**Experiment-2**

**Part A**

**Aim:** Simulation of Virtual Local Area Network

**Prerequisite:** Nil

**Outcome:** To impart knowledge of Computer Networking Technology

**Theory:** A VLAN, or Virtual Local Area Network, is a technology used in computer networking to logically segment a physical network into smaller, isolated virtual networks. This segmentation is done to enhance network efficiency, security, and management. VLANs allow devices in different physical locations to communicate as if they are on the same network, even though they might be physically separated.

In a VLAN, devices are grouped together based on certain criteria, such as their functional roles, departments, or projects, rather than their physical location. This grouping is achieved through network configuration rather than physical wiring. Devices within the same VLAN can communicate with each other as if they were connected to the same network switch, even if they are connected to different switches.

VLANs offer several benefits, like reduced broadcast traffic, enhanced security, and

flexibility in network design.

**Benefits:**

1. Network Segmentation: Divide a network into smaller isolated sections for better management.
2. Improved Security: Enhance data protection by isolating traffic between different sections.
3. Enhanced Performance: Optimize data flow by allocating bandwidth effectively within sections.
4. Flexibility and Scalability: Easily adapt the network as it grows by adding new sections.
5. Isolation of Faults: Prevent network issues from spreading by confining them within sections.
6. Resource Sharing: Facilitate controlled access to shared resources like printers.
7. Efficient Network Design: Design networks based on function rather than physical location.

**Types:**

1. Port-Based: Grouping by physical switch ports.

2. Tagged (802.1Q): VLAN tagging for traffic separation.

3. Protocol-Based: Segregation based on protocol used.

4. MAC-Based: VLANs assigned by device MAC addresses.

5. Private VLAN (PVLAN): Provides further isolation within a VLAN by segmenting it into subgroups, allowing some devices to communicate while others remain isolated.

6. Community VLAN: In a private VLAN setup, devices within the same community VLAN can communicate with each other, while devices in different community VLANs are isolated.

7. Wireless VLAN: For wireless networks, this VLAN separates wireless traffic from wired traffic and allows for different security policies and quality of service settings.

**Procedure:**

1. Open Cisco Packet Tracer and simulate the sample topologies with required size of

VLAN.

2. Perform Necessary Operation on Switch to create and configure VLAN.

3. Check the connectivity between the devices.

**Part – B**

**Steps:**

1. Open Cisco Packet Tracer and choose the devices for your setup.

2. Connect the devices to create your VLAN topology.

3. Configure VLANs on switches, assigning ports to respective VLANs.

4. Test VLAN isolation by trying to ping devices within and across VLANs.

**Output:**

**1. VLAN Topology**

**2. IP Configuration**

**a. PC 1**

**b. PC 2**

**c. PC 3**

**d. PC 4**

**3. Switch CLI Commands**

**4. Ping from PC 1 to PC 4**

**Observation & Learning:**

Observing isolated communication within VLANs and limited inter-VLAN connectivity highlights the efficiency and security of VLANs. Learning includes configuring VLANs on switches for segmentation, minimizing broadcast traffic, and understanding their role in network organization and security.

**Conclusion:**

Understanding VLAN principles and simulations is crucial for professionals in the field of networking. The utilization of VLAN simulations is instrumental in achieving proficiency in setting up, diagnosing issues, and enhancing performance. This practice significantly contributes to the effective management and design of networks. This practical exercise provides hands-on exposure to simulating VLANs, enabling a better grasp of their benefits and the enhancement of skills related to segmenting networks.

**Questions:**

**1. What is the maximum number of VLAN can be created in a network?**

**Ans:** The maximum number of Virtual LANs (VLANs) that can be created in a network depends on several factors, including the specific networking equipment and protocols being used. The maximum number of VLANs that can be created in a network is determined by the VLAN ID space.

In traditional Ethernet networks, VLANs are identified by a 12-bit VLAN ID, allowing for a theoretical maximum of 4096 VLANs (2^12 = 4096). However, not all these IDs are usable, as some are reserved for special purposes like VLAN 1 for default/native VLAN, VLANs for management, etc.

**2. What is mean by MTU? What is the value of MTU in Ethernet?**

**Ans:** MTU stands for Maximum Transmission Unit. It represents the largest size of a packet or frame that can be transmitted over a network in a single data transmission. In simpler terms, it is the maximum size of data that can be sent in one go without being fragmented into smaller pieces.

For Ethernet, the most common value for the MTU is 1500 bytes. This means that the largest Ethernet frame that can be transmitted without fragmentation is 1500 bytes in size. It is worth mentioning that while the standard Ethernet MTU is 1500 bytes, there are variations and considerations to be made depending on the specific network equipment, software, and network protocols in use. In cases where a network link or device has a lower MTU, larger packets may need to be fragmented into smaller units for transmission and reassembled at the receiving end.

**3. What happens when the broadcast operation is performed from a system in certain VLAN?**

**Ans:** When a broadcast operation is performed from a system in a certain VLAN (Virtual LAN), the broadcast frames are only propagated to devices within the same VLAN. This means that the broadcast traffic will only be received and processed by devices within the same VLAN, and it will not cross over to other VLANs.