ACTIVITY 2

WORKSHOP WEEK 2 - BASIC SWITCH SETUP AND TELNET CONFIGURATION

INTRODUCTION

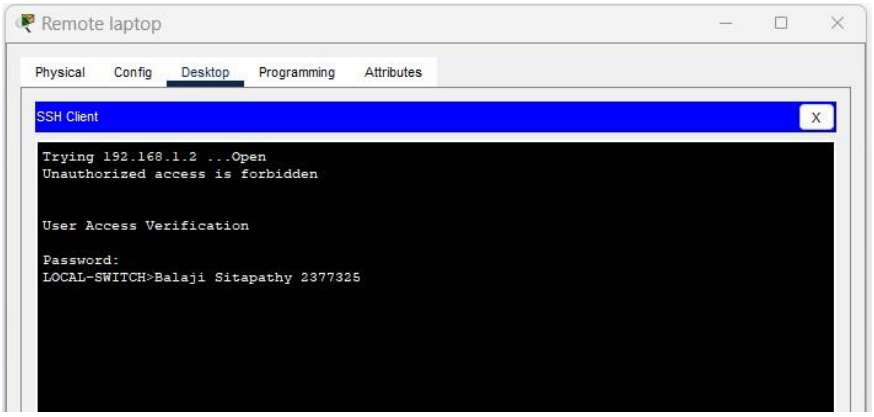
In this assessment, I undertook the task of configuring a Cisco switch from scratch using Cisco Packet Tracer. The primary goal was to set up the switch and enable remote management through Telnet. This process is crucial for ensuring a secure and efficient network setup within an enterprise environment. Through this activity, I gained hands-on experience in using command-line interface (CLI) commands to configure network devices and secure access to them.

ACTIVITY OVERVIEW

The assessment involved several key steps to configure the switch, which I performed as follows:

1. *Changing the Switch Hostname:*
   I began by assigning a unique hostname, LOCAL-SWITCH, to the switch. This step was necessary to identify the switch within the network and make it easier to manage.

2. *Setting a Message of the Day (MOTD):*
   Next, I configured a message of the day that displays a warning whenever someone attempts to access the switch. The message "Unauthorized access is forbidden" was set to deter unauthorized users from attempting to access the switch.



Picture 1 – Warning message display

3. *Configuring a Privileged Mode Password:*
   To secure the privileged EXEC mode, I set up a password (cisco) and encrypted it using the MD5 algorithm. This ensures that the password is stored securely, preventing unauthorized access to critical switch configurations.

4. *Setting Up Console Access:*
   I then configured console access by setting a password (ciscoconsole) for anyone attempting to access the switch via the console line. This step is vital for securing direct physical access to the switch's CLI.

5. *Configuring Telnet Access:*
   Remote management was enabled by configuring Telnet access on the switch. I set a Telnet password (ciscotelnet) and allowed remote connections through the switch's virtual terminal lines. This setup allows network administrators to manage the switch from remote locations.

6. *Assigning IP Address and Default Gateway:*
   To make the switch accessible over the network, I configured the IP address 192.168.1.2 and set the default gateway as 192.168.1.1. This configuration is essential for network communication and remote device access.

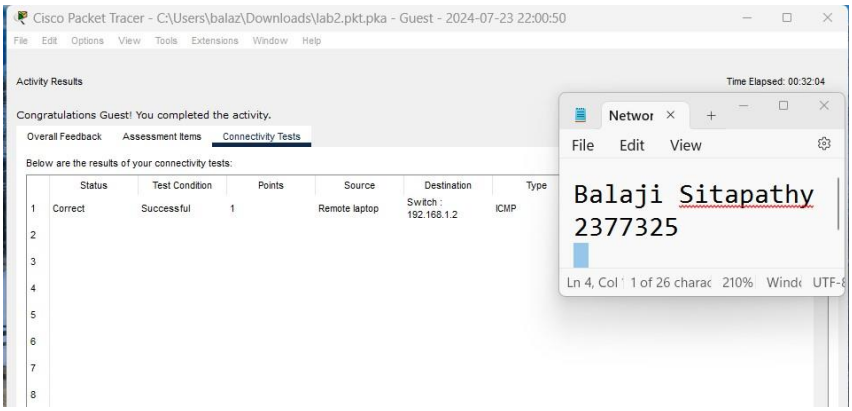
TESTING AND VERIFICATION

After completing the configuration, I tested the setup to ensure everything was functioning correctly:

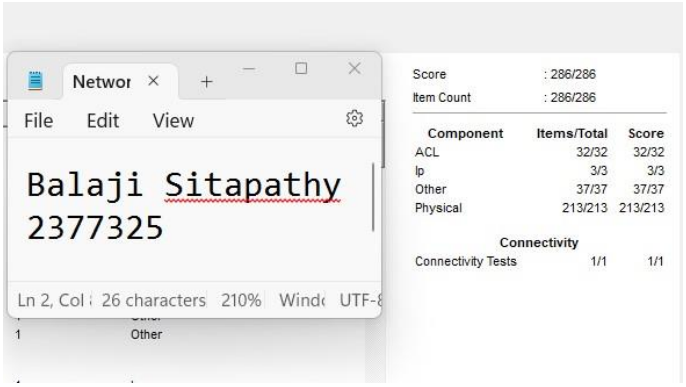
1. *Laptop IP Configuration:*
   I configured the IP settings on both the local and remote laptops. The remote laptop was set with an IP address of 172.16.1.2, while the local laptop connected directly to the switch was given 192.168.1.3.

2. *Telnet Connection:*
   I successfully established a Telnet connection from the remote laptop to the switch using the IP address 192.168.1.2. Upon connecting, I was prompted to enter the Telnet password (ciscotelnet), confirming that the configuration was successful.

3. *Connectivity Test:*



I used Packet Tracer's built-in connectivity tests to verify that all configurations were correct. The tests confirmed that the switch was set up properly, allowing for secure remote management and communication within the network.



CONCLUSION

Completing this assessment provided me with practical experience in configuring a Cisco switch and securing it for network deployment. By setting up the hostname, implementing security features, enabling Telnet access, and configuring basic network connectivity, I ensured that the switch was ready for use in a professional environment. This exercise reinforced my understanding of CLI commands and their application in real-world network management scenarios.