LAB: SSH

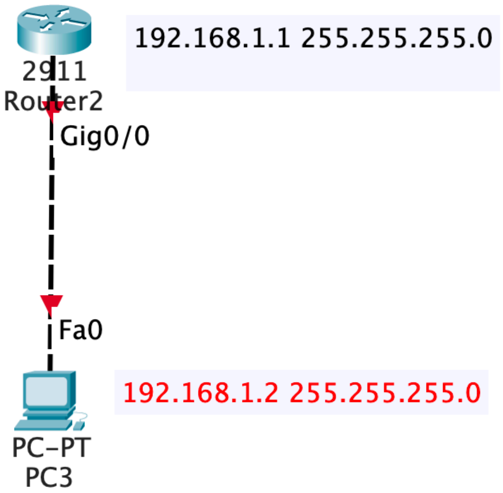
Lab Objective

The objective of this lab exercise is for you to learn and understand how to enable SSSH access to a device - in this case, a Cisco router.

Lab Purpose:

It is never a good idea to permit Telnet access to network devices, especially in corporate settings. SSH is a secure way to connect to network devices.

Lab Topology



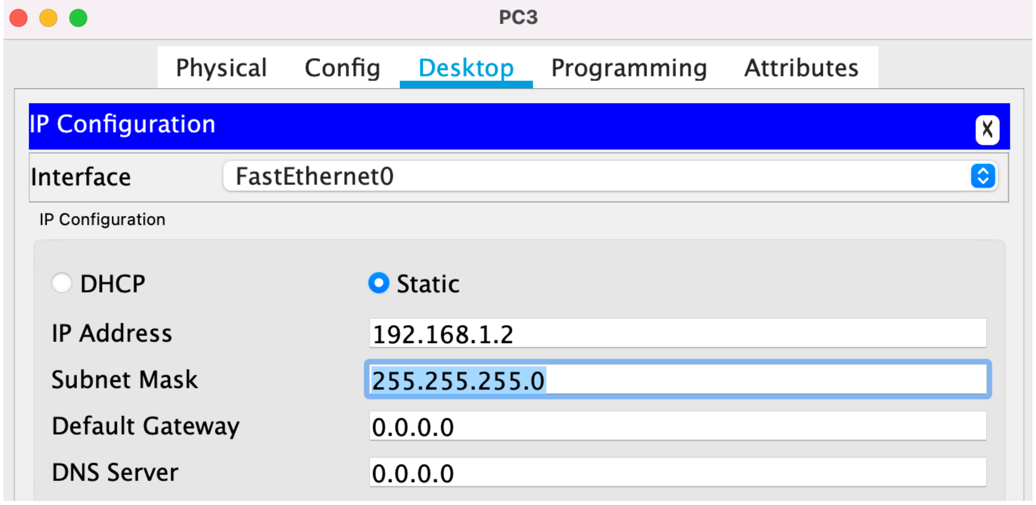
Task 1:
Configure the hostname on Router 1 as R2.
You must always answer 'NO' at the start because the routers will drop into a question-and-answer mode in an attempt to self-configure. The hostname to use will be: R2

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialogue? [yes/no]: no


Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#
```

Task 2:
Add an IP address to each Ethernet Interface and ‘no shut’ the router interface in order to bring them up. Ensure you can ping across the link. Your router may have a gigabit interface so feel free to configure whatever yours has.

```
R2(config)#interface gigabitethernet0/0
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

On the PC:



Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address 192.168.1.2

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

```
R2#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

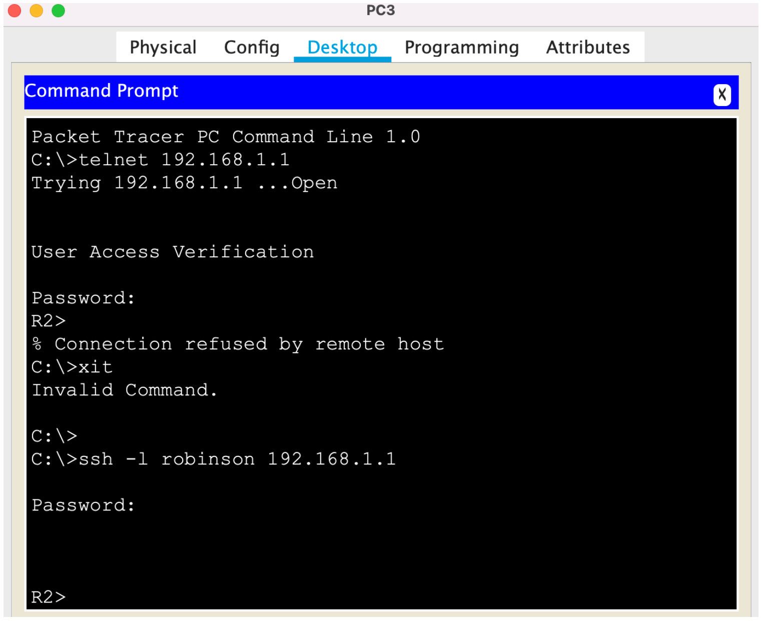
Task 3:
Secure R2 so that it accepts SSH incoming connections. We need to set a domain name and generate keys. As options, we have set retries for the password to 2 attempts and a timeout of 60 seconds if there is no activity.

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip domain-name tavcollege.com
R2(config)#crypto key generate rsa
The name for the keys will be: R2.tavcollege.com
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]

R2(config)#ip ssh time-out 60
*Mar 1 0:8:27.406: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#ip ssh authentication-retries 2
R2(config)#line vty 0 15
R2(config-line)#transport input ssh
R2(config-line)#password cisco
R2(config-line)#end
R2#
```

Next, you can go to the router Telnet lines. There are 16 available lines on most Cisco devices numbered 0 to 15 inclusive. You need to permit incoming SSH connections on these.

```
R2#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 60 secs; Authentication retries: 2
```

Task 4:
Connect to Router 2 from your PC using SSH. You should be prompted for the password which, as you can see above, is ‘cisco’. You can add a username for the connection which I’ve done here by using the -l switch (lowercase letter L).



```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
R2>
% Connection refused by remote host
C:\>xit
Invalid Command.

C:\>
C:\>ssh -l robinson 192.168.1.1

Password:



R2>
```

You can quit the session by typing ‘exit’ at the command prompt.

Notes: Almost any model of the router will do for this lab. Just make sure you connect them with a crossover cable because we aren’t using a switch in this lab.