南通大學人工智能与计算机学院（阿里云大数据学院）
School of Artificial Intelligence and Computer Science, Nantong University（人工智能研究院合署）

计算机网络课程设计

Curriculum Design for Computer Networks

LAB REPORT ON

VLAN Configuration Experiment

Supervisor

Dr. 万杰（Wan Jie）

Associate Professor

School of Artificial Intelligence and Computer Science
Nantong University

Submitted By

Vaskar Chakma

2130130204

Class of 2021

2024 年 12 月 10 日

一、Relate Knowledge

1. Introduction of the Basic Knowledge Required

The VLAN (Virtual Local Area Network) is a fundamental concept in modern networking, allowing the segmentation of a physical network into multiple logical networks. This segmentation enables devices within a VLAN to communicate as though they are on the same physical network, regardless of their actual physical location. VLANs enhance security by isolating sensitive data and reducing the risk of unauthorized access. They also improve network performance by limiting broadcast traffic to specific VLANs, ensuring efficient bandwidth usage. Understanding key concepts such as VLAN IDs, trunk ports, and access ports is essential for configuring and managing VLANs. These principles form the basis for creating flexible, scalable, and secure network designs, which are particularly useful in enterprise environments.

The principles behind VLAN configurations involve segmenting networks logically to meet organizational requirements. This lab uses Cisco Packet Tracer as a simulation tool to explore VLAN setup and configuration, emphasizing practical applications of theoretical knowledge. By creating VLANs, assigning ports, and configuring trunk connections, this lab demonstrates how to manage and optimize network performance and security.

2. Lab Principle

The principle of the VLAN configuration experiment revolves around the logical segmentation of a network to enhance its performance, security, and manageability. In a traditional flat network, all devices are part of the same broadcast domain, which means that broadcast traffic from one device is sent to all devices in the network. This can lead to excessive broadcast traffic, consuming bandwidth and reducing the efficiency of the network. Moreover, such a setup lacks proper isolation, which increases the risk of security breaches, as any device can access the network by connecting to any available port. VLAN technology addresses these challenges by dividing a physical network into multiple logical networks, each representing a distinct broadcast domain. Devices within the same VLAN can communicate directly, but communication between VLANs requires the use of Layer 3 devices like routers or Layer 3 switches. By isolating broadcast domains, VLANs reduce unnecessary traffic and improve communication efficiency.

The experiment demonstrates the implementation of VLANs using Cisco switches. VLAN segmentation is achieved by assigning specific ports to VLANs and configuring trunk ports to enable VLAN-tagged traffic between switches. The lab also explores inter-VLAN communication using a router or Layer 3 switch, illustrating how VLANs interact in a multi-switch environment. This principle underscores the importance of VLANs in modern network design, particularly in environments requiring high scalability, security, and traffic optimization.

3. Lab Steps

The VLAN configuration process consists of two main parts:
Single Switch VLAN Configuration and Inter-Switch (Cross-Switch) VLAN Configuration.

二、Lab Report

1. Lab Objective and Requirements

The objective of this lab is to provide students with a practical understanding of configuring Virtual Local Area Networks (VLANs) using Cisco Packet Tracer. VLANs are crucial in modern networking as they allow for the logical segmentation of a physical network into multiple broadcast domains, thereby improving network performance, security, and manageability. In this lab, students will learn how to create and assign VLANs to specific switch ports, configure trunk links between switches to facilitate VLAN communication, and verify the correct configuration through various diagnostic commands. The lab will also emphasize troubleshooting techniques to resolve common issues that might arise during VLAN configuration.

To achieve this, students need a basic understanding of networking concepts, including IP addressing, switch operation, and VLAN principles. The lab environment requires at least two Cisco switches, which will be connected to each other to simulate a real-world scenario of inter-switch VLAN communication. Multiple end devices, such as PCs, will be connected to the switches to test the segmentation and inter-VLAN communication. Cisco Packet Tracer, a network simulation software, will be used to set up and configure the network devices. This tool allows students to simulate network devices and their configurations without needing physical hardware, making it an ideal platform for this lab. For successful completion of the lab, students should have a foundational knowledge of configuring Cisco devices using the command-line interface (CLI), including tasks such as enabling ports, assigning IP addresses, and configuring basic network settings. Additionally, they should be familiar with VLAN concepts, such as how VLANs are used to segregate network traffic. The lab environment will require Cisco Packet Tracer, which should be installed on the student's computer. Students will be given the necessary Packet Tracer files or tasked with creating their own network topology, which will include two or more switches interconnected via trunk links, with various PCs or end devices assigned to different VLANs.

By the end of the lab, students will have practical experience in setting up VLANs, configuring trunk links between switches, and troubleshooting common network issues related to VLANs. This hands-on experience is designed to reinforce the theoretical knowledge gained in the classroom and equip students with the skills needed to configure and manage VLANs in a multi-switch environment. The lab serves as an essential building block for understanding more advanced network configurations and prepares students for real-world network administration tasks.

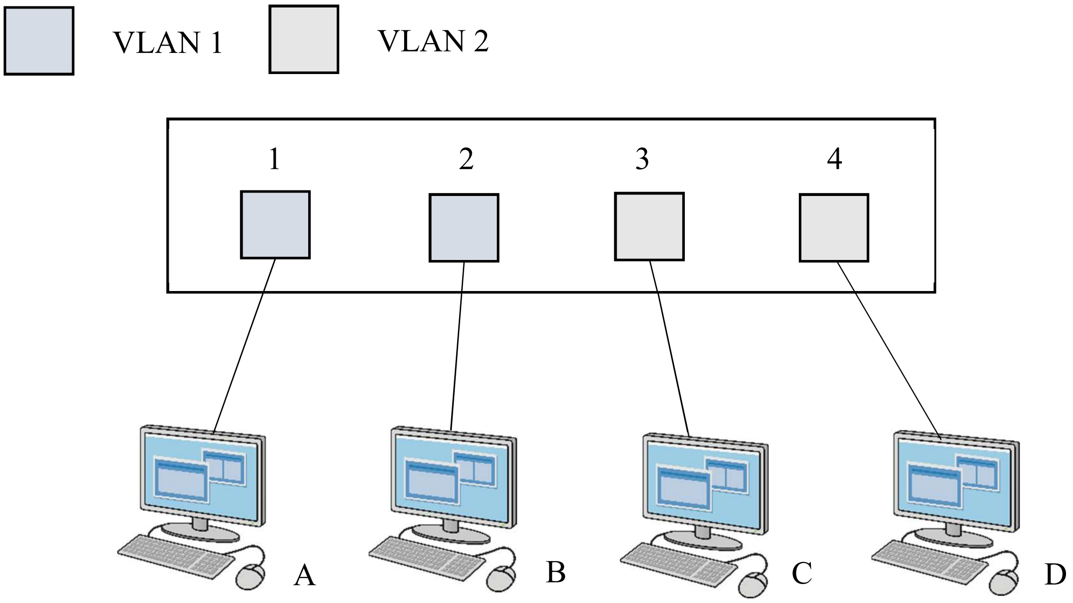
2. Lab Environment

The lab was conducted using Cisco Packet Tracer as a simulation tool. The following setup was used:

***Fig – 1:** Software → Cisco Packet Tracer*

3. Lab Design

The lab design focuses on building a simulated network using Cisco Packet Tracer, where multiple VLANs are configured across a set of interconnected switches. The network layout consists of two or more switches, each connected to several end devices (like PCs), and these devices are segmented into different VLANs to simulate real-world network environments. The design includes both access ports and trunk ports to manage traffic between devices within the same VLAN and between switches. Each switch will have a number of VLANs configured, with each VLAN assigned to a specific range of IP addresses, ensuring that devices in the same VLAN can communicate with one another, while preventing devices in different VLANs from directly communicating unless configured to do so. This segregation helps to optimize network performance and enhance security by isolating broadcast traffic within VLANs. In terms of physical setup, devices such as PCs and servers will be connected to the switches via access ports. The trunk ports, configured using IEEE 802.1Q, allow the switches to transmit traffic from multiple VLANs between each other. The design ensures that each VLAN is properly tagged and recognized by each switch to maintain network segmentation across the switches.



Port	VLAN
1	1
2	1
3	2
4	2

Fig-2: *Port Based VLAN*

The PCs and other end devices will be assigned static IP addresses within the appropriate VLAN subnet. Each PC will be configured to belong to a specific VLAN, and the necessary configurations will be made on the switches to ensure the correct VLAN membership. Additionally, students will configure and verify IP addressing for each device and test network connectivity using commands like ping. The design also incorporates tasks such as enabling and configuring VLAN routing, though this might not be explicitly required in the lab setup. The primary focus remains on VLAN creation, port assignment, and trunk configuration, which will allow students to observe how VLANs operate in a network environment. By the end of the lab, students will have hands-on experience with VLAN configuration, inter-switch communication, and basic troubleshooting techniques.

4. Lab Process and Recording

Single Switch VLAN Configuration

- ***Experiment Preparation***

In this experiment, the goal is to configure VLANs on a single switch and ensure that network devices within those VLANs can communicate according to the designed settings. The devices, including PCs and a switch, will be configured with specific IP addresses and VLAN assignments. For instance, PC0 is assigned IP `192.168.1.2` with a subnet mask of `255.255.255.0` and a default gateway of `192.168.1.1`. PC1 is similarly configured with IP `192.168.1.3`, while PC2 and PC3 are assigned IP addresses in the `192.168.2.2` and `192.168.2.2` range. Each PC will connect to a specific port on the switch configured for its respective VLAN.

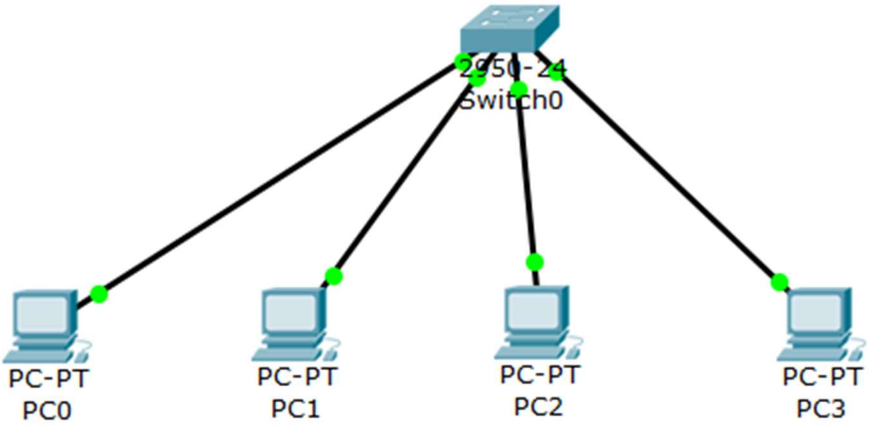
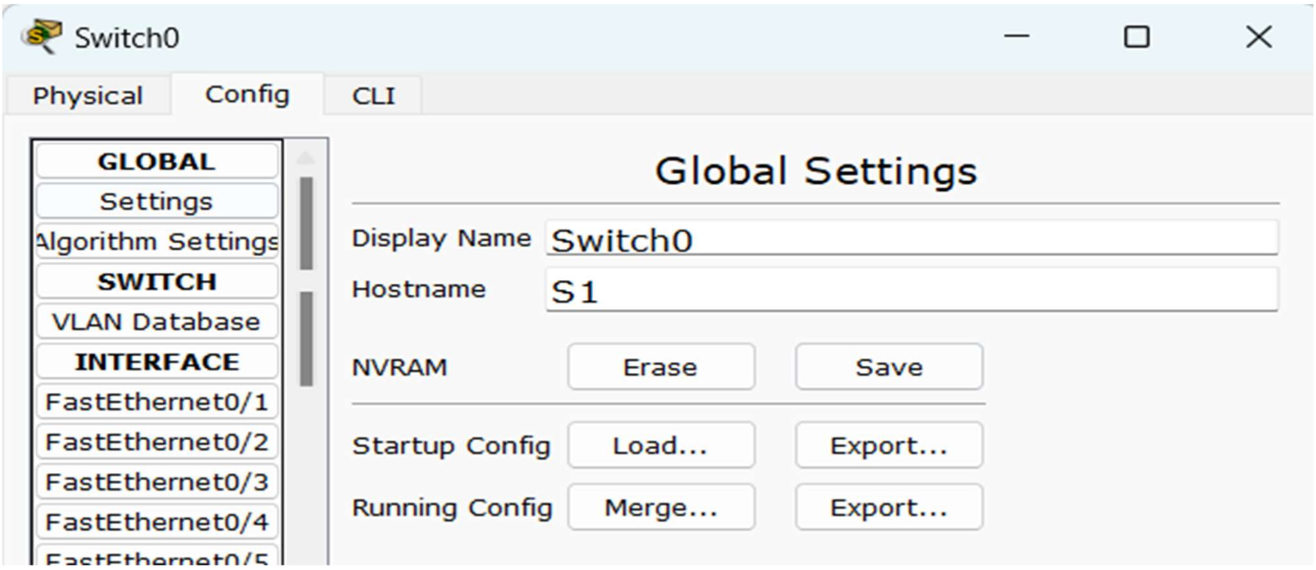


Fig-3: *Single Switch VLAN Configuration*

- ***Experimental Process***

<u>Step One: Basic Switch Configuration</u>

First, the hostname of the switch is set using the command `hostname s1` to identify the switch in the network. Then, DNS lookup is disabled to prevent the switch from trying to resolve incorrect domain names, using the command `*no ip domain-lookup*`.

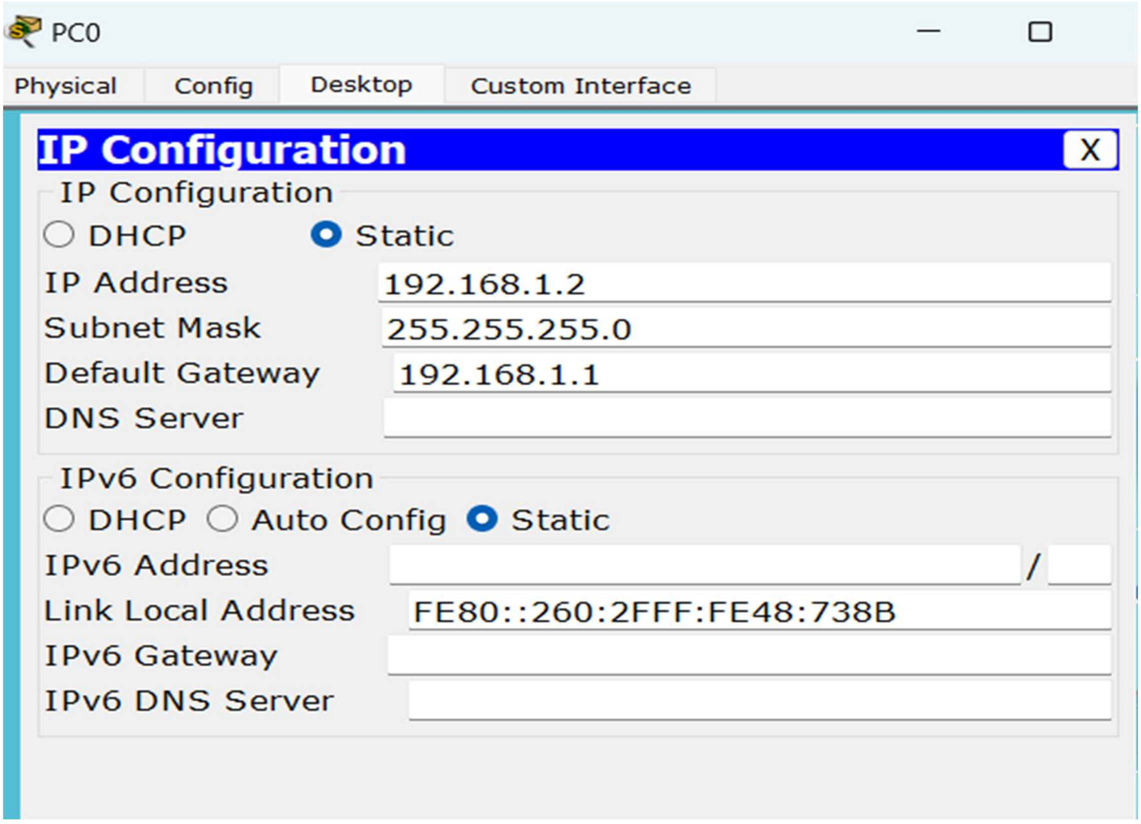


Global Settings

Display Name: Switch0

Hostname: S1

Fig-4: *Switch0 Hostname Change*



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::260:2FFF:FE48:738B

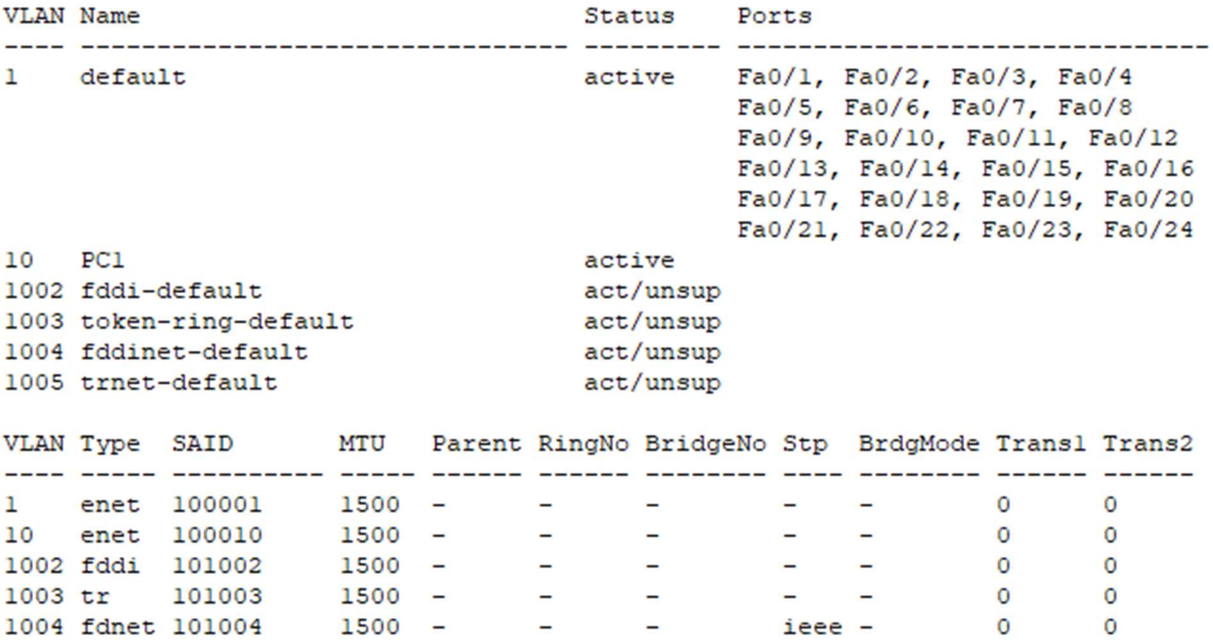
IPv6 Gateway:

IPv6 DNS Server:

Fig-5: PC0's IP Configuration

Step Two: Verifying VLAN Status

Without initially configuring any VLANs, the command `show vlan` is used to verify the default VLAN configuration on the switch. By default, all ports belong to VLAN 1, which is the default broadcast domain. The output will show VLAN 1, and all switch ports will be in this VLAN unless reconfigured.

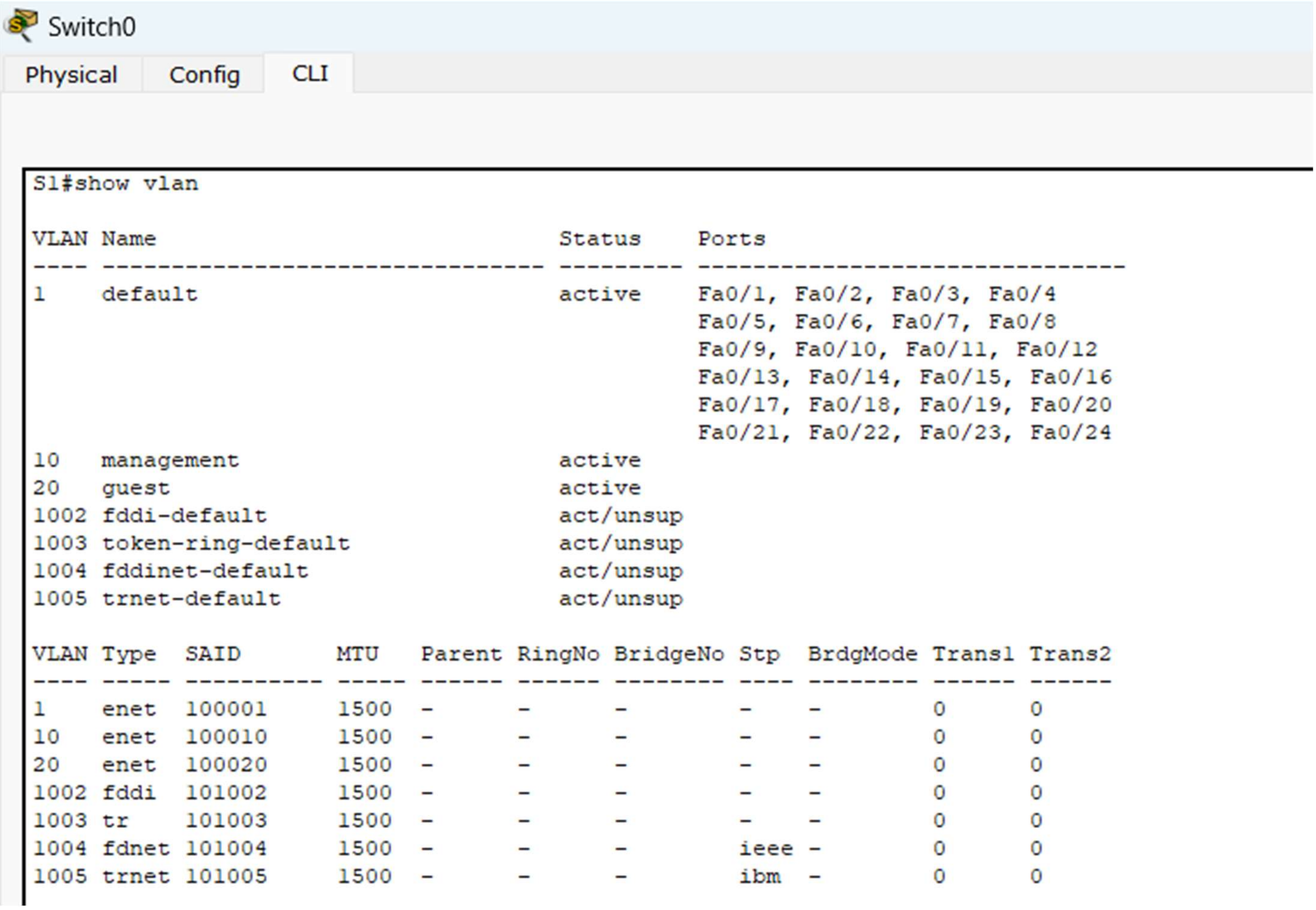


```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   PC1                              active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
```

Fig-6: show vlan (1)

Step Three: Creating VLANs

In global configuration mode, two VLANs are created: VLAN 10 for management and VLAN 20 for guest users. This is done by entering `vlan 10` followed by `name management` and `vlan 20` followed by `name guest`. The `show vlan` command is then used again to verify that the VLANs have been created, though they do not yet have any assigned ports.



```
S1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   management                       active
20   guest                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

Fig-7: *show vlan (2)*

Step Four: Assigning Ports to VLANs

Ports on the switch are assigned to the newly created VLANs. For example, ports `Fa0/1` and `Fa0/2` are assigned to VLAN 10 by using the commands `switchport access vlan 10`, and ports `Fa0/3` and `Fa0/4` are assigned to VLAN 20. The command `show vlan` is used again to verify that the ports have been correctly assigned to their respective VLANs.

Step Five: Configuring Management VLAN

The switch's management VLAN is then configured. Instead of using the default VLAN 1 (which is considered insecure), VLAN 99 is configured for management purposes. The interface for VLAN 99 is configured with an IP address of `192.168.3.1` and a subnet mask of `255.255.255.0`, and the interface is activated using the `no shutdown` command. This IP address allows the switch to be accessed remotely for management tasks.

Step Six: Testing Connectivity

Finally, the connectivity between the devices is tested. Using the command `ping`, PC0 tests communication with other devices in the same VLAN, such as PC1 (`192.168.1.3`), and also with devices in different VLANs, like PC3 (`192.168.2.3`). The expected result is that devices within the same VLAN should be able to communicate, while communication between devices in different VLANs will not occur without additional routing configurations.

Step Seven: Saving Configuration

After the VLAN configurations are completed and tested, the final step is to save the configuration to prevent the changes from being lost when the switch is rebooted. The `write` command is used to save the configuration.

Inter-Switch (Cross-Switch) VLAN Configuration

In a cross-switch VLAN configuration, we configure switches so that devices in different physical locations but on the same VLAN can communicate. The concept of trunk ports is essential in this scenario, where the switchport mode is set to trunk, allowing multiple VLANs to pass through a single port, also known as a trunk link. This setup ensures that VLAN traffic is carried across multiple switches, allowing devices on the same VLAN to communicate even if they are physically connected to different switches.

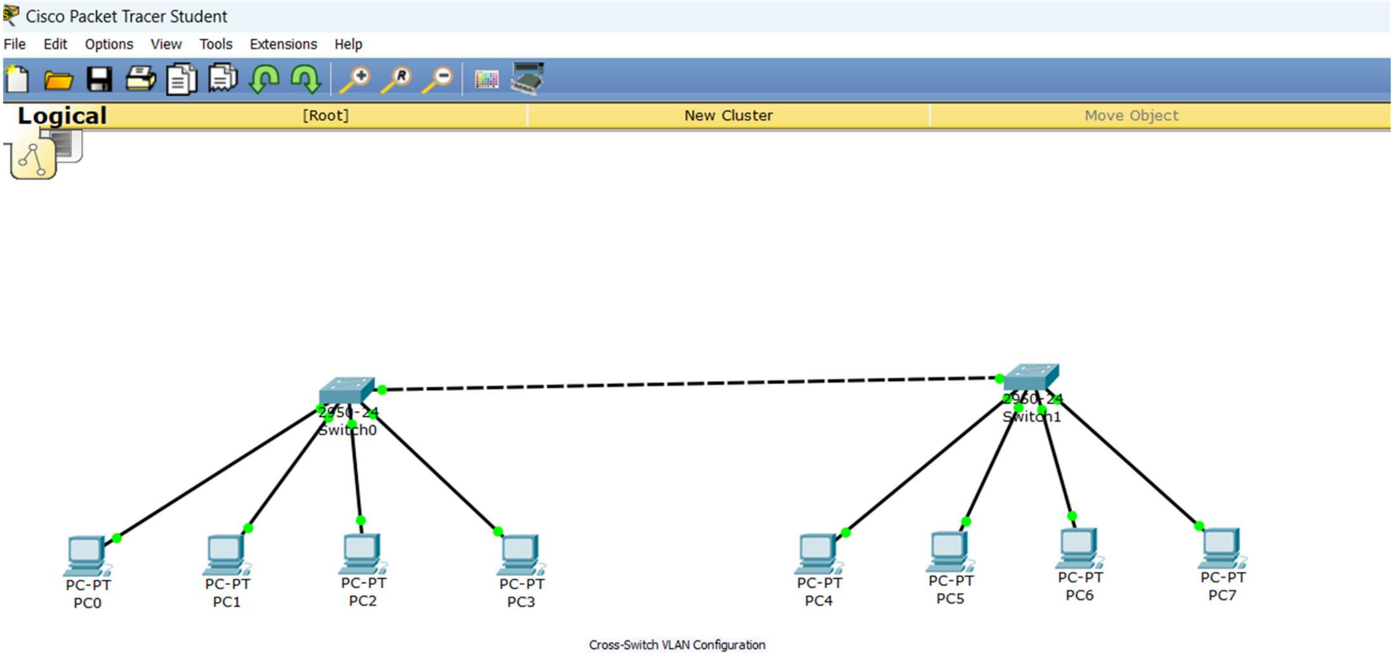


Fig-8: *Inter-Switch (Cross-Switch) VLAN Configuration Interface*

- **Experimental Process**

Step 1: VLAN Configuration

First, we configure both switches (S1 and S2) to include VLAN 10 and VLAN 20. On each switch, ports are assigned to the respective VLANs. For example, on S1, ports F0/1 and F0/2 are moved to VLAN 10, while F0/3 and F0/4 are assigned to VLAN 20. The same configuration is applied to Switch S2.

Step 2: Configuring Trunk Links

To allow VLAN traffic to pass between switches, we configure port F0/24 on both switches as trunk ports. On

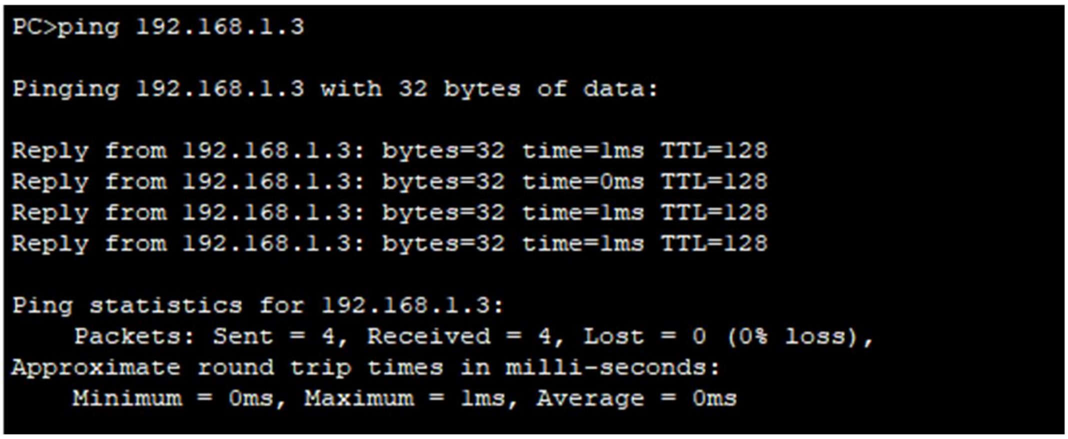
S1, the command *switchport mode trunk* is used, and VLANs 10 and 20 are allowed to pass through with *switchport trunk allowed vlan 10,20*. Similarly, on S2, port F0/24 is set to trunk mode, with *switchport trunk encapsulation dot1q* enabling IEEE 802.1Q frame encapsulation, allowing multiple VLANs to be transmitted. Both switches' trunk ports are brought up with the *no shutdown* command.

Step 3: Testing Connectivity

Finally, connectivity is tested by pinging devices across switches. For example, PC0 on Switch S1 pings PC4 on Switch S2 (same VLAN 10), and PC2 pings PC6 (same VLAN 20). Devices in the same VLAN should be able to communicate successfully. If successful, it confirms that VLANs are correctly configured and trunking is properly set up between the switches.

5. Lab Results and Analysis

First Result:

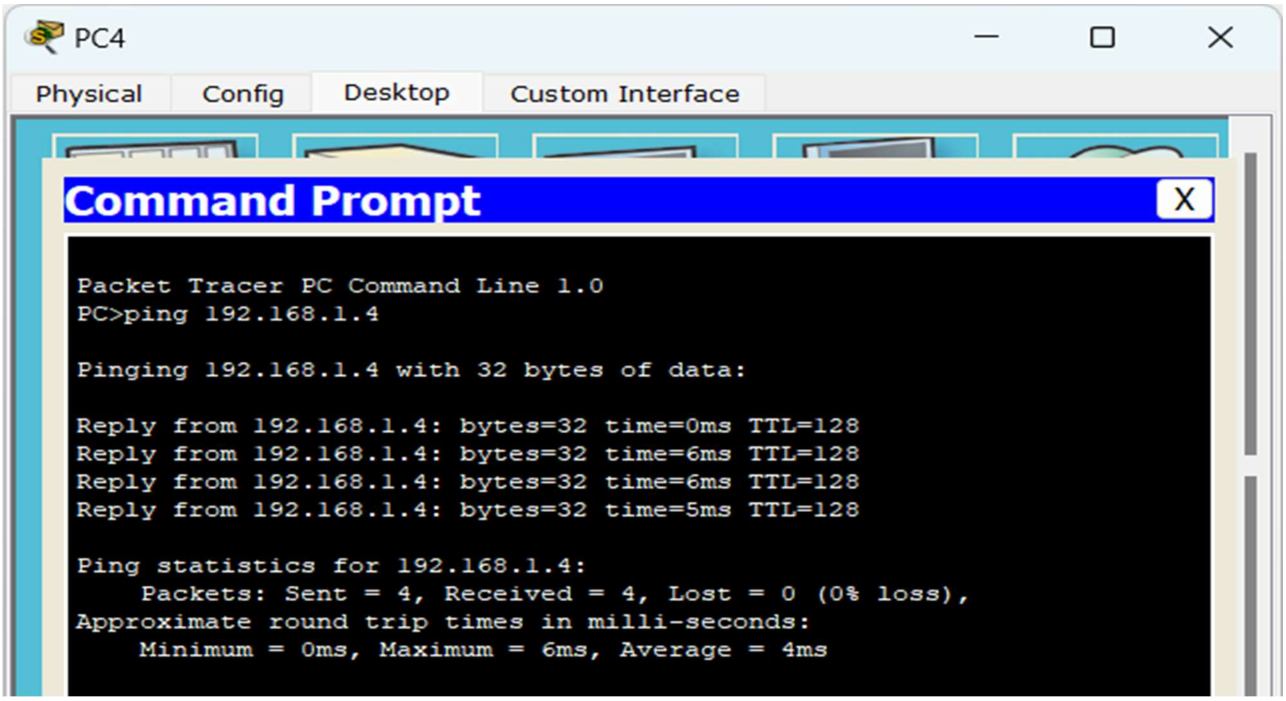


```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fig-9: *Ping to 192.168.1.3*

1. Four packets were sent and received successfully, indicating no packet loss (0% loss).
2. The round-trip time for the pings was minimal, with a recorded minimum, maximum, and average time of 0 ms.
3. The TTL (Time to Live) value is 128, which is typical for Windows-based systems.
4. This indicates that the device at 192.168.1.3 is reachable and on the same network with minimal latency.

Second Result:



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=6ms TTL=128
Reply from 192.168.1.4: bytes=32 time=6ms TTL=128
Reply from 192.168.1.4: bytes=32 time=5ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 4ms
```

Fig-10: *Ping to 192.168.1.4*

1. Similar to the first result, all four packets were sent and received successfully, with no packet loss (0%).
2. The round-trip times varied slightly, ranging between 0 ms (minimum) and 6 ms (maximum), with an average of 4 ms.
3. The TTL value remains at 128, suggesting the device is on the same or a directly reachable network.
4. The slight variation in ping times could be due to a minor difference in network paths or processing delays at the target device.

The results confirm successful connectivity between the devices configured within the VLAN environment. The absence of packet loss and minimal latency indicate proper VLAN segmentation and routing, ensuring that the devices communicate effectively. The slight variation in response time for 192.168.1.4 suggests possible network or device-level delays but does not indicate any significant issue. This validates that the VLAN configuration is functioning as intended, supporting seamless communication between devices.

三、Lab Summary

In this lab, we studied the process of configuring VLANs (Virtual Local Area Networks) on Cisco switches and enabling communication between VLANs across multiple switches. The primary focus was on creating two VLANs, VLAN 10 for management and VLAN 20 for guest users, and assigning specific switch ports to these VLANs. Initially, on Switch S1, ports F0/1 and F0/2 were assigned to VLAN 10, while ports F0/3 and F0/4 were moved to VLAN 20. The same configuration was mirrored on Switch S2 to ensure proper segmentation of network traffic. Once the VLANs were configured, we enabled trunking on the interconnecting ports (F0/24) of both switches to allow multiple VLAN traffic to pass between the switches. By setting these ports to trunk mode and specifying the allowed VLANs, we facilitated communication between devices in different VLANs across the switches. The experiment further involved verifying the configuration using the `show vlan` and `show interfaces trunk` commands to ensure that the VLANs were correctly set up and that trunking was enabled. To test connectivity, we performed ping tests from devices in different VLANs (PCO in VLAN 10 pinging PC4 in VLAN 10 and PCI in VLAN 20 pinging PC6 in VLAN 20) across the two switches. The successful responses confirmed that the trunk ports were functioning correctly and that devices in different VLANs were able to communicate via the trunked link.

This lab strengthened the importance of trunk ports in allowing multiple VLANs to communicate across switches and demonstrated how to configure VLANs, assign ports to VLANs, and implement trunking to ensure proper network segmentation and connectivity. The ability to properly configure VLANs and trunking is a fundamental skill in managing scalable and secure networks, ensuring that different departments or user groups are logically separated but can still communicate when needed.