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:

- Network simulation tool: Packet Tracer

Procedure:

Procedure for Activity A:

The network topology was created as shown in figure 1, and the following steps were performed. The PCs and switches were connected according to the figure. Each PC was assigned the subnet mask 255.255.255.0. VLAN 2 and VLAN 10 were created in all switches, and interfaces FastEthernet 0/8 to 0/12 were assigned to VLAN 2, while interfaces FastEthernet 0/16 to 0/22 were assigned to VLAN 10. Connectivity between PCs was tested, and additional connections between switches were added and tested for improved connectivity. The trunk ports on switches were configured, and the results were compared with the previous configurations.

Procedure for Activity B:

The subnet mask for all PCs was changed to 255.255.255.192, and connectivity between each computer was tested. Default gateways were set for each PC according to the new subnet. The router was connected to the switches using specified interfaces and IP addresses. Connectivity between computers was tested again to ensure successful packet routing between different networks.

Procedure for Activity C:

All additional links between Switch1 and Router0 were removed, and a single trunk port was configured on Switch0 to connect to Router0. Sub-interfaces were created on Router0 for each VLAN with appropriate

IP addresses. Connectivity between each computer was tested to verify the configuration. Different VLANs were selectively removed from the trunk ports to test the connectivity under varying conditions.

Observation

Activity A:

1. Each PC was connected with the given interface and subnet mask 255.255.255.0 for each PC.

2. The ping command response was successful from each PC to another, indicating a complete connection.

5. The connectivity from PC0 to PC3 and PC6 was successful as they had the default VLAN 1 configured at the interface from the switch. The ping from PC1 to PC4 and PC7 failed because there was no interface of assigned VLANs between Switch0 and Switch1. Similarly, the ping from PC2 to PC5 failed.

6. After connecting interface FastEthernet 0/12 of Switch0 with FastEthernet 0/12 of Switch1 and connecting interface FastEthernet 0/11 of Switch1 with FastEthernet 0/11 of Switch2, the ping between PC1, PC4, and PC7 was successful. However, the ping between PC2 and PC5 failed.

7. After connecting interface FastEthernet 0/20 of Switch0 with FastEthernet 0/20 of Switch1, the ping between PC2 and PC5 was successful. However, the ping between different VLANs failed.

8. After configuring interfaces GigabitEthernet0/1 and GigabitEthernet0/2 of all three switches as trunk ports, the ping between all PCs of similar VLANs was successful. This was because the trunk ports allowed VLAN traffic to pass through, enabling communication between VLANs across different switches.

Activity B:

1. After changing the subnet mask to 255.255.255.192 for all PCs, the ping was still successful in all cases. This is because the IP addresses (200.1.1.2, 200.1.1.3, 200.1.1.4) and (200.1.1.66, 200.1.1.67, 200.1.1.68) and (200.1.1.130, 200.1.1.131) were on the same network of the given mask. However, not all PCs were on the same network.

4. After configuring the router with interface FastEthernet0/2 of Switch0 to GigabitEthernet0/0 of Router0 with IP Address 200.1.1.1/26, connecting interface FastEthernet0/9 of Switch1 to GigabitEthernet0/1 of Router0 with IP Address 200.1.1.65/26, and connecting interface FastEthernet 0/20 of Router0 with IP Address 200.1.1.129/26, the ping was successful between each PC of different networks and different VLANs.

Activity C:

1. The configuration of interface GigabitEthernet 0/1 of Switch0 as a trunk port (if not configured yet) and establishing a connection to the GigabitEthernet0/0 interface of Router0 was completed.

3. The ping from all PCs to other PCs was successful.

4. In Activity B, InterVLAN routing was done using the traditional approach where each VLAN had a corresponding interface to the router. In Activity C, sub-interfaces were used to route between VLANs via a single Gigabit Ethernet interface.

5-7. When VLAN 1 was removed from both trunk ports of Switch1, connectivity was lost. When VLAN 1 was allowed and VLAN 2 was removed from both trunk ports of Switch1, connectivity for VLAN 1 was restored, but VLAN 2 lost connectivity. Similarly, other VLANs (e.g., VLAN 10) were tested by removing them from the trunk ports, and connectivity was observed to be lost for the removed VLANs.

Conclusion

This lab provided hands-on experience with VLAN configuration and InterVLAN routing. We successfully created VLANs, extended them across multiple switches, and routed packets between different VLANs using both traditional and router-on-a-stick methods. The use of trunk ports and sub-interfaces demonstrated efficient VLAN management and packet routing. The importance of VLANs in network segmentation and traffic management was clearly observed through the activities performed.

Exercise Questions

I. What is VLAN? Explain its importance with basic configuration steps.

A VLAN (Virtual Local Area Network) is a logical grouping of devices on a network that can be on the same physical network but segmented into different broadcast domains. VLANs improve network management and security by segregating traffic and reducing broadcast domains.
Basic configuration steps:

- Enter privileged EXEC mode: `Switch> enable`
- Enter global configuration mode: `Switch# configure terminal`
- Create a VLAN: `Switch(config)# vlan vlan_ID`
- Name the VLAN: `Switch(config-vlan)# name Vlan_name`
- Assign an interface to the VLAN: `Switch(config)# interface interface_ID`
- Set the interface to the VLAN: `Switch(config-if)# switchport access vlan vlan_ID`
- Exit configuration mode: `Switch(config-if)# end`

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

Packets can be forwarded between computers within the same VLAN but connected at different switches using trunk ports. A trunk port allows traffic from multiple VLANs to pass through a single physical link between switches. The trunk port is configured to carry traffic for all VLANs, ensuring that packets are properly forwarded between switches.

III. How can packets be routed between computers at different VLANs? Explain.

Packets can be routed between computers at different VLANs using InterVLAN routing. This can be accomplished using a router or a Layer 3 switch. There are two main methods:

- Traditional InterVLAN Routing: Each VLAN is connected to a separate physical interface on the router.

- Router-on-a-stick: A single physical interface on the router is divided into multiple sub-interfaces, each configured for a different VLAN. The switch port connected to the router is set to trunk mode.

InterVLAN routing allows traffic to be forwarded between VLANs by routing packets through the router, which acts as the default gateway for each VLAN.