PRACTICAL LAB: SECURE SHELL (SSH) CONFIGURATION

JORDAN ALLISON
jallison1@glos.ac.uk

Practical Lab: Secure Shell (SSH) Configuration - JA

Table of Contents

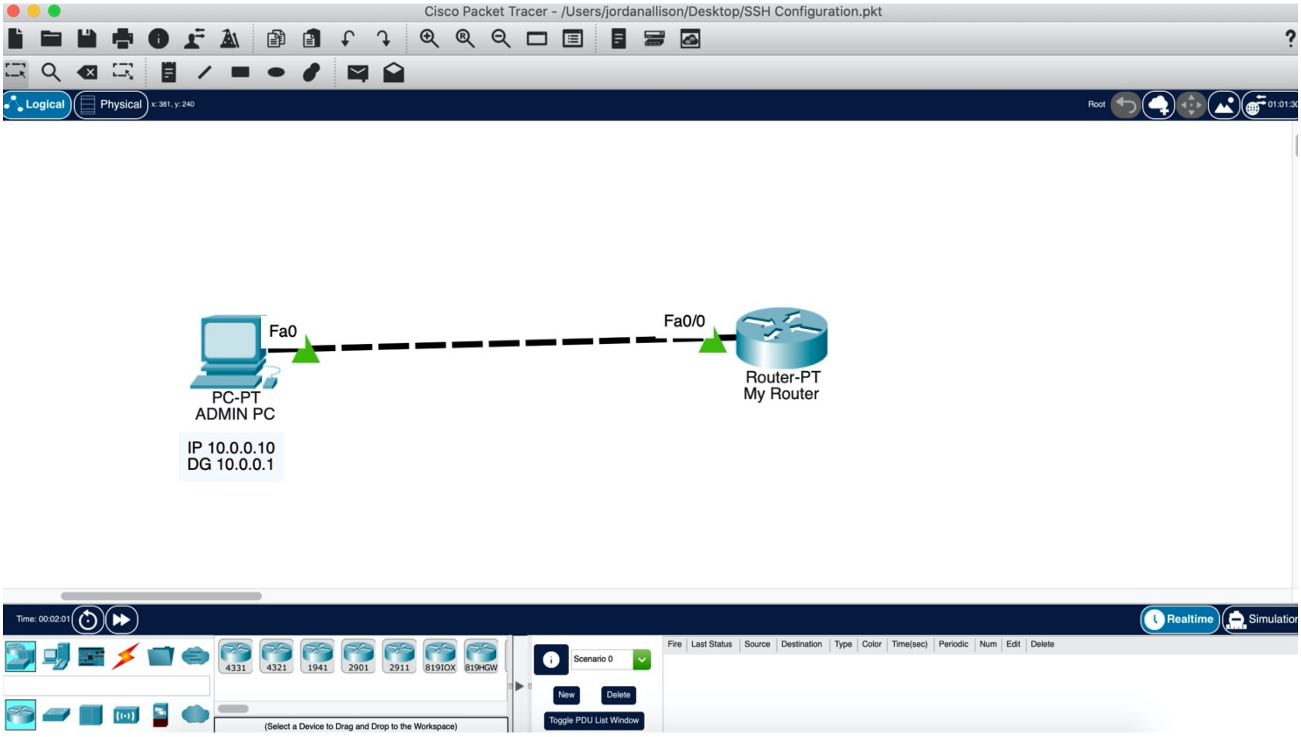
1 Introduction

For this practical we will be using *Cisco Packet Tracer,* a tool provided by Cisco to build and test Cisco networks. In this lab we are going to configure Secure Shell (SSH) for a router. SSH enables a user to access a remote device and manage it remotely. However, data transmitted over SSH is encrypted, so it is more secure. SSH is a client-server protocol, with a SSH client and a SSH server. The client machine (e.g. a PC or Laptop) establishes a connection to a SSH server running on a remote device (e.g. a router). Once the connection is established, a network administrator can execute commands on the remote device.

2 SSH Configuration on a Router

2.1 Setting Up Devices

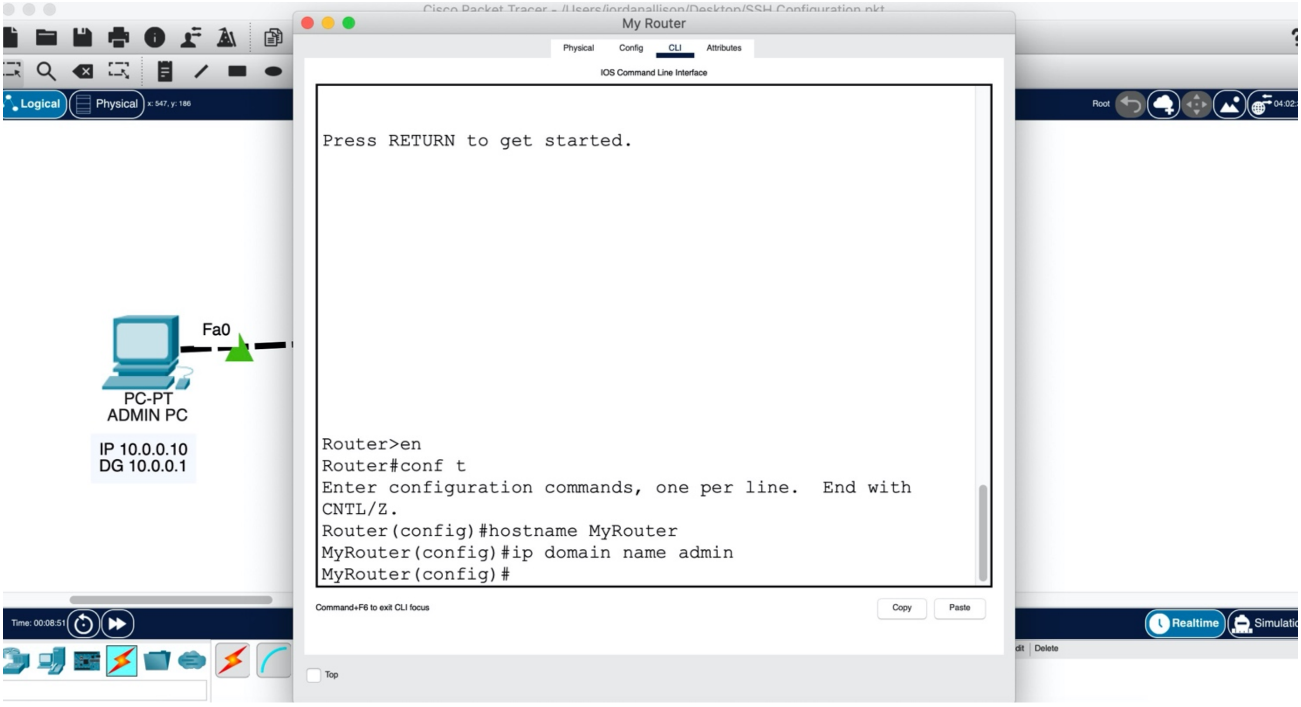
Set up the following devices:



Device	Interface	IP Addresses	Subnet Mask	Default Gateway
Admin PC	N/A	10.0.0.10	255.0.0.0	10.0.0.1
My Router	Fa0/0	10.0.0.1	255.0.0.0	N/A

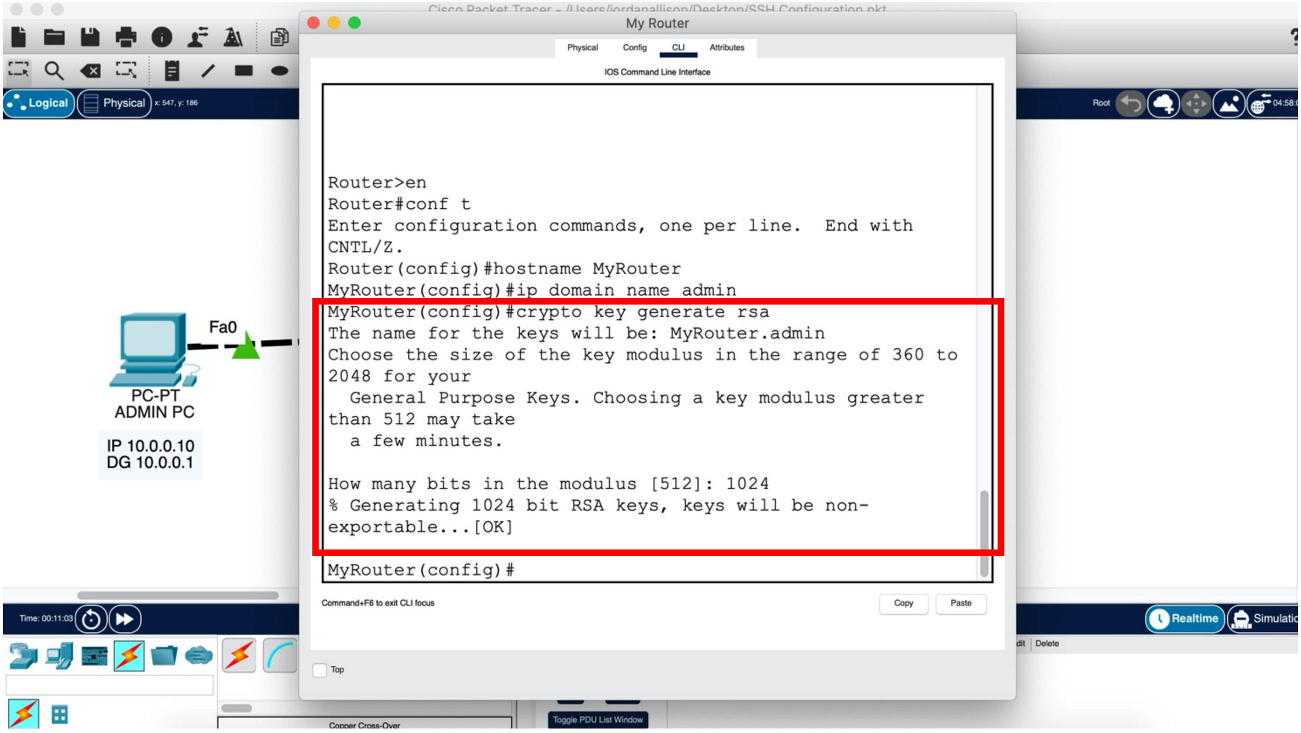
2.2 Router Configuration

Set the Router hostname as MyRouter, and also set the IP Domain name as admin. Both the hostname and domain name will be used for generating encryption keys.



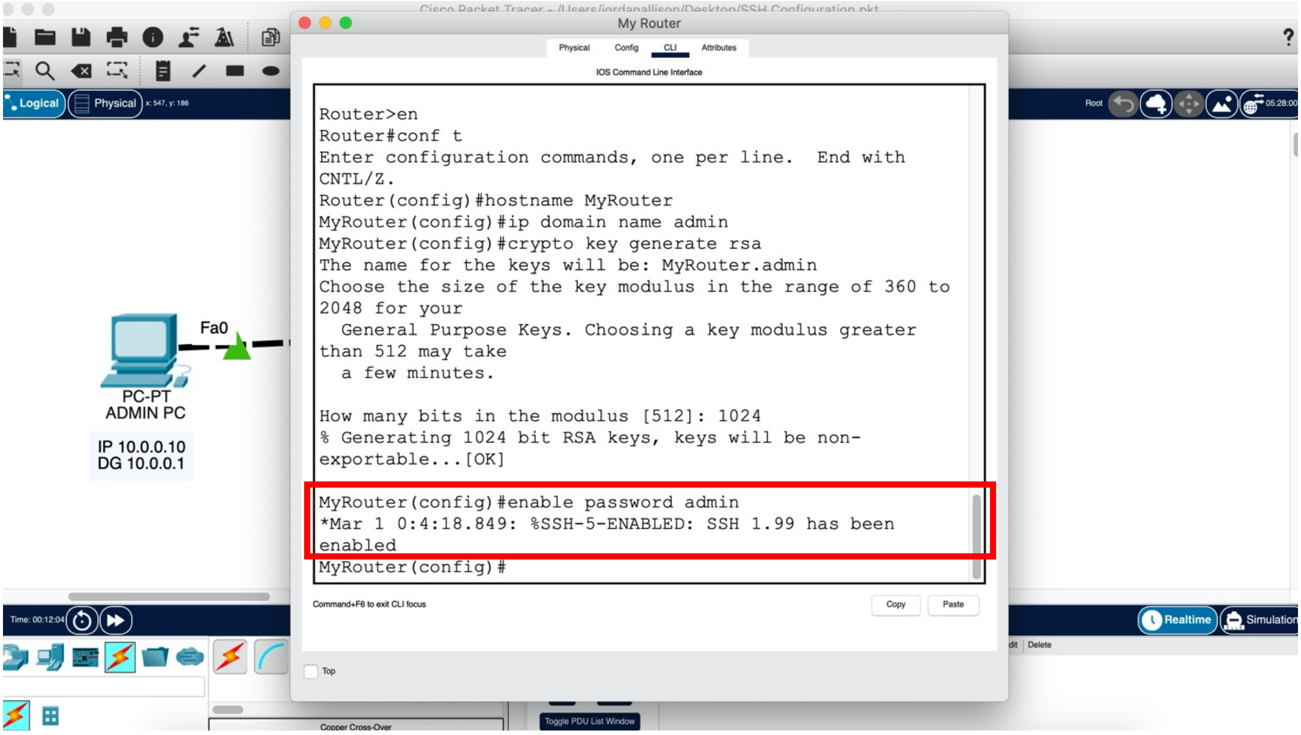
```
Press RETURN to get started.









Router>en
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname MyRouter
MyRouter(config)#ip domain name admin
MyRouter(config)#
```

Now generate encryption keys for securing the session using the command: crypto key generate rsa. Then choose the number of bits for the modulus (in the case below, I chose 1024).



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname MyRouter
MyRouter(config)#ip domain name admin
MyRouter(config)#crypto key generate rsa
The name for the keys will be: MyRouter.admin
Choose the size of the key modulus in the range of 360 to
2048 for your
  General Purpose Keys. 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]

MyRouter(config)#
```

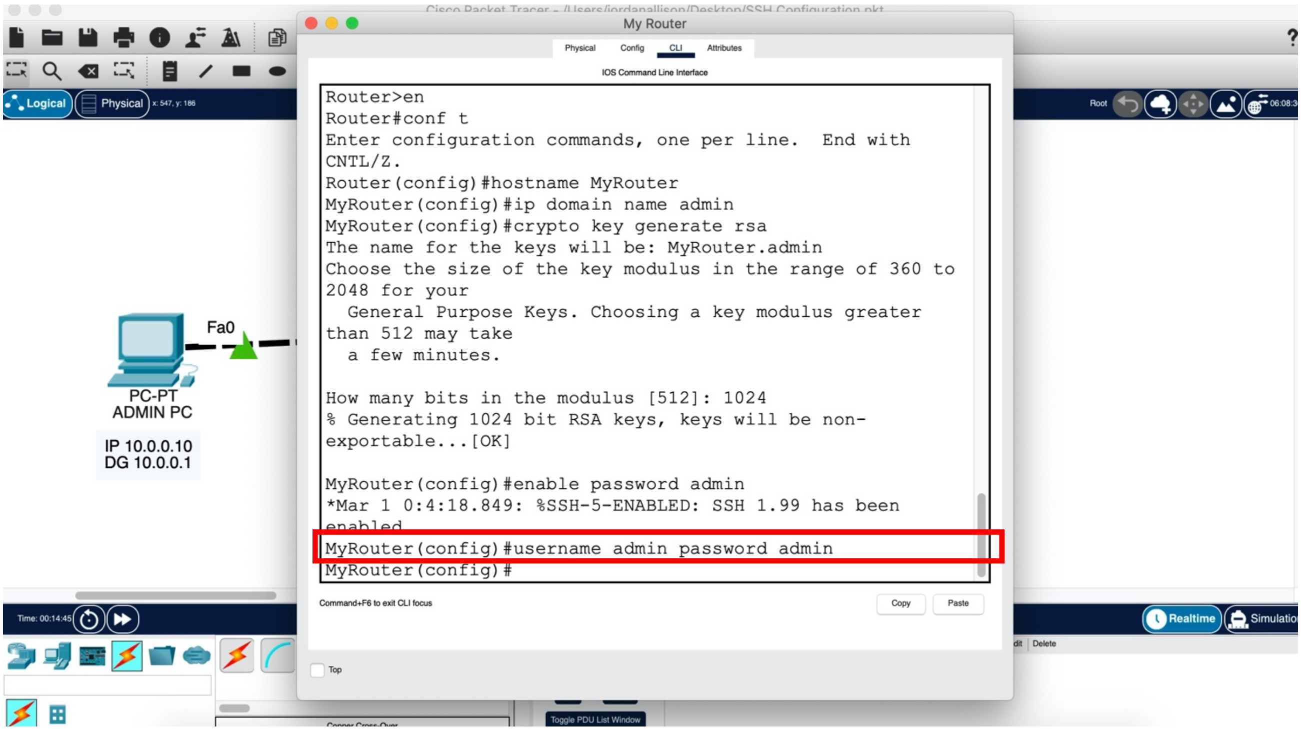
Now set an enable password. I chose admin below:



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname MyRouter
MyRouter(config)#ip domain name admin
MyRouter(config)#crypto key generate rsa
The name for the keys will be: MyRouter.admin
Choose the size of the key modulus in the range of 360 to
2048 for your
  General Purpose Keys. 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]

MyRouter(config)#enable password admin
*Mar 1 0:4:18.849: %SSH-5-ENABLED: SSH 1.99 has been
enabled
MyRouter(config)#
```

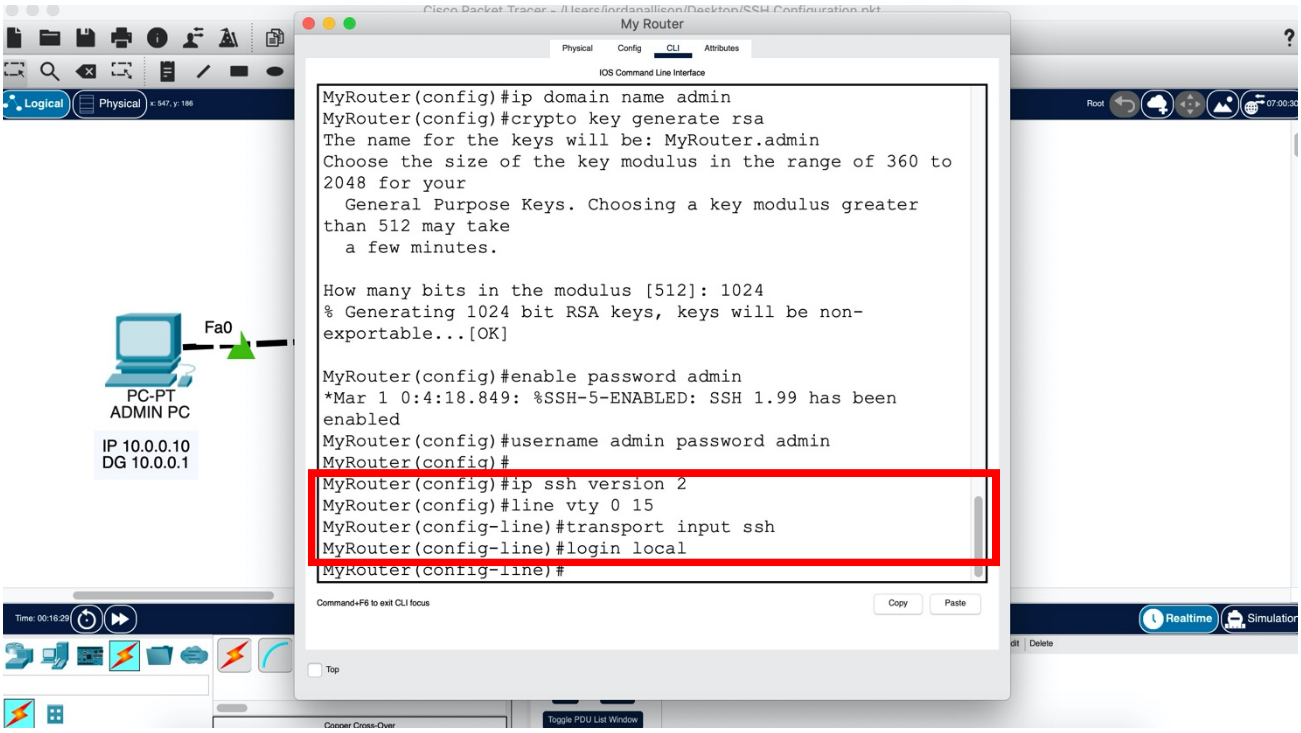
This password is not for use with SSH. It is for accessing the privileged executive mode of the router after you are able to access the CLI remotely via SSH.

Now set a username and password for local login. This will have to be provided before you can access the CLI of the router when using SSH. In the example below, I chose a username of admin, and password of admin.



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname MyRouter
MyRouter(config)#ip domain name admin
MyRouter(config)#crypto key generate rsa
The name for the keys will be: MyRouter.admin
Choose the size of the key modulus in the range of 360 to
2048 for your
  General Purpose Keys. 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]

MyRouter(config)#enable password admin
*Mar 1 0:4:18.849: %SSH-5-ENABLED: SSH 1.99 has been
enabled
MyRouter(config)#username admin password admin
MyRouter(config)#
```

Now you need to specify what version of SSH you would like to use and connect to VTY (virtual terminal) lines of the router and configure the SSH protocol.

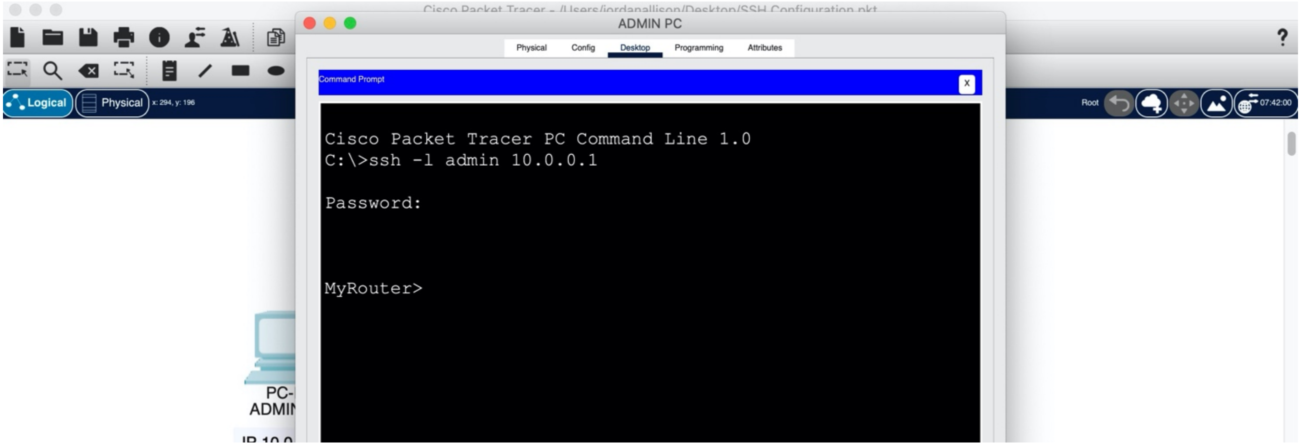


```
MyRouter(config)#ip domain name admin
MyRouter(config)#crypto key generate rsa
The name for the keys will be: MyRouter.admin
Choose the size of the key modulus in the range of 360 to
2048 for your
  General Purpose Keys. Choosing a key modulus greater
than 512 may take
  a few minutes.

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

MyRouter(config)#enable password admin
*Mar 1 0:4:18.849: %SSH-5-ENABLED: SSH 1.99 has been
enabled
MyRouter(config)#username admin password admin
MyRouter(config)#
MyRouter(config)#ip ssh version 2
MyRouter(config)#line vty 0 15
MyRouter(config-line)#transport input ssh
MyRouter(config-line)#login local
MyRouter(config-line)#
```

2.3 Test SSH Connectivity

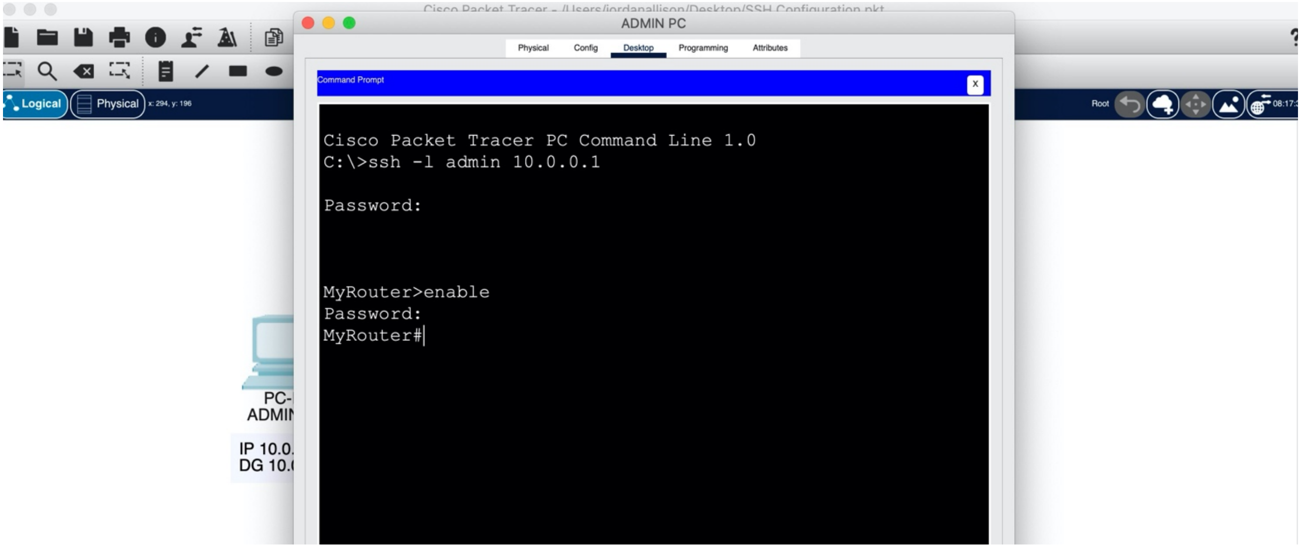
On the command prompt of the Admin PC, open a SSH session to the remote router by typing the command: ssh -l admin 10.0.0.1

It will ask for the password, so enter the password you chose (in this case admin). However, the password will not show up, just type it and press enter. You will then have the following.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 10.0.0.1

Password:



MyRouter>
```

Now you are in the CLI of the router. Type enable and provide the enable password to access the privileged executive mode.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 10.0.0.1

Password:



MyRouter>enable
Password:
MyRouter#
```

Congratulations, you can now proceed and conduct configurations on the router remotely through SSH.