Name: Ronak Panchal

Roll no.: 22BCP192

Experiment - 2

Aim: Simulation of Virtual Local Area Network

Outcome: To Impart knowledge of Computer Network Technology

Theory:

A virtual local area network (VLAN) divides a network to limit the number of broadcasts and users' access levels. The "virtual" in VLAN refers to the fact that the local area network is physically unchanged, but a logic layer splits it into multiple pieces.

A VLAN breaks a single network into multiple sections by logically separating ports and switches, creating multiple standalone networks from the same backbone. This enhances security and reduces the number of broadcasts individual devices receive.

VLAN offers several advantages such as simplified administration, increased performance, greater flexibility, and more.

1. Saves cost: Workstations or devices associated with a particular VLAN can communicate via switches, eliminating the need to use routers required to receive and send data on computer networks from outside the virtual LAN.
2. Offer greater flexibility: Virtual LANs are more flexible than physical networks. They can be easily configured, updated, and assigned based on port, subnet criteria, and protocol.
3. Simplified administration and enhanced security: Virtual LANs don’t require in-depth administrative monitoring. These networks allow you to limit, change, delete, update, or modify access controls and permissions rights.

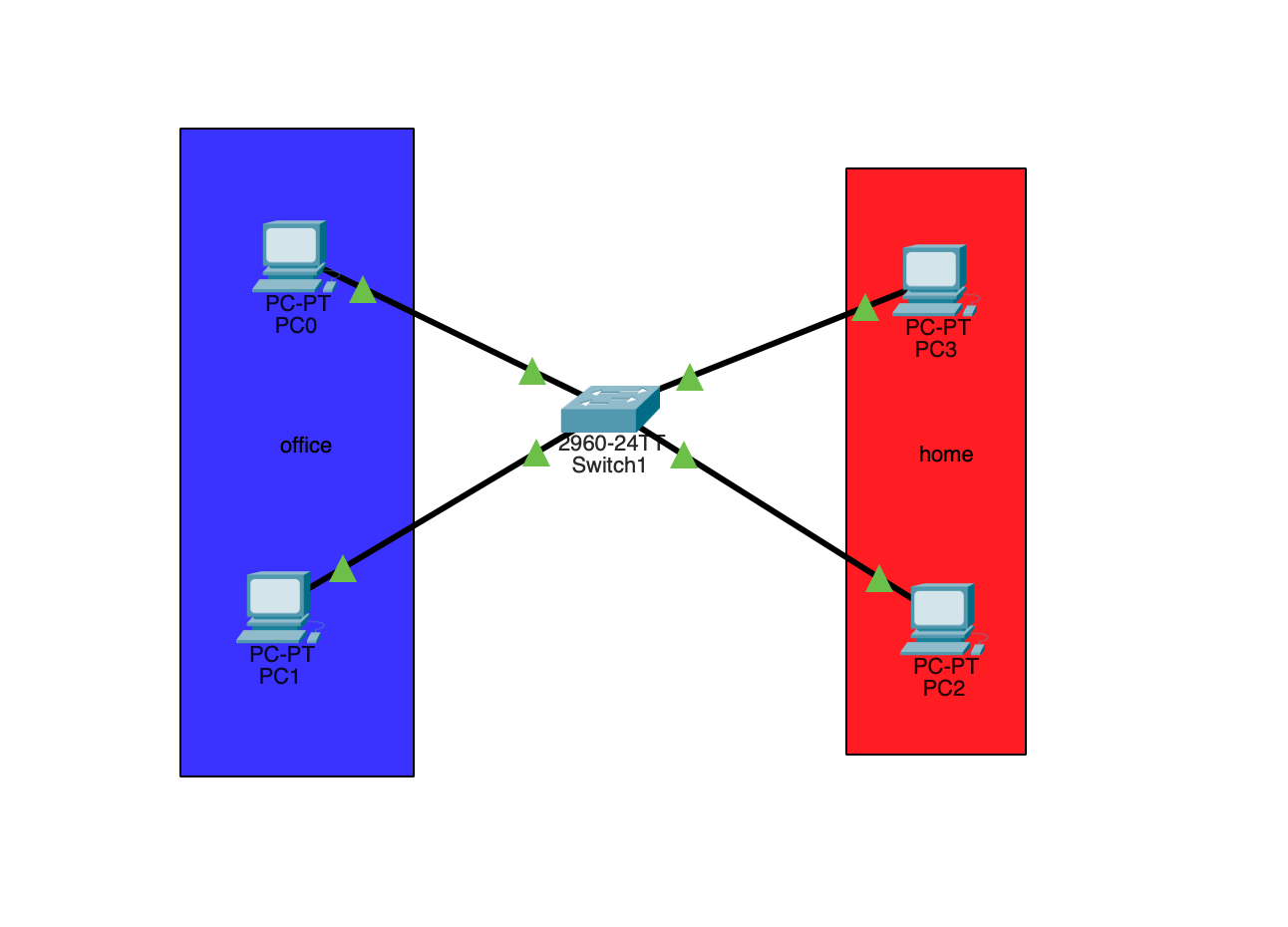
Procedure:

1. Open Cisco Packet Tracer and simulate the sample topologies of the required size.
2. Perform necessary operation on switch to create and configure vlan
3. Check the connectivity between the devices.

Steps:

1. Add a switch, 4 pcs and connect them
2. Give ip addresses to all the PC.
3. Select rectangle from the navigation bar.
4. Create 1st rectangle for home and 2nd for office.
5. Give them name.
6. Perform some operations on switch to create a vlan.

Output:







Observation & Learning:

1.VLANs divide a physical network into multiple logical networks. For example,you might have different VLANs for departments like Home and office, etc. Devices on one VLAN cannot directly communicate with devices on another VLAN without a router or switch.

2.VLANs enhance security by isolating network traffic. For example, sensitive data from the office can be kept separate from home, reducing the risk of data breaches.

3.By creating VLANs, you reduce the size of the broadcast domain. Broadcast traffic is only sent within the VLAN, not to the entire network, which can improve network performance.

4.VLANs provide the flexibility to manage network traffic and resources. Devices in the same VLAN can be spread across different physical locations, yet still be part of the same logical network.

Conclusions:

1. VLANs allow you to segment the network into different logical groups (e.g., “Office” and “Home”). Even though all devices are connected to the same physical switch, they are logically separated into distinct networks.
2. By placing devices into separate VLANs, you can isolate sensitive data and restrict access to certain parts of the network. In this case, the “Office” and “Home” networks are isolated, preventing unauthorized access between them.
3. VLANs help reduce the size of broadcast domains, minimising unnecessary network traffic. Broadcasts within a VLAN are confined to that VLAN and do not propagate to others, which can lead to improved network performance and efficiency.
4. VLANs offer flexibility in network design, allowing you to group users and devices logically rather than physically. This makes it easier to manage and scale the network as your organization grows or as new devices are added.

Questions:

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

Ans.

Under IEEE 802.1Q, the maximum number of VLANs on a given Ethernet network is 4,094 (4,096 values provided by the 12-bit VID field minus reserved values at each end of the range, 0 and 4,095).

1. What is meant by MTU? What is the value of MTU in ethernet?

Ans.

MTU stands for maximum transmission unit and refers to the largest data packet size a network device can accept. It's a measurement of the entire packet, including headers and payload, and is usually measured in bytes. In Ethernet networks, the standard MTU is 1,500 bytes, excluding the 18–20 byte Ethernet header.

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

Ans. When a broadcast operation is performed from a system within a specific VLAN, The broadcast message is sent to all devices within the same VLAN. This means that every device connected to the VLAN will receive the broadcast frame. The broadcast is contained within the VLAN and does not propagate to other VLANs.