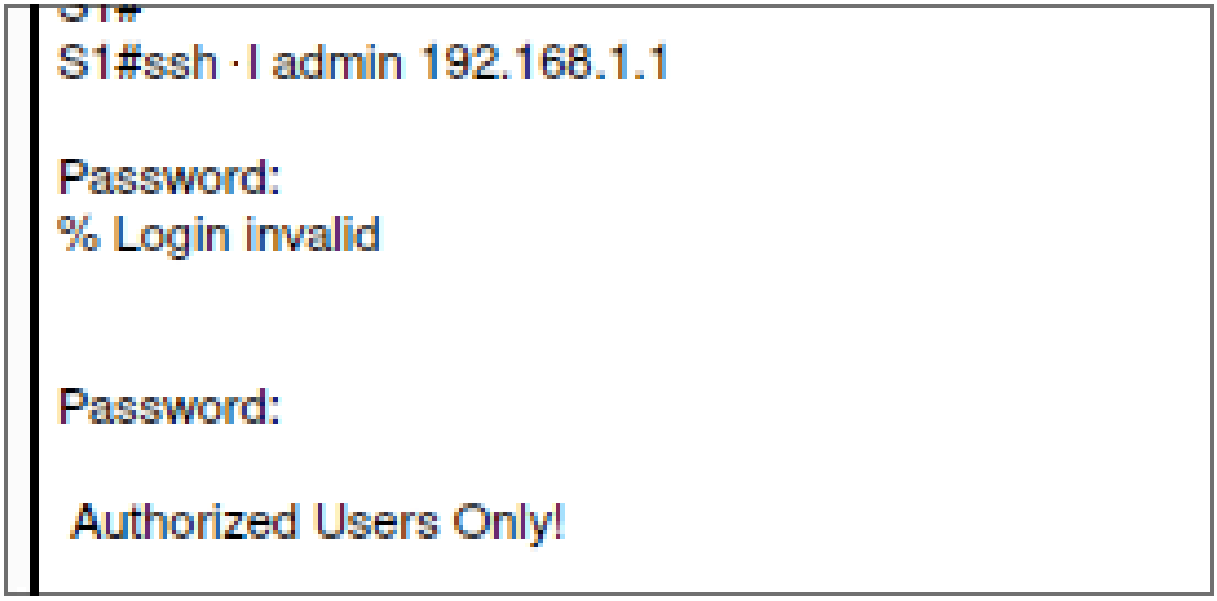
Daniel Alejandro Osornio López 0244685@up.edu.mx

Resultado



Pasos

Router

1. Console into the router and enable privileged EXEC mode.

   ```
   > enable
   ```

2. Enter configuration mode.

   ```
   # configure terminal
   ```

3. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

   ```
   (config)# no ip domain-lookup
   ```

4. Assign class as the privileged EXEC encrypted password.

   ```
   (config)# enable secret class
   ```

5. Assign cisco as the console password and enable login.

   ```
   (config)# line console 0 (config-line)# password cisco (config-line)# login
   ```

6. Assign cisco as the VTY password and enable login.

   ```
   (config)# line vty 0 4 (config-line)# password cisco (config-line)# login
   ```

7. Encrypt the plaintext passwords.

   ```
   (config)# service password-encryption
   ```

8. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.

   ```
   (config)# banner motd $ No entrar $
   ```

9. Configure and activate the G0/0/1 interface on the router using the information contained in the Addressing Table.

```
(config)# interface g0/0/1 (config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# no shutdown
```

10. Save the running configuration to the startup configuration file.

```
# copy running-config startup-config
```

Step 4: Configure PC-A.

1. Configure PC-A with an IP address and subnet mask.
2. Configure a default gateway for PC-A.

Switch

1. Console into the switch and enable privileged EXEC mode.

```
> enable
```

2. Enter configuration mode.

```
# configure terminal
```

3. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

```
(config)# no ip domain-lookup
```

4. Assign class as the privileged EXEC encrypted password.

```
(config)# enable secret class
```

5. Assign cisco as the console password and enable login.

```
(config)# line console 0 (config-line)# password cisco (config-line)# login
```

6. Assign cisco as the VTY password and enable login.

```
(config)# line vty 0 15 (config-line)# password cisco (config-line)# login
```

7. Encrypt the plain text passwords.

```
(config)# service password-encryption
```

8. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.

```
(config)# banner motd $ Authorized Users Only! $
```

9. Configure and activate the VLAN 1 interface on the switch according to the Addressing Table.

```
(config)# interface vlan 1 (config-if)# ip address 192.168.1.11 255.255.255.0
(config-if)# no shutdown
```

10. Save the running configuration to the startup configuration file.

```
# copy running-config startup-config
```

Step 2: Configure the switch for SSH connectivity.

Use the same commands that you used to configure SSH on the router in Part 2 to configure SSH for the switch.

1. Configure the device name as listed in the Addressing Table.

```
(config)# hostname S1
```

2. Configure the domain for the device.

```
(config)# ip domain-name ccna-lab.com
```

3. Configure the encryption key method.

```
(config)#crypto key generate rsa
```

The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Key+ Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable…[OK]

```
(config)#
```

1. Configure a local database username.

```
(config)# username admin secret aesrAESR7=
```

2. Enable Telnet and SSH on the VTY lines.

```
(config)# line vty 0 15 (config-line)# transport input ssh
```

3. Change the login method to use the local database for user verification.

```
(config-line)# login local (config-line)# end
```