An overview of SSH

Secure Shell, just like Telnet, enables a user to access a remote device and manage it remotely. However, with SSH, all data transmitted over a network (including usernames and passwords) is **encrypted and secure** from eavesdropping.

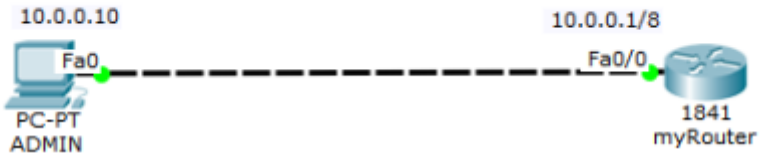
SSH is a **client-server** protocol, with a SSH client and a SSH server. The client machine (such as a PC) establishes a connection to a SSH server running on a remote device (such as a router). Once the connection has been established, a network admin can execute commands on the remote device.

Configuring SSH on a router in Packet Tracer

For this tutorial, we'll configure SSH on the router so that you as the admin can access and manage it remotely using an SSH client on the admin PC.

And now on to it:

First build the network topology.



Then do these basic IP configurations on the PC and the router:

Router

```
Router(config)#int fa0/0

Router(config-if)#ip add 10.0.0.1 255.0.0.0

Router(config-if)#no shut

Router(config)#exit
```

PC : **IP address** 10.0.0.10 **Subnet mask** 255.0.0.0 **Default gateway** 10.0.0.1

Now, to set up SSH on the router, you'll need to:

1. Set Router's **hostname**

```
Router(config)#hostname myRouter
```

2. Set **domain name**

```
myRouter(config)#ip domain name admin
```

Both the *hostname* and *domain name* will be used in the process of **generating encryption keys.**

3. Now generate **encryption keys** for securing the session using the command *crypto key generate rsa.*

```
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]
```


4. Set an **enable password .**

```
myRouter(config)# enable password admin
```

Note that this password is not for use with SSH; its only for use in accessing the privileged executive mode of the router after you are able to access its CLI remotely via SSH .

5.Set **username** and **password** for local login.

```
myRouter(config)#username admin password admin
```

The password will have to be provided before you can access the CLI of the router when using SSH.

6.Specify the **SSH version** to use.

```
myRouter(config)#ip ssh version 2
```

7.Now connect to **VTY** lines of the Router and configure the SSH protocol.

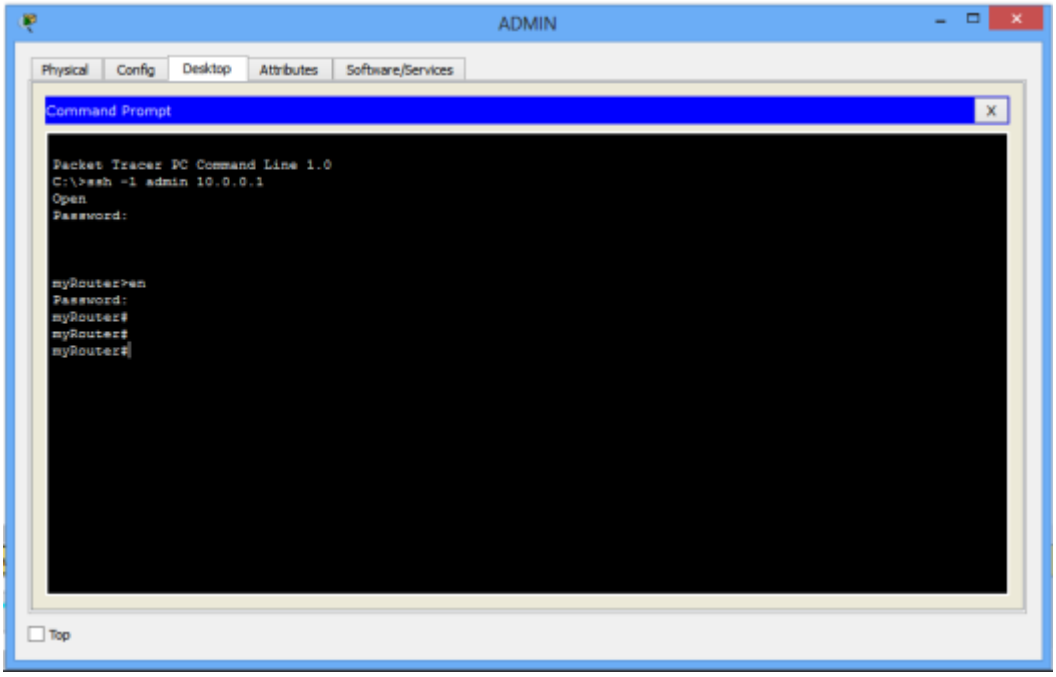
```
myRouter(config)#line vty 0  15

myRouter(config-line)#transport input ssh

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

That's all for configuration. Move on to see if you can access the router remotely from the PC.

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

admin is the **username** set in step 5.

9. Provide the **login password** which you set in step 5 and press enter. You're now probably in the CLI of the router. Provide the **enable password** (the one you set in step 4) to access the privileged executive mode.



You can proceed and do configurations on the Router.You're now managing the router remotely from the PC.

That's it!

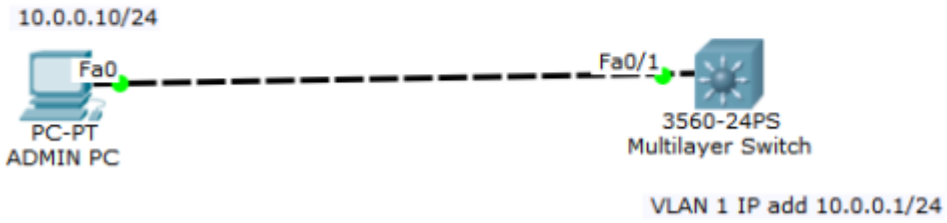
At this point, let's move on and configure SSH on a **switch**.

SSH configuration on a Switch

Here, we'll configure SSH on a multi-layer switch. The commands remain almost the same as for the router; only that in a switch, we'll use the IP address of its **VLAN interface** to access it from the PC.

So then, let's move on.

1. Begin by creating the network topology.



Then configure basic IP addressing on the PC and the switch. On the switch, we'll assign an IP address to a VLAN interface, just as we've said.

Switch

```
Switch(config)#int vlan 1

Switch(config-if)#ip add 10.0.0.1  255.0.0.0

Switch(config-if)#no shut
```

Give the **ADMIN PC** IP address 10.0.0.10 /8

Now, to configure SSH on the multilayer switch, here are the steps.

1.Configure **hostname**

```
Switch(config)#hostname SW1
```

2. Configure IP **domain name**

```
SW1(config)#ip domain name admin
```


Both the host name and domain name will be used in the process of generating encryption keys.

3. Now generate **encryption keys** for securing the session.

```
SW1(config)#crypto key generate rsa
```

```
The name for the keys will be: SW1.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]
```

4.Set an **enable password.**

```
SW1(config)#enable password admin
```

Again, note that enable password is not necessarily used in configuring SSH; it will allow the admin to access the **privileged executive mode** of the switch once a remote connection to the switch via SSH is established.

5. Set **username** and **password** for local login.

```
SW1(config)#username admin password admin
```

6. Specify the **SSH version** to use.

```
SW1(config)#ip ssh version 2
```


7. Now connect to the **VTY** lines of the switch and configure SSH on the lines.

```
SW1(config)#line vty 0 15
```

```
SW1(config-line)#transport input ssh

SW1(config-line)#login local
```

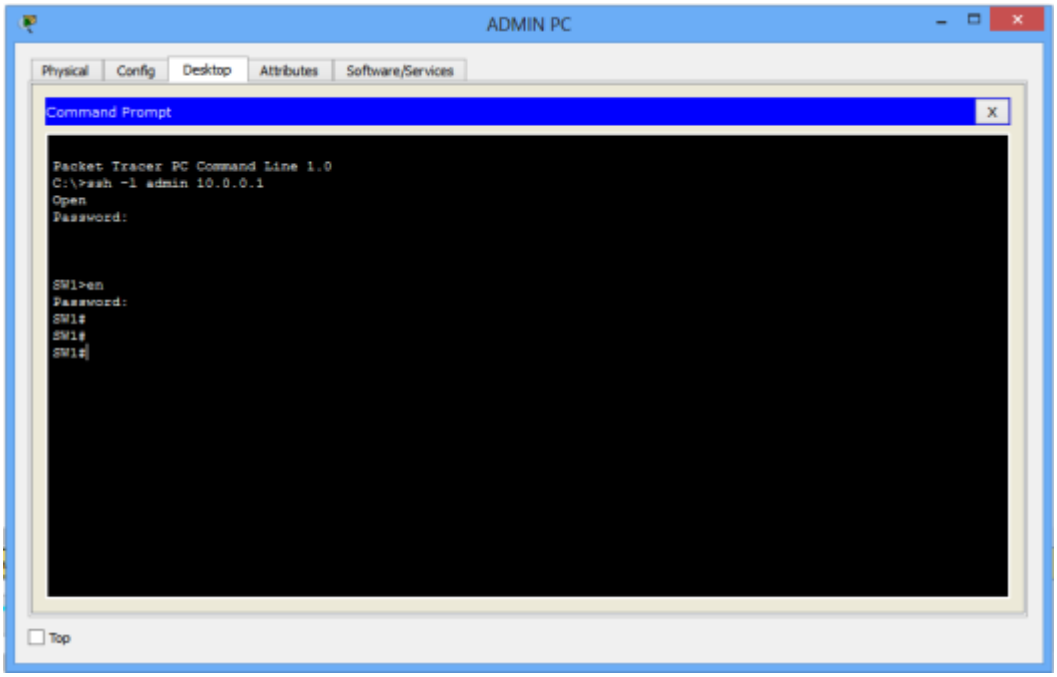
That's all for SSH configuration on the switch. Move on and try to access the switch remotely from the PC.

So then:

8. On the command prompt of the **Admin PC**, open a SSH session to the switch using the command **ssh -l admin 10.0.0.1**

Note that: ***admin*** is the username defined in step 5 while **10.0.0.1** is the IP address of the VLAN interface of then switch.

command prompt



Note:

- We used a multi layer switch because we couldn't find support for SSH on layer 2 switches in Packet Tracer.
- We can still start a SSH session to a router/switch from another router/switch instead of a PC, as long as the router/switch supports SSH.