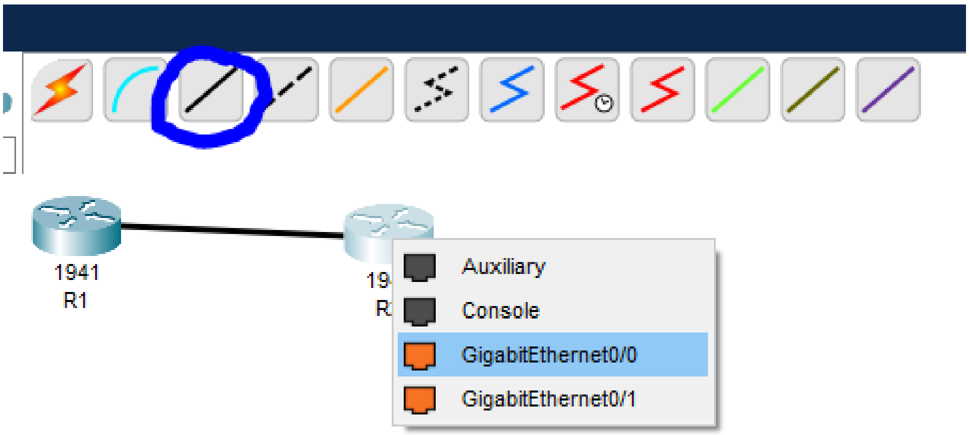
Cisco Packet Tracer Project 1: Basic Router Security

Step-by-step Process:

1. Connect R1 with R2 by their GigabitEthernet0/0 interfaces
2. Setting the Hostnames to “R1” and “R2”
3. Set the enable password on each router to “cisco”
4. View if the password is encrypted
5. Enable password encryption on each router
6. Viewing again if the password is encrypted
7. Disabling password encryption on each router
8. Viewing if the password is encrypted after the changes made

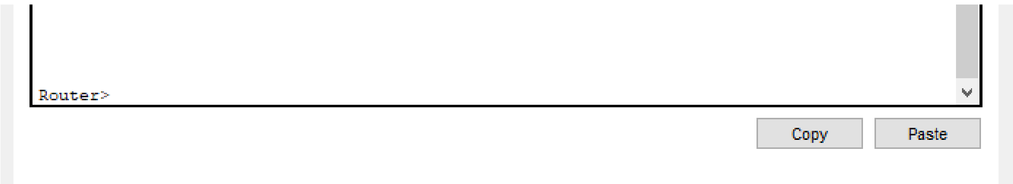
Connecting R1 with R2 by their Gigabit Ethernet0/0 Interfaces

In this stage of the mini-project, I’m going to connect the 2 routers to their Gigabit Ethernet0/0 Interfaces with a copper cable

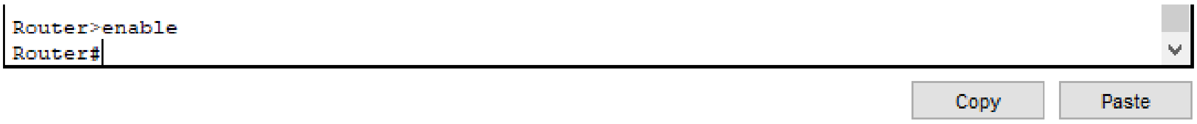


Setting the Hostnames to “R1” and “R2”

In this stage of this mini-project, we have to change both router’s hostnames to “R1” and “R2” using the application’s Command Line Interface (CLI) feature, which allows you to configure all the network devices.



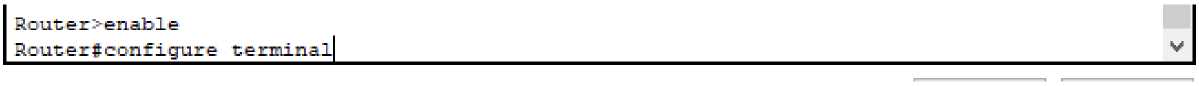
```
Router>
```



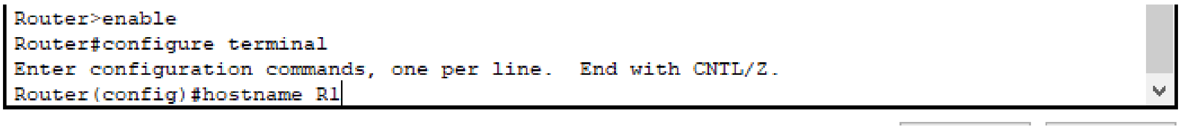
```
Router>enable
Router#
```

In order to change the hostnames of the router, we have to be in privileged exec mode. To do that, we have to enter the command “**enable**” to enter privileged exec mode.

Further to that, we have to enter to the global configuration mode in order to finally being able to set the hostname of the router. To enter global configuration mode, type the command “**configure terminal**”



```
Router>enable
Router#configure terminal
```



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
```

To change the hostname of the router, type the command “**hostname [New Name]**” in our case R1.

After that, it should automatically change the hostname of the router to R1.

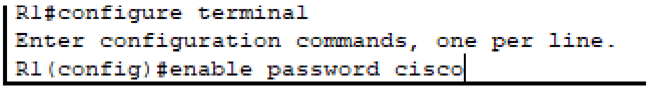
THE SAME THING APPLIES TO R2

Set the enable password on each router to “cisco”

Usually when wanting to enter privileged exec mode, it would require a password to gain that privilege, which wasn’t the chase for the example above. This is why in this section we will set a password for this router.

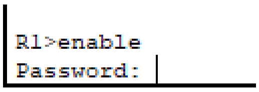
To enable the password, you would need to be in the global configuration mode again (***SEE THE EXAMPLE ABOVE ON HOW TO ENTER GLOBAL CONFIGURATION MODE***)

After entering global configuration mode, type the command “enable password [password name]” in order to finally enable passwords when trying to enter privileged exec mode.



```
R1#configure terminal
Enter configuration commands, one per line.
R1(config)#enable password cisco
```

Below is a picture which showcases that I successfully enabled passwords for the router when trying to enter privileged exec mode.

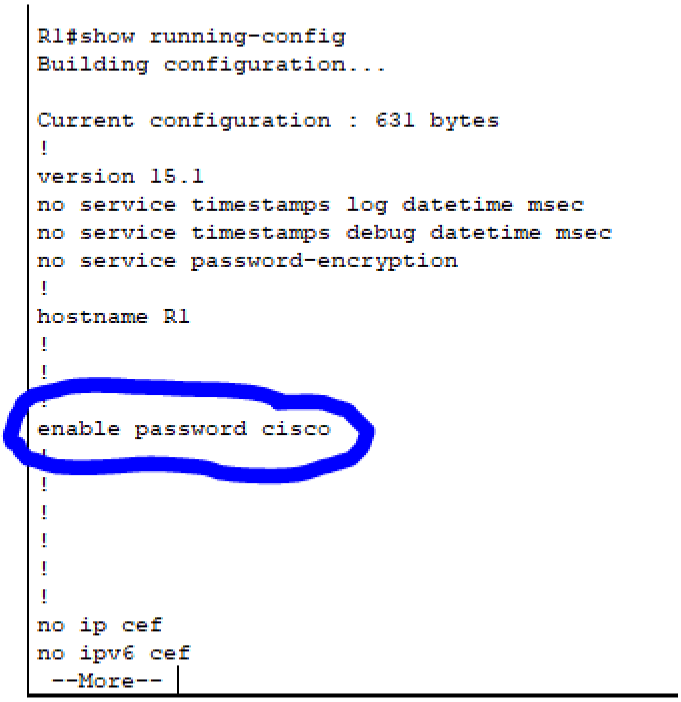


```
R1>enable
Password:
```

Viewing the password

In order for us to view our password, we have to be in privileged exec mode first of all.

After enter privileged exec mode, enter the command “**show running-config**”



```
R1#show running-config
Building configuration...

Current configuration : 631 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
enable password cisco
!
!
!
!
!
!
no ip cef
no ipv6 cef
 --More--
```

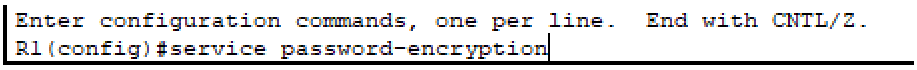
This will show you all the configurations that you (as the user) have done to this router, from changing its hostname to adding a password.

This image further shows that there is no encryption at the time being, as it doesn't encrypt the router's password, which is "cisco".

Enabling password encryption on the router

In order to enable password encryption, you have to be in global configuration mode.

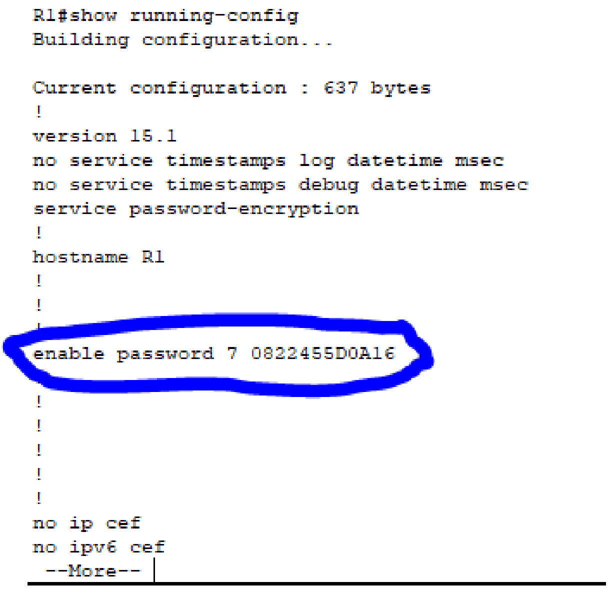
After that is done, enter the command "**service password-encryption**" to enable encryption on the router's password.



```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service password-encryption
```

Viewing the password for encryption

Like before, use the command "**show running-config"** to see the configurations and the password of the router



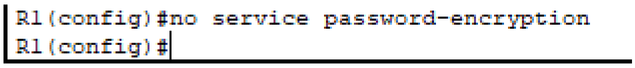
```
R1#show running-config
Building configuration...

Current configuration : 637 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
no ipv6 cef
 --More--
```

We see from this picture that now the password is encrypted and is not openly seen by anybody unless they decrypt the password.

Disabling password encryption

Just like when enabling the password, we have to be in global configuration mode. To disable passwords, just type the command “**no service password-encryption**”.

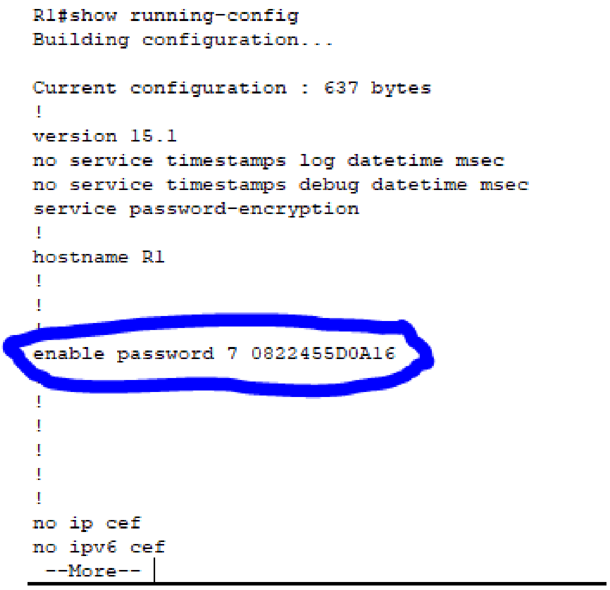


```
R1(config)#no service password-encryption
R1(config)#
```

Viewing the password for encryption

Like last time, we type the command “**show running-config**” to show us the configurations made and possibly the unencrypted password.

EVEN THOUGH WE DISABLED PASSWORD ENCRYPTION, THIS COMMAND WILL NOT DECRYPT PASSWORDS THAT ARE ALREADY ENCRYPTED!



```
R1#show running-config
Building configuration...

Current configuration : 637 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable password 7 0822455D0A16
!
!
!
!
!
no ip cef
no ipv6 cef
 --More--
```