ACTIVITY 1

WORKSHOP WEEK 1 – BASIC ROUTER SETUP

In this workshop, I performed the initial configuration of a Cisco ISR router to secure administrative access, using Cisco Packet Tracer as the simulation environment. The exercise involved several critical tasks aimed at securing the router and ensuring proper management protocols are in place.

1. INITIAL SETUP AND CONNECTION

I began by configuring a laptop's terminal software to communicate with the router. This involved adjusting the terminal settings to 9600 baud rate, 8 data bits, no parity, and 1 stop bit. Establishing this connection was necessary to access the router's command line interface (CLI) for further configuration.

2. ROUTER HOSTNAME CONFIGURATION

Using the CLI, I changed the router's hostname to "GATEWAY." This is an essential step in network management, as it helps in identifying the router within the network, especially in environments with multiple devices.

3. SETTING ENABLE PASSWORD AND SECRET

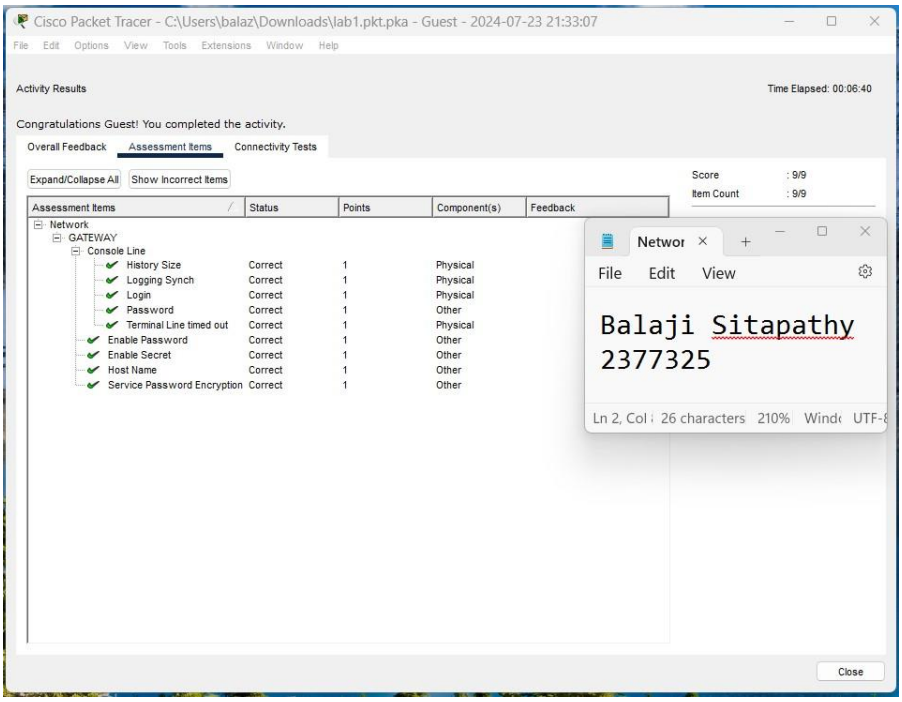
I configured both an enable password and an enable secret, setting both to "cisco." The enable password controls access to the router's privileged EXEC mode, while the enable secret provides an additional layer of security by storing the password as an MD5 hash. Despite the warning about using the same password for both, this configuration was done to meet the lab requirements.

4. ENABLING PASSWORD ENCRYPTION

To further secure the router, I enabled service password-encryption. This command encrypts all plain-text passwords on the router, ensuring that sensitive information is not easily exposed to unauthorized users. This step is crucial in maintaining the security of network credentials.

5. CONFIGURING CONSOLE ACCESS

I configured the router's console access to require a password ("cisco") and added features such as logging synchronous (to prevent command output from interrupting typed commands), setting the command history size, and defining a session timeout. These configurations ensure that only authorized users can access the router via the console port and that the session is managed securely.



SUMMARY

This workshop provided hands-on experience in securing a Cisco ISR router. By following a series of structured tasks, I configured the router's basic security settings, including hostname setup, enable password and secret creation, password encryption, and console access management. These steps are foundational in securing network devices and are crucial for maintaining the integrity and security of network infrastructure. The successful completion of these tasks was confirmed using the "Check Results" feature in Cisco Packet Tracer, with all steps verified as correct.