LAB NO: 4

Experiment: Introduction to Cisco Packet Tracer

Complete the following task in Cisco Packet Tracer Switch. Use 6 Computers in your lab scenario[3 each in a network]. Assign IP addresses from the following pool.

i. 192.168.0.0/24

ii. 192.168.1.0/24

Show the switch device to facilitate internetworking communication i.e., make a pc from network (i) to be reachable from network (ii). Also change system name for switch. Iii)check if pc within a network pings or not.

Apparatus Required:

* Personal Computer/Laptop (to run simulation)
* Cisco Packet Tracer software
* Switch (1 unit – e.g., 2960)
* 6 PCs (3 in each network)
* Ethernet cables (straight-through)

Tools Used Here: Cisco Packet Tracer (for network simulation and configuration)

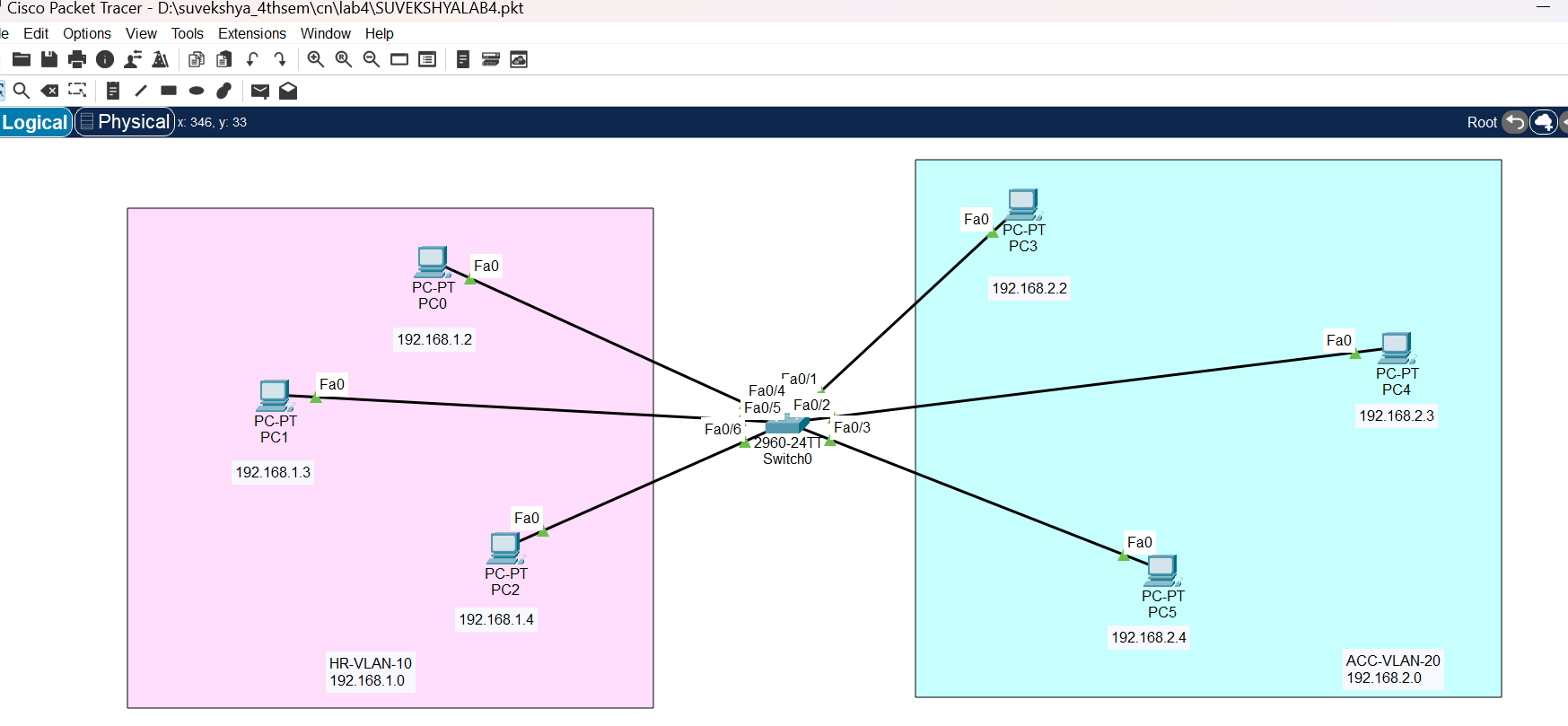
Theory:

**Introduction to Cisco Packet Tracer:** Cisco Packet Tracer is a powerful network simulation tool developed by Cisco that allows users to design, configure, and test networks virtually without requiring physical hardware. It provides a graphical workspace where devices such as routers, switches, and PCs can be placed and interconnected. Users can configure these devices using either the Command Line Interface (CLI) or graphical IP settings. Packet Tracer also enables testing of network connectivity and troubleshooting through tools like ping, which helps students and professionals understand network behavior and device interactions in a controlled, risk-free environment.

**Switch:**

A switch is a networking device that operates at Layer 2 of the OSI model, also known as the Data Link Layer. Its primary function is to connect multiple devices within the same local area network (LAN) and forward data frames based on the devices’ MAC addresses. Unlike a hub, which broadcasts data to all connected devices, a switch intelligently learns the MAC addresses of devices connected to its ports and forwards data only to the intended recipient. This makes network communication faster and more efficient by reducing unnecessary traffic. However, a switch is limited to a single subnet and cannot provide communication between different IP networks. For this reason, while switches are essential for building local connectivity within a network, a router is required when communication between separate networks or subnets is needed.  
**IP Addressing:** IP addressing is a fundamental aspect of networking, as each device in a network must have a unique IP address to ensure accurate delivery of data. Routers use their interface IP addresses as default gateways for devices in their respective networks, enabling communication outside the local subnet. Proper IP addressing allows routers to determine the correct path for data packets and ensures that information is sent to the intended destination network without conflicts or misrouting.

**Lab diagram:**



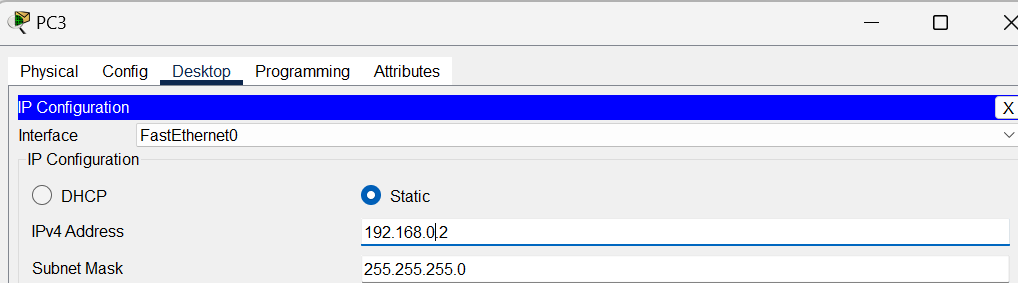
Procedure:

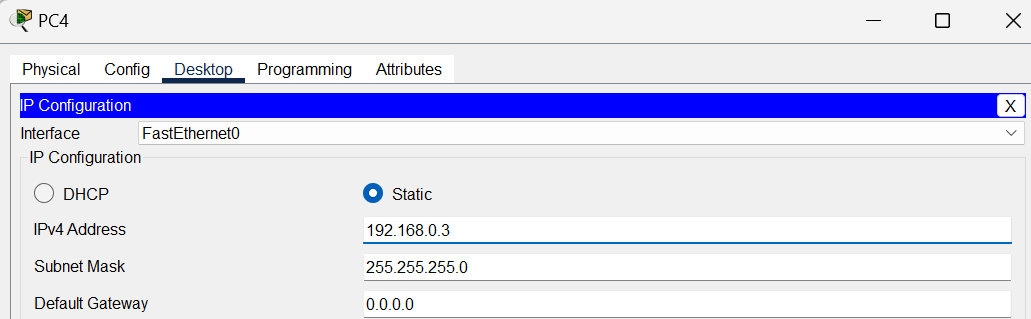
1.**Network Setup:**

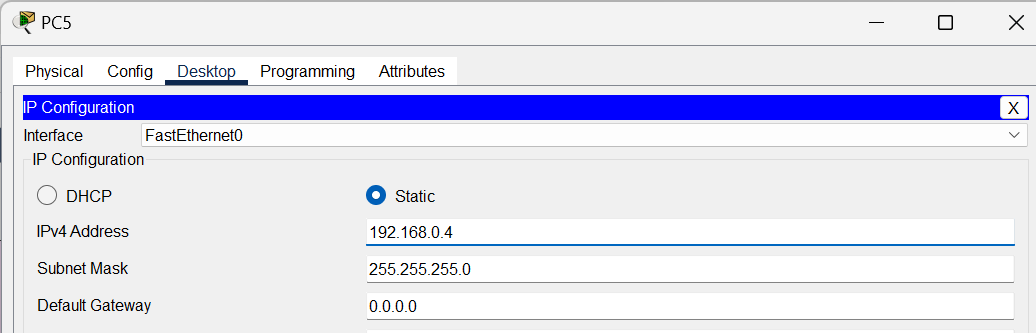
* Open Cisco Packet Tracer and create a simple topology consisting of one switch and six PCs.
* Divide the PCs into two groups, representing two departments, with three PCs in each department.
* Connect all PCs to the single switch using straight-through Ethernet cables.

2.**IP Address Assignment:**

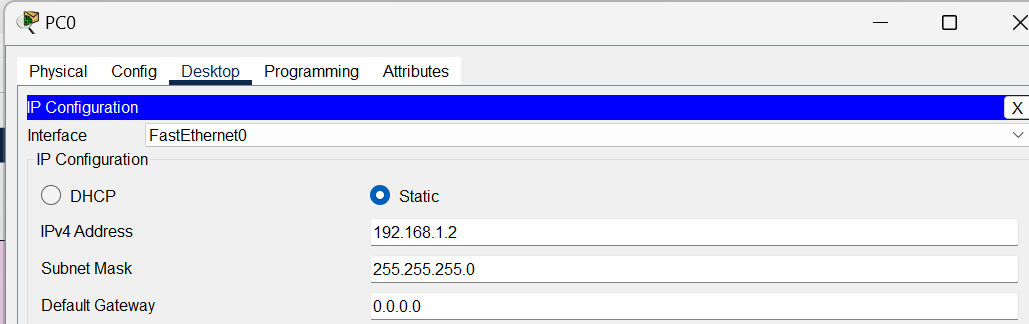
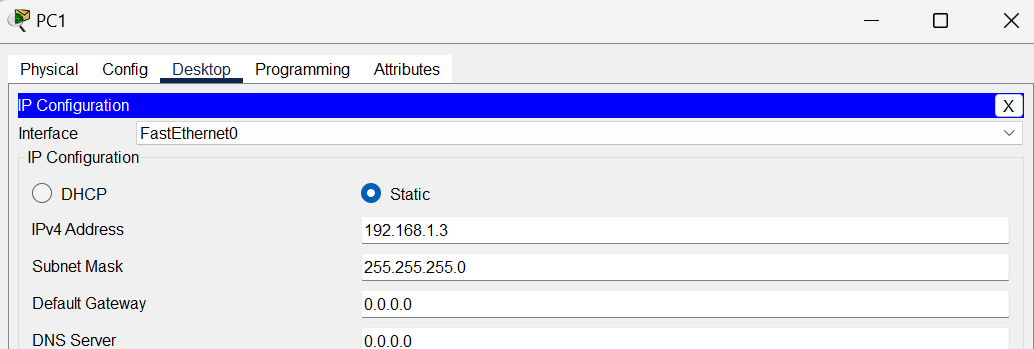
* Assign IP addresses from the **192.168.0.0/24** network to the PCs of Department 1.

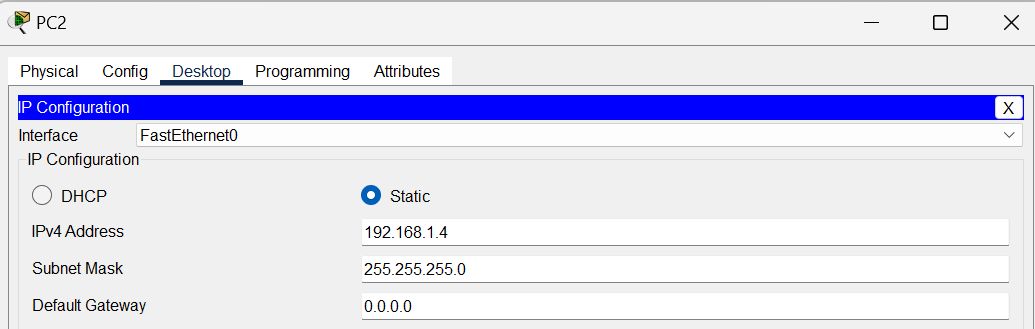






* Assign IP addresses from the **192.168.1.0/24** network to the PCs of Department 2.

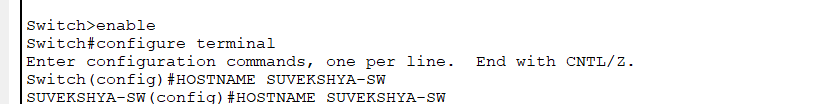
  




* Ensure that each PC has a unique IP address within its respective department network.

**3.Switch Configuration:**

* Open the switch CLI ,enable witch,configure terminal and change the hostname for identification ie.suvekshya-SW1.



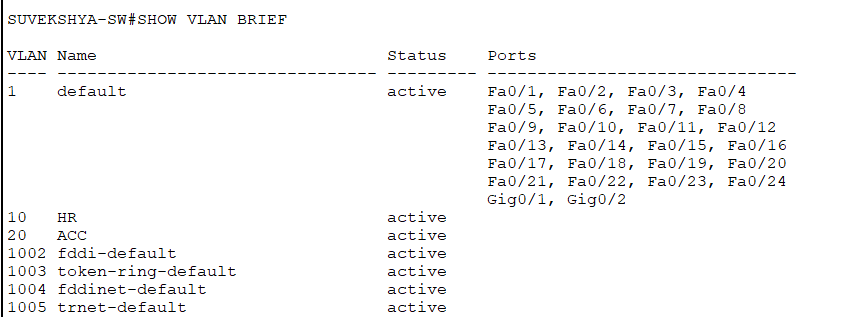
* Enter VLAN configuration mode and assign an IP address to **VLAN 10** (HR department) so that the switch can be managed remotely.



* Enter VLAN configuration mode and assign an IP address to **VLAN 20** (Account department) so that the switch can be managed remotely.

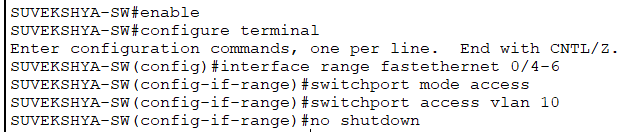


* Show vlan brief

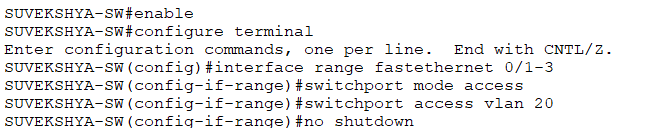


* Enable all switch ports so they can forward traffic to the PCs:

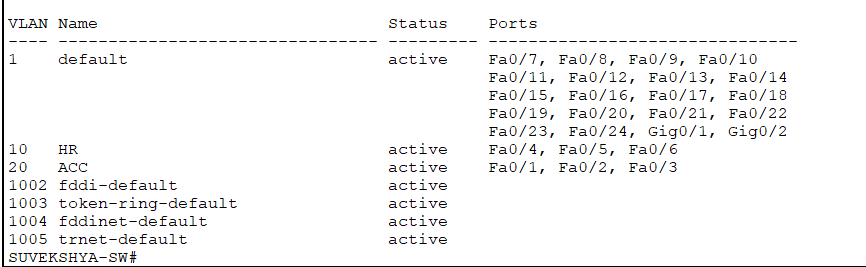
1. Configure for VLAN 10:



1. Configure for VLAN 20:



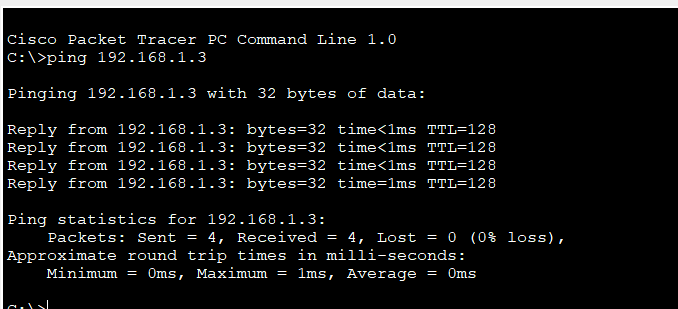
Now check if they are assigned correctly:



Testing:

**1.Ping within same VLAN (intra-VLAN communication)**

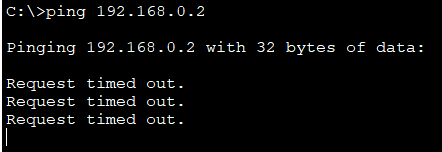
* PCs in the same VLAN should be able to communicate with each other.
* Example:  
  + From **PC0 (192.168.1.2)** → ping **PC1 (192.168.1.3)**

****

It succeeds

**2.Ping across different VLANs (inter-VLAN communication)**

* **Since no router or Layer 3 device is configured, PCs in different VLANs cannot communicate.**
* **Example:**
  + **From PC0 (192.168.1.2) → ping PC3 (192.168.0.2)**

****

It fails.

## 

## Conclusion

In this lab, VLANs were successfully created and configured on a switch to divide the network into two logical segments: HR (VLAN 10) and ACC (VLAN 20). The experiment verified that PCs within the same VLAN were able to communicate with each other, while devices in different VLANs could not communicate directly. This demonstrated the role of VLANs in improving security and managing broadcast domains by logically separating departments within the same physical switch. Furthermore, it highlighted the need for a Layer 3 device such as a router or a Layer 3 switch to enable inter-VLAN communication when required.