Lab Number 9

VLAN setup and Inter-VLAN Routing

Aim: To Configure VLAN setup and Inter-VLAN Routing

Theory:

VLAN Setup: A Virtual Local Area Network (VLAN) is a network configuration that allows multiple logically segmented networks to exist within a single physical network. VLANs can be used to group devices based on function, department, or application rather than physical location. Each VLAN is treated as a separate broadcast domain, which reduces broadcast traffic and improves network performance.

Inter-VLAN Routing (IVR): IVR is the process that enables communication between devices on different VLANs. Since VLANs are separate broadcast domains, they cannot communicate with each other directly. IVR is achieved by routing traffic between VLANs using a router or a Layer 3 switch. Typically, a router or Layer 3 switch is configured with sub-interfaces, each associated with a different VLAN, and routing protocols or static routes are used to manage traffic between these VLANs.

Advantages

VLAN Setup:

1. **Improved Security:** By segregating networks, VLANs can help limit broadcast traffic and isolate sensitive data.
2. **Reduced Broadcast Traffic:** VLANs reduce the scope of broadcast traffic to only those devices within the same VLAN.

Inter-VLAN Routing:

1. **Centralized Routing:** Provides a centralized point for routing between VLANs, making management easier.
2. **Scalability:** Supports complex network architectures and inter-VLAN communication.

Limitations

VLAN Setup:

1. **Complexity:** VLAN configurations can be complex and require careful planning and management.
2. **Increased Overhead:** Improperly configured VLANs can lead to increased network overhead and inefficient routing.

Inter-VLAN Routing:

1. **Performance Bottleneck:** A single router or Layer 3 switch handling all inter-VLAN traffic can become a performance bottleneck if not properly scaled.
2. **Configuration Complexity:** Configuring and maintaining inter-VLAN routing can be complex, especially in large networks.

CODE:

1. VLAN Setup on Layer 2 Switch (Switch1)

1. Create VLANs:

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 200
Switch1(config-vlan)# name student
Switch1(config-vlan)# exit
Switch1(config)# vlan 300
Switch1(config-vlan)# name company
Switch1(config-vlan)# exit
```

2. Assign VLANs to Switch Ports:

```
Switch1(config)# interface range gigabitEthernet 0/1 - 2
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 200
Switch1(config-if-range)# exit

Switch1(config)# interface range gigabitEthernet 0/3 - 4
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 300
Switch1(config-if-range)# exit
```

```
Switch#show vlan br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
200  student                           active    Fa0/2, Fa0/3, Fa0/4
300  company                           active    Fa0/5, Fa0/6, Fa0/7
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

3. **Configure Trunk Port to Router or Layer 3 Switch:**

Switch1(config)# interface gigabitEthernet 0/24

Switch1(config-if)# switchport mode trunk

Switch1(config-if)# switchport trunk allowed vlan 10,20

Switch1(config-if)# exit

4. **Inter-VLAN Routing on Router (Router1)**

1. **Configure Sub-Interfaces for Each VLAN:**

Router1> enable

Router1# configure terminal

Router1(config)# interface gigabitEthernet 0/0.10

Router1(config-if)# encapsulation dot1Q 10

Router1(config-if)# ip address 192.168.10.1 255.255.255.0

Router1(config-if)# exit

Router1(config)# interface gigabitEthernet 0/0.20

Router1(config-if)# encapsulation dot1Q 20

Router1(config-if)# ip address 192.168.20.1 255.255.255.0

Router1(config-if)# exit

Enable IP routing (if it's a router or Layer 3 switch that requires it)

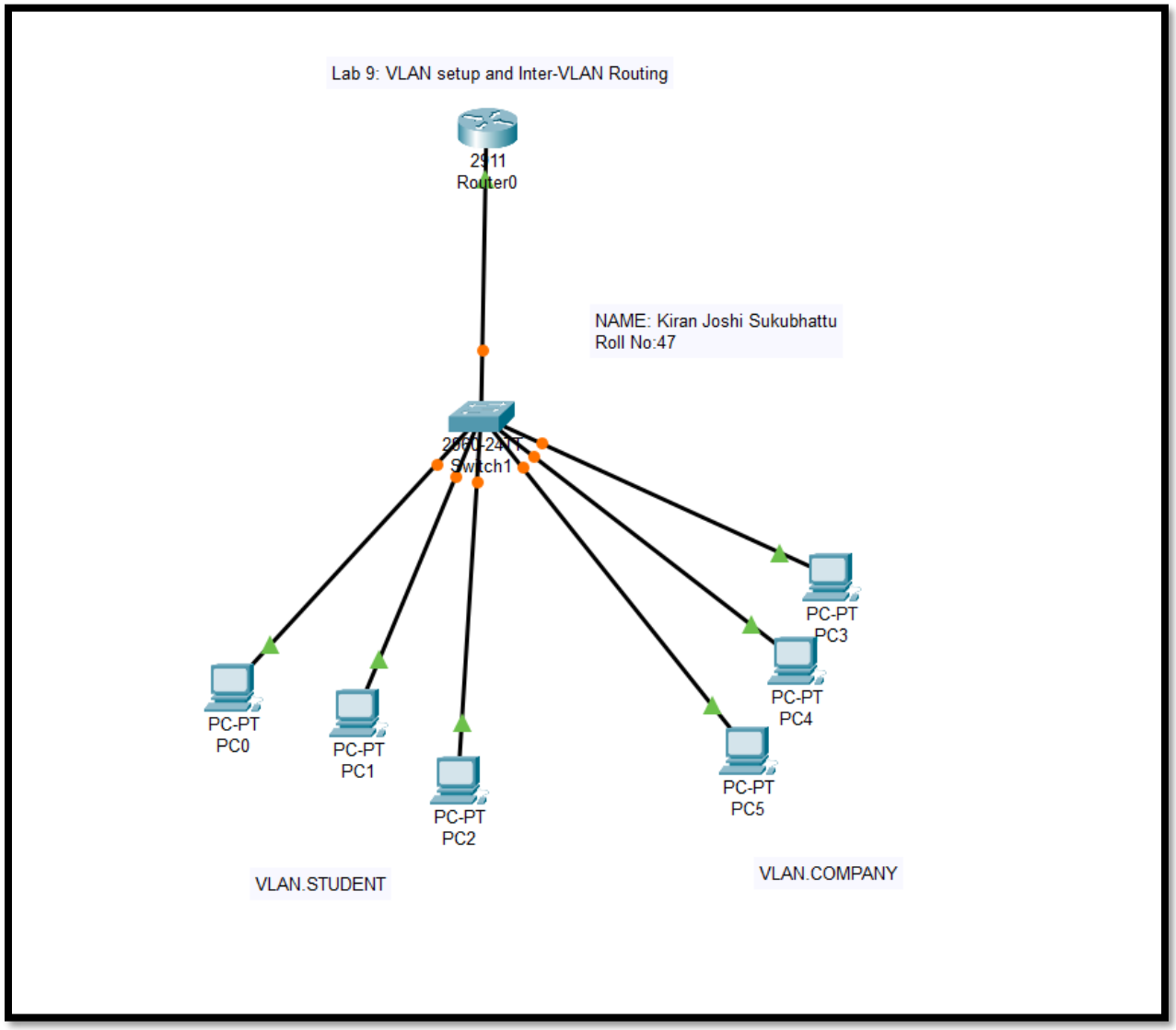
Router1(config)# ip routing

2. **Verify Configuration:**

- On **Switch1**, you can use commands like show vlan brief and show interfaces trunk to verify VLAN and trunk configurations.
- On **Router1**, use commands like show ip interface brief to check the status of the sub-interfaces and show ip route to verify routing information.

5. Testing Connectivity

1. **Connect Devices:**
    - Connect a device to a port in VLAN 200 (e.g., PC1) and assign it an IP address in the 192.168.10.3/24 network .
    - Connect a device to a port in VLAN 300 (e.g., PC2) and assign it an IP address in the 192.168.10.3/24 network.
2. **Test Inter-VLAN Communication:**
    - From PC1, try to ping PC2 to test connectivity across VLANs.
    - Check routing and ARP tables to troubleshoot if necessary.



Before Deny:

```
C:\> ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

After Deny:

```
C:\> ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Conclusion:

In this example, VLANs were configured on a Layer 2 switch to segment network traffic, and Inter-VLAN Routing was set up on a router to allow communication between the VLANs. This setup ensures that devices in different VLANs can communicate with each other while maintaining logical separation and reducing broadcast traffic.

Discussion:

Implementing VLANs and Inter-VLAN Routing requires careful planning and consideration of network design. Network administrators must balance the benefits of improved security and network management against the complexity and potential performance issues. Additionally, the choice of hardware and configuration strategies can significantly impact network performance and reliability.For optimal performance, it's essential to ensure that the routing device handling inter-VLAN traffic is adequately scaled to handle the expected load and to regularly review and update VLAN and routing configurations as the network evolves. Proper monitoring and maintenance practices will help in managing network complexity and ensuring that the network meets organizational needs efficiently.