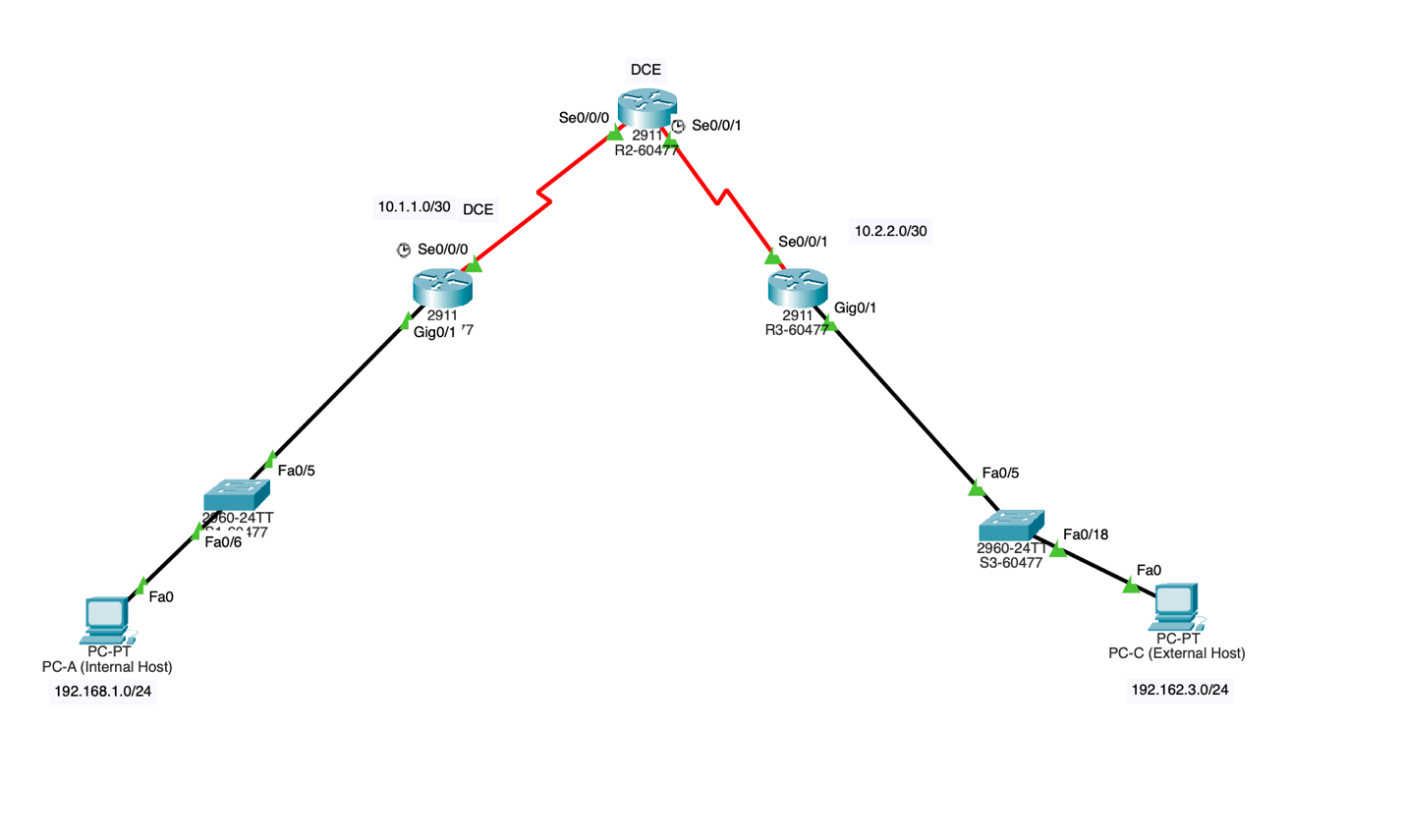
**Task 1: Configure Basic Device Settings**

**Configured on Tutorial 1**

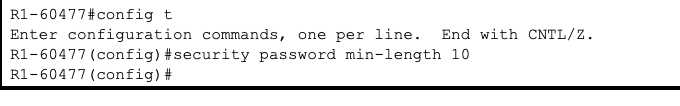


**Task2: Control Administrative Access for Routers**

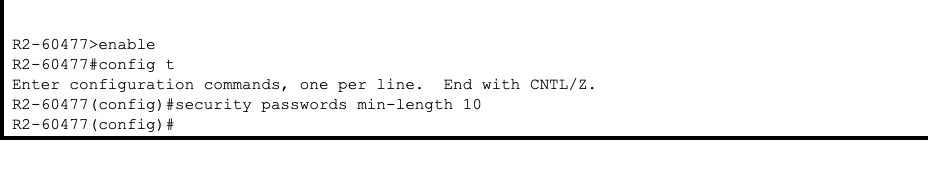
**Step 1: Configure and Encrypt Passwords on Routers R1-59585 and R3-59585.**

Configuring a minimum password length for the router passwords.

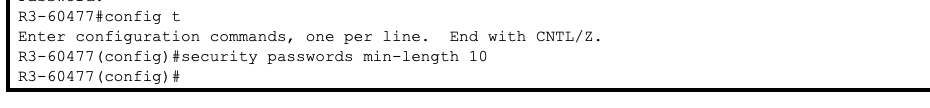
R1-60477:



R2-60477:

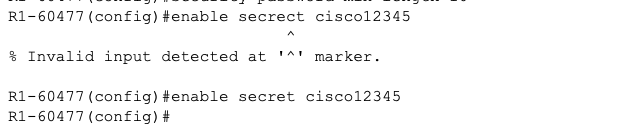


R3-60477:

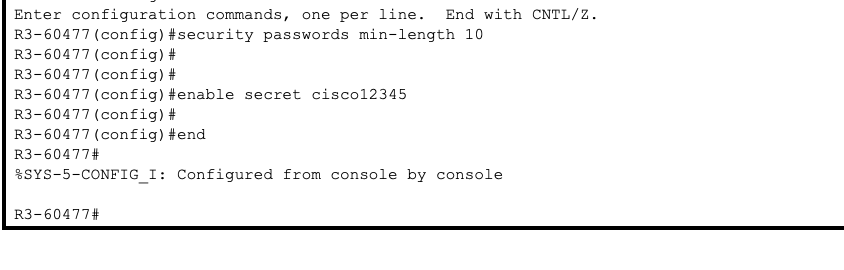


The enable secret password configured – cisco12345

R1-60477:

****

R3-60477:

****

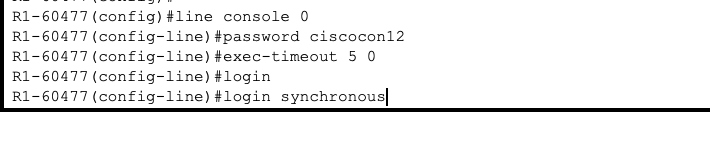
**How does configuring an enable secret password help to protect a router from being compromised by an attack?**

**Answer:**  
Configuring an enable secret password ensures the security of the router by requiring password authentication before granting privileged access in the EXEC environment. The password is stored in the configuration as an encrypted hash, rather than in plain text. This encryption makes it difficult for unauthorized individuals to retrieve the password, even if they gain access to the configuration file. As a result, this measure prevents unauthorized parties from taking full control of the router.

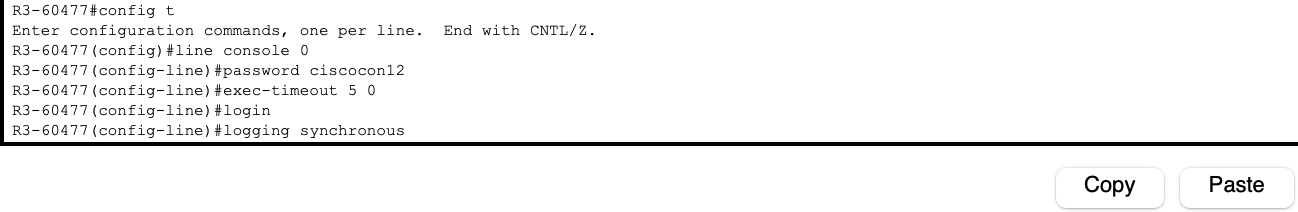
**Configuring basic console, auxiliary port, and virtual access lines.**

1. **Console**

R1-60477

****

R3-60477

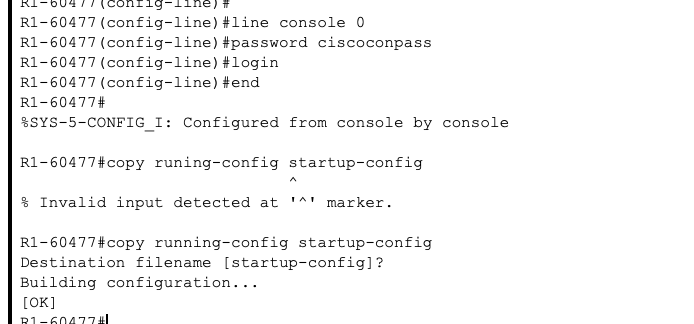
****

1. New password for console - cisconpass

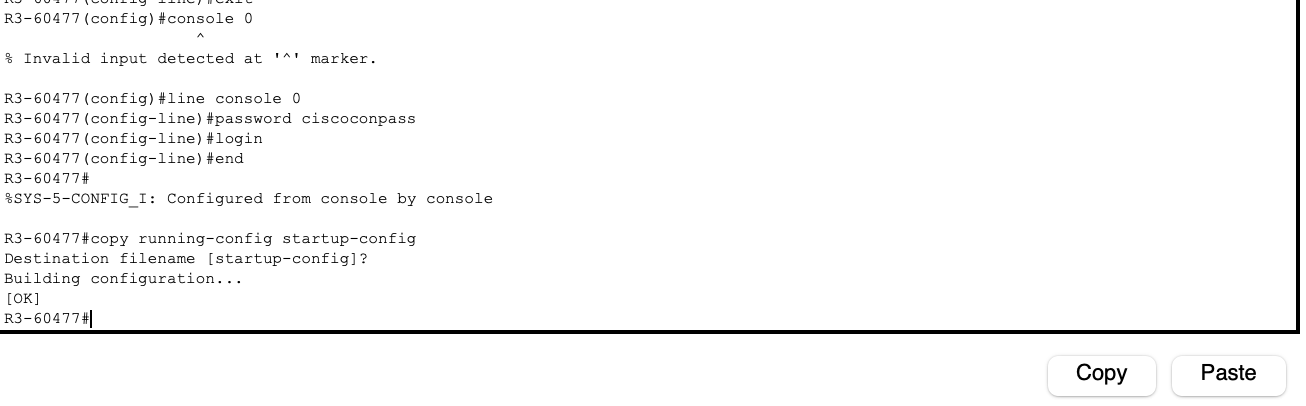
**When you configured the password for the console line, what message was displayed?**

**Answer:** When the console line password was configured, the router displayed the message: *Configured from console by console*

R1-60477

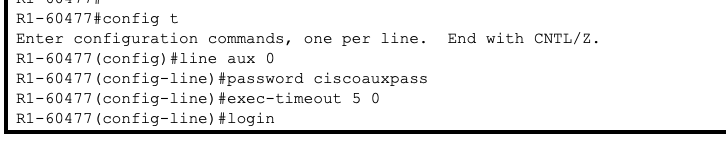
**

R3-60477

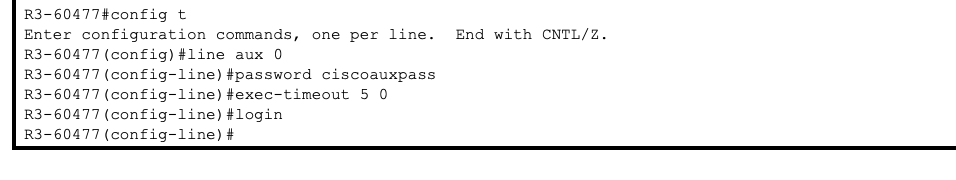
****

1. **Configuring password for the AUX port for router:**

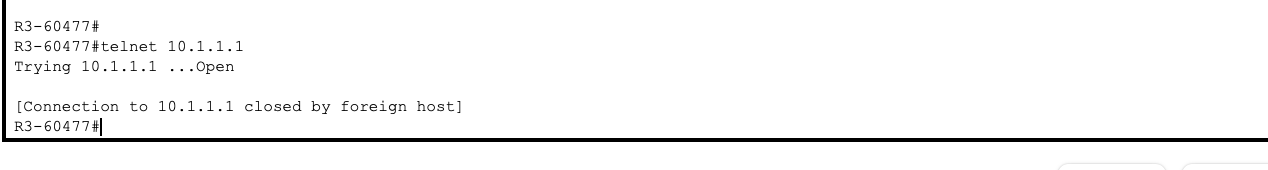
R1-60477

****

R3-60477

****

**d. Telnet from R2-60477 to R1-60477**

****

**Were you able to login? Explain.**

**Answer:**  
No, I was unable to log in. The Telnet connection was immediately terminated because the VTY lines on R1 were not configured with a password or a login command.

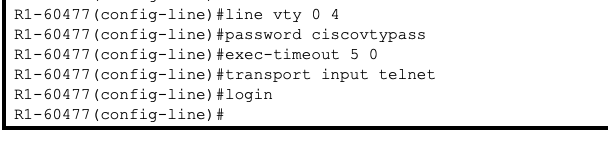
**What messages were displayed?**

**Answer:** The following message displayed:

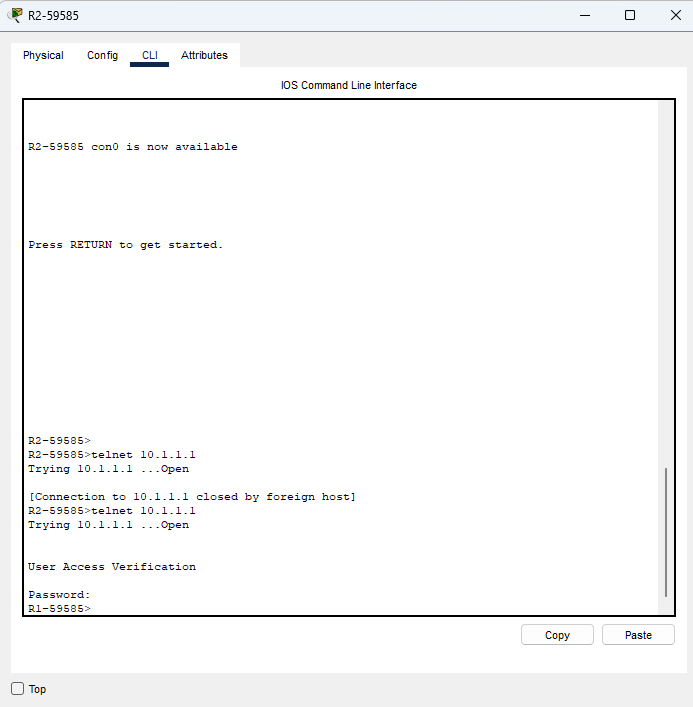
Trying 10.1.1.1 ... Open

[Connection to 10.1.1.1 closed by foreign host]

**Configuring password on the vty lines for router R1-59585**

****

**Telnet from R2-60477 to R1-60477 again. Were you able to login this time?**

**Answer:**  
Yes, I was able to log in this time. After configuring a password and enabling login on the VTY lines on R1, R2 successfully established a Telnet connection to R1. When attempting to connect to Telnet at 10.1.1.1, the password prompt appeared on the router. After entering the correct password, access to the user EXEC mode of R1 was granted.****

**Enter privileged EXEC mode and issue the show run command. Can you read the enable secret password? Explain.**

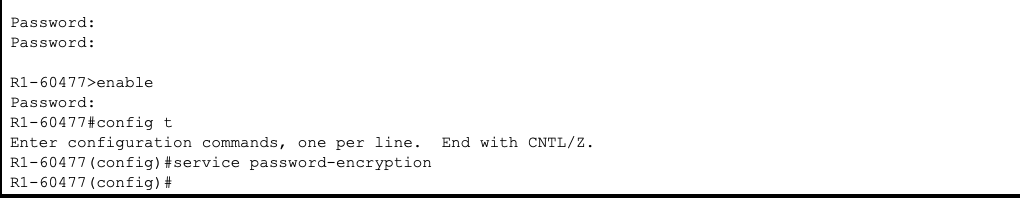
**Answer:**  
The enable secret password is stored in an encrypted format and cannot be viewed in plain text. In Packet Tracer, it appears as a 5 MD5 hash in the configuration. This ensures that even if someone accesses the running configuration, they cannot easily determine the actual password.

**Can you read the console, aux, and vty passwords? Explain.**

**Answer:**  
The line passwords are visible in the configuration, but they are encrypted using a weak Type 7 encryption when the service password-encryption command is applied. Unlike the enable secret password, Type 7 encryption is reversible, making it less secure.

**Encrypt clear text passwords.**

**a.**

****

**b. Issue the show run command. Can you read the console, aux, and vty passwords? Explain.**

- When the service password-encryption command is enabled, the passwords for the console, aux, and VTY lines are not shown in plain text. Instead, they appear as Cisco’s Type 7 encryption. While this obscures the passwords from casual viewers, the encryption is weak and can be easily decrypted if someone gains access to the configuration file.

**At what level (number) is the default enable secret password encrypted?**

* At Type 5

**At what level (number) are the other passwords encrypted?**

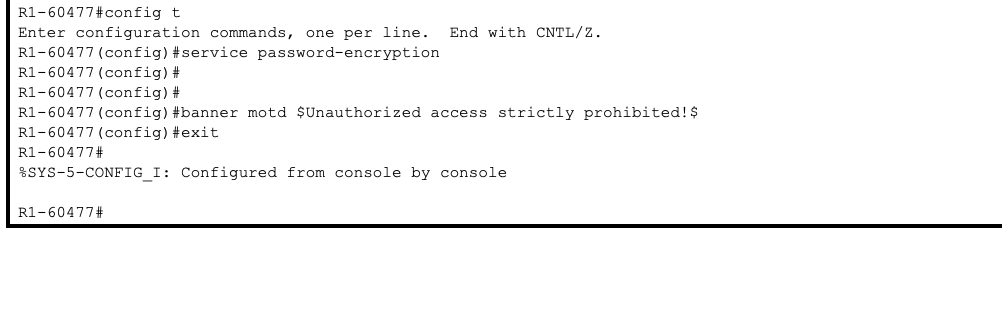
* At Type 7

**Which level of encryption is harder to crack and why?**

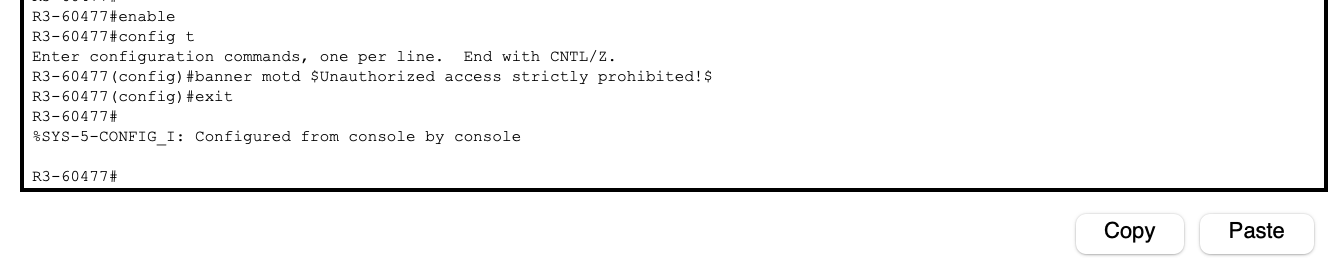
* The enable secret password, which uses MD5 or SCRYPT (Type 5 or Style 9) encryption, is significantly more secure as it employs a one-way hashing algorithm, making it difficult to reverse-engineer the original password. In contrast, Type 7 encryption is weak and easily reversible, making it vulnerable to attackers.

**Step 2: Configuring a Login Warning Banner on Routers R1-59585 and R3-59585.**

**R1-60477**

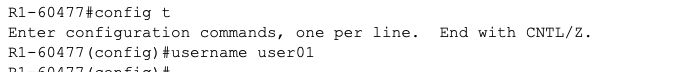
****

**R3-60477**

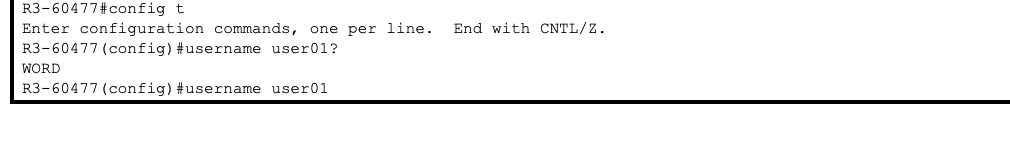
****

**Step 3: Configuring Enhanced Username Password Security on Routers R1-60477 and R3-60477.**

**R1-60477**

****

**R3-60477**

****

Question: What options are available?

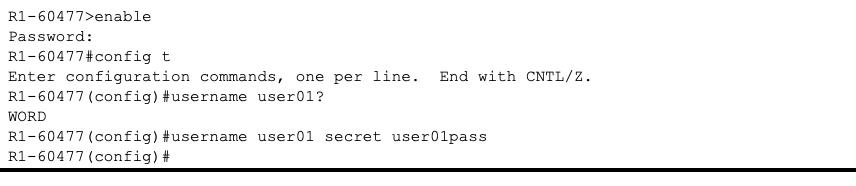
Answer:

**Password (Text):** The password is stored in plain text, which is weaker and can be decrypted using the password-encryption command.

**Recommended:** Use an encrypted password, preferably stored as a hash (e.g., MD5/Type 5 or SCRYPT/Type 9).

**Privilege:** Assign an access level ranging from 0 to 15, with 15 providing full administrative privileges.

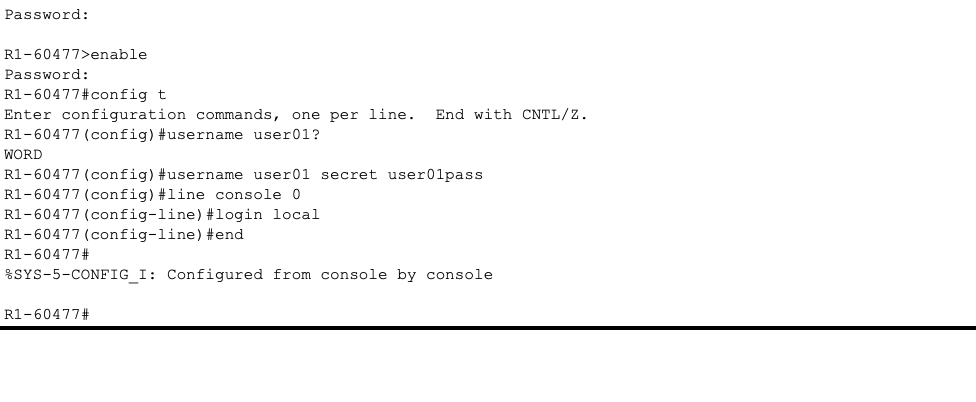
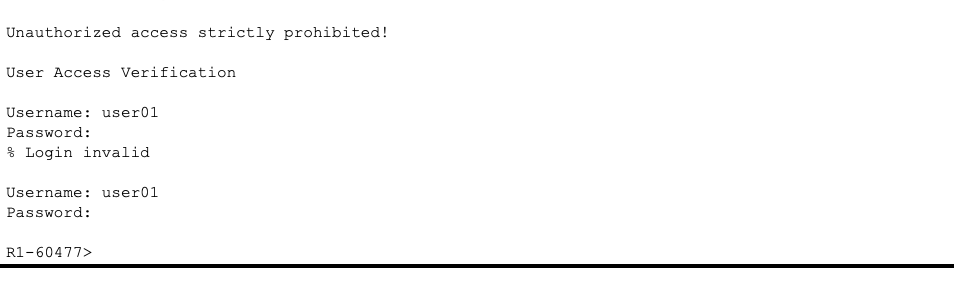
**Creating a new user account with a secret password.**



**Display the running configuration. Which hashing method is used for the password?**

**Answer:**  
The running configuration stores the password as an MD5 hash (Type 5). As a result, the actual password is not displayed in plain text, but rather as an MD5 hash.

**Testing the new account by logging in to the console.**



**What is the difference between logging in at the console now and previously?**

**Answer:** Previously, access to the console was secured by a simple line password. However, when login local is configured on the device, authentication requires a username and secret to be verified against the local database. This provides better security and accountability compared to using a single console password.

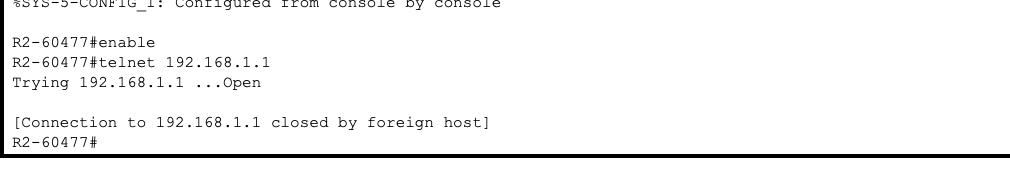
**After logging in, issue the show run command. Were you able to issue the command? Explain.**

**Answer:**  
I couldn’t execute the show running-config command immediately. By default, a local user without privilege level 15 is placed in user EXEC mode, which only allows access to basic commands. To run privileged EXEC commands like show run, higher access levels are required.

**Enter privileged EXEC mode using the enable command. Were you prompted for a password? Explain.**

**Answer:**  
Yes, I was prompted to enter the enable secret password. This is required to access privileged EXEC mode, as authentication with the enable secret, which is hashed, serves as an additional layer of security.

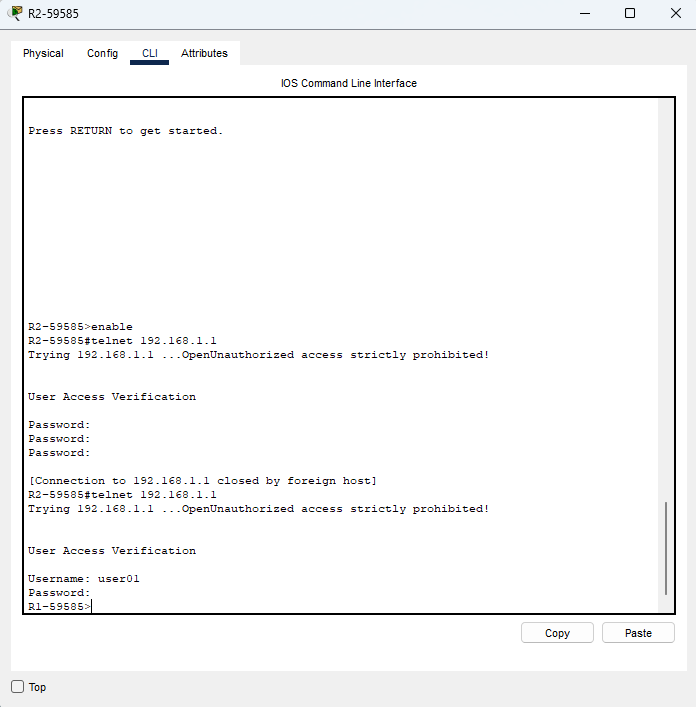
**Test the new account by logging in from a Telnet session.**

****

**Were you prompted for a user account? Explain.**

**Answer:**  
No, I wasn’t prompted to enter a username. The VTY lines were configured with a line password and the login command, but they did not utilize the local user account.

**Login Again**

****

**Were you prompted for a user account? Explain.**

**Answer:**  
Yes, I was prompted for a username. This was because the VTY lines were reconfigured with the login local command, which forces the router to authenticate using its local user database. As a result, I had to enter the username (user01) along with its corresponding password to log in.

**d.** Log in as user01 with a password of **“user01pass”.**

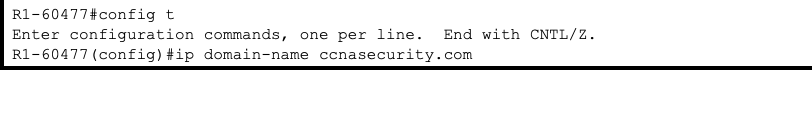
**e. During the Telnet session to R1-60477, access privileged EXEC mode with the enable command.**

**What password did you use?**

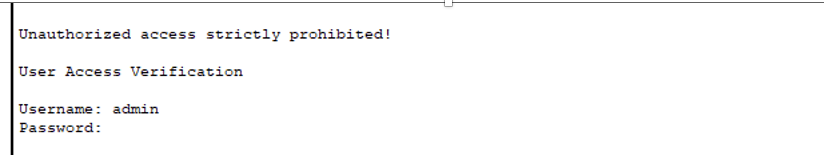
Answer: cisco12345

**Step 4: Configure the SSH Server on Router R1-60477 and R3-60477.**

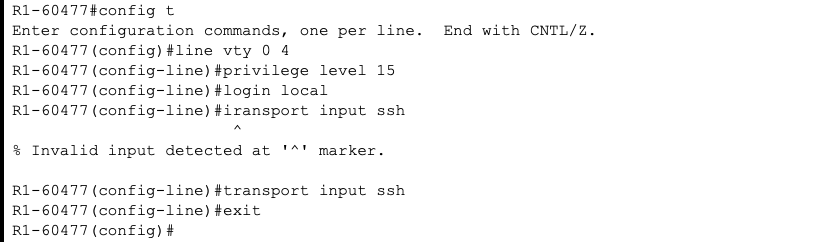
**Configure a domain name.**



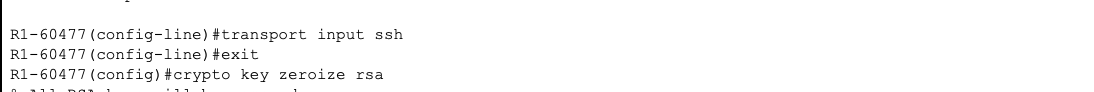
**Configure a privileged user for login from the SSH client.**



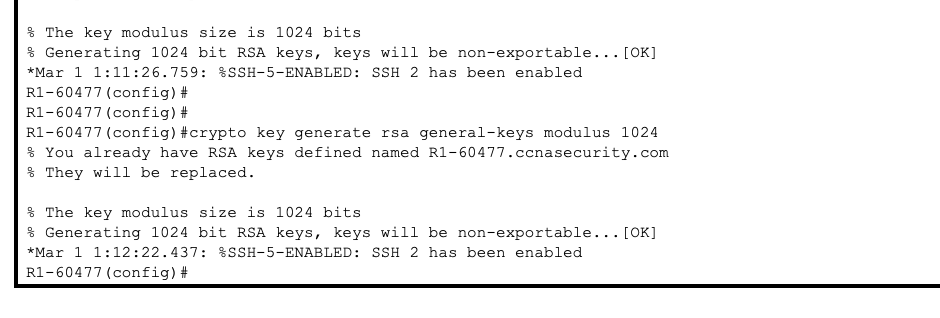
**Configure the incoming vty lines.**

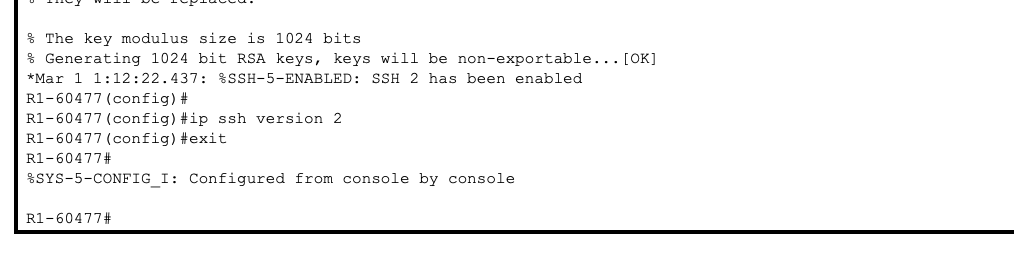
****

**Erasing existing key pairs on the router.**

****

**Generating the RSA encryption key pair for the router.**

****



**Configure SSH timeouts and authentication parameters.**

