Faculty of Engineering &Technology
Electrical & Computer Engineering Department

ENCS4130

Report Exps 7 and 8

Switching and VLANs

Prepared by:

Abdallah Mohammad 1190515

Instructor: Ismail Khater

Assistant: Burhan Dar Assi

Section: 3

Date: 2022/8/21

Abstract

The aim of this experiment is to learn about VLANs (Virtual Local Area Network) and learn how to use to group devices that separated physically into one network or separate devices that connected physically into different networks then learn about multi-layer switch.

Table of Contents

Theory

How does a switch work?

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.

What is VLAN?

A VLAN (Virtual Local Area Network) is a type of local area network that does not have its own dedicated physical infrastructure, but instead uses another LAN to carry its traffic. The traffic is encapsulated so that a number of logically separate VLANs can be carried by the same physical LAN.

IEEE 802.1Q VLAN

IEEE 802.1Q is a protocol for carrying VLAN traffic on an Ethernet.

Tagging

802.1Q VLAN frames are distinguished from ordinary Ethernet frames by the insertion of a 4-byte VLAN tag into the Ethernet header. It is placed between the source MAC and the EtherType fields see Table below.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18…
Destination address						Source address						VLAN tag				EtherType		Payload
												0x8100		TCI				

Table 1

VLAN numbering

Each 802.1Q VLAN is identified by a 12-bit integer called a VID (VLAN Identifier) in the range 1 to 4094 inclusive. The values 0 and 4095 are reserved and should not be used.

The first VLAN is with a VID of 1.

The remaining values have no special status and can be used freely, but be aware that many network devices place a limit on the number of VLANs that can be configured so it will not necessarily be feasible to make use of all 4094 possible VIDs.

Trunk and access ports

There are two ways in which a machine can be connected to a switch carrying 802.1Q VLAN traffic: via an access port, where VLAN support is handled by the switch (so the machine sees• ordinary, untagged Ethernet frames); or via a trunk port, where VLAN support is handled by the attached machine (which sees• 802.1Q-tagged Ethernet frames).

The main purpose of trunk is to manage the VLAN traffic. It uses a concept called tagging to mark each packet so each switch knows where to forward the traffic. There are many cases that we can use a trunk. It can be used between two switches or between a router and switch. It can also be used between a layer-three switch and ordinary switch.

It is also possible to operate a switch port in a hybrid mode, where it acts as an access port for one VLAN and a trunk port for others (so the attached Ethernet segment carries a mixture of tagged and untagged frames). This is not recommended due to the potential for VLAN hopping.

VLAN hopping: VLAN Hopping is an attack where the attacker is able to send traffic from one VLAN into another. There are two different methods to one of them is:

Double tags: the idea behind the attack is that the attacker is connected to an interface in access mode with the same VLAN as the native untagged VLAN on the trunk. The attacker sends a frame with two 802.1Q tags, the “inner” VLAN tag is the VLAN that we want to reach and the “outer” VLAN tag is the native VLAN. When the switch receives the frame, it will remove the first (native VLAN) 802.1Q tag and forwards the frame with the second 802.1Q tag on its trunk interface(s). The attacker has now “jumped” from the native VLAN to the victim’s VLAN.It’s a one way trip but it could be used perhaps for a DOS attack.[1]

Sub interface on Routers

This is a part of a main interface on a router. It takes part of the bandwidth and passes special kind of traffic. It has also its own IP address and encapsulation number (which is used to tag traffic). Main interface does not have to get an IP address in case of sub interfaces.

Initializing IP address for a sub interface

```
Router(config-subif)#encapsulation dot1Q <VLAN-ID>
Router(config-subif)#ip address <IP-ADDRESS> <SUBNET-MASK>
```

These commands are used to add an IP address to a sub-interface, the encapsulation command is used to configure the sub-interface as part of IEEE 802.1Q standards and the IP address is to add IP for that sub-interface.

Third layer switch

A layer three switch, as the name indicates, has some capabilities that are not found in an ordinary one. It can perform routing in parallel with switching. It combines the functionality of a switch and a router. It acts as a switch to connect devices that are on the same subnet or virtual LAN at lightning speeds and has IP routing intelligence built into it to double up as a router. It can support routing protocols, inspect incoming packets, and can even make routing decisions based on the source and destination addresses.

Procedure & Discussion

Building first Topology (exp7)

First, build the topology, assign IPs to PCs, router interfaces and router sub-interface and configure OSPF routing. To configure routers sub-interfaces (repeat for all sub-interface):

```
Router(config)# interface Fa0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.115.10.1 255.255.255.0
```

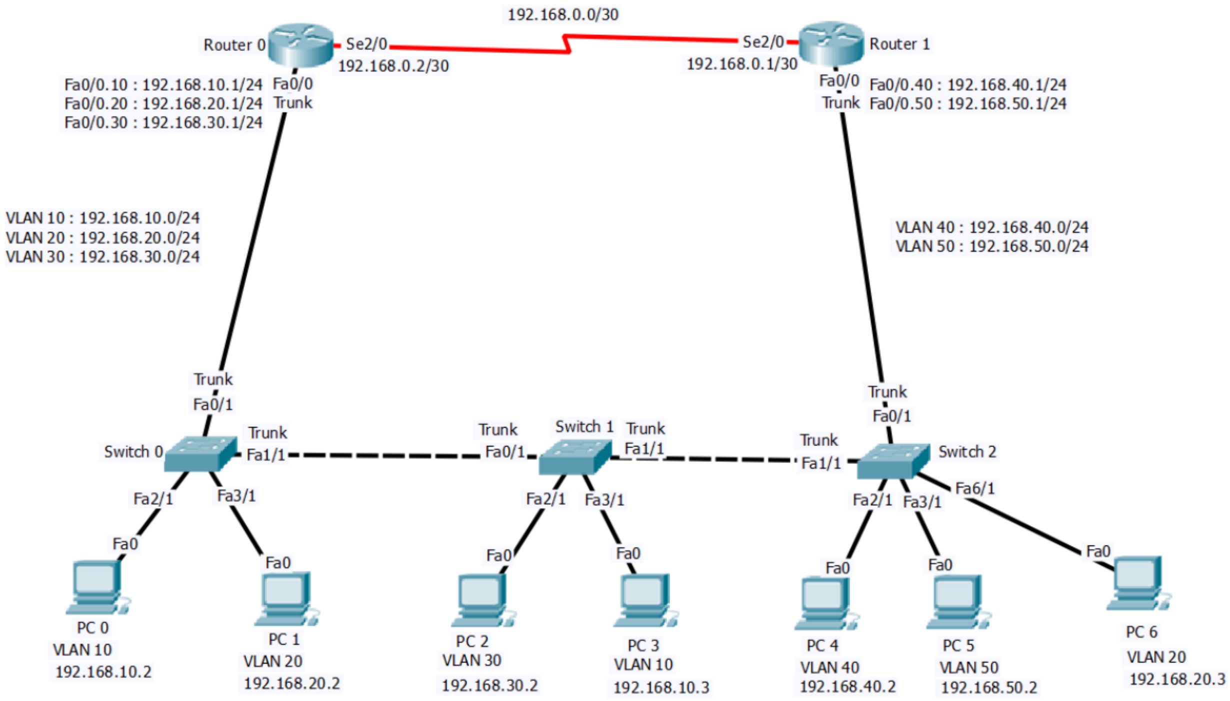

Figure 1

Configuring Switch Access and Creating a VLANs

Assigning an interface to an existing VLAN we must access the needed port and perform the access command:

```
Switch(config-if)# switchport access
```

We used the following commands and repeat for all access ports:

```
Switch(config)# interface Fa2/1
Switch(config-if)# switchport access VLAN 10
```

I use this command before creating the VLAN where it will be created automatically after write commands above. But in some cases there some VLANs have to be created on the switch but weren't created when assign access ports, for example: in **switch1** we have to create **VLAN 20** to pass packets from switch0 and switch2 when PC1 wants to communicate PC6.

Configuring Switch Trunk

We assigned the interfaces between switches and between switches and routers to be trunk by the following command:

```
Switch(config -if)# switchport mode trunk
```

Building second Topology (exp8)

In this experiment we add the multi-layer switch with VLAN 60 and VLAN 70.

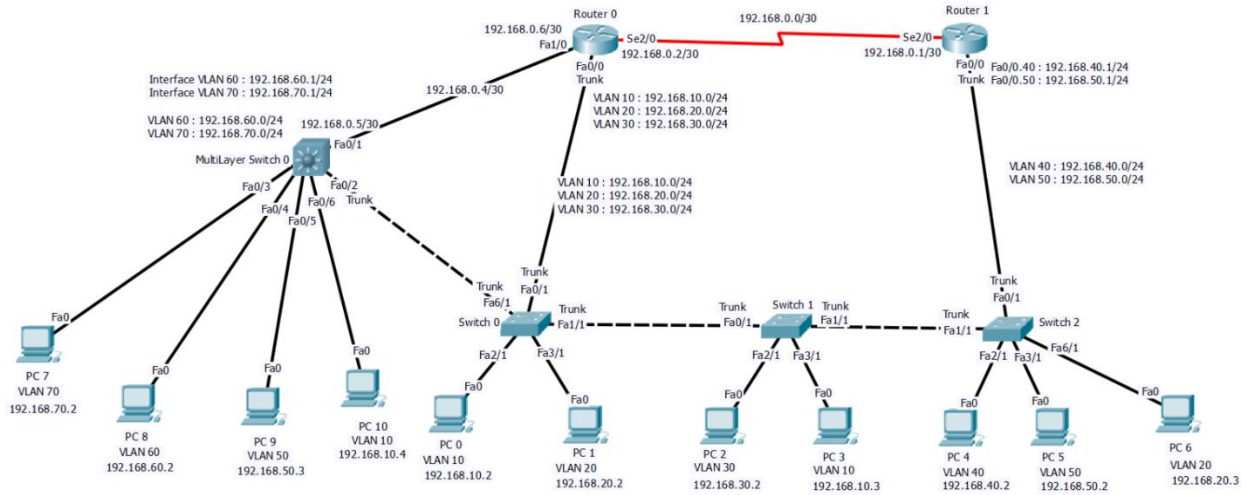

Figure 2

Configure Multi-Layer Switch to Router link

We need to change the switch port to a router port and then add the IP address, so we used the commands below:

```
Switch(config)#interface fa0/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.115.0.5 255.255.255.252
```

Multi-Layer Switch Configuring VLAN Interfaces IPs (Switch Virtual Interfaces)

We will use the following commands to configure switch virtual interfaces on the switch to act as default gateways for the new VLANs (VLAN 60 and VLAN 70):

```
Switch(config)#interface vlan 60
Switch(config-if)# ip address 192.115.60.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface vlan 70
Switch(config-if)# ip address 192.115.70.1 255.255.255.0
```

Enable routing on Multi-Layer Switch and configuring OSPF

We configured OSPF routing protocol for both routers 0 the Multi-layer switch. To configure, by default, the routing is disabled on the third layer switch, in order to enable it we use the following command:

```
Switch(config)# ip routing
```

Configuring Switch Access and Creating a VLANs on multi-layer switch

This part made as was been make in regular switches before.

Note: do not forget to create **VLAN 10** on the multi-layer switch.

Configuring Trunk on Multi-Layer Switch

To configure a trunk on a third layer switch, we need to encapsulate that switch, to do this we used the following commands:

```
Switch(config)#interface Fa0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
```

Note this made just between **multi-layer switch** and **switch 0** but **not router 0** where multi-layer switch works as router on the interface between it and the router.

Conclusion

In conclusion, we can use VLANs to group devices that do not have its own dedicated physical infrastructure or to separate devices that connected physically.

Multi-layer switch uses as switch and router at the same time.

References

[1] networklessons.com - cisco - ccnp-switch - vlan-hopping