



Faculty of Engineering & Technology
Electrical & Computer Engineering Department

ENCS4130

Experiments No.7 – No.8

Switching and VLANs

Prepared by : Tareq Shannak

ID Number : 1181404

Instructor : Dr. Ahmad Alsadeh

Teaching Assistant : Katy Sadi

Section : 2

Date : 13/8/2021

Abstract

The aim of this experiment is to configure a Cisco IOS Switch using the IOS command-line interface (CLI), use switch simulator, split Cisco router into sub-interfaces and split Cisco switches into multiple virtual ones and create VLANs.

Table of Contents

1. Theory	1
1.1. Switching	1
1.1.1. Circuit Switching	1
1.1.2. Packet Switching.....	1
1.2. VLAN Definition	2
1.2.1. IEEE 802.1Q VLAN.....	2
2. Procedure & Discussion	3
2.1. Topology	3
2.2. Networks IPs	3
2.3. Configuring Routers	4
2.3.1. Configuring interfaces and sub-interfaces	4
2.3.2. Configuring OSPF Routing.....	4
2.4. Configuring Switches	4
2.4.1. Creating a VLAN.....	4
2.4.2. Configuring Switch ports	4
2.5. Configuring Multilayer Switch	4
2.5.1. Configuring switchport to router link	4
2.5.2. Configuring VLAN Interfaces IPs	5
3. Results	6
4. Conclusion	8
5. References	9

Table of Figures

Figure 1 - Circuit Switching	1
Figure 2 - Packet Switching.....	2
Figure 3 - Topology	3
Figure 4 - Ping Requests	6
Figure 5 - Path of the message's packets from PC1 to PC6.....	6
Figure 6 - Path of the message's packets from PC9 to PC10.....	7

Table of Tables

Table 1 - Networks IPs	3
Table 2 – Switchports	4

1. Theory

1.1.Switching

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes.

A switch usually works as soon as it is plugged into a power source. Whenever a device is sending a frame at one of its ports, the switch extracts the MAC address of that device and links it to the port. At the end, a switch builds a table of MAC-Port mappings so it can deliver packets from one device to another.

1.1.1. Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There is a need of pre-specified route from which data will travels and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place. Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases: establish a circuit, transfer the data and disconnect the circuit.

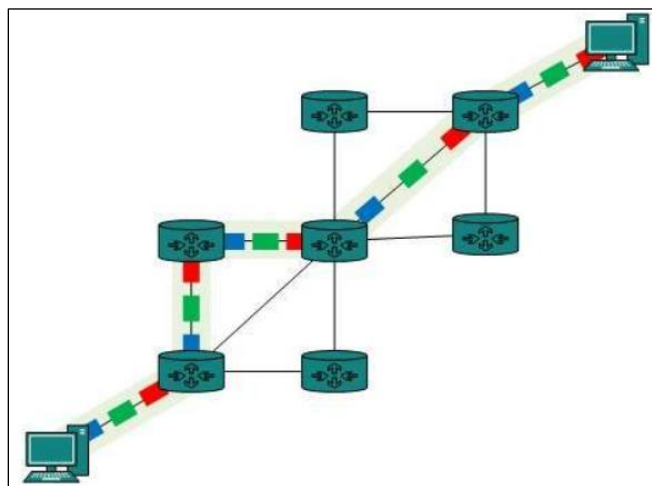


Figure 1 - Circuit Switching

1.1.2. Packet Switching

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently. It is easier for intermediate networking devices to store small size packets and they do not

take much resources either on carrier path or in the internal memory of switches. Figure 2 shows the packet switching.

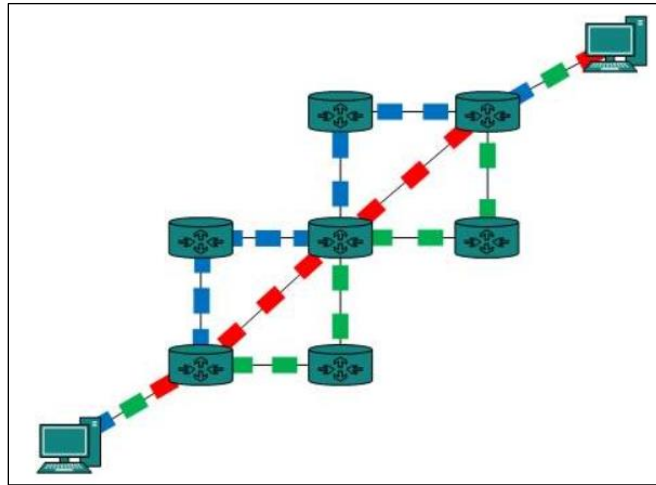


Figure 2 - Packet Switching

Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

1.2.VLAN Definition

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic. VLANs work by applying tags to network frames and handling these tags in networking systems - creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.

1.2.1. IEEE 802.1Q VLAN

IEEE 802.1Q, often referred to as Dot1q, is the networking standard that supports virtual LANs (VLANs) on an IEEE 802.3 Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also contains provisions for a quality-of-service prioritization scheme commonly known as IEEE 802.1p and defines the Generic Attribute Registration Protocol.

2. Procedure & Discussion

2.1. Topology

Figure 3 shows the topology that we will built in this experiment.

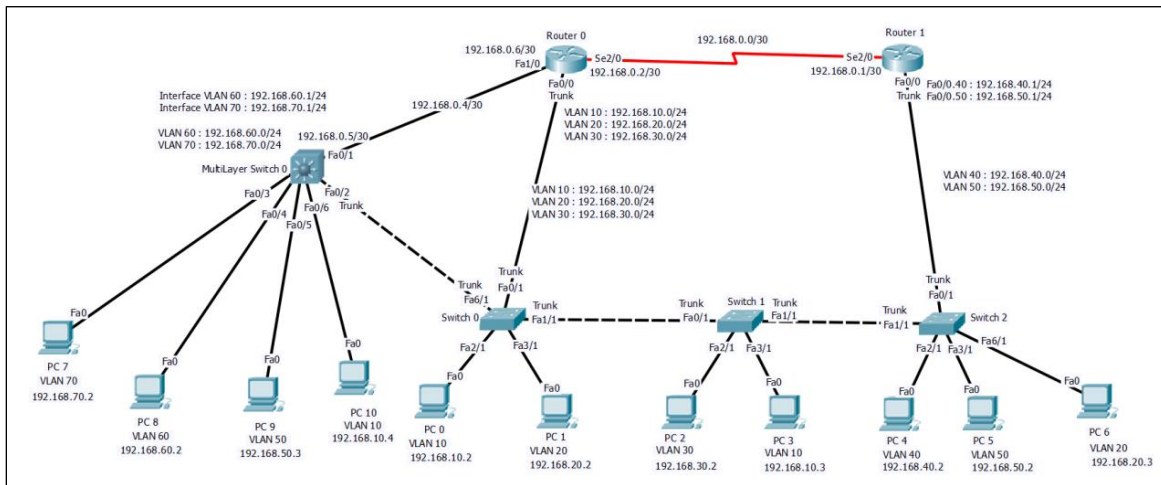


Figure 3 - Topology

2.2. Networks IPs

Table 1 shows sub-netting the IPs of networks and identify the areas to configure the router interfaces, sub-interfaces and PCs. Each PC has been configured its IP address, subnet mask and gateway.

#Area	#Net	Network	Device	Interface	IP	Subnet Mask	Wildcard Mask	VLAN ID
A0	0	192.168.0.0/30	Router 1	Se2/0	192.168.0.1	255.255.255.252	0.0.0.3	1
			Router 0	Se2/0	192.168.0.2	255.255.255.252	0.0.0.3	1
	1	192.168.10.0/24	Router 0	Fa0/0.10	192.168.10.1	255.255.255.0	0.0.0.255	10
			PC0	Fa0	192.168.10.2	255.255.255.0	0.0.0.255	10
			PC3	Fa0	192.168.10.3	255.255.255.0	0.0.0.255	10
	2	192.168.20.0/24	Router 0	Fa0/0.20	192.168.20.1	255.255.255.0	0.0.0.255	20
			PC1	Fa0	192.168.20.2	255.255.255.0	0.0.0.255	20
			PC6	Fa0	192.168.20.3	255.255.255.0	0.0.0.255	20
	3	192.168.30.0/24	Router 0	Fa0/0.30	192.168.30.1	255.255.255.0	0.0.0.255	30
			PC2	Fa0	192.168.30.2	255.255.255.0	0.0.0.255	30
	4	192.168.40.0/24	Router 1	Fa0/0.40	192.168.40.1	255.255.255.0	0.0.0.255	40
			PC4	Se2/0	192.168.40.2	255.255.255.0	0.0.0.255	40
	5	192.168.50.0/24	Router 1	Fa0/0.50	192.168.50.1	255.255.255.0	0.0.0.255	50
			PC5	Fa0	192.168.50.2	255.255.255.0	0.0.0.255	50
			PC9	Fa0	192.168.50.3	255.255.255.0	0.0.0.255	50
	6	192.168.60.0/24	MLS 0	VLAN 60	192.168.60.1	255.255.255.0	0.0.0.255	60
PC8			Fa0	192.168.60.2	255.255.255.0	0.0.0.255	60	
7	192.168.70.0/24	MLS 0	VLAN 70	192.168.70.1	255.255.255.0	0.0.0.255	70	
		PC7	Se2/0	192.168.70.2	255.255.255.0	0.0.0.255	70	
8	192.168.0.4/30	Router 0	Fa1/0	192.168.0.6	255.255.255.252	0.0.0.3	1	
		MLS 0	Se2/0	192.168.0.5	255.255.255.252	0.0.0.3	1	

Table 1 - Networks IPs

2.3. Configuring Routers

2.3.1. Configuring interfaces and sub-interfaces

The routers have been turned on for each interface that we used in the network and each interface has been given a certain IP address. Also, the sub interfaces have been configured for a specific VLANs in each router.

2.3.2. Configuring OSPF Routing

After that, OSPF has been configured by writing commands in the routers that specify process ID of the routing, and select which networks contain this specified router by writing the network ID, wildcard mask and the area number.

2.4. Configuring Switches

2.4.1. Creating a VLAN

In each switch, the VLANs 10-70 have been created to make the switch familiar with these VLANs.

2.4.2. Configuring Switch ports

The ports in each switch were configured if they are trunk or access port according to Table 2.

Switch	Port	Kind	VLAN
Switch 0	Fa0/1	Trunk	---
	Fa1/1	Trunk	---
	Fa2/1	Access	VLAN 10
	Fa3/1	Access	VLAN 20
Switch 1	Fa0/1	Trunk	---
	Fa1/1	Trunk	---
	Fa2/1	Access	VLAN 30
	Fa3/1	Access	VLAN 10
Switch 2	Fa0/1	Trunk	---
	Fa1/1	Trunk	---
	Fa2/1	Access	VLAN 40
	Fa3/1	Access	VLAN 50
	Fa6/1	Access	VLAN 20

Table 2 – Switchports

2.5. Configuring Multilayer Switch

2.5.1. Configuring switchport to router link

The interface fa0/1 in the multilayer switch has been configured as a router link using 'no switchport' command.

2.5.2. Configuring VLAN Interfaces IPs

In this multilayer switch, we had two VLANs (60+70). Hence, we configured an IP address for these two VLANs in the multilayer switch using 'interface VLAN ID' command.

After that we created the VLANs and configured the switchports as we configured them in the simple switch. But in trunk mode we added the encapsulation command. In routing, we enabled the routing in the multilayer switch using 'ip routing' and configured OSPF protocol as we configured it in the simple router.

3. Results

Figure 4 shows that the messages have been received successfully to the PCs that we chose randomly. Therefore, our network's devices communicate with each other perfectly.

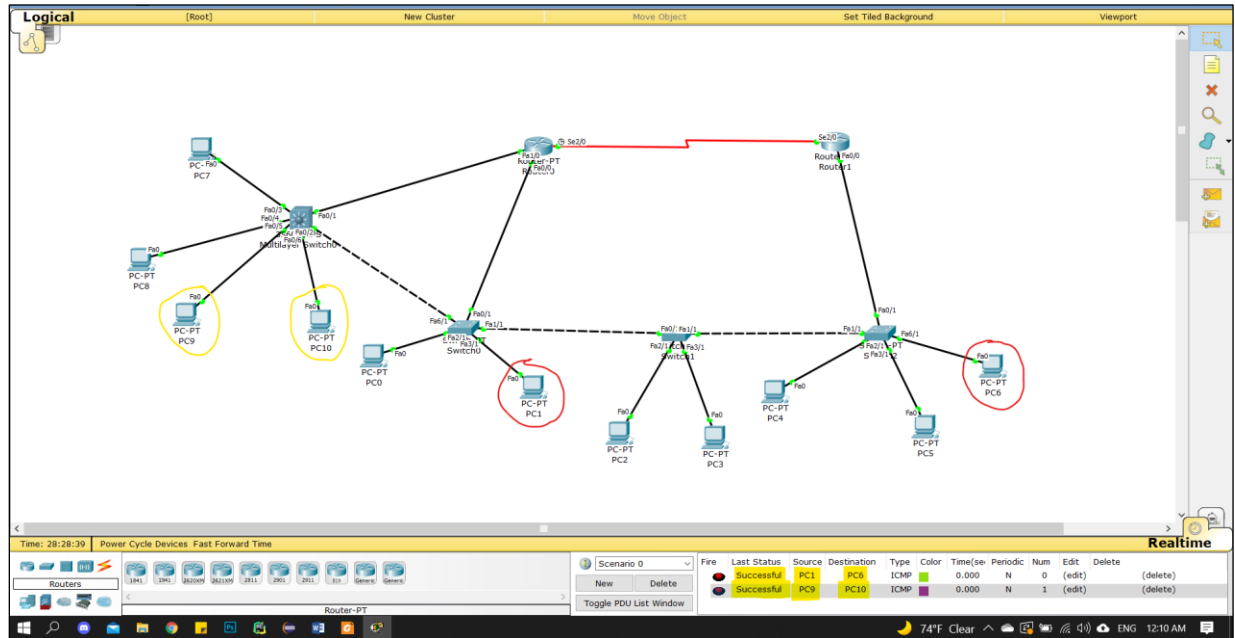


Figure 4 - Ping Requests

To see the paths of our messages that have been passed from PC1 to PC6 and from PC9 to PC10, a message request has been simulated as shown in Figures 5 and 6.

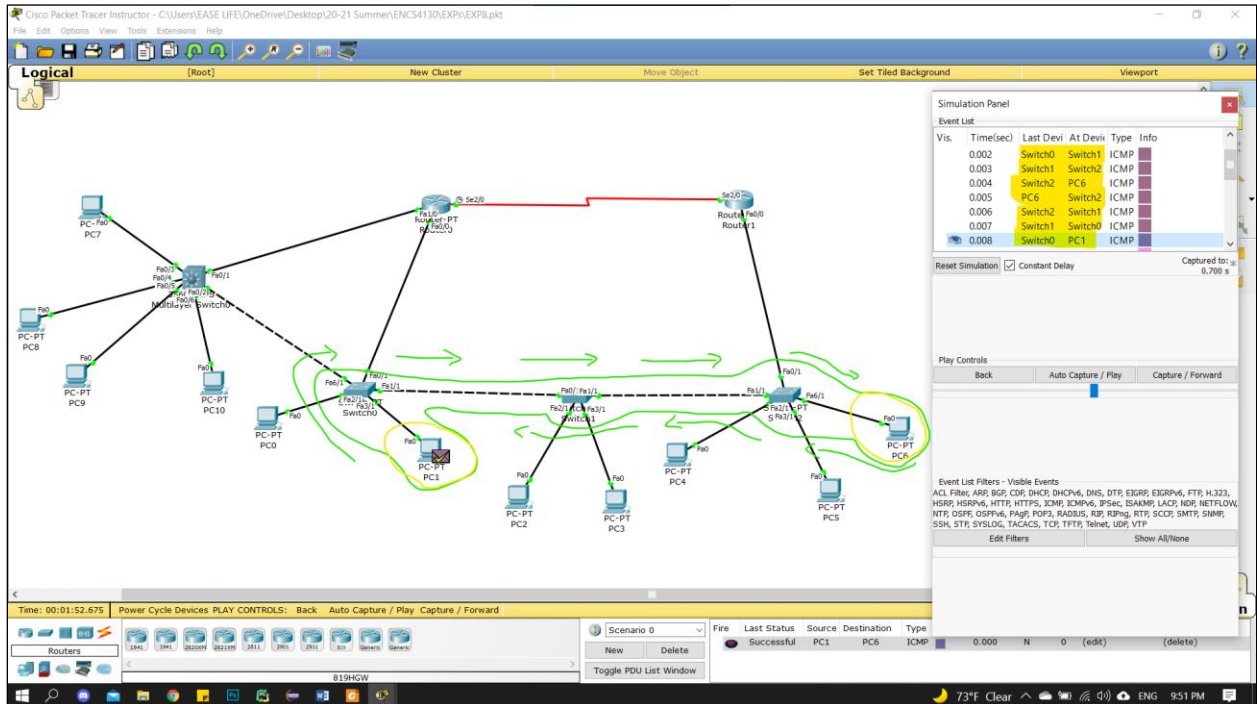


Figure 5 - Path of the message's packets from PC1 to PC6

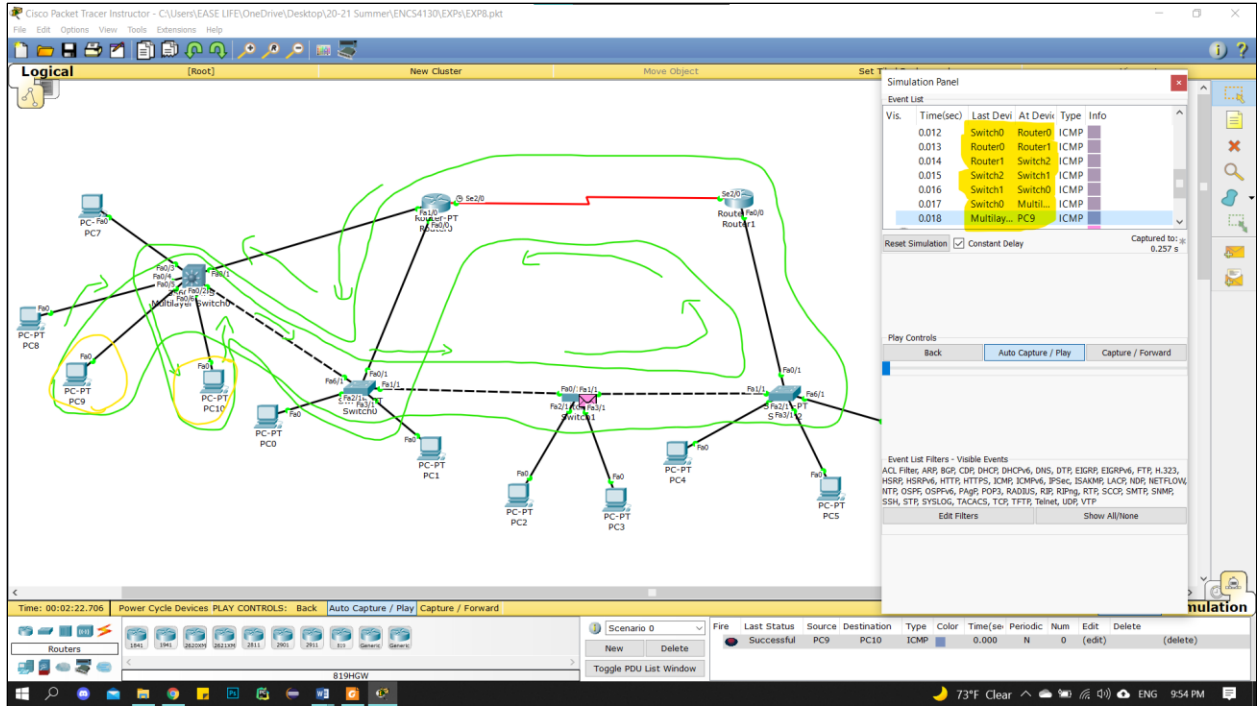


Figure 6 - Path of the message's packets from PC9 to PC10

4. Conclusion

The results that were obtained from the previous procedures are successful and agree with the theoretical results. Moreover, we conclude that we can use Cisco Packet Tracer to build our topologies and advertise them, so we became more familiar with this program. We learned what every number in the IP address means and does.

We learnt how to setup and configure a LAN, how to build and simulate network topologies, how to configure and simulate a dynamic routing protocol and how to configure and simulate VLANs.

We became more familiar with the multilayer switch which we benefited from it as a switch and as a router.

5. References

- [1] Jim Kurose and Keith Ross. *Computer Networking: A Top Down Approach*, 8th Edition, Addison-Wesley, 2021.
- [2] https://en.wikipedia.org/wiki/Virtual_LAN
Accessed on August 13, 2021 11:22pm.
- [3] <https://www.geeksforgeeks.org/configuration-of-router-on-a-stick/>
Accessed on August 14, 2021 2:06pm.
- [4] https://www.tutorialspoint.com/data_communication_computer_network/physical_layer_switching.htm
Accessed on August 14, 2021 5:17pm.
- [5] ENCS4130 Course Slides and Lab Manual.
- [6] ENCS3320 Course Slides.
- [7] Cisco Packet Tracer.