Experiment No. - 5

Objective: Configuration of a VLAN using access mode.

VLAN stands for **Virtual Local Area Network**. It is a type of network created using one or more existing LANs. VLAN allows devices from different networks (wired or wireless) to work together as if they are on the same network. This virtual network can be managed just like a real physical network. To create a VLAN, the network devices such as **routers or switches** must support VLAN settings.

We need to divide a LAN into **two virtual LANs (VLANs)** so that:

- Devices in one VLAN cannot communicate with devices in the other VLAN.
- Devices within the same VLAN can communicate with each other.

Steps to Configure and Verify a VLAN using access mode:

Step 1: First, open the Cisco packet tracer desktop and select the devices given below:

(Draw the below tables at the left side of your copy)

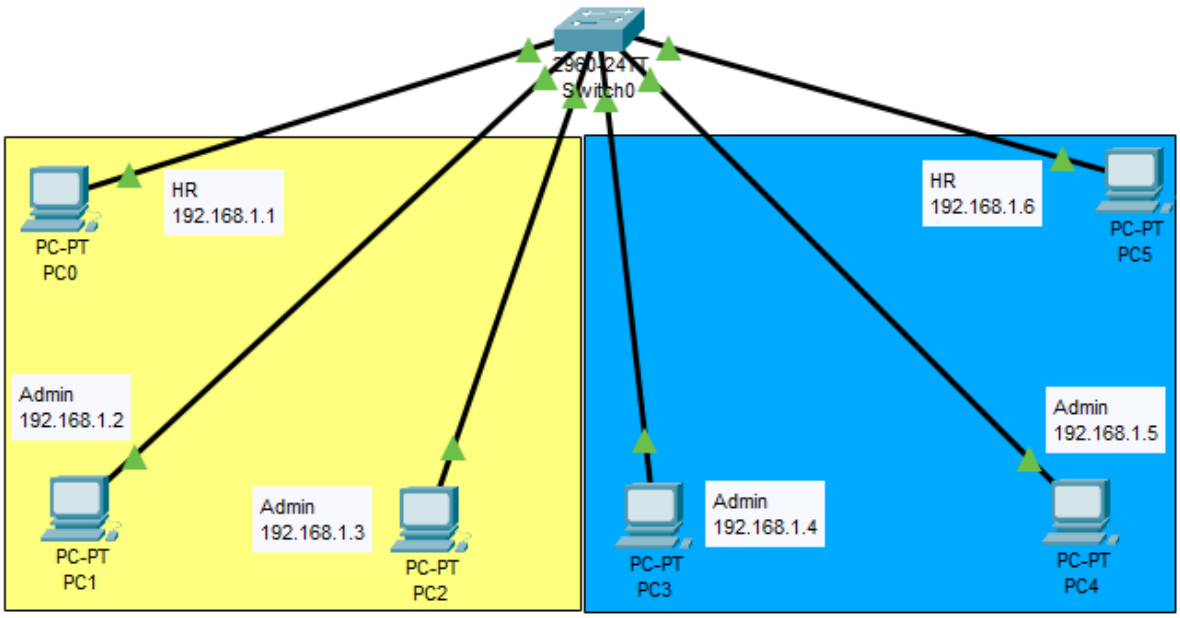
S.No.	Device	Model Name	Qty.
1.	PC	PC	6
2.	Switch	2960	1

IP Addressing Table:

S. No.	Device	IPv4 Address	Subnet mask
1.	PC0	192.168.1.1	255.255.255.0
2.	PC1	192.168.1.2	255.255.255.0
3.	PC2	192.168.1.3	255.255.255.0
4.	PC3	192.168.1.4	255.255.255.0
5.	PC3	192.168.1.5	255.255.255.0
6.	PC3	192.168.1.6	255.255.255.0

- Then, create a network topology as shown below the image.
- Use an Automatic connecting cable to connect the devices with others.

Network Diagram (Draw this to the left side of your copy.)



Step 2: Configure the PCs (hosts) with IPv4 address and Subnet Mask according to the IP addressing table given above.

- To assign an IP address in PC0, click on PC0.
- Then, go to desktop and then IP configuration and there you will IPv4 configuration.
- Fill IPv4 address and subnet mask.

(Write in left side of the copy)

- Assigning an IP address using the ipconfig command, or we can also assign an IP address

with the help of a command.

- Go to the command terminal of the PC.
- Then, type ipconfig <IPv4 address><subnet mask>(if needed)

Example: ipconfig 192.168.1.1 255.255.255.0

- Repeat the same procedure with other PCs to configure them thoroughly.

Step 3: To configure VLANs' on switch (click on switch>click on CLI>Press Enter)

Create two VLAN's on the switch as vlan10 and vlan20 named as HR and ADMIN respectively for this use the following commands.

(Write the below commands in the left side of page)

```
Switch>enable
Switch#config terminal

<Enter configuration commands, one per line. End with CTRL+Z>

Switch(config)#vlan 10
Switch(config-vlan)#name HR
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name ADMIN
Switch(config-vlan)#exit
```

To Exit use the command
Switch(config)# CTRL+Z

You can see the configuration by the command
Switch# show vlan brief

Step 4: An access mode is to be assigned in vlans. These ports are configured for the switch port that connect to the devices with NIC. In our case we will configure the switch interface by command given below:

(Write the below commands in the left side of page)

```
Switch#config terminal
Switch(config)#int fa0/1
Switch(config-if)#switchport access vlan 10
Switch(config)#exit

Switch(config)#int fa0/6
Switch(config-if)#switchport access vlan 10
Switch(config)#exit

Switch(config)#int range fa0/2-5
```

Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit

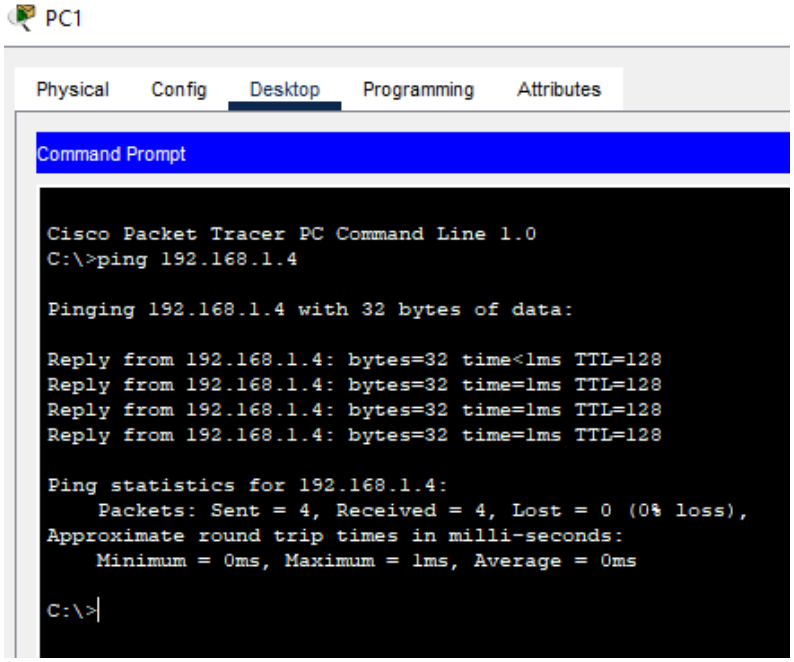
To Exit use the command
Switch(config)# CTRL+Z

You can see the configuration by the command
Switch# show vlan brief

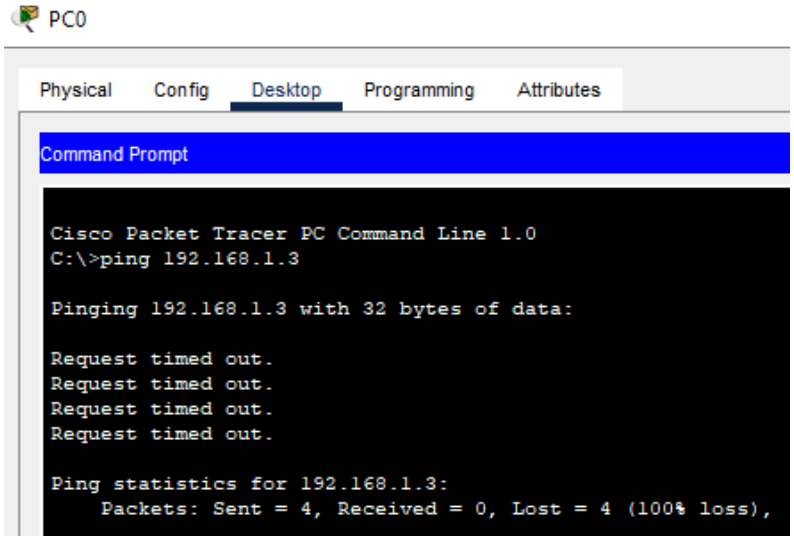
To Save the configuration use the command
Switch#wr

Step 5: Verifying the network by pinging the IP address of any PC.

- We will use the ping command to do so.
- First, click on PC0 then Go to the command prompt.
- Then type ping <IP address of targeted node>.
- As we can see in the below image we are getting replies between PCs on the same VLAN.



- The PCs on different VLAN do not communicate with each other.
- Which means the VLANs configuration is working properly.



Conclusion:

In this VLAN lab using Cisco Packet Tracer, we successfully divided a single LAN into two separate Virtual LANs. Devices within the same VLAN were able to communicate with each other, while communication between different VLANs was restricted. This demonstrates how VLANs improve network security, efficiency, and traffic management by logically segmenting a network without needing additional physical hardware. The results were verified using the ping command to test connectivity between devices.

After creating the network, we were able to:

1. Create multiple VLANs using CLI commands.
2. Assign switch ports to specific VLANs using the `switchport access vlan` command.
3. Verify VLAN configuration using the `show vlan brief` command.
4. Ensure that devices within the same VLAN could communicate with each other.
5. Confirm that devices from different VLANs could not communicate directly without routing.

*****