# **Network Switch Configuration Report**

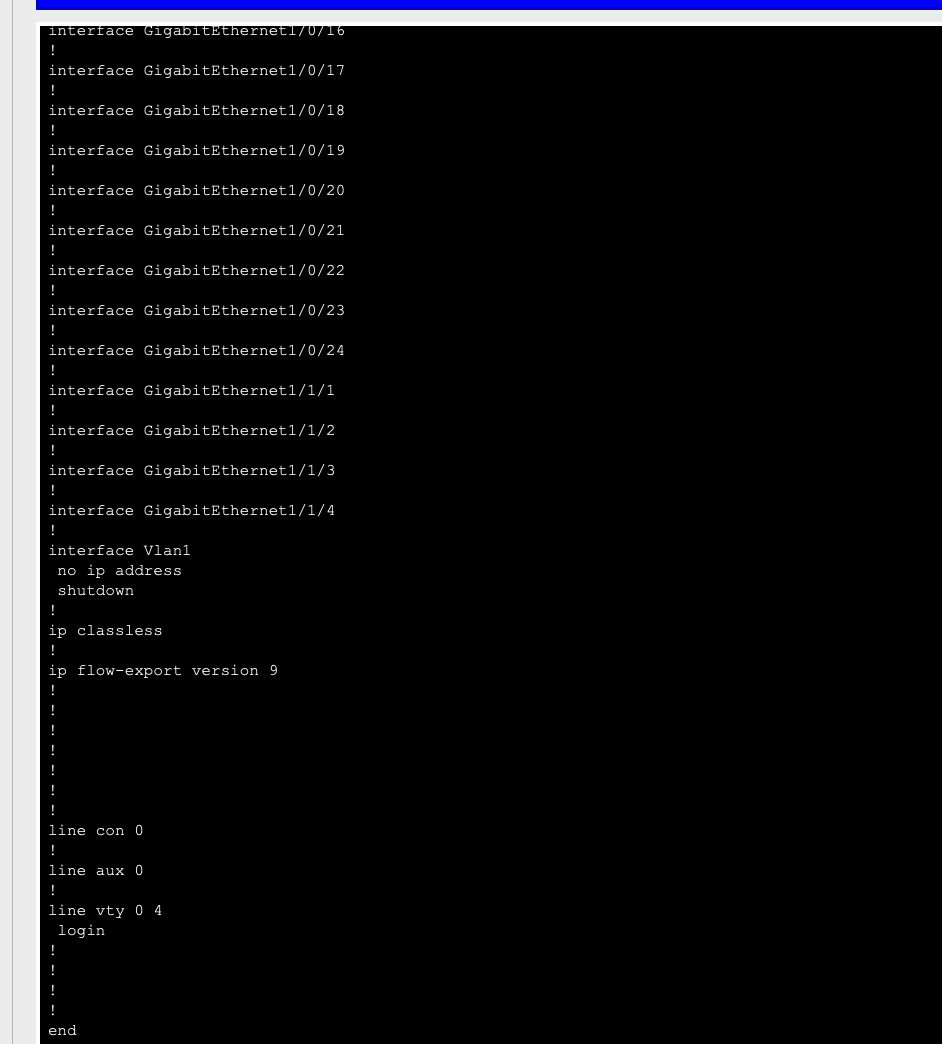
**SAPARBEK IMANZHUSIP SE-2226**

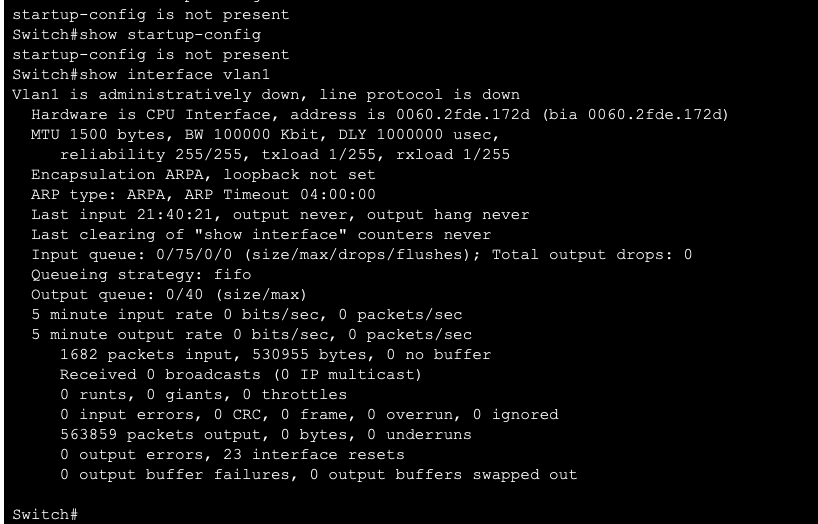
## **Introduction**

This report summarizes the configuration and management of a Cisco network switch (S1) as part of a lab activity. The objective was to establish a basic switch configuration, implement security measures, verify connectivity, and test remote management capabilities.

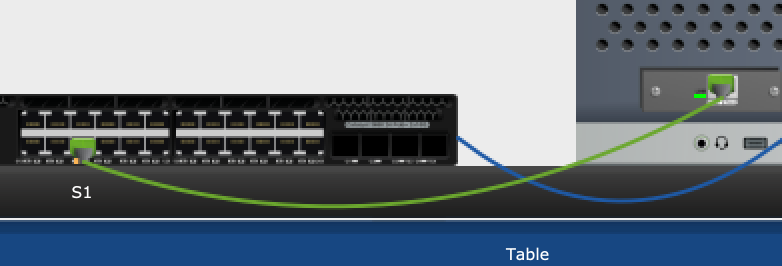
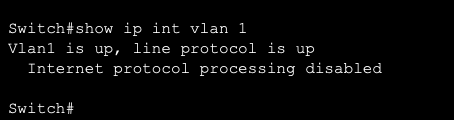
## **Configuration Overview**

During the configuration process, the following tasks were accomplished:

**Cabling the Network:**

A console cable was connected from device PC-A to switch S1 to establish an initial connection for configuration.

**Verifying Default Switch Configuration:**

The default settings of the switch were examined, including interface properties and VLAN information.

The command show running-config was used to display the current configuration, revealing the number of GigabitEthernet interfaces and the range of values for vty lines.

**Basic Switch Settings Configuration:**

Basic settings were configured, including hostname, service password encryption, and a banner message.

The management VLAN was changed from the default VLAN 1 to VLAN 99 to enhance security.

**Assigning IP Address and Default Gateway:**

An IP address was assigned to VLAN 99, and the default gateway was configured to facilitate remote management.

**Testing Connectivity:**

End-to-end connectivity was verified using ping tests to ensure PC-A could communicate with S1 over both IPv4 and IPv6.

**Remote Management:**

Telnet was used to access the switch remotely, confirming the successful configuration of virtual terminal lines and the ability to manage the switch from a different device.

## **Reflection Questions**

### **1. Why should you configure the vty password for the switch?**

Configuring the vty (virtual terminal) password is essential for securing remote access to the switch. Without a vty password, anyone on the network can attempt to access the switch using Telnet or SSH, which poses a significant security risk. By setting a vty password, you can restrict access to authorized users only, thus preventing unauthorized configuration changes and protecting the integrity of the network device.

### **2. Why change the default VLAN 1 to a different VLAN number?**

Changing the default VLAN from VLAN 1 to a different VLAN number enhances security. VLAN 1 is the default VLAN for all Cisco switches and is often a target for attacks. By moving management traffic to a different VLAN, such as VLAN 99, you reduce the risk of potential vulnerabilities associated with default configurations. This practice helps in obscuring the management traffic and makes it more difficult for unauthorized users to access the management interface of the switch.

### **3. How can you prevent passwords from being sent in plaintext?**

To prevent passwords from being sent in plaintext, you can enable encryption for passwords within the switch configuration. Cisco devices allow you to configure the following options:

* **Enable service password-encryption:** This command encrypts all plaintext passwords stored in the configuration file, making them unreadable if someone accesses the configuration.
* **Use SSH instead of Telnet:** SSH (Secure Shell) is a secure protocol that encrypts all data sent over the network, including usernames and passwords. This prevents eavesdroppers from capturing sensitive information during transmission.
* **Implement strong password policies:** Using complex passwords that are difficult to guess adds an extra layer of security, even if encrypted passwords are somehow compromised.

## **Conclusion**

The successful configuration and management of the switch demonstrate the importance of implementing security measures and verifying connectivity in a network environment. By configuring basic settings, changing the default VLAN, and securing access through passwords and encryption, the integrity and security of the network can be significantly improved.