**Experiment No .6**

**Title: Design and Simulation of Virtual LAN**

**Aim:** To design and simulate the working of VLAN

**Objective:**

1. Create the network topology
2. Create two different VLANs
3. Assign switch ports to VLANs
4. Assign IP addresses to different computers in network
5. Configure inter VLAN routing
6. Test the VLAN and inter VLAN connectivity
7. Record the observation

**Theory:**

*Virtual LAN (VLAN)* is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divide broadcast domain but broadcast domain can be divided by switches using the concept of VLAN.

A broadcast domain is a network segment in which if a device broadcast a packet then all the devices in the same broadcast domain will receive it. The devices in the same broadcast domain will receive all the broadcast packets but it is limited to switches only as routers don’t forward out the broadcast packet. To forward out the packets to different VLAN (from one VLAN to another) or broadcast domain, inter VLAN routing is needed. Through VLAN, different small-size sub-networks are created which are comparatively easy to handle.

**VLAN ranges –**

* **VLAN 0, 4095:**These are reserved VLAN which cannot be seen or used.
* **VLAN 1:**It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can’t be deleted or edit but can be used.
* **VLAN 2-1001:** This is a normal VLAN range. We can create, edit and delete these VLAN.
* **VLAN 1002-1005:** These are CISCO defaults for fddi and token rings. These VLAN can’t be deleted.
* **VLAN 1006-4094:** This is the extended range of VLAN

**Types of connections in VLAN –**

There are three ways to connect devices on a VLAN, the type of connections are based on the connected devices i.e. whether they are VLAN-aware (A device that understands VLAN formats and VLAN membership) or VLAN-unaware (A device that doesn’t understand VLAN format and VLAN membership).

1. **Trunk Link**   
   All connected devices to a trunk link must be VLAN-aware. All frames on this should have a special header attached to it called tagged frames.
2. **Access Link**   
   It connects VLAN-unaware devices to a VLAN-aware bridge. All frames on the access link must be untagged.
3. **Hybrid Link**   
   It is a combination of the Trunk link and Access link. Here both VLAN-unaware and VLAN-aware devices are attached and it can have both tagged and untagged frames.

**Advantages**

* **Performance**   
  The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destinations. e.g.-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain, therefore, all will receive the traffic i.e. wastage of bandwidth but if we make VLANs, then the broadcast or multicast packet will go to the intended users only.
* **Formation of virtual groups**  
  As there are different departments in every organization namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.
* **Security**   
  In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.
* **Flexibility**   
  VLAN provide flexibility to add, remove the number of host we want.
* **Cost reduction**   
  VLANs can be used to create broadcast domains which eliminate the need for expensive routers.  
  By using VLAN, the number of small size broadcast domain can be increased which are easy to handle as compared to a bigger broadcast domain.

**Input:** VLAN Requirement of KITCOE Kolhapur

Two different departments CSE and Mechanical having two computers each in existing physical network. Two different departments are connected using two switches.

CSE Department: PC0 and PC1

Mechanical Department: PC2 and PC3

PC0 from CSE department and PC2 from Mechanical department are assigned to Project 1.

PC1 from CSE department and PC3 from Mechanical department are assigned to Project 2.

Traffic between two computers which are assigned on same project should not be passed to other computers in network.

**Software Tool:** CISCO Packet Tracer

**Guidelines:**

As a Network Engineer we have to first understands the requirements of the organization (client/customer) for which you are designing and developing the VLAN.

1. In Cisco Packet Tracer, **create the network topology**
2. **Create 2 VLANs on the switch having name CSE and Mechanical**

Switch#config terminal

Switch(config)#vlan 10

Switch(config-vlan)#name CSE

Switch(config-vlan)#vlan 20

Switch(config-vlan)#name Mechanical

1. **Assign switch ports  to the VLANs**

Configure switch interfaces fa 0/1 and  fa 0/2 as access ports to connect to our PCs. Here, interfaces fa 0/1 and fa 0/2 are assigned to VLAN 10 CSE while interfaces fa 0/1 and fa 0/2 are assigned to VLAN 20 Mechanical.

Switch0>enable

Switch0#config terminal

Switch0(config)#int fa0/1

Switch0(config-if)#switchport mode access

Switch0(config-if)#switchport access vlan 10

Switch0(config-if)#int fa0/2

Switch0(config-if)#switchport mode access

Switch0(config-if)#switchport access vlan 10

Switch1(config-if)#int fa0/1

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 20

Switch1(config-if)#int fa0/2

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 20

Switch *Interface*fa0/3 will be configured as trunk port, as it will be used to carry traffic between the two VLANs.

Switch0(config)#int fa 0/3

Switch0(config-if)#switchport mode trunk

Switch1(config)#int fa 0/3

Switch1(config-if)#switchport mode trunk

1. Assign static IP addresses to the four PCs which are located in the separate VLANs. PC0 and PC1 fall in VLAN 10 while PC2 and PC3 fall in VLAN 20.

**PC0**   **IP address** 192.168.1.10    **Subnet mask** 255.255.255.0

**PC1:** **IP address** 192.168.1.20   **Subnet mask** 255.255.255.0

**PC2: IP address** 192.168.2.10    **Subnet mask** 255.255.255.0  

**PC3: IP address**  192.168.2.20 **Subnet mask**   255.255.255.0  

1. **Test the connectivity**

**Output:** Two VLANs for created for two different Projects as per the requirement of KITCOEK