International Journal of Research in Engineering, Science and Management
Volume-2, Issue-8, August-2019
www.ijresm.com | ISSN (Online): 2581-5792

Use of Virtual LANs for Network Segmentation and Organization

Shubham Annigeri[1], Anushka Chauhan[2], Jaikishin Chhatlani[3]
[1,2,3]*Student, Department of Electronics and Telecommunication Engineering, Vivekanand Education Society's Institute of Technology, Mumbai, India*

***Abstract*: In any organization where there are multiple computing devices connected through a network; segmentation is a significant problem. It is helpful to separate sets of devices on a network into logical segments for the purpose of privacy and functionality. However, it is not practical to give all the segments different physical Local Area Networks(LANs). It would require significant investment to create different physical networks for different purposes, especially for a growing business or institutions. Therefore, the need for a Virtual LAN(VLAN) arises. Using the concept of VLAN it is possible to separate networks such that some sets of devices can function as if they are on their own different LANs even though they would physically be in the same LAN. In this paper, we have demonstrated this using Cisco Packet Tracer (CPT).**

***Keywords*: CPT, Cisco Packet Tracer Simulation, Network Segmentation, Trunks, Trunking Protocol, Virtual LANs, VLANs.**

1. Introduction

When a device is connected to a switch, the switch automatically configures the device to communicate with all the other devices connected on the default LAN (VLAN 1 in Cisco Packet Tracer). To create a VLAN, the switch has to be configured to support it. Once a VLAN is added in the switch, we have to assign ports that will be part of the created VLAN. Only the devices connected to those ports will have access to other devices in that VLAN.

In CPT, up to 1005 different VLANs can be configured into a *2960 switch*, although it has only 24 Fast Ethernet and 2 Gigabit Ethernet ports. Thus to configure more than 26 devices, we need to use two switches.

This creates a new problem. If only a single VLAN can be assigned to a port, it would be very difficult for two devices on the same VLAN but on different switches to communicate as we would need a connection for each VLAN. This would not only waste the ports of a switch as the number of ports used just for switch-to-switch transfer of packets would be equal to the number of VLANs in them. Trunking has been used to solve this problem. A trunk is a special type of connection that has the ability to support multiple VLANs in a single port connection. Thus, in this simulation, trunks have been used for communication between two switches.

2. Virtual LAN

VLAN is the concept of partitioning a broadcast domain into logically different parts. In a broadcast domain, a packet sent by one device goes to all others via the network and the individual devices decide whether or not they will accept that packet. Dividing a broadcast domain helps in improving the performance and reducing the network traffic as the packets are not allowed to exit the VLAN (broadcast domain) that they are a part of. So, as the network does not have to deal with all the extra(dropped) packets, the traffic reduces and performance increases.

3. VLAN Connections

VLAN supports two types of linking: access link and trunk link. In the access link, only a single VLAN can be assigned in a system. If we want to create more than one VLAN we have to use a hub, connect users to the hub and then divide it into multiple VLANs. This method is tedious as well as not an economical solution. Thus the solution lies in using a trunk link. In a trunk link, multiple VLANs can be assigned in a single link. Trunking allows us to transfer data over the network that is accessible only to certain VLANs. In the simulation, we have used a trunk link to connect both the switches as all the same VLANs on either side should be able to communicate with each other.

4. VLAN Trunking Protocol (IEEE 802.1Q)

A trunk port is a port that is used to carry traffic for all the VLANs that are accessible by a specific switch, a process known as trunking. Trunk ports mark frames with unique identifying tags either 802.1Q tags or Inter-Switch Link (ISL) tags as they move through the trunked connection. Therefore, every single frame is directed to its designated VLAN using the tags assigned to them. This ensures accurate delivery of packets to the appropriate VLANs. A trunk port carries traffic to/from all VLANs by default. All VLAN IDs are permitted on all trunks. However, it is possible to remove/block the traffic of certain VLANs from entering a switch. In this simulation, we have used trunk link ports for communication between VLANs on different switches.

IEEE 802.1Q is the networking standard that supports

VLANs on an Ethernet network. This standard defines a system that tags frames passing through trunked connections to be used by bridges and switches for sorting them into appropriate LANs. There is also a provision to prioritize the frames originating from certain VLANs for maintaining QoS(Quality of Service).

The requirements for VLAN trunk to communicate information between switches are:

1. All the switches have to run the same version of VTP.
2. The domain name of VTP must be the same on all switches.

5. Dynamic Trunking Protocol (DTP)

DTP is enabled in all Cisco switches. In DTP if we configure one port of a switch (connected with a port of another switch) to be a trunk connection, then the port of the other switch is automatically configured to carry packets from those VLANs that the first switch was configured with. This is extremely useful as we don't have to configure the other switch separately saving a lot of time and effort. In this particular case, it also allows the admin to telnet into both the switches giving him absolute control of the network.

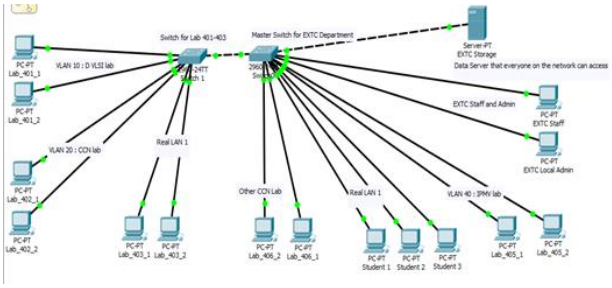

Fig. 1. Network map

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 90
% Access VLAN does not exist. Creating vlan 90
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
10   DVLSI                             active    Fa0/2
20   CCN_402                           active    Fa0/3, Fa0/4
50   common                            active
90   VLAN0090                          active    Fa0/1
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Fig. 2. VLAN

```
Vlan1              Down    1       <not set>          00D0.BA81.DBE9
Vlan50             Up      50      192.168.50.102/24  00D0.BA81.DB01
Hostname: Switch
```

Fig. 3. Hostname

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line vty 0 15
Switch(config-line)#password d14b@extc_1
Switch(config-line)#exit
Switch(config)#enable secret d14b@extc_1
```

Fig. 4. Configuration

6. Simulation

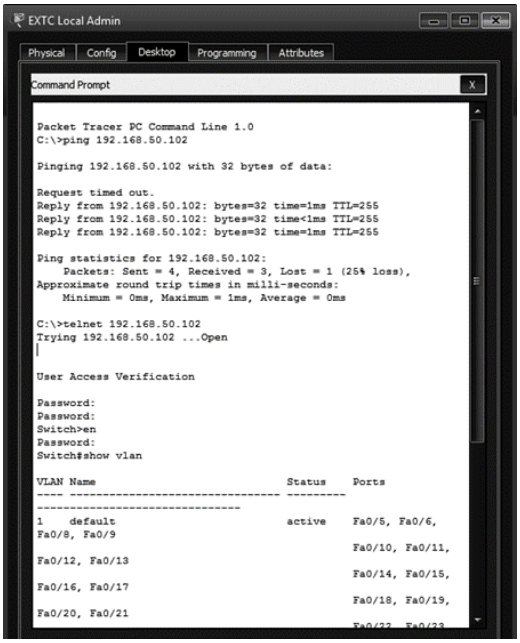

Fig. 5. Command prompt

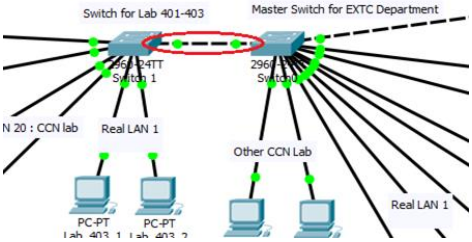

Fig. 6. Connections

```
Switch>
Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa 0/7
Switch(config-if)#switchport mode trunk
Switch(config-if)#sw
Switch(config-if)#switchport trunk allowed vlan 1-90
Switch(config-if)#
```

Fig. 7. Code

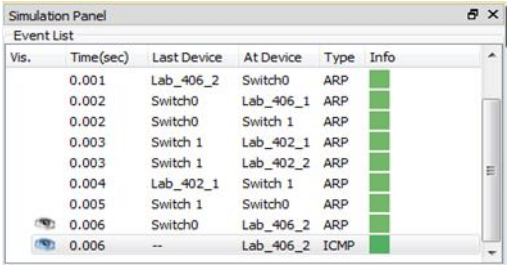

Fig. 8. Simulation panel

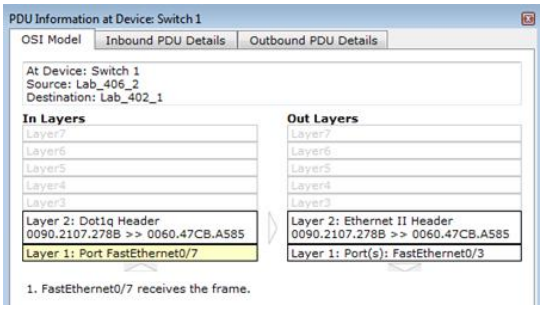

Fig. 9. PDU Information at device: Switch 1

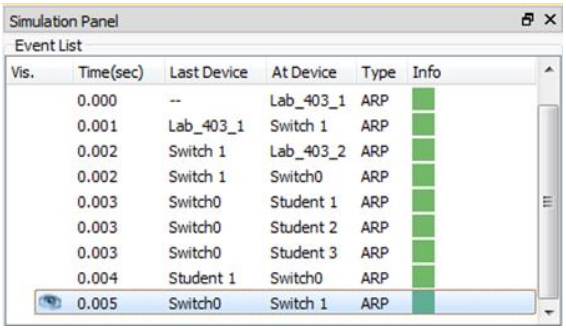

Fig. 10. Event list

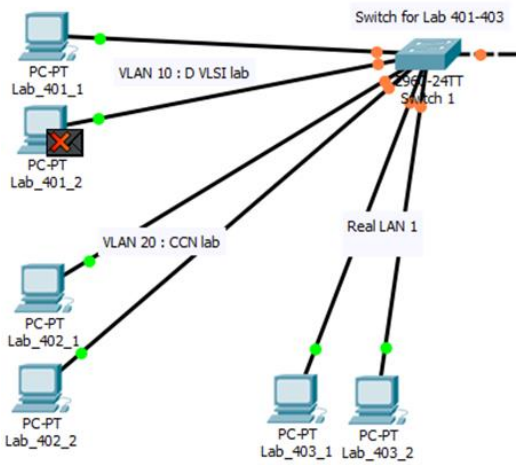

Fig. 11. VLAN connections

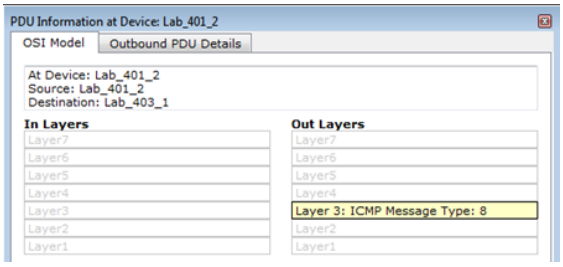

Fig. 12. OSI model

In fig. 1 the network map is shown. On the switch to the left, we can see that there are three VLANs, viz. vlan1, the default VLAN, vlan 20, the VLAN for CCN lab and vlan 10, the VLAN for DVLSI lab. The PCs in the vlan 20 can communicate only with each other. They can neither send nor receive any packets from outside their VLAN. However, vlan 1 and vlan 20 are trunked to both the switches. This means that the PCs in vlan 1 can access any PC that is a part of the default LAN as well as any other PC that is connected to a non-configured port. The PCs on vlan 20 can access PCs on the other switch that are in vlan 20. The switch itself is assigned an IP address and put in a VLAN that matches with the VLAN of the admin PC. This ensures that the admin can access the switch and change the settings and configuration using TELNET. The network is segmented into logical parts based on their functionality and the resources they need.

Here, we have assigned a port to a VLAN that we have dynamically created. If a VLAN doesn't exist while assigning a port to it, it will automatically be created.

To, provide telnet access to an admin PC, we need to assign an IP address and make it a part of the same VLAN that the Admin PC is in. Here, it is VLAN 50. This process is shown in fig .4 and 5.

The trunked connection is set up on switch 1 for port 7. Almost immediately, it is observed that the switch 2 automatically configures itself to assign a trunked connection to port 24 which is the line connected to port 7 of switch 1. This is shown in fig. 6 and 7.

Finally, once the network was set up. Several test cases were implemented some of which are mentioned. The first case mentioned is shown in fig. 8 and 9. In this scenario, PC2 in lab 406 (Lab_406_2) communicates with PC1 in lab 402 (Lab_402_1). This communication is successful as shown in the figure with the acknowledgment received. A similar case is shown in fig 6.c where two PCs on the real VLAN(default) on two different switches communicate. Both these scenarios together push the concept of VLAN trunking as signals of both the VLANs are being sent through the same (trunk) link. Similarly, the failure to communicate between two PCs on different VLANs reinforces the core concept of VLAN. This is shown in fig. 11 and 12.

7. Observations

Through this research, we have identified the following points regarding VLANs.

A. *Advantages*

Broadcast Traffic Containment: In a network with a default configuration, all computers share the same broadcast domain. Such a case would require the use of additional network devices such as routers. It would also cause a lot of congestion in the network as even the packets that will be dropped by the device will be sent to the port. Whereas, in case of VLANs, flooding of a packet is limited to the switch ports of only that particular VLAN. Hence by confining the broadcast domain, we can contain the traffic without having to deploy routers.

Security: As mentioned above, all the computers of a network contain the same broadcast domain by default. This allows all the computers to access data from every other node

on the network. For example, in the shown CPT model setup, had there been no VLAN implementation, the PCs of CCN lab would be able to access IPMV lab resources. In organizations, this raises serious security concerns. Through VLANs, we have separated our network into smaller networks which do not broadcast the packets with others. End stations are prevented from receiving broadcasts not meant for them. Furthermore, different VLANs can communicate only via routers which can be configured with various security options.

Reduced Latency: One of the principal advantages of VLANs is that it reduces latency in the network. Routers would have to be used instead of switches to segment the network if VLANs were not used. Each hop from router to router introduces latency. Hence latency increases as the number of routers in the network increases. By making use of VLANs, we reduce, in a way, optimize the number of routers in our network.

Flexibility across Physical and Geographical Barriers: Being able to create logical boundaries over a physical network is one of the key features of a VLAN. In simple terms, VLANs enable logical grouping of end stations even when they are spread over physically disparate locations and not connected to the same routers of switches.

B. Drawbacks

Performance Inefficiencies: As identified in [1], sometimes the actual path taken by the data to travel from one switch to the other might be substantially longer than the shortest physical path available introducing longer delays, redundant transmissions, and loops.

8. Conclusion

In this paper, we have explored the possibility of using VLANs for network segmentation and management. The simulation of the same on Cisco Packet Tracer provides a 'proof of concept' for the proposed solution.

Key points identified:

- VLANs prove to be an effective tool for managing and creating a hierarchy in a network.
- Dynamic Trunking Protocol (DTP) makes the work easy for the network system designer by configuring the second switch reflexively when one switch is configured on a link.
- TELNET protocol can be used in VLANs to remotely configure any device.

References

[1] Prashant Garimella, Yu-Wei Sung, Nan Zhang, and Sanjay Rao. Characterizing VLAN usage in an Operational Network, 2007.
[2] Yu-Wei Eric Sung, Sanjay G. Rao, Geoffrey G. Xie, and David A. Maltz. Towards Systematic Design of Enterprise Networks, 2008.
[3] Mario Ernesto Gomez-Romero, Mario Reyes-Ayala, Edgar Alejandro Andrade-Gonzalez and Jose Alfredo Tirado-Mendez. Design and Implementation of a VLAN.
[4] Xiaoying Wang, Hai Zhao, Mo Guan, Chengguang Guo, Jiyong Wang. Research and implementation of VLAN based on service, 2003.
[5] M. Casado, T. Garfinkel, A. Akella, M. Freedman, D. Boneh, N. Mc Keown, and S. Shenker. SANE: A protection architecture for enterprise networks. In Usenix Security, Aug. 2006.
[6] H. Boehm, A. Feldmann, O. Maennel, C. Reiser, and R. Volk. Network-wide inter-domain routing policies: Design and realization. Apr. 2005.
[7] Virtual LAN (VLAN). https://www.geeksforgeeks.org/category/computer-subject/computer-network