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

Basic Configuration Experiment of Switches

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 06 日

一、Relate Knowledge

1. Introduction of the Basic Knowledge Required

To complete this lab, the basic knowledge required is how to set up network switches using Cisco commands. Cisco switches are important tools that help control network traffic by connecting different devices in a network. Some important ideas to understand are *VLANs (Virtual Local Area Networks),* which divide a network into smaller, logical parts for better control and security. Also, configuring individual *switch ports* is important for connecting devices to the network. Security measures, like setting passwords for local and remote access, are essential to keep the switch safe from unauthorized access. Lastly, the *Network Time Protocol (NTP)* is used to make sure the switch's clock matches a network time server, which helps with accurate timestamps for logs and other time-sensitive tasks. These concepts are key for managing and securing network systems effectively.

2. Lab Principle

The goal of this lab is to get hands-on experience with setting up switches with basic security features. This involves:

- Accessing the Switch: Connecting to the switch through its console port and using the command-line interface (CLI).
- Naming the Switch: Giving the switch a unique name to help identify it on the network.
- Setting Passwords: Creating passwords for accessing the switch locally and remotely via Telnet.
- Encrypting Passwords: Turning on password encryption to make it more secure by hiding the passwords.
- Saving the Setup: Making sure the switch keeps its settings after a restart by saving them in the startup-config.

By doing these steps, network managers can make sure the switch is set up securely and works properly.

3. Lab Steps

Accessing the Switch	Connect to the switch via the console port using terminal emulation software.
Host Name Configuration	Set the switch’s hostname to identify it within the network.
Password Configuration	Set up passwords for console and VTY (remote access).
Password Encryption	Enable encryption for all passwords on the switch.
Setting the Time	Configure the time on the switch to synchronize with the NTP server.
Saving Configuration	Save the running configuration to ensure it persists after reboot.

二、Lab Report

1. Lab Objective and Requirements

The goal of this lab is to understand how to configure and secure a Cisco switch using various basic commands. The specific tasks include configuring the switch hostname, setting up console and Telnet passwords, enabling password encryption, and ensuring that the configuration persists after a reboot. The requirements for completing the lab include:

- Cisco Packet Tracer or physical Cisco switch
- Console connection to the switch
- Basic understanding of Cisco commands

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

Connection: Console port (using terminal emulation software for CLI access)

3. Lab Design

The lab was designed to allow users to configure a Cisco switch from scratch. The switch started with a default configuration, and through a series of steps, the switch was configured with a custom hostname, passwords, and security features. The design of the lab followed a straightforward approach where each configuration step built upon the previous one. The steps include configuring basic features like the hostname, setting up passwords, and ensuring security by encrypting those passwords.

4. Lab Process and Recording

The basic configuration of switches involves several key commands to ensure proper functionality, security, and management within a network. One of the foundational tasks is configuring switch ports. Individual ports can be selected using the interface command, for example, Switch(config)# interface fastethernet 0/10, to specify a particular port. For managing multiple ports simultaneously, the range command is used, such as Switch(config-if)# range fastethernet 0/1 - 24. Additional commands like Switch(config-if)# speed 100 and Switch(config-if)# duplex full allow for configuring port speed and duplex mode, ensuring optimal performance. The Switch(config-if)# negotiation auto command enables automatic negotiation of port settings where applicable.

Another essential aspect is configuring the switch's address. To set an IP address on the VLAN interface, the interface vlan 1 command is used, followed by ip address [IP address] [subnet mask] to assign the desired IP and subnet mask. The no shutdown command activates the interface. These configurations ensure the switch can be managed remotely and integrated into the network effectively.

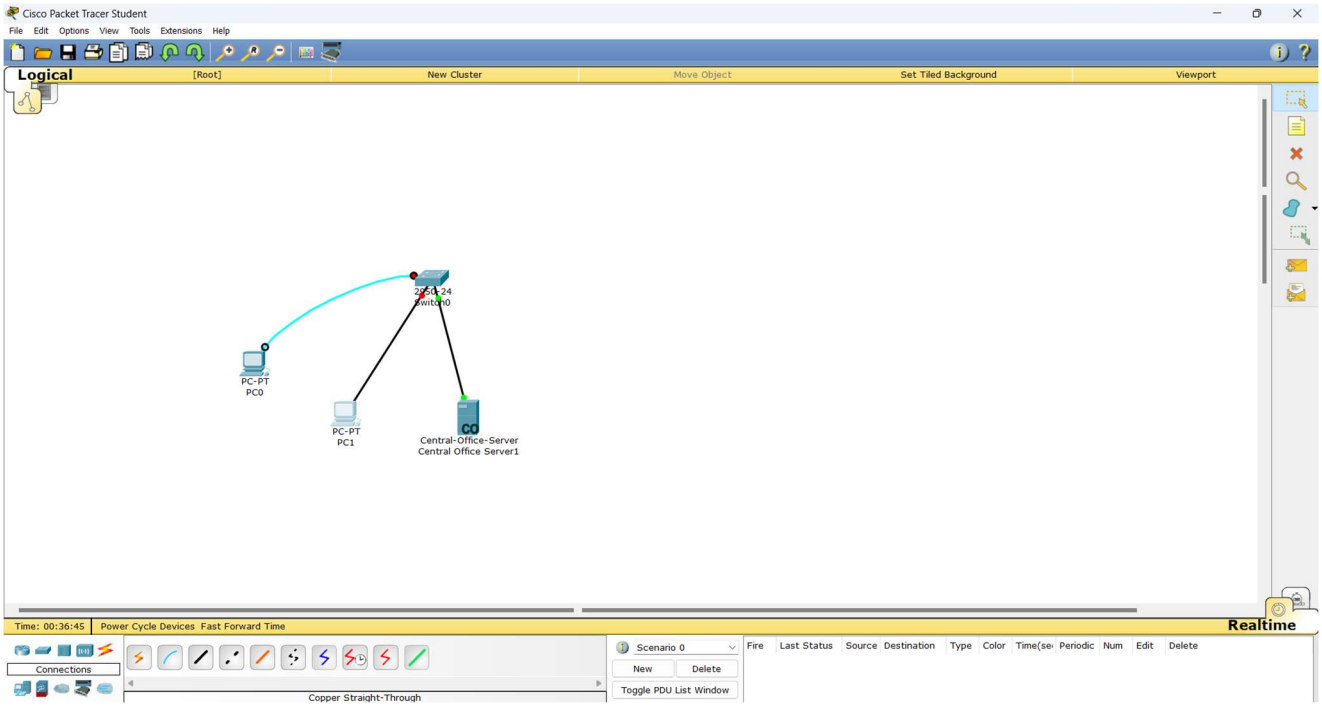

Fig-1: *Cisco Packet Tracer network simulation showing two PCs connected to a switch, which is linked to a central office server.*

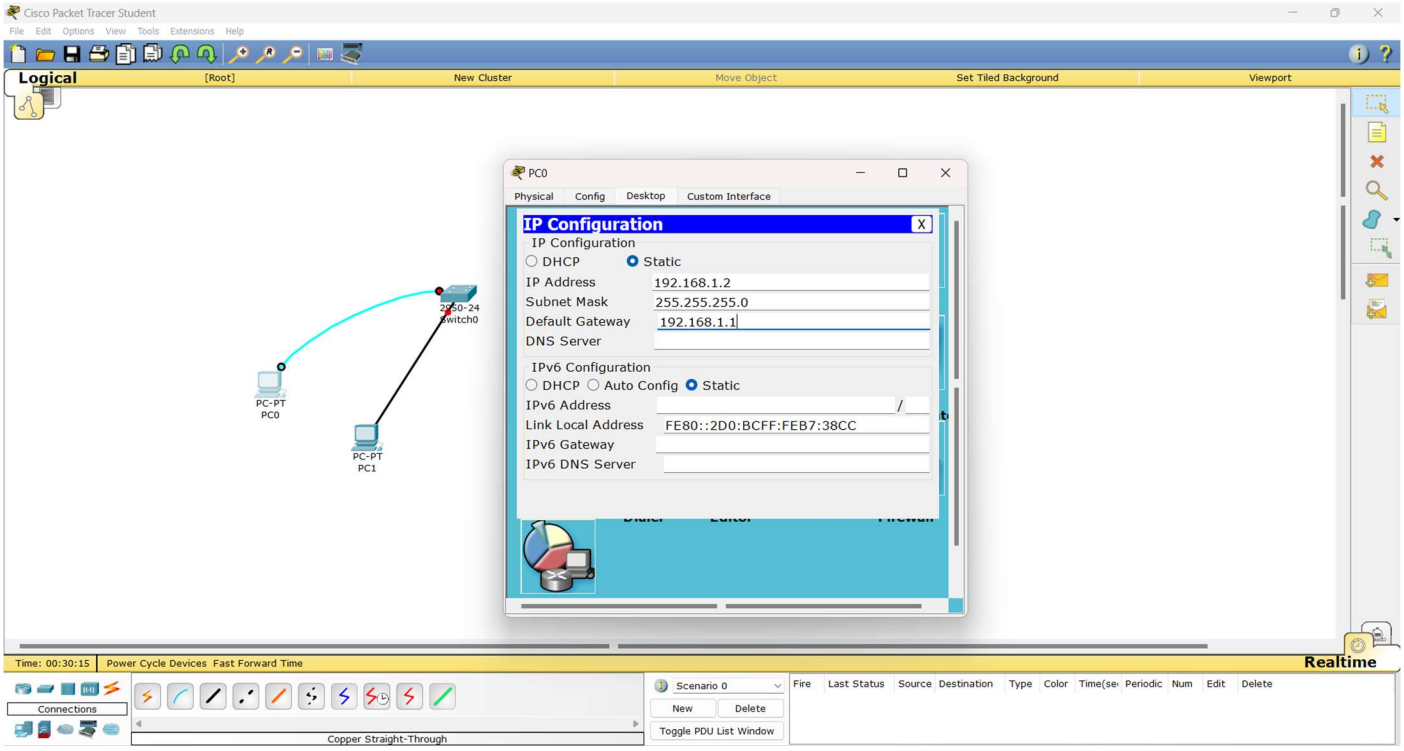

Fig-2: IP Configuration

Common management commands play a significant role in ensuring switch accessibility and security. Setting the device's time and date using `Switch(config)# clock set [time] [date]` and configuring the hostname with `Switch(config)# hostname [switch-name]` provide basic administrative setup. Security can be enhanced by configuring passwords, such as the enable password with `Switch(config)# enable password [password]` and console access passwords through `Switch(config)# line console 0` followed by the `password` and `login` commands. Finally, maintaining and managing switch configurations is critical for long-term network stability. The running configuration should be saved to the startup configuration using `Switch# copy running-config startup-config`, ensuring that settings persist across reboots. If necessary, previously saved configurations can be cleared with `Switch(config)# erase startup-config`. These commands collectively form the foundation of basic switch configuration, enabling efficient and secure network operations.

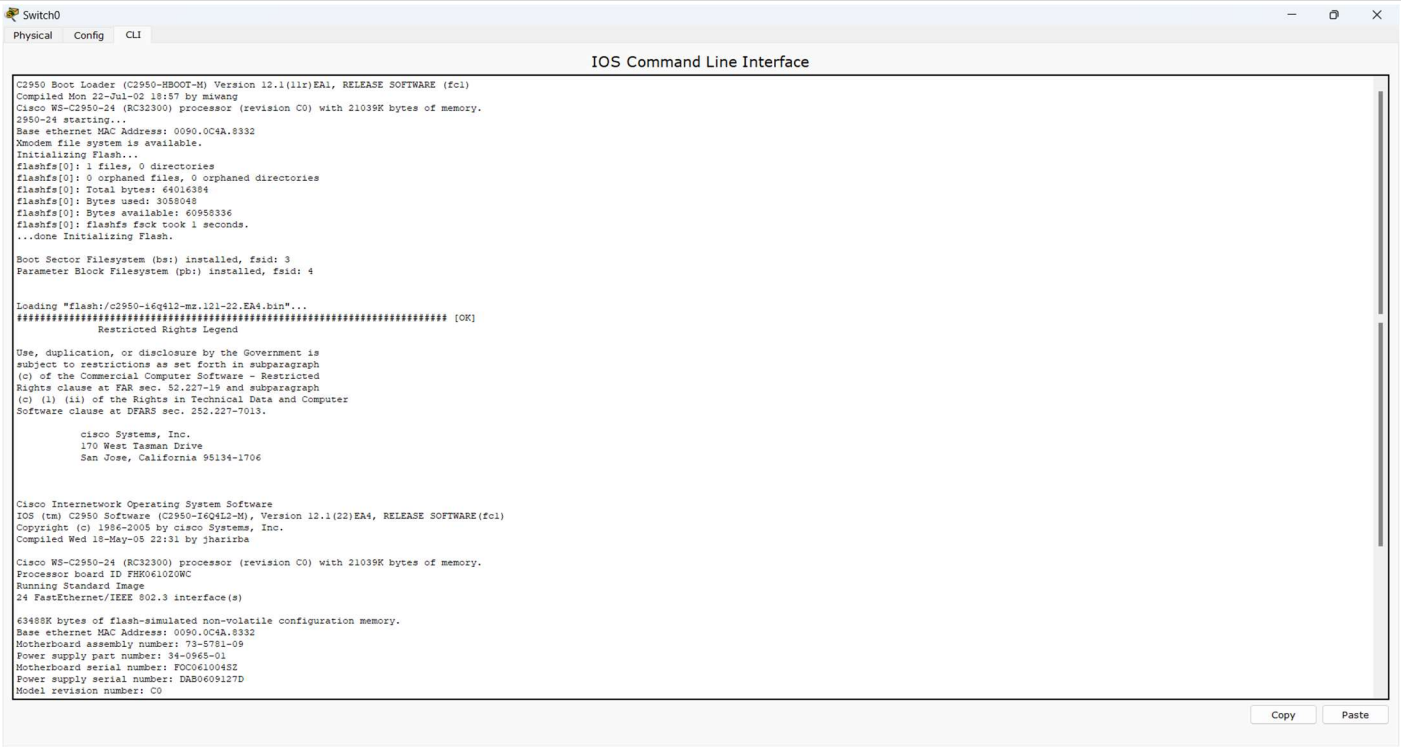

Fig-3: Command Line Interface

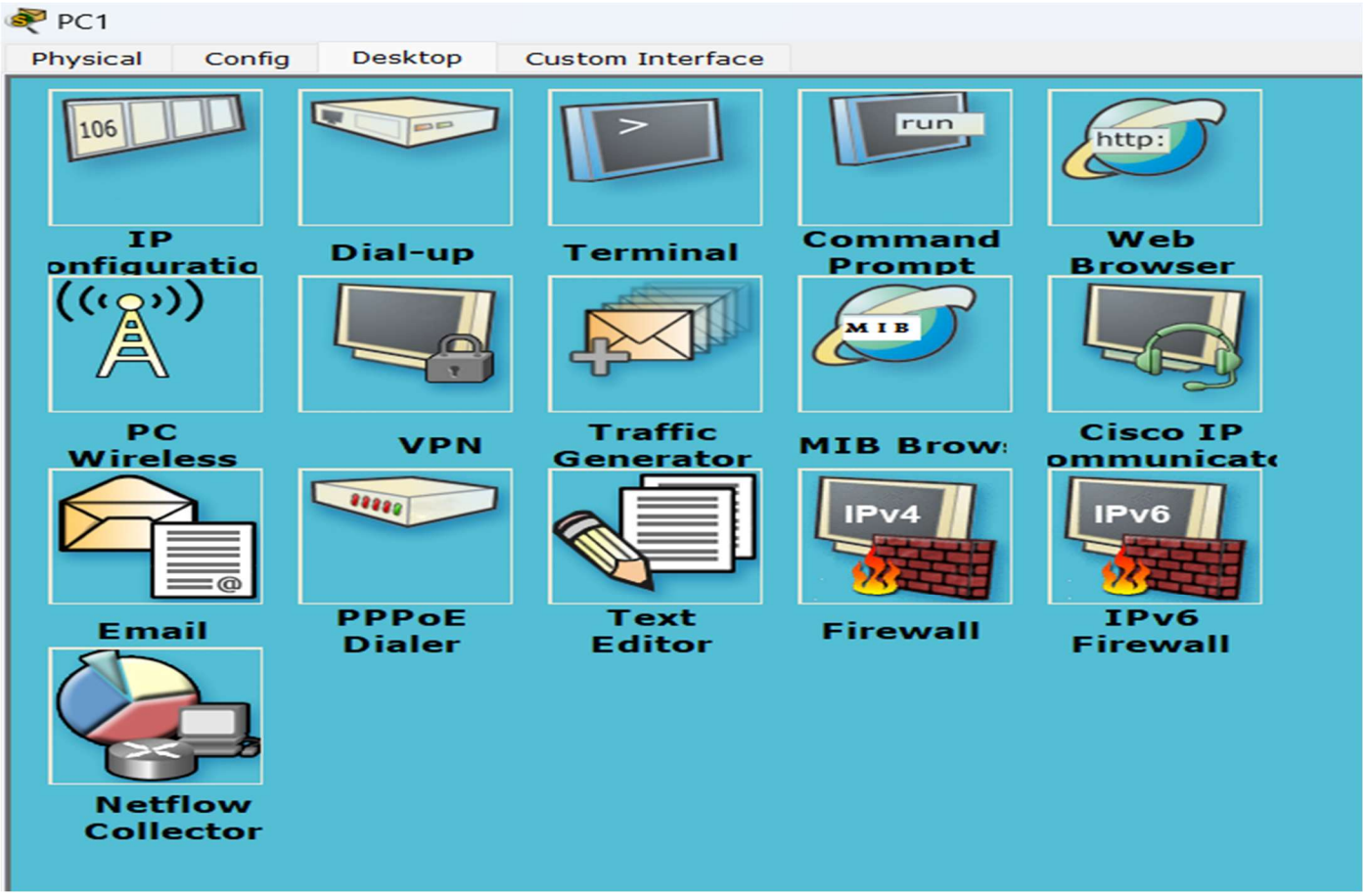

Fig-4: Desktop Interface

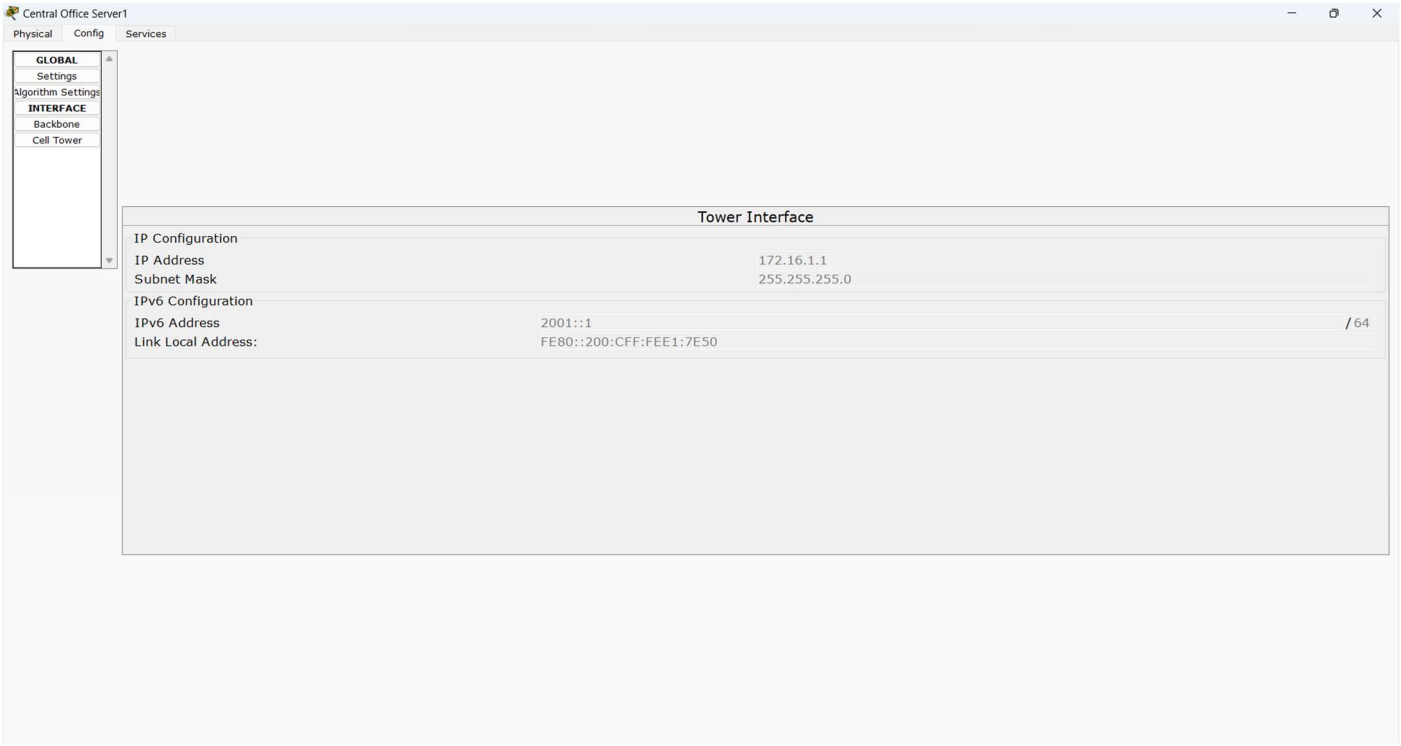

Fig-5: Server – Tower Interface

5. Lab Results and Analysis

The lab successfully demonstrated the process of configuring a Cisco switch using basic commands. The switch's hostname was changed to ***LabSwitch***, providing a unique identifier within the network. Security features were implemented by setting console and Telnet passwords, ensuring that only authorized users could access the device locally or remotely. The passwords were encrypted using the service password-encryption command, preventing plain-text passwords from being visible in the configuration file. Additionally, a ***Message of the Day (MOTD)*** banner was configured to display a security warning, which appeared correctly upon login attempts, reinforcing the importance of compliance and security awareness. The configuration changes were verified and saved using the copy running-config startup-config command, ensuring that all settings persisted after the device was rebooted.

The lab's outcome highlights the importance of properly securing network devices during initial setup. Each configuration step was performed accurately, and the results were consistent with the objectives, reflecting a practical understanding of managing and securing Cisco switches. The analysis confirms the successful implementation of key security and configuration practices necessary for effective network management.

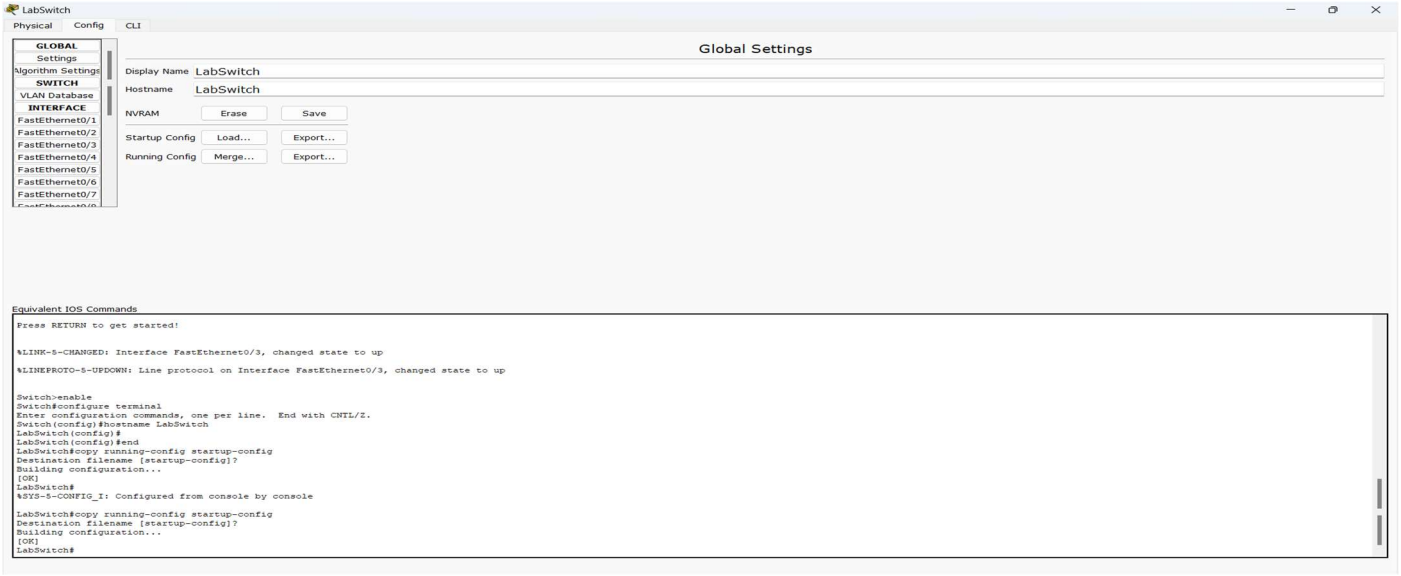

Fig-6: LabSwitch Commands

三、Lab Summary

This lab involved setting up a Cisco switch using basic commands, which helped me understand how to configure and secure switches. The main tasks were renaming the switch, setting passwords for local and remote access, encrypting these passwords, and creating a warning message for unauthorized users. These settings were saved so they would stay in place after restarting the switch, showing how important it is to keep configurations stable in network management.

The lab highlighted the importance of basic switch settings in protecting and managing network systems. By doing this lab, I learned how to use the Cisco command-line interface (CLI) and apply key security steps to keep the network safe from unauthorized access. This experience improved my technical abilities and taught me important security and management practices, which are crucial for real-world networking situations.