LAB NO: 5

Experiment: Introduction to VLAN (Access and Trunk)

Assume that you are assigned the role of Network Administrator in Thames College. You are provided two IP address pools:

i) 192.168.X.0/27

ii) 192.168.X.32/27

You are assigned to create two different networks from the given IP pools one for Account Section and the other for Computer LAB. Now make use of VLAN technology to separate these two networks. Assume that you are given 2 Cisco 2960 switches one for each block. Refer to the network diagram given below to realize the necessary architecture. Test network reachability.

**Apparatus Required (in Cisco Packet Tracer)**

* **2 × Cisco 2960 Switches** (Switch0 and Switch1)
* **8 × PCs** (PC0 – PC7)
* **Copper Straight-Through Cables** (to connect PCs to switches)
* **1 × Copper Straight-Through Cable** (to connect Switch0 ↔ Switch1 uplink ports, e.g., Gi0/1 ↔ Gi0/1)

**Tools Used**

* **Cisco Packet Tracer Software** (simulation environment)
* **CLI (Command Line Interface)** of Cisco 2960 switch inside Packet Tracer
* **PC → Desktop → IP Configuration Tool** (to assign static IP addresses to PCs)
* **PC → Desktop → Command Prompt (ping)** (to test connectivity between PCs)
* **Verification Commands on Switches:**
  + show vlan brief → to check VLAN membership of ports

**Theory**

**1. VLAN (Virtual Local Area Network)**

A **VLAN** is a logical segmentation of a switch into multiple broadcast domains. By default, all ports in a switch belong to VLAN 1. When multiple VLANs are created:

* Devices in the **same VLAN** can communicate directly as if they are in the same LAN, even if they are connected to different physical switches (provided trunking is configured).
* Devices in **different VLANs** cannot communicate directly without a router or a Layer-3 device (this provides isolation and security).

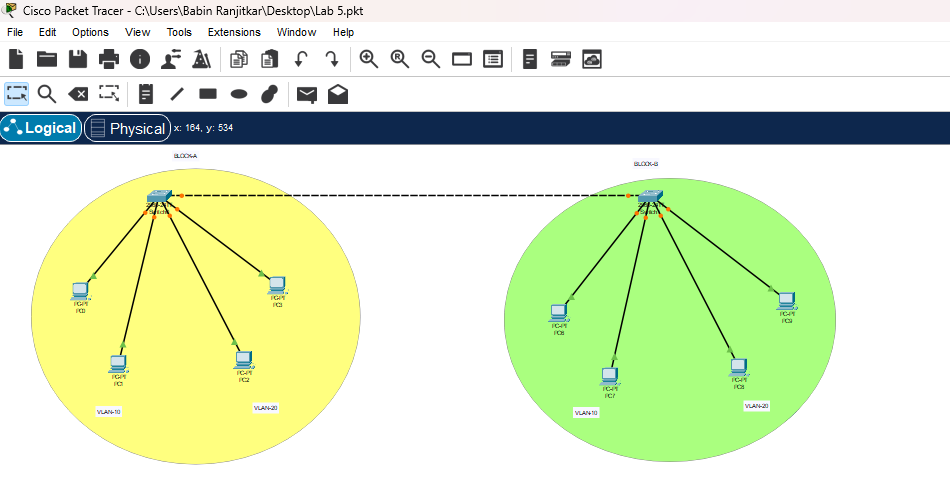
**2. Access Ports**

* An **access port** carries traffic for **only one VLAN**.
* When a PC is connected to a switch via an access port, all frames sent/received on that port are associated with that VLAN.
* Example: Fa0/1 configured as **access VLAN 10** means the PC connected there becomes part of VLAN 10.

**4. Benefits of VLANs**

* **Segmentation:** Each VLAN is its own broadcast domain, reducing unnecessary traffic.
* **Security:** Sensitive departments (e.g., Accounts) can be isolated from others.
* **Flexibility:** Hosts in the same VLAN can be spread across multiple switches using trunks.
* **Scalability:** VLANs make large networks easier to manage.

**Lab Diagram:**

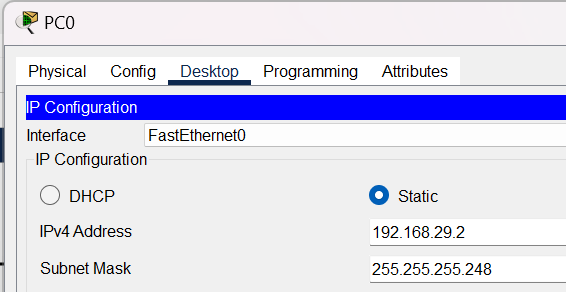


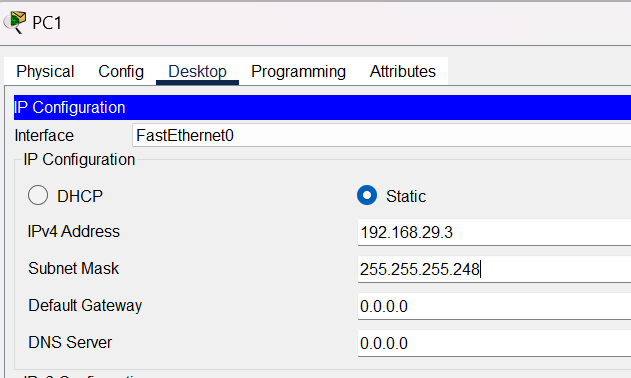
**1. Network Topology Setup**

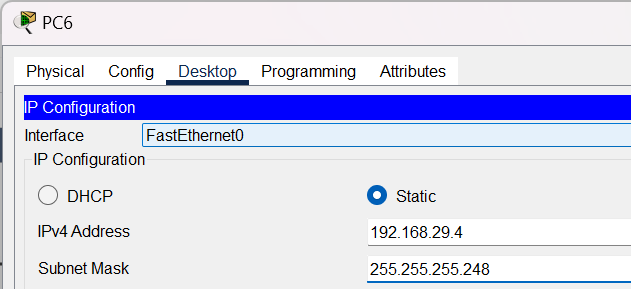
1. Open **Cisco Packet Tracer**.
2. From the device list, drag and drop:
   * **2 × Switches (Cisco 2960)**
   * **8 × PCs (PC0 – PC7)**
3. Arrange them into **two blocks**:
   * **Block-A:** PC0, PC1, PC2, PC3 → connect to **Switch0**
   * **Block-B:** PC6, PC7, PC8, PC9 → connect to **Switch1**
4. Use **Copper Straight-Through cables** to connect each PC’s **FastEthernet0** interface to one FastEthernet port on the
5. Also ,connect the two switches.

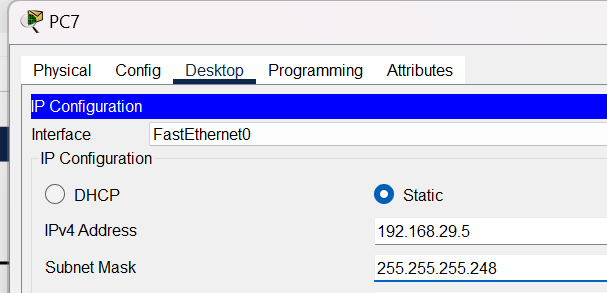
2.IP configuration in each pc:

For pcs in vlan-10:

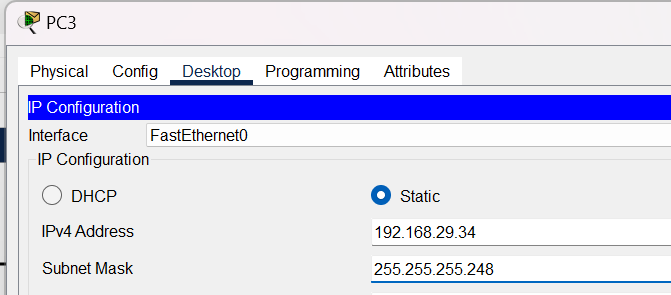


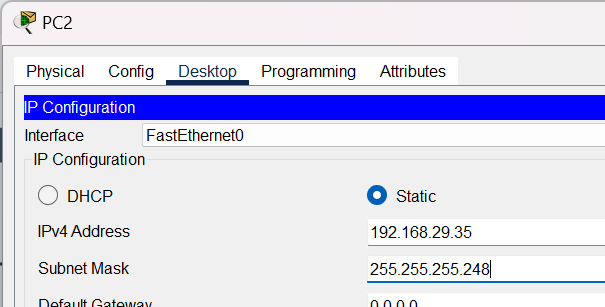


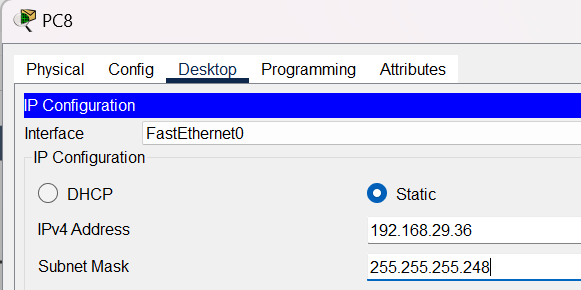


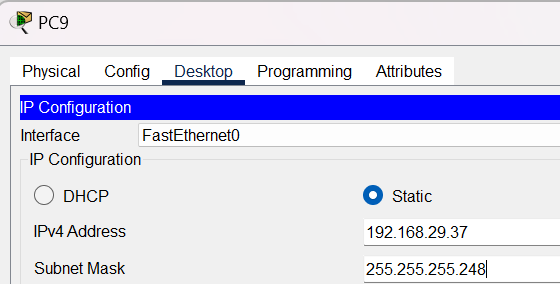


For pcs in vlan 20:



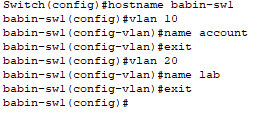






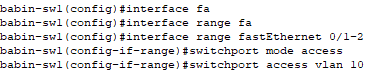
**3. Configure VLANs on Switches**

On **both Switch0 and Switch1**:



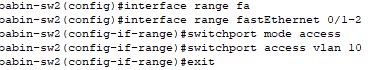
**4. Assign Access Ports to VLANs**

**Switch0 (Block-A):**





Switch1(block-B):





5.Configuring Trunk Port and Allowing VLANs

In switch 1:

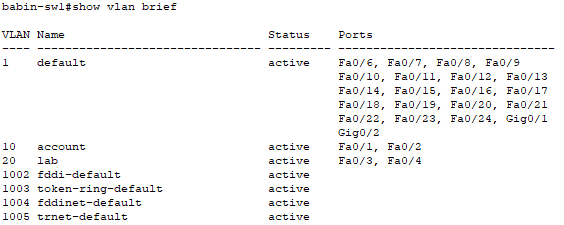


In switch 2:

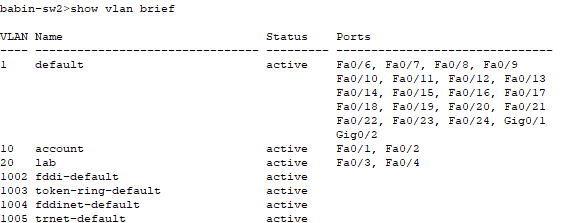


Testing :

1. Checking VLAN configuration in switch 1(suv-sw1):

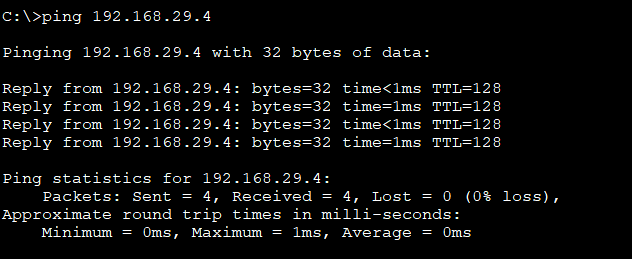


1. Checking VLAN configuration in switch 2(suv-sw2):



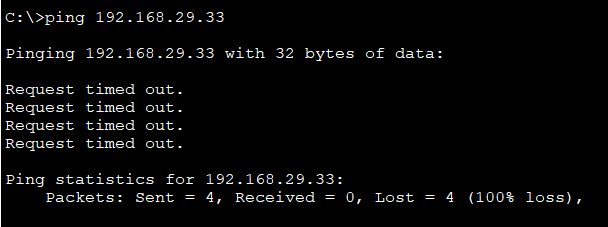
3.ping in pcs of same VLAN:

i.e 192.168.29.3 (Block-A) to 192.168.29.4(Block-B)



4.ping in between pcs of different vlan:

i.e from 192.168.29.3(Block-A,VLAN-10) to 192.168.29.33(Block-B,VLAN-20)



**Conclusion**

In this experiment, we successfully implemented VLAN technology to logically separate the Account Section and Computer Lab networks using VLAN 10 and VLAN 20. Devices placed in the same VLAN were able to communicate with each other, while communication between different VLANs was restricted, ensuring proper network segmentation. Trunk ports were configured between the switches to allow VLAN 10 and VLAN 20 traffic to pass, which enabled connectivity for hosts belonging to the same VLAN but connected through different switches.

This demonstrates that VLANs provide improved security, better management of broadcast domains, and efficient utilization of network resources. The lab verified that VLANs isolate traffic as expected, and inter-VLAN communication requires a Layer 3 device such as a router or multilayer switch.