Management VLAN.

1. INTRODUCTION

The development of virtual local area network VLAN led the great organizations such as companies, universities, enterprises, etc., to build their network schemes depending on VLAN encapsulation method. VLAN is a data link layer aspect that allows the implementation of the logical networks with respect to the physical ones [1]. This means, that the computers, servers, and other network devices in a VLAN are connected logically regardless their physical locations. Hence, even if these devices are located in different places, VLAN can logically group them into separate virtual networks. The purpose behind applying VLAN is to improve the security, traffic management, and make a network simpler. As an example, consider that there exist three story office building contains computers belong to certain departments and are mixed with computers belong to other departments in the same floor. Consider that the departments are identified by accounting, shipping, and management department. All these computers in these three departments are all connected to a switch, so they all are on the same segment on the local area network. Hereby, all the network broadcast traffics are mixed in with the other departments. Under this act, the departments can see their each other network traffic. Suppose that we wanted to separate the network broadcast traffic among these proposed departments such that the accounting department does not see any traffic from shipping department and management department does not see any traffic from shipping department and so on.

Dlnya Abdulahad Aziz *is currently B.Sc. student in Computer Technical Engineering at ALKITAB University, Iraq.*
E – Mail: *dilnea89@gmail.com*

That is the suggestion that does not make any sense, while there is an easier way to accomplish this task by creating VLANs. VLANs can logically create several virtual networks to separate the network broadcast traffic through VLAN switch. In this case, three VLANs must be created for the three departments (accounting, shipping, and management). Under this act, the traffics among the three departments are isolated, so they won't see any traffic created from the other departments and they only see their own network traffic even though all the computers from the different departments share the same cable and switch [2, 3]. In this proposed example, the VLANs was created on the switch which is done by designating specific ports on the switch and assigning those ports to specific VLAN. Hence, the switch incudes the VLAN of the management department that is the computers of that department are plugged to its corresponding ports in the switch, and then additional ports on the same switch are designated to plug the other VLAN of accounting department, and finally another additional setup ports on the switch are designated for the VLAN of shipping department. Hereby, the network traffics are separated among three departments because of the VLANs. As stated before, there are several reasons for creating VLANs and the one main reason is for traffic management because as the local area network grows and more network devices are added, the frequency of the broadcast will increase accordingly and the network will get heavily congested with data. However, by creating VLANs which divide the network into smaller broadcast domains then the broadcast traffic will be eliminated.

2. VIRTUAL LOCAL AREA NETWORK VLAN

A group of computer devices connected together through a common link is called local area network denoted as LAN. The local area network shown in Fig.1 connects devices in limited geographical areas inside office, building, university campus and etc. LANs are the communication form that offers the availability of

internet connection technology locally through local area network in certain location with various methodologies. It is worth mentioning that the LANs can be extended to be larger and larger to cover larger areas with respect to signal bitrate and baud rate.

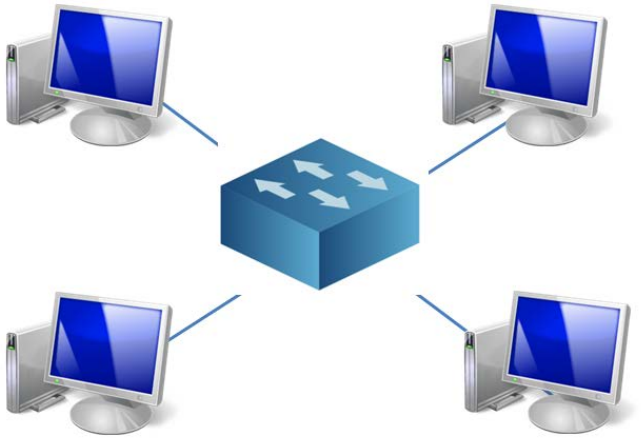

Fig.1. Simple Local Area Network Connection

Local area network activates the sharing point among the computers, mobile devices,, printers, and network storage devices. LANs can communicate among limited number of users in a small office or can communicate among hundred users in a larger location. LANs activate a network connection area by employing several components such as Switches, Routers, and another ways that guarantee the communication between the internal servers and the LANs through the wide area network WAN. The LANs can be connected with each other either through the Ethernet or the Wi-Fi connection methodologies. The Ethernet is the way allows the computer devices to be communicated effectively via Ethernet cables. While Wi-Fi connection employs the radio waves to connect the computers with each other inside the LANs. Local area networks use several topologies such as ARCNET, Token Ring, and Fiber Distributed Data Interface to connect the devices in the LANs. Furthermore, such a development excited the universe to offer the usability of the virtual local area network VLAN, which gives the main network partition the right to group the nodes of a network logically and partially with fewer infrastructures [4]. VLAN is considered the abstracted level of the local area network such that the VLAN can guarantee data connectivity for a sub network. Hereby, VLAN is recognized as managing method for LANs with separated polices. The particularity based on such networks is very important with respect to use wired or wireless connections. The proposed network works based on a heretical structure regarding the security layout, which assign VLANs to be classified as the most robust networks. Moreover, VLANs controls communication bit rate and the traffics in a network by allowing the possibility of the communication with respect to the ranges, while some problem might appear in the setup process of network hardware [5].

3. Corresponding VLAN Types

The usability of VLAN depends drastically on different types according to specific tasks. The important types are identified by native, default, and management VLAN. Native and management VLANs work under the supervision of 802.1q trunking protocol. While, native VLAN has better security than default VLAN. The switch that holds an unmarked frame through the trunking link excites the native VLAN to complete the operation. As a result, the security of a network can be fulfilled by addressing the untagged frames to the corresponding ways. Furthermore, if a switch received a frame randomly through a certain VLAN, the default VLAN will be responsible for delivering the frame to the corresponding switch with respect to the existence of the trunking port and the native VLAN [6].

4. Packet Tracer Software

Packet tracer software offers an environment to create networks based on the network components that allowed in the software such as routers, switches, cables, servers, etc. Packet tracer allows functional area for the students and researchers to create connection points and to demonstrate the simulation scenarios in less complexity with respect to geographical ranges while participation in Cisco packet tracer program [7]. In addition, CCNA Cisco versions allow several environments, embedded labs, and experiments particularly for students in the classes or even based on NETLAB system. Packet tracer is considered the powerful network simulation program that is employed considerably to apply the test and the experiments on different network topologies and environments that offer a lot of devices to be communicated with each other via robust cables.

5. Proposed Work Configuration

Virtual local area network VLAN is responsible for allowing communication among hosts that belong to the same network classification but in different places. The proposed work was satisfied depending on a simple example, which demonstrates the connection of classified networks in two different regions. The regions are represented by two buildings almost have the same features. In this work, various VLAN types are discussed such as native, data, and default VLAN in order to present the performance of the Virtual local area network in certain regions. The simple example shows two regions in the same place were connected with each other based on ordinary Cisco switches. Firstly, network 1 that represents the first region guarantees the existence of three main devices identified by default VLAN, Student data VLAN, and Management VLAN respectively. Consider that these devices are the main terminal, data registration department, and management department for a certain college in a university. Secondly, the same network classification is created in

another floor to manage the jobs of another college in the same university regardless management department that is considered uniformed for the whole university. The two network packet tracer schemes shown in Fig.2 can communicate with each other depending on the programing methodology of both switches in each side.

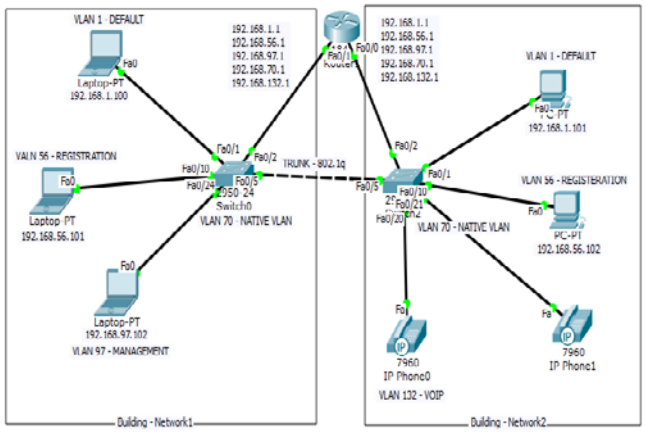

Fig.2. Network Example Scheme

For clarity, it is intended to demonstrate the employed IPs in this work as shown in Table 1.

TABLE 1
PROPOSED IP CLASSIFICATIONS

VLAN Type	IP Class	Subnet Mask
Default	192.168.1.1	255.255.255.0
Data	192.168.56.101	255.255.255.0
Management	192.168.97.102	255.255.255.0
Native	192.168.70.1	255.255.255.0
VOIP	192.168.132.1	255.255.255.0

The entire network was created in a critical protected procedure such that the default VLAN in both regions is considered tricky which created to protect the other sub networks such as registration and the management departments from the attackers or systematic network hackers. Moreover, the configuration of the default network was arranged automatically with respect to the switches, while the VLANs of the other departments were configured in both switches Switch0 and Switch1 as follows:

Switch Name: Switch0&Switch1
Switch>en
Switch#conf t
Switch(config)#vlan 56
Switch(config-vlan)#name student
Switch(config-vlan)#vlan 97
Switch(config-vlan)#name management
Switch(config-vlan)#exit
As demonstrated in the previous configuration, the student registration and the management departments were classified by network VLAN order numbers 56 and 97, which were interfaced with Switch0 through fastEthernet 0/10 and 0/24 respectively as follows:

Switch#conf t
Switch(config)#interface fastEthernet 0/10
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 56
Switch(config)#interface fastEthernet 0/24
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 97
Switch(config-if)#exit

For more confirmation, it is intended to test the communication inside one of the proposed VLANs by defining an IP address for a device in Management department (VLAN 97) as shown in Fig.3 and as follows:

Switch#conf t
Switch(config)#interface vlan 97
Switch(config-if)#ip address 192.168.97.2 255.255.255.0
Switch(config-if)#no shutdown

```
PC>ping 192.168.97.2

Pinging 192.168.97.2 with 32 bytes of data:

Reply from 192.168.97.2: bytes=32 time=0ms TTL=255
Reply from 192.168.97.2: bytes=32 time=0ms TTL=255
Reply from 192.168.97.2: bytes=32 time=0ms TTL=255
Reply from 192.168.97.2: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.97.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fig.3. Management VLAN Network IP Test

In the next stage, trunking protocol identified by Trunk 802.1q plays a great role specially for allowing the two regions to communicate with each other through one link. It is worth mentioning that the communication methodology without configuring trunking links is considered complicated and costly due to the set of links that are needed to be as much as the devices in order to assign the communication among the devices. Hereby, the trunking methodology that guarantees the successful communication among all VLANs (1 – 97) in both sides through one trunk link identified by fastEthernet 0/5 was configured as follows:

Switch#conf t
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1-97
Switch(config-if)#end
Now, the same network classification devices in both sides (colleges) can communicate with each other as shown in Fig.4.

```
PC>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=0ms TTL=128
Reply from 192.168.1.100: bytes=32 time=0ms TTL=128
Reply from 192.168.1.100: bytes=32 time=13ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

Fig.4. Default VLAN Network IP Test

Furthermore, the creation of native VLAN is very important to deal with uncisco devices that do not support the trunking protocol 802.1q. In this work, the native VLAN with order number 70 was configured in both network switches through fastEthernet 0/5 as follows:

Switch#conf t
Switch(config)#vlan 70
Switch(config-vlan)#name native
Switch(config-vlan)#exit
Switch#conf t
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#switchport trunk native vlan 70
Switch(config-vlan)#exit

By assigning the required interfaces among the devices and the switches, the simulation results expose the information of transporting a packet among the PCs as shown in Fig.5.

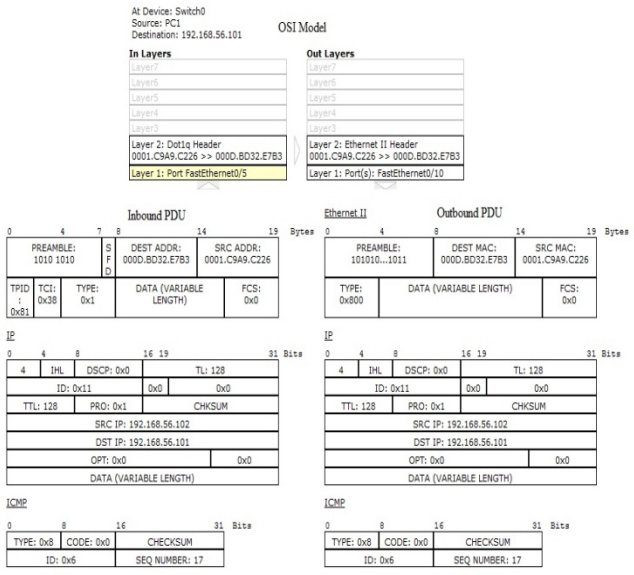

Fig.5. Packet Transport Simulation Result

In addition, it is intended to create VLAN responsible for dealing with calls and voice services through network 2 and the configuration was done with respect to Switch1via fastEthernet 0/20 with order number of 132 as follows:

Switch>en
Switch#conf t
Switch(config)#vlan 132
Switch(config-vlan)#name voice
Switch(config-vlan)#exit
Switch#conf t
Switch(config)#interface fastEthernet 0/20
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 132
Switch(config-if)#exit

The new created VLAN 132 is a trunk based VLAN through fastEthernet 0/2 which can be added to the other set of VLANs as follows:

Switch#conf t
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1-97,132
Switch(config-if)#switchport trunk native vlan 70
Switch(config-if)#end

In order to define voice communication among the departments, the voice over IP service VOIP was created by interfacing the Switch1 with the IP phone devices shown in Fig.6.

Fig.6. Voice Over IP Cisco Phone

The proposed phones were labeled by IP phone0 and IP phone1 and interfaced through fastEthernet 0/20 and fastEthernet 0/21 respectively. Hereby the configuration was done as follows:

Switch#conf t
Switch(config)#interface fastEthernet 0/20
Switch(config-if)#switchport mode access
Switch(config-if)#switchport voice vlan 132
Switch(config)#interface fastEthernet 0/21
Switch(config-if)#switchport mode access

Switch(config-if)#switchport voice vlan 132
Switch(config-if)#end

The routing protocol based on Router0 was configured in order to connect the two networks through the terminals fastEthernet 0/0 and fastEthernet 0/1 regardless the trunk link as follows:

Router>en
Router#conf t
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config)#interface fastEthernet 0/1
Router(config-if)#no shutdown

The interfacing terminals of Router0 are required to be configured as separated gateway assigned for each network by subdividing the interfacing terminals into the number of the VLANs available in the entire network as follows:

Router>en
Router#conf t
Router(config)#interface fastEthernet 0/0.1
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#interface fastEthernet 0/0.56
Router(config-subif)#encapsulation dot1q 56
Router(config-subif)#ip address 192.168.56.1 255.255.255.0
Router(config-subif)#interface fastEthernet 0/0.97
Router(config-subif)#encapsulation dot1q 97
Router(config-subif)#ip address 192.168.97.1 255.255.255.0
Router(config-subif)#interface fastEthernet 0/0.70
Router(config-subif)#encapsulation dot1q 70
Router(config-subif)#ip address 192.168.70.1 255.255.255.0
Router(config-subif)#interface fastEthernet 0/0.132
Router(config-subif)#encapsulation dot1q 132
Router(config-subif)#ip address 192.168.132.1 255.255.255.0
Router(config-subif)#end
Router#conf t
Router(config)#interface fastEthernet 0/1.1
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#interface fastEthernet 0/1.56
Router(config-subif)#encapsulation dot1q 56
Router(config-subif)#ip address 192.168.56.1 255.255.255.0
Router(config-subif)#interface fastEthernet 0/1.97
Router(config-subif)#encapsulation dot1q 97
Router(config-subif)#ip address 192.168.97.1 255.255.255.0
Router(config-subif)#interface fastEthernet 0/1.70
Router(config-subif)#encapsulation dot1q 70
Router(config-subif)#ip address 192.168.70.1 255.255.255.0
Router(config-subif)#interface fastEthernet 0/1.132
Router(config-subif)#encapsulation dot1q 132
Router(config-subif)#ip address 192.168.132.1 255.255.255.0
Router(config-subif)#end

The voice sharing approach among the proposed VLANs was configured via VOIP methodology through VLAN 132 in Router0 as follows:

Router#conf t
Router(config)#ip dhcp pool voip
Router(dhcp-config)#network 192.168.132.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.132.1
Router(dhcp-config)#option 132 ip 192.168.132.1
Router(dhcp-config)#end
Router#conf t
Router(config)#telephony-service
Router(config- telephony)# max-dn 12
Router(config- telephony)# max-ephones 8
Router(config- telephony)# ip source-address 192.168.132.1 port 3000
Router(config- telephony)# auto assign 1 to 10
Router(config- telephony)# end

Finally, the two IP phones can communicate with each other over the dialing number specified by 74882 and 74883 for IP Phone0 and IP Phone1 respectively. Hence, the configuration will be as follows:

Router#conf t
Router(config)# ephone-dn 1
Router(config- ephone-dn)# number 74882
Router(config)# ephone-dn 2
Router(config- ephone-dn)# number 74883
Router(config- ephone-dn)# end

6. CONCLUSIONS

This paper shows the impact of VLAN implementation on the performance and the security of the entire network. This work proposes a method to separate the regions in the same network classification into independent sub networks based on VLANs appreciations. The implementation confirmed that the broadcast traffics of the computers that act in different departments but belong to the same network classification can be isolated among and yet same cable and switch will be shared among the regions. In addition, the security policy was satisfied due to separation approach applied among the departments and due to the configuration of the default VLAN to pay attention of the attackers and the hackers from the original sub networks identified by the student data and management VLANs. It has to be mentioned that there are several reasons for creating VLANs, while the main reason is the traffic management because as long as the LAN grows up and more network devices are added, the frequency of the broadcast increases accordingly and the network will get heavily congested with data. Finally, it can be stated that creating VLANs divides the network into smaller broadcast domains leading the broadcast traffic to be faded out.

References

[1] Li Zichao, Hu Ziwei, Zhang Geng, Ma Yan;: "Ethernet topology discovery for virtual local area networks with incomplete information" 4th IEEE

International Conference on Network Infrastructure and Digital Content, Beijing, China, IEEE, pp: 252 - 256, 2014.

[2] Abdul Hameed, Adnan Noor Mian;: "Finding efficient VLAN topology for better broadcast containment" Third International Conference on The Network of the Future (NOF), Gammarth, Tunisia, IEEE, pp: 1 - 6, 2012.

[3] Mohammed Suhel Inamdar, Ali Tekeoglu;: "Security Analysis of Open Source Network Access Control in Virtual Networks" 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, Poland, IEEE, pp: 475 - 480, 2018.

[4] Satoshi Kodama, Rei Nakagawa, Toshimitsu Tanouchi, Shinya Kameyama;: "Management system by using embedded packet for hierarchical local area network" IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, New York, NY, USA, IEEE, pp: 1 - 4, 2016.

[5] C. Fancy, L. Mishal Mohammed Thanveer;: "An evaluation of alternative protocols-based Virtual Private LAN Service (VPLS)" International Conference on IoT and Application (ICIOT), Nagapattinam, India, IEEE, pp: 1 - 6, 2017.

[6] Li Xinzhan, Cheng Chuanqing;: "Discuss on VLAN Stacking in Packet Network" International Symposium on Intelligent Ubiquitous Computing and Education, Chengdu, China, IEEE, pp: 389 - 392, 2009.

[7] Andrew Smith, Colin Bluck;: "Multiuser Collaborative Practical Learning Using Packet Tracer" Sixth International Conference on Networking and Services, Cancun, Mexico, IEEE, pp: 356 - 362, 2010.

IJSER

ABOUT AUTHOR:

Dlnya Abdulahad Aziz is currently B.Sc. student (Final Year) in Computer Technical Engineering at ALKITAB University, Iraq.

Email: dilnea89@gmail.com