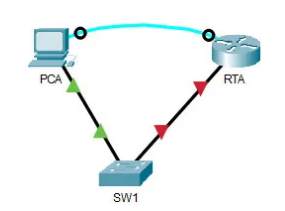
**Lab # 02**

**OBJECT**

***Configure Secure Passwords and SSH***

**TOPOLOGY:**



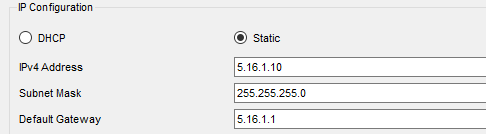
**LAB TASK:**

**Part 1: Configure Basic Security on the Router**

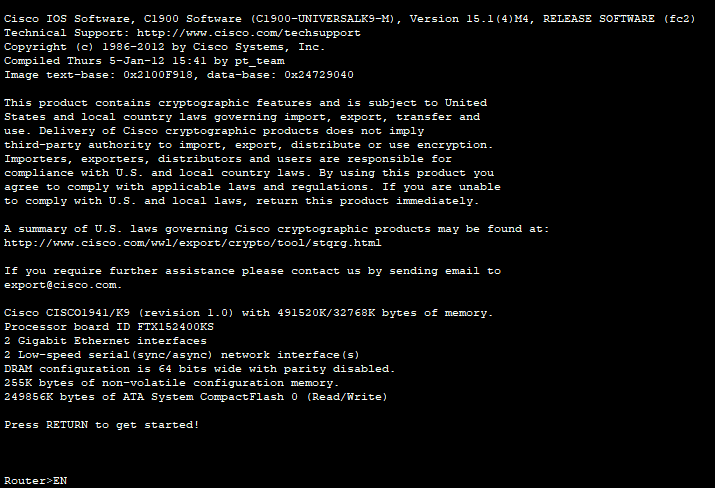
**Part 2: Configure Basic Security on the Switch**

**Part 1: Configure Basic Security on the Router**

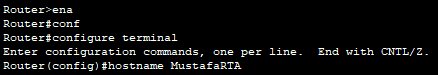
a. Configure IP addressing on PCA according to the Addressing Table.



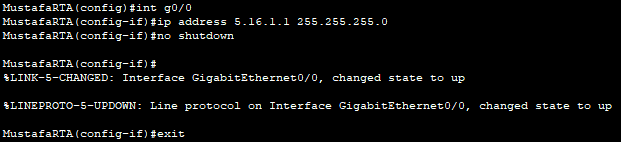
b. Console into RTA from the Terminal on PCA.



c. Configure the hostname as RTA.



d. Configure IP addressing on RTA and enable the interface.



e. Encrypt all plaintext passwords.



f. Set the minimum password length to 10.



g. Set a strong secret password of your choosing. 

Note: Choose a password that you will remember, or you will need to reset the activity if you are locked out of the device.

h. Disable DNS lookup.



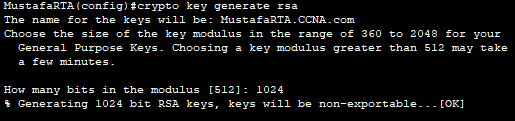
i. Set the domain name to **CCNA.com** (case-sensitive for scoring in PT).



j. Create a user of your choosing with a strong encrypted password.



k. Generate 1024-bit RSA keys.

**Note:** In Packet Tracer, enter the crypto key generate rsa command and press Enter to continue. 

l. Block anyone for three minutes who fails to log in after four attempts within a two-minute period.



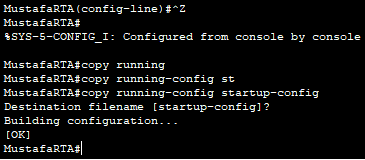
m. Configure all VTY lines for SSH access and use the local user profiles for authentication.



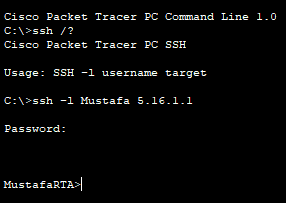
n. Set the EXEC mode timeout to 6 minutes on the VTY lines.



o. Save the configuration to NVRAM.

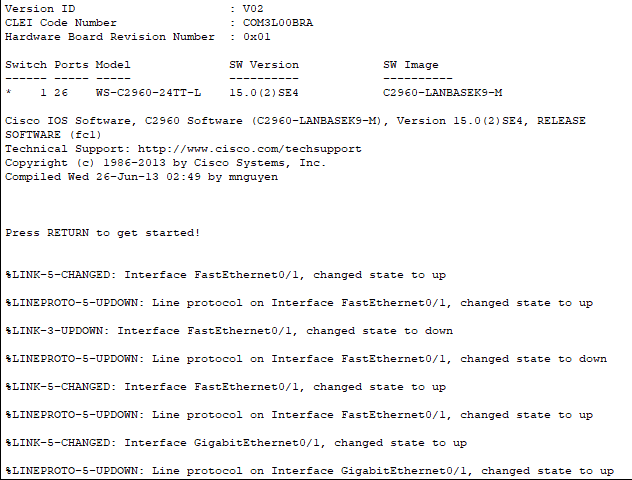


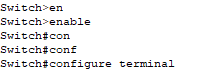
p. Access the command prompt on the desktop of **PCA** to establish an SSH connection to **RTA.**  
(Make sure you have IP configured for PCA)



**Part 2: Configure Basic Security on the Switch**

Configure switch SW1 with corresponding security measures. Refer to the configuration steps on the router if you need additional assistance.

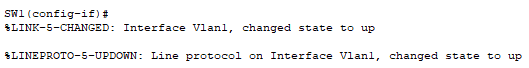
1. Click on SW1 and select the CLI tab.
2. Configure the hostname as SW1.





c. Configure IP addressing on SW1 VLAN1 and enable the interface.

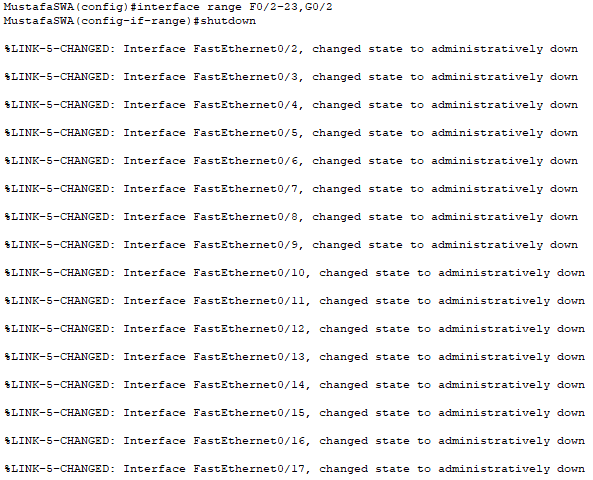


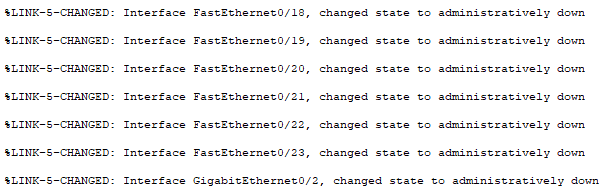


d. Configure the default gateway address.



e. Disable all unused switch ports.

Note: On a switch it is a good security practice to disable unused ports. One method of doing this is to simply shut down each port with the ‘shutdown’ command. This would require accessing each port individually.



f. Encrypt all plaintext passwords.



g. Set a strong secret password of your choosing.



h. Disable DNS lookup.

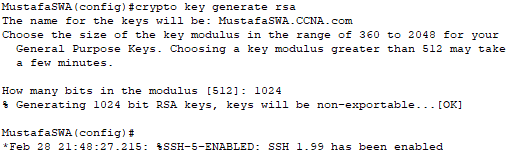


i. Set the domain name to **CCNA.com** (case-sensitive for scoring in PT).



j. Create a user of your choosing with a strong encrypted password.



k. Generate 1024-bit RSA keys. 

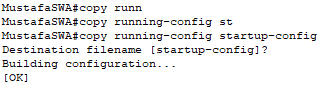
l. Configure all VTY lines for SSH access and use the local user profiles for authentication.



m. Set the EXEC mode timeout to 6 minutes on all VTY lines.



n. Save the configuration to NVRAM.



**Answer the following questions regarding the lab you have performed:**

1. Which type of wires have you used to connect devices?

ANS: Console and Copper straight Through

1. What is the IP default-gateway of PC-A?

ANS: 172.9.1.1 3.

1. What port n.o is used to configure SSH?

ANS: 22 4.

1. What is the difference between enable password and enable secret?

ANS: The main difference between enable and enable secret is encryption. With enable, the password that you give is stored in a plain text format and is not encrypted. With enable secret password, the password is actually encrypted with MD5. In the simplest sense, enable secret is the more secure way.

1. Which command will configure the router or switch to allow SSH as a protocol for management with a fallback of Telnet?

ANS: Which command will configure the router or switch to allow SSH as a protocol for management with a fallback of Telnet? The command transport ssh telnet will configure the VTY line to accept SSH as a login protocol and fallback to Telnet

1. How many versions of SSH do we have and what is the main difference between them?

ANS: There are mainly two versions of SSH protocol. The initial version was SSH-1, which was released in July 1995. In 2006, IETF (Internet Engineering Task Force) published RFCs for a revised version of the SSH protoco