# Computer Networks

## Lab No.: 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:

- Network simulation tool: Packet Tracer

## VLAN (Virtual Local Area Network)

- When computers are plugged into a switch and give them all IP addresses in the same network, a LAN (Local Area Network) is created
- A VLAN (Virtual Local Area Network) is a logical collection of devices that are grouped together to create separate networks, using layer 2 devices, such as an Ethernet switch
- With VLANs, we connect all the PCs to a single switch but we can make the switch behave as if having multiple independent switches
- Each VLAN is its own broadcast domain and IP subnet
- VLANs can be local within a single layer 2 device or be trunked over multiple layer 2 devices
- Router is used to route the packets between multiple VLANs
- Because VLANs are based on logical instead of physical connections, they are extremely flexible

## Configuration of VLAN

### Creating VLANs

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan vlan_ID
Switch(config-vlan)# name Vlan_2
Switch(config-vlan)# end
Switch#
```

## Assigning an Interface to particular VLAN

- `Switch> enable`
- `Switch# configure terminal`
- `Switch(config)#interface FastEthernet0/11`
- `Switch(config-if)#switchport access vlan 2`
- `Switch(config-if)#end`
- `Switch#`

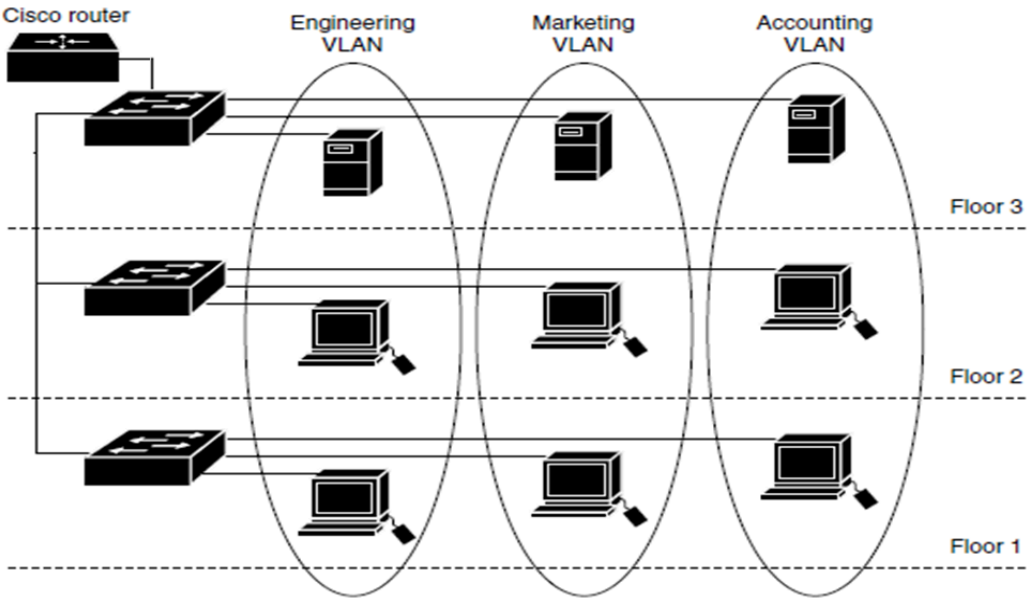



Figure: Different VLANs interconnected by a Router

## Extension of VLAN using Multiple Switches

- Trunk port is used to connect different VLANs configured in different layer 2 devices such as switches
- A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list
- Otherwise separate connections are required in between switches for each VLANs

## Trunk Port Configuration:

Assigning an Interface of Switch to Trunk Mode

- `Switch> enable`
- `Switch#configure terminal`
- `Switch(config)#interface fa0/20`
- `Switch(config-if)#switchport mode trunk`

To allow all VLANs via Trunk Port

- `Switch(config-if)#switchport trunk allowed all`

To remove VLAN 1 from Trunk Port

- `Switch(config-if)#switchport trunk allowed vlan remove 1`

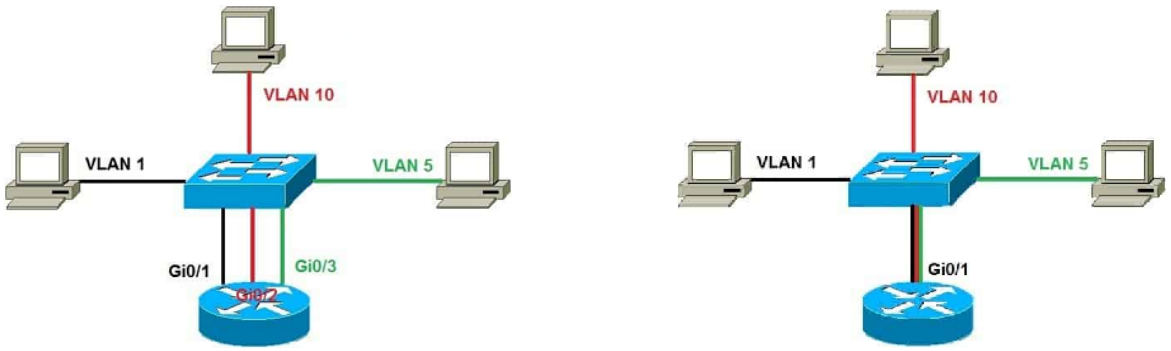
To add VLAN 1 in a Trunk Port

- `Switch(config-if)#switchport trunk allowed vlan add 1`

## Inter-VLAN Routing

- Inter-VLAN routing can be defined as a way to forward traffic between different VLAN by using a router in the network
- There are two ways in which inter-VLAN routing can be accomplished
    - Traditional inter-VLAN routing
    - Router-on-a-stick

**Traditional inter-VLAN Routing**: The switch ports of individual VLAN are connected to the router interface. Each interface of the router can then accept traffic from the VLAN associated with the switch interface that it is connected to, and traffic can be routed to the other VLANs connected to the other interfaces. In traditional inter-VLAN routing the router needs an individual LAN interface for each VLAN, so a router may need a large number of LAN interfaces if there are a large number of VLANs. So this approach is not efficient.




(a) Traditional (b) Router-on-a-stick

Figure: Inter-VLAN Routing

**Router-on-a-stick**: In this mode router's single LAN interface is connected with a switch in which the corresponding switch-interface is configured as a trunk port. The Router's single interface is divided into sub-interfaces with IP addresses of each of the VLAN, which acts as a default gateway to their respective VLANs.

Inter-VLAN Routing Configuration

```
Router0>enable
Router0#config t
Router0(config)#interface gigabitethernet 0/0.1
Router0(config-subif)#
Router0(config-subif)#encapsulation dot1Q [VLAN ID]
Router0(config-subif)#
Router0(config-subif)#ip address 200.1.1.1 255.255.255.192
```

## Activities:

**Note**: Choose the switches and routers as specified. Similarly interconnect the interfaces of devices as mentioned in the activities list.

A. Create the network topology as shown in figure 1 below and perform the following activities:

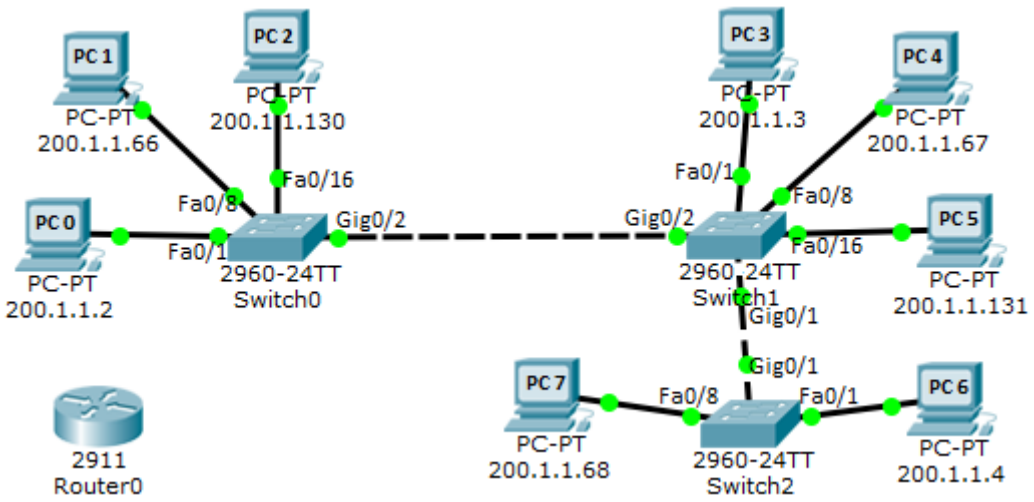



Figure 1: Network Topology 1

1. Connect the PCs and switches as shown in figure 1 above.
   - Connect each of the PCs with given interfaces of corresponding switches.
   - Connect each of the switches with another switch with interfaces as specified in the given figure.
   - Use the subnet mask of **255.255.255.0** for each of the PCs.
   - Select the specified model of Switch so that you won't have any problem while creating the given topology.
2. Observe the result by testing the connectivity between each computer.
3. Create the VLAN 2 and VLAN 10 in all switches i.e. Switch0, Switch1 and Switch 2.

4. Assign interfaces FastEthernet 0/8, 0/9, 0/10, 0/11, 0/12 of all three switches to VLAN 2. Similarly, assign interfaces FastEthernet 0/16, 0/17, 0/18, 0/19, 0/20, 0/21, 0/22 of all three switches to VLAN 10.
5. Observe the result by testing the connectivity between each computer - Does the ping from PC0 to PC3 & PC6 succeed? Similarly, does the ping from PC1 to PC4 & PC7 succeed? State reason. Test connectivity from PC0, PC1 & PC2 to all other PCs.
6. Connect interface FastEthernet 0/12 of Switch0 with FastEthernet 0/12 of Switch1 and connect interface FastEthernet 0/11 of Switch1 with FastEthernet 0/11 of Switch2. Test connectivity from PC0, PC1 & PC2 to all other PCs. Note down, in which case connection is successful and state reason. (Is ping successful from PC1 to PC4 and PC7?)
7. Now, again connect the interface FastEthernet 0/20 of Switch0 with FastEthernet 0/20 of Switch1. Test connectivity from PC0, PC1 & PC2 to all other PCs. Compare the result with that of step 6. Note down, in which case connection is successful and state reason. (Does ping become successful from PC2 to PC5 in this step?)

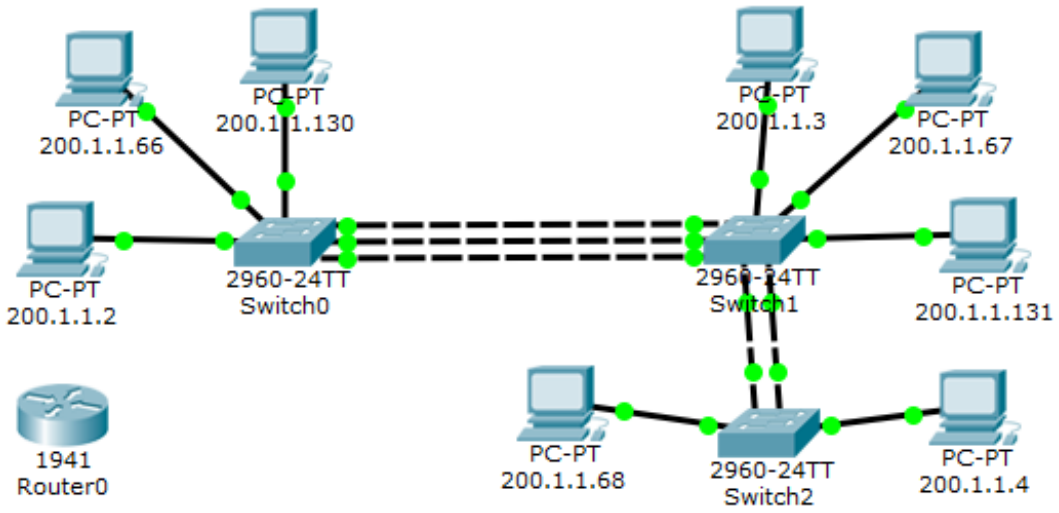



Figure 2: Network Topology 2

8. Now, remove the additional links between switches that you have added in **step 6** & **step 7**, and perform the followings:
   - Configure interfaces GigabitEthernet0/1 and GigabitEthernet0/2 of all three switches as a Trunk port
   - Observe the result by testing the connectivity between each computers
   - Does the ping from PC0 to PC3 & PC6 succeed? State reason
   - Does the ping from PC1 to PC4 & PC7 succeed? State reason
   - Does the ping from PC2 to PC5 succeed? State reason
   - Compare the current configuration with above configuration

B. From the above activity A, change the subnet mask to **255.255.255.192** for all PCs, and perform the followings:
   1. Test the connectivity from each computer to another computer. Does ping succeed in all cases? State with reason.
   2. Now the computers are on different networks, so routing is essential to forward packets from one network to another network. For this set the default gateway of PC0, PC3 & PC6 as 200.1.1.1. Similarly the default gateway of PC1, PC4 & PC7 as 200.1.1.65. Also set the default gateway of PC2 & PC5 as 200.1.1.129.
   3. Connect interface FastEthernet0/2 of Switch0 to GigabitEthernet0/0 of Router0 with IP Address of 200.1.1.1/26, similarly connect interface FastEthernet0/9 of Switch1 to GigabitEthernet0/1 of Router0 with IP Address of 200.1.1.65/26. And connect interface FastEthernet 0/20 of Router0 with IP Address of 200.1.1.129/26.
   4. Again test the connectivity from each computer to another computer. Does ping succeed in all cases? State reason

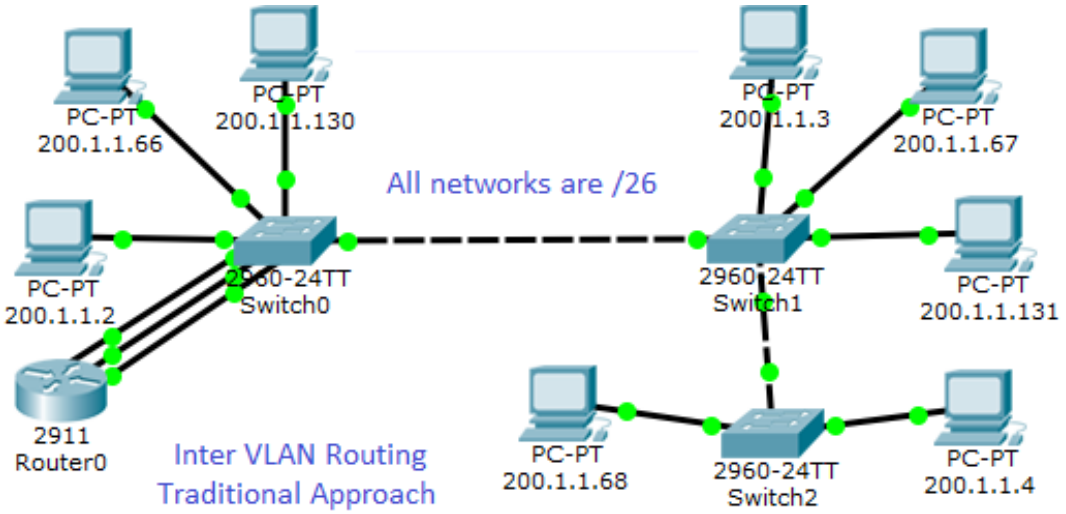



Figure 3: Network Topology 3

C. There are still more than one connection from switch to router. There is only one connection between switches using the trunk port to forward frames between computers of the same VLAN connected via different switches. Similarly we can use a single connection between switch and router to route packets between multiple VLANS.
Remove all the links between Switch1 and Router0. Also remove the IP address & subnet mask of all interfaces of router and perform the followings:
   1. Configure interface GigabitEthernet 0/1 of Switch0 as Trunk port (if not configured yet) and establish connection to the GigabitEthernet0/0 interface of Router0
   2. Now configure sub-interfaces in Router0 as:

```
Router0>
Router0>enable
Router0#
Router0#config t
Router0(config)#
Router0(config)#interface gigabitethernet 0/0.1
```

```
Router0(config-subif)#
Router0(config-subif)#encapsulation dot1Q [VLAN ID i.e. 1 or 2 or 10]
Router0(config-subif)#
Router0(config-subif)#ip address 200.1.1.1 255.255.255.192
```

Similarly configure another sub-interface as GigabitEthernet0/0.2 on the same physical interface for another VLAN with IP address of 200.1.1.65/26.
Again configure another sub-interface as GigabitEthernet0/0.3 on the same physical interface for another VLAN with IP address of 200.1.1.129/26.
And finally activate this physical interface by using no shutdown command.

3. Again test the connectivity from each computer to another computer. Does ping succeed in all cases? State reason
4. Compare this configuration with previous (i.e. in activity B).

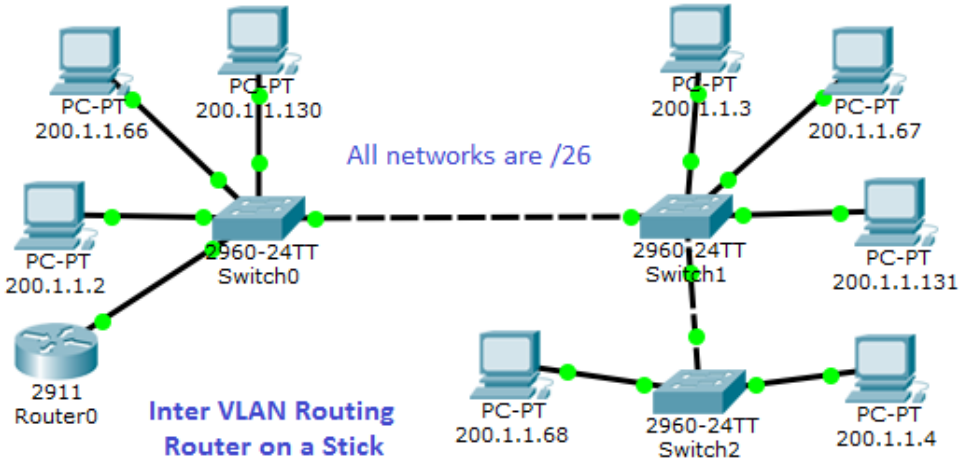



Figure 4: Network Topology 4

5. Remove the VLAN 1 from both trunk ports of Switch 1 and test the connectivity.
6. Now allow VLAN 1 in both trunk ports and remove the VLAN 2 from both trunk ports of Switch 1 and test the connectivity.
7. Similarly you can test for another VLAN i.e. VLAN 10 also. You can also try by removing any VLAN in other switches also.

Exercises:

I. What is VLAN? Explain its importance with basic configuration steps.
II. How can packets be forwarded between computers within the same VLAN but connected at different switches? Explain.
III. How can packets be routed between computers at different VLANs? Explain.
IV. Note down the results of each and step of above activities with reason.

***