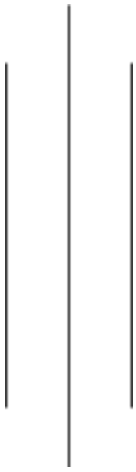
TRIBHUVAN UNIVERSITY
INSTITUTE OF ENGINEERING
PULCHOWK CAMPUS

Lab - 8: VLAN Configuration and InterVLAN Routing

Computer Networks



Submitted By:
Name: Roshani Poudel
Roll No: 077BCT071
Group: C

Submitted To:
Department of Electronics
and Computer Engineering

Lab 8: VLAN Configuration and InterVLAN Routing

Objectives:

- To be familiar with VLAN and its uses

- To create VLANs and extend it using multiple switches

- To route packets between computers at different VLANs (InterVLAN Routing)

Requirements:

- Laptop with Cisco Packet Tracer installed.

Exercises:

1. What is VLAN? Explain its importance with basic configuration steps.
=> A VLAN (virtual LAN) is a logical subdivision of a network, used to create separate virtual (i.e. logical) networks within a single physical network infrastructure. And upon division, each virtual network acts as though its a part of a different physical network, even if the connections occur within a single physical device i.e. a switch. It operates at Layer 2 (Data Link Layer) of the OSI model.

Steps of configuring a VLAN:
1. Creating a VLAN:

```
switch# configure terminal
switch(config)# vlan [Vlan_ID]
switch(config-vlan)# name [Vlan_name]
```

2. Assigning a switch interface to a VLAN:

```
switch(config)#interface [interface name]
switch(config-if)#switchport access vlan [Vlan_ID]
```

Vlan_ID = an integer between 0 and 4095.
Vlan_name = any valid string.

VLANs enable network segmentation, improving security and reducing broadcast traffic. By segmenting traffic, VLANs can reduce congestion and improve overall network performance. They provide flexibility by allowing logical grouping of devices based on function, department, or application rather than physical location. VLANs can isolate sensitive data and reduce the risk of unauthorized access.

2. How can packets be forwarded between computers within the same VLAN but connected at different switches? Explain.

=> In order for packets to be forwarded between computers in same VLAN but connected to different switches, we need to either make sure that the connection between the switch interfaces are in the same VLAN i.e. the interface that is in VLAN 1 of switch 1 needs to be connected to an interface that is in VLAN 1 of switch 2 and so on, or both connected interfaces need to be in trunk mode.
Configure trunk ports on both switches:

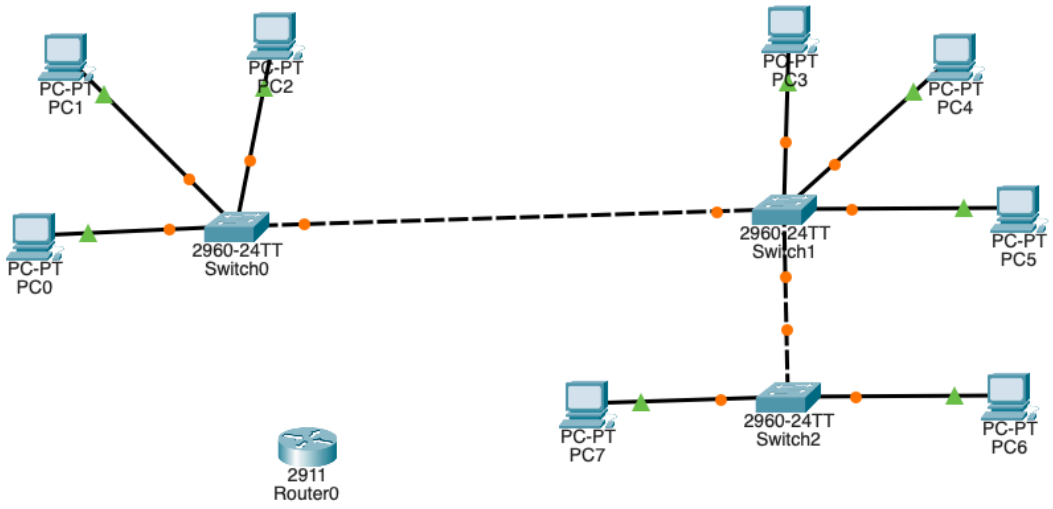
```
Switch(config)# interface <interface_ID>
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan <vlan_IDs>
```

3. How can packets be routed between computers at different VLANs? Explain.
=> Packets are routed between computers in different VLANs the same way they are routed between computers in different networks. A sub-interface of a router is connected physically to an interface of a switch in the corresponding VLAN and after configuring the corresponding ip and subnet masks, packet routing occurs. Router interfaces can be subdivided in order to lessen the requirement of a higher number of physical ports using encapsulation. This setup is also known as a router on a stick.
Configuration:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0.<subif_number>
Router(config-subif)# encapsulation dot1Q <VLAN_ID>
Router(config-subif)# ip address <IP_address> <subnet_mask>
Router(config-subif)# no shutdown
```

Activity A:

A network topology as given, with proper routers and switches was created.
1. The PCs were connected to given interfaces of corresponding switches, each of the switches was connected with another switch with interfaces as specified in the given figure. Subnet masks of 255.255.255.0 were given for each of the PCs.



2. All PCs could ping each other.

3. We created VLAN 2 and VLAN 10 in all switches i.e. Switch0, Switch1 and Switch2. It was done using: vlan <vlan_id>.

4. The interfaces FastEthernet 0/8, 0/9, 0/10, 0/11, 0/12 of all 3 switches were assigned to VLAN 2. Interfaces FastEthernet 0/16, 0/17, 0/18, 0/19, 0/20, 0/21, 0/22 of 3 switches were assigned to VLAN10.

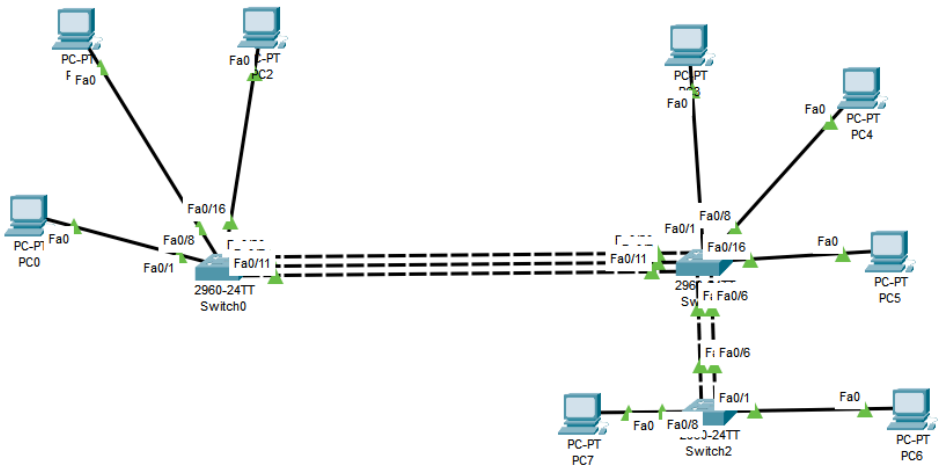
```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#in
Switch(config)#interface f
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport access vlan 10
Switch(config-if)#end
```

5. Only the pings between PC0, PC3 and PC6 were successful, this is because the connected switch interfaces are implicitly in VLAN 1 (having the same broadcast domain) that is the default VLAN.

However, PC0 is not able to reach PC1 and PC4 as they belong to a different VLAN (VLAN 2) after configuration in exercise 4. When interfaces are in different VLANs, the switch forwards the incoming packets to only the interfaces which are in the same VLAN as the incoming interface.

6. Interface FastEthernet 0/12 of Switch0 was connected with FastEthernet 0/12 of Switch1 and interface FastEthernet 0/11 of Switch1 with FastEthernet 0/11 of Switch2. PC0 could ping PC3 and PC6 only, PC1 could only ping PC4 and PC7 while PC2 could not ping any of the other PCs. This is because we have connected the 2 switches through VLAN 2 here, and VLAN 1 earlier but not through VLAN 10.

7. The interface FastEthernet 0/20 of Switch0 was connected with FastEthernet 0/20 of Switch1. Now, all the PCs within the same VLAN can ping each other, as we have connected wires across all VLANs. PC0, PC3 and PC6 in VLAN1. PC1, PC4 and PC7 in VLAN2. PC2 and PC5 in VLAN 10.



8. The additional links between switches added in step 6 & step 7 were removed. Interfaces GigabitEthernet0/1 and GigabitEthernet0/2 of all three switches were configured as a Trunk port.

The ping from PC0 to PC3 & PC6 succeeds because they are in the same VLAN and since the port through which the switch is connected to another is in trunk mode, packets sent from VLAN1 are sent to the second switch. Similarly, the ping from PC1 to PC4 & PC7 and the ping from PC2 to PC5 succeeds.

Previously the connections between different switch VLANs were physical and due to that the packets were forwarded via those ports, now after using the switch in trunk modes, the packet frames are encapsulated and then forwarded such that a packet sent from one VLAN is received only in its corresponding VLAN in the next switch.

Activity B: The subnet mask for all PCs was changed to 255.255.255.192, forming multiple networks.

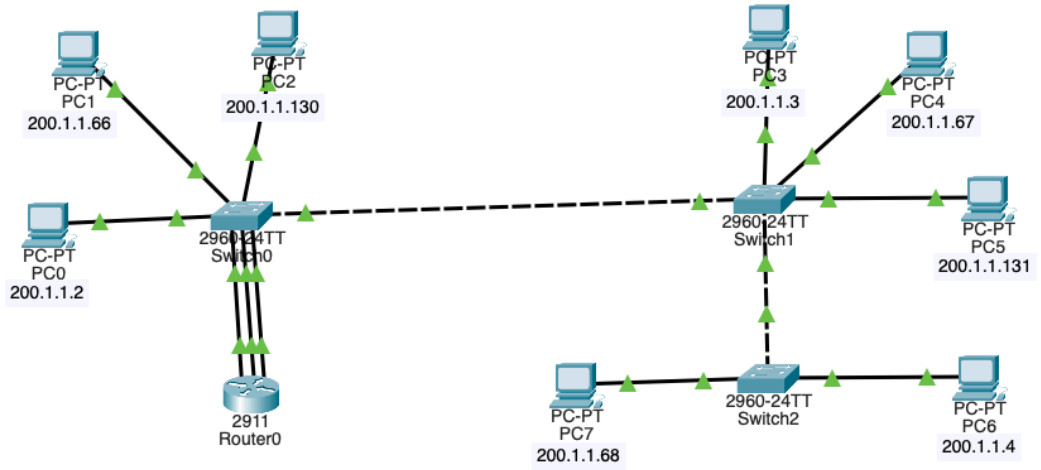
1. Because the PCs are in different VLANs as well as in different subnets, they cannot ping each other. Only the PCs that are in the same VLAN and in the same subnet can ping each other.

PC0 is able to ping PC3 & PC6 and vice-versa. PC1 is able to ping PC4 & PC7 and vice-versa. PC2 is able to ping PC5 only and vice-versa.

2. As the computers are on different networks, routing is essential. The default gateway of PC0, PC3 & PC6 was set as 200.1.1.1. The default gateway of PC1, PC4 & PC7 was set as 200.1.1.65. The default gateway of PC2 & PC5 was set as 200.1.1.129.

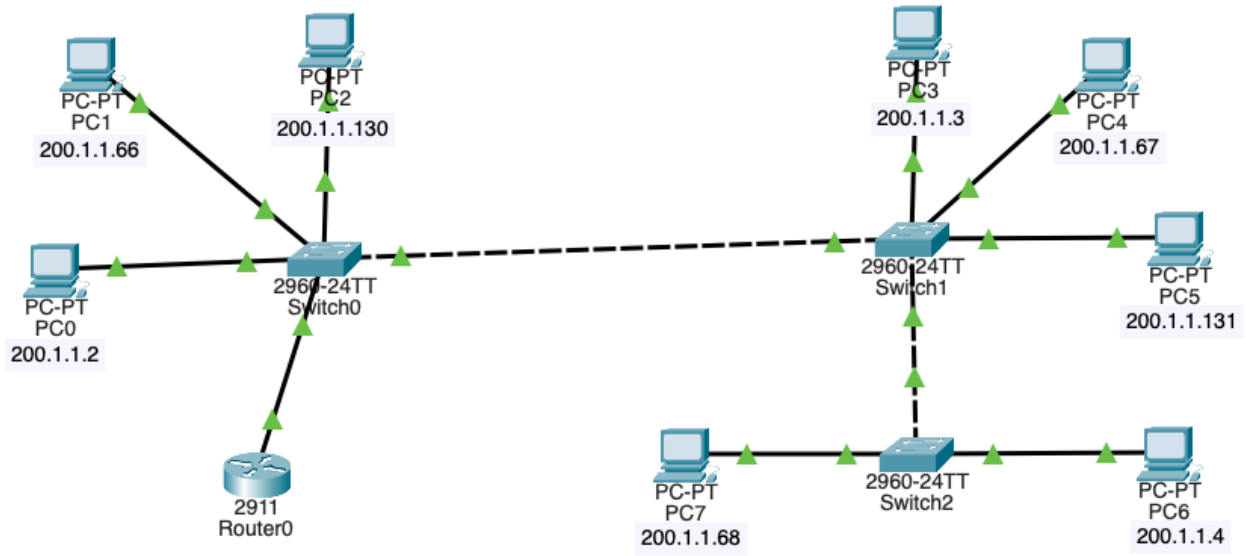
3. Interface FastEthernet0/2 of Switch0 was connected to GigabitEthernet0/0 of Router0 with IP Address of 200.1.1.1/26, interface FastEthernet0/9 of Switch0 was connected to GigabitEthernet0/1 of Router0 with IP Address of 200.1.1.65/26, and interface FastEthernet 0/20 of Switch0 was connected with IP Address of 200.1.1.129/26.

4. Now, all pings are successful, i.e. any PC could reach any other PC. This is because of the fact that we have added a router to handle the routing between multiple subnets and VLANs.



Activity C:

To implement router-on-a-stick, we removed all the links between Switch0 and Router0. Also removed the IP address & subnet mask of all interfaces of the router.



1. We configured interface GigabitEthernet 0/1 of Switch0 as Trunk port and connected to the GigabitEthernet0/0 interface of Router0.

```
Switch(config)#interface GigabitEthernet 0/1
Switch(if-config)#switchport mode trunk
```

2. Now sub-interfaces were configured in Router0 as:

```
Router0#configure terminal
Router0(config)#interface gigabitethernet 0/0.1
Router0(config-subif)#encapsulation dot1Q 1 2 10
Router0(config-subif)#ip address 200.1.1.1 255.255.255.192
```

Similarly we configured another sub-interface as GigabitEthernet0/0.2 on the same physical interface for another VLAN with IP address of 200.1.1.65/26.
Also, another sub-interface as GigabitEthernet0/0.3 on the same physical interface for another VLAN with IP address of 200.1.1.129/26.

3. All pings were successful. This was because encapsulation was used to divide a single interface of the router into three individual sub interfaces through which the routing was done.
4. Activity B utilized three different interfaces to perform routing within different VLANs while the current configuration divided a single interface into three different sub interfaces which was used to

perform routing among various VLANs. Thus only a single interface of switch0 (in trunk mode) and a single interface of router0 was used unlike in activity B.

5. Removing the VLAN 1 from both trunk ports of Switch 1:

```
Switch(config)#interface gigabitEthernet 0/2
Switch(config-if)#switchport trunk allowed vlan remove 1
Switch(config-if)#exit
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport trunk allowed vlan remove 1
```

Here, PC0 is able to reach PC1 and PC2 as it still has an active trunk port allowing VLAN 1 to the router. But since the trunk port from Switch0 to Switch1 and Switch1 to Switch2 don't allow VLAN 1, PC0 is unable to reach other PCs. Also, VLAN 1 hosts, PC3 and PC6 are now isolated and unable to reach any other PC. The rest of the devices are working as normal and able to reach each other.

6. Now, VLAN 1 is allowed in both trunk ports by adding back using the command,

```
Switch(config)#interface gigabitEthernet 0/2
Switch(config-if)#switchport trunk allowed vlan add 1
Switch(config-if)#exit
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport trunk allowed vlan add 1
```

In removing the VLAN 2 from both trunk ports of Switch 1, Similar results as in Q5 were seen, but this time the PCs in VLAN2 are affected and unreachable.

7. Testing for another VLAN i.e. VLAN 10, we saw similar result as the previous two questions, but this time it's PCs in VLAN 10.

Discussion

In this lab, we explored VLAN configuration and inter-VLAN routing to understand how Virtual Local Area Networks can segment network traffic and facilitate communication between different VLANs. Initially, the setup involved connecting PCs and switches and ensuring all devices could communicate within the same network without VLAN segmentation.

After creating VLANs and assigning specific interfaces to VLAN 2 and VLAN 10, we observed that PCs within the same VLAN could communicate, while those in different VLANs could not. This highlighted the fundamental role of VLANs in segmenting network traffic to improve security and manageability. Configuring trunk ports allowed traffic from multiple VLANs to pass between switches, enabling inter-switch communication within the same VLAN. This demonstrated how trunking helps maintain VLAN separation while sharing physical links.

The lab further involved configuring a router with subinterfaces for each VLAN, allowing PCs in different VLANs to communicate. This step was crucial in understanding inter-VLAN routing, where the router acts as an intermediary to route traffic between VLANs, treating each as a separate network. Proper subnetting and gateway configuration ensured that traffic was correctly routed, emphasizing the importance of accurate network configuration.

Conclusion:

We demonstrated the VLAN setup, learned about Trunk ports, intra-VLAN routing and inter-VLAN routing using routers and switches. Both physical connections as well as interface division using encapsulation in routing and trunk mode in switches were used to achieve this. VLAN segmentation proved effective in enhancing network security and reducing broadcast domains, while trunk ports facilitated efficient communication across switches. Inter-VLAN routing using a router taught the necessity of routing in managing traffic between different VLANs.