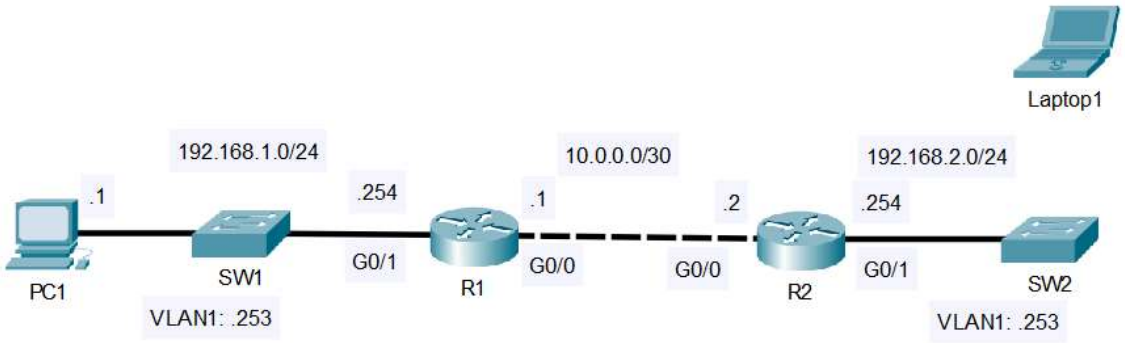
SSH Configuration on a Cisco Switch

In this lab, we'll configure SSH on a Cisco switch for remote access. **SSH (Secure Shell)** is a cryptographic network protocol that ensures secure communication ov an otherwise unsecured network. SSH was designed to replace insecure protocol like **Telnet** and other remote Unix shell protocols. You can follow along by downloading this SSH Config Packet Tracer File and opening it in Cisco's Free Packet Tracer Simulator (*create a free account, enroll in one of the free courses and download the free software*).

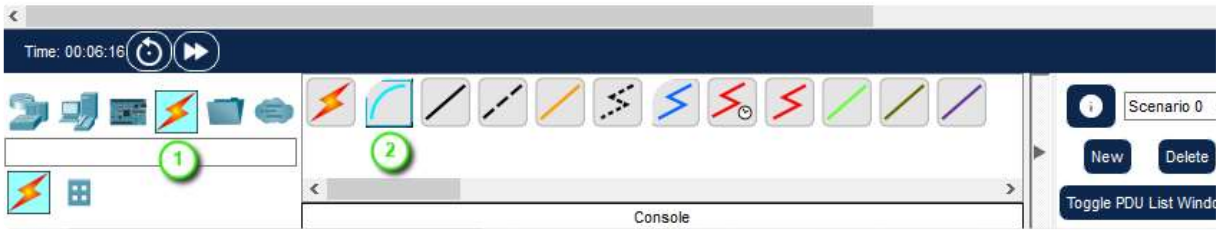


*SW2 has been new ly added to the netw ork, but has not yet been configured.
1.Connect Laptop1 to SW2's console port to perform the follow ing configurations:
Host name: SW2
Enable secret: ccna
Username/PW: aaron/ccna
VLAN1 SVI: 192.168.2.253/24
Default gatew ay: R2

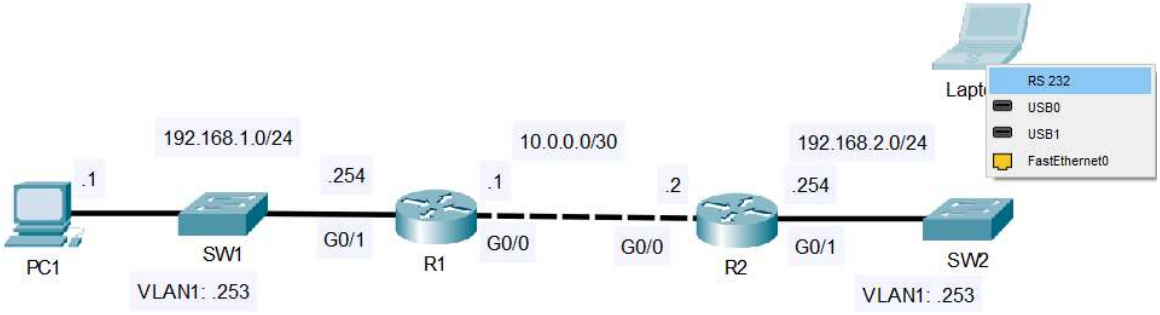
2. Configure the follow ing console line security settings on SW2:
Authentication: Local user
Exec timeout: 5 minutes

3. Configure SW2 for remote access via SSH:
Domain name: aaronguild.net
RSA key size: 2048 bits
Authentication: Local user
Exec timeout: 5 minutes
Protocols: SSH only
+Limit access to PC1 ONLY

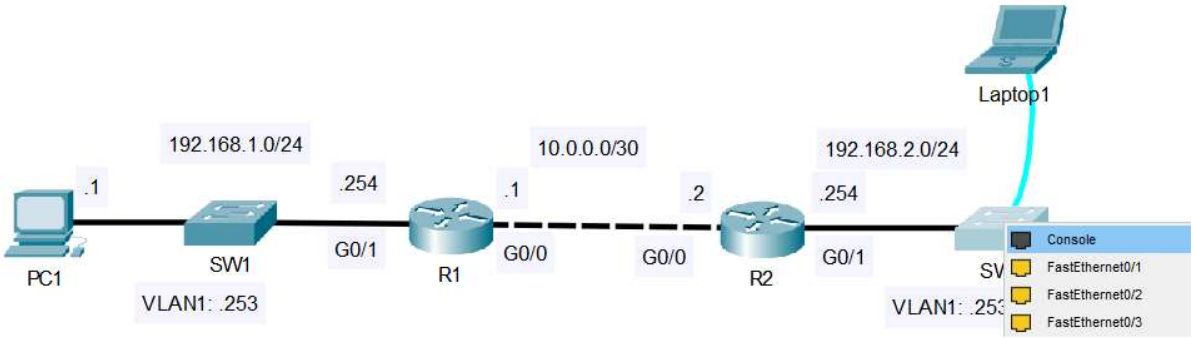
First we need to connect Laptop1 to SW2 via a console cable:



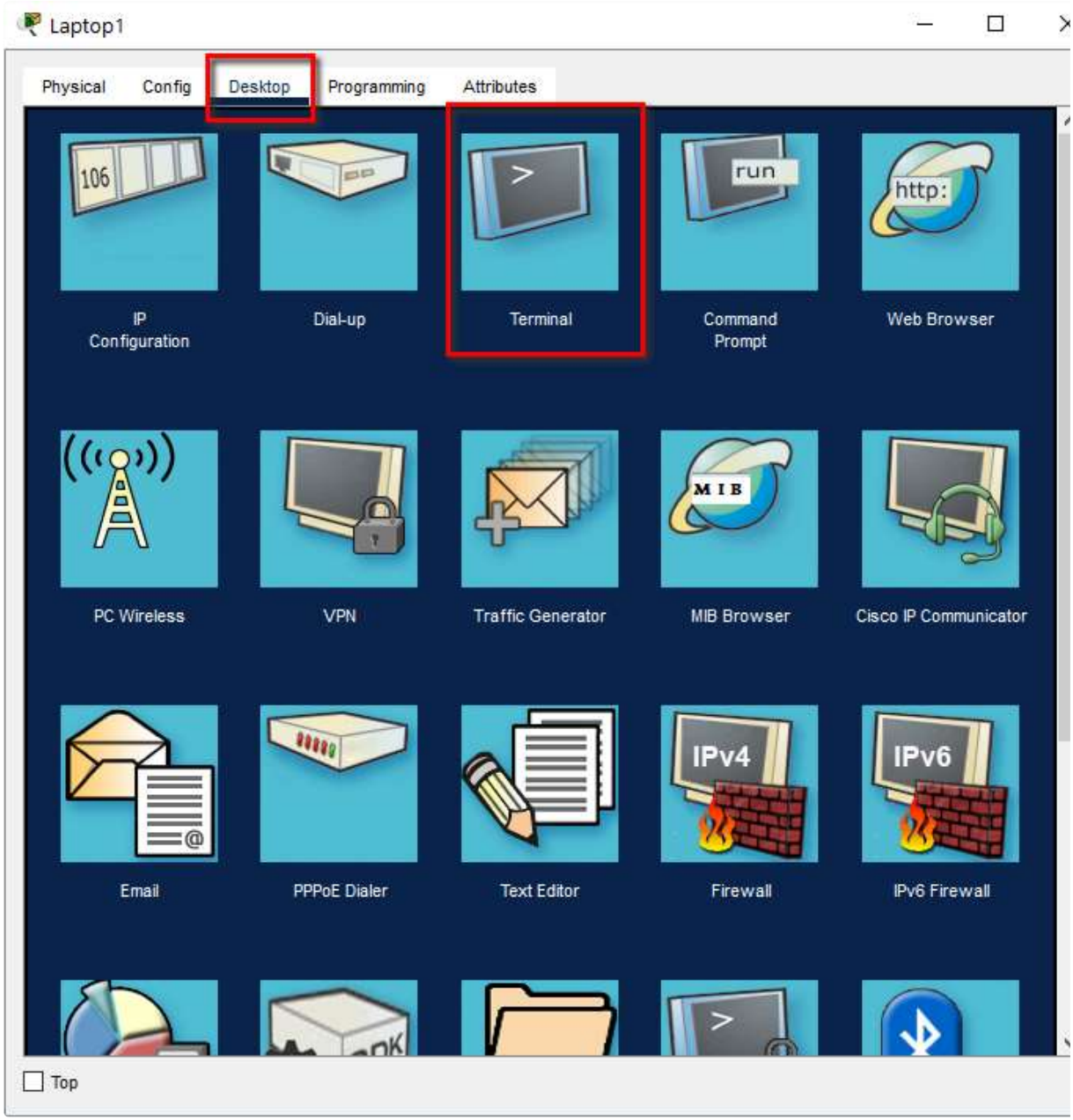
Now make the connection by clicking on Laptop1 and selecting the **RS 232** port:



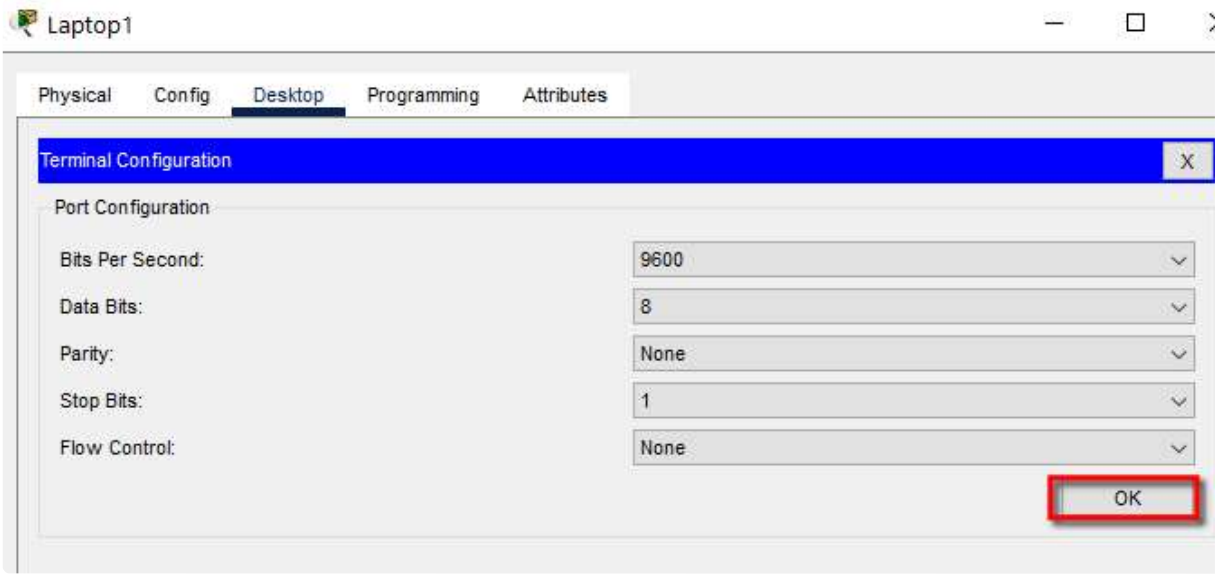
Nex click on SW2 and select the Console port:



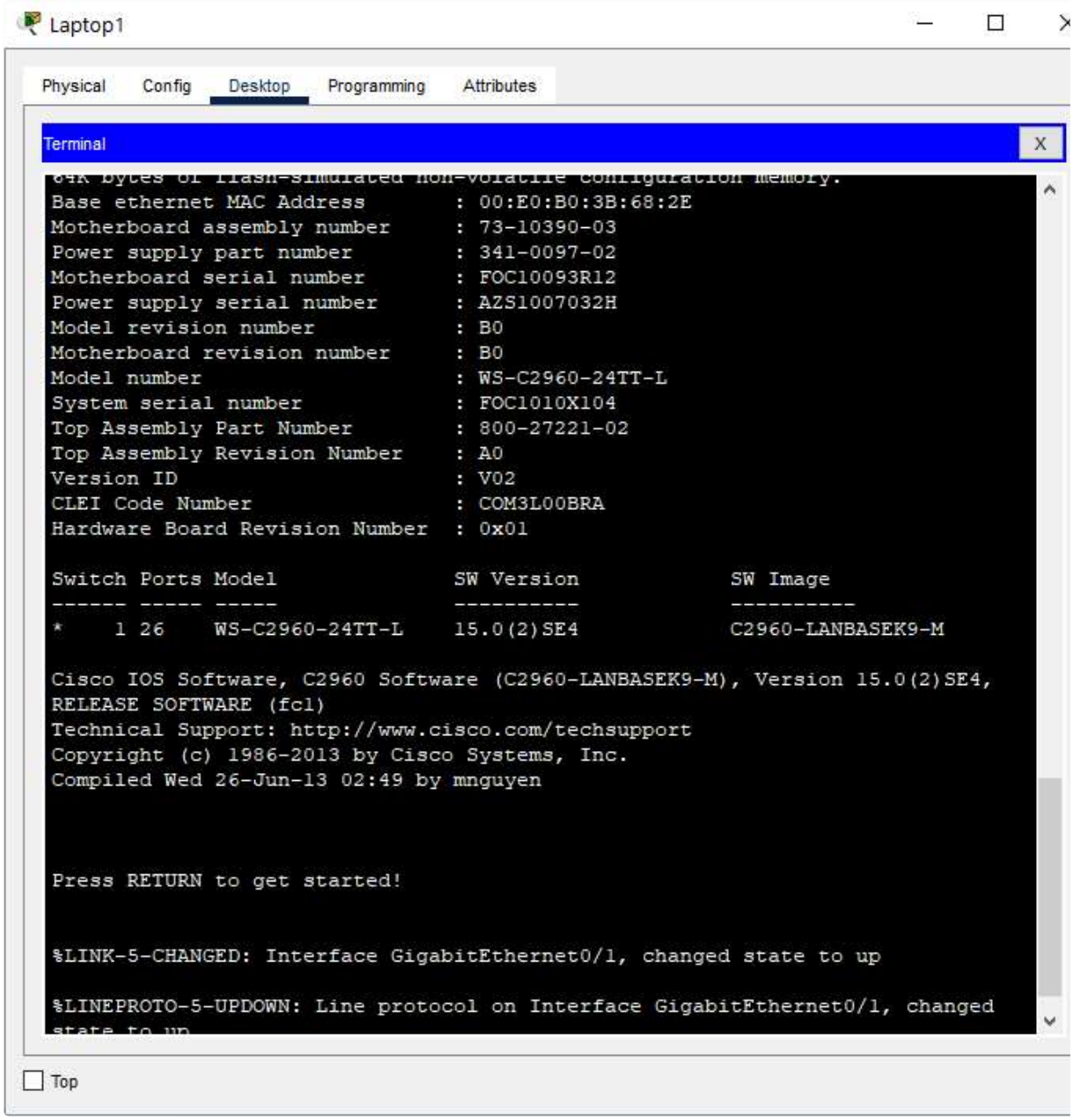
Click on Laptop1 and open the Desktop tab. From there open the Terminal connection:



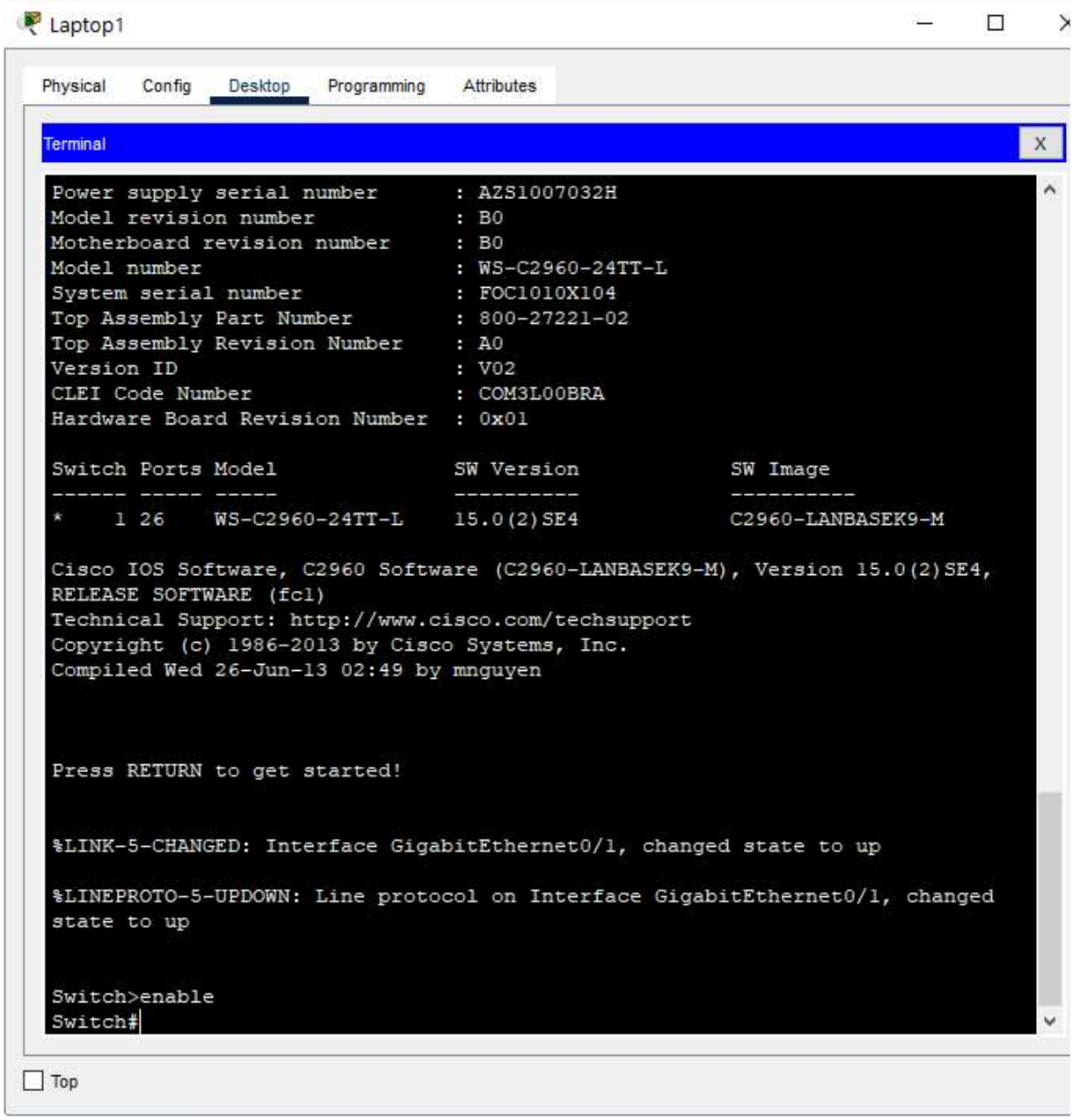
Leave the Terminal Configuration screen at their defaults and hit OK:



If you've followed the previous steps correctly, you should see information about SW2:



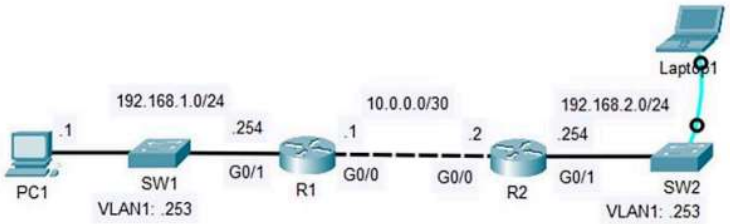
Click in the Terminal > press **Enter** > issue the ***enable*** command:



Now you're ready to actually start the SSH configuration process. Use the below commands to correctly finish the labs:

Required for SSH:

1. Change hostname to anything but the default.
2. The device must have an IP address.
3. Config a DNS domain name
4. Generate RSA key pair
5. Config an enable secret for 'enable mode'.
6. Config a Username/PW for SSH login
7. Config the VTY lines



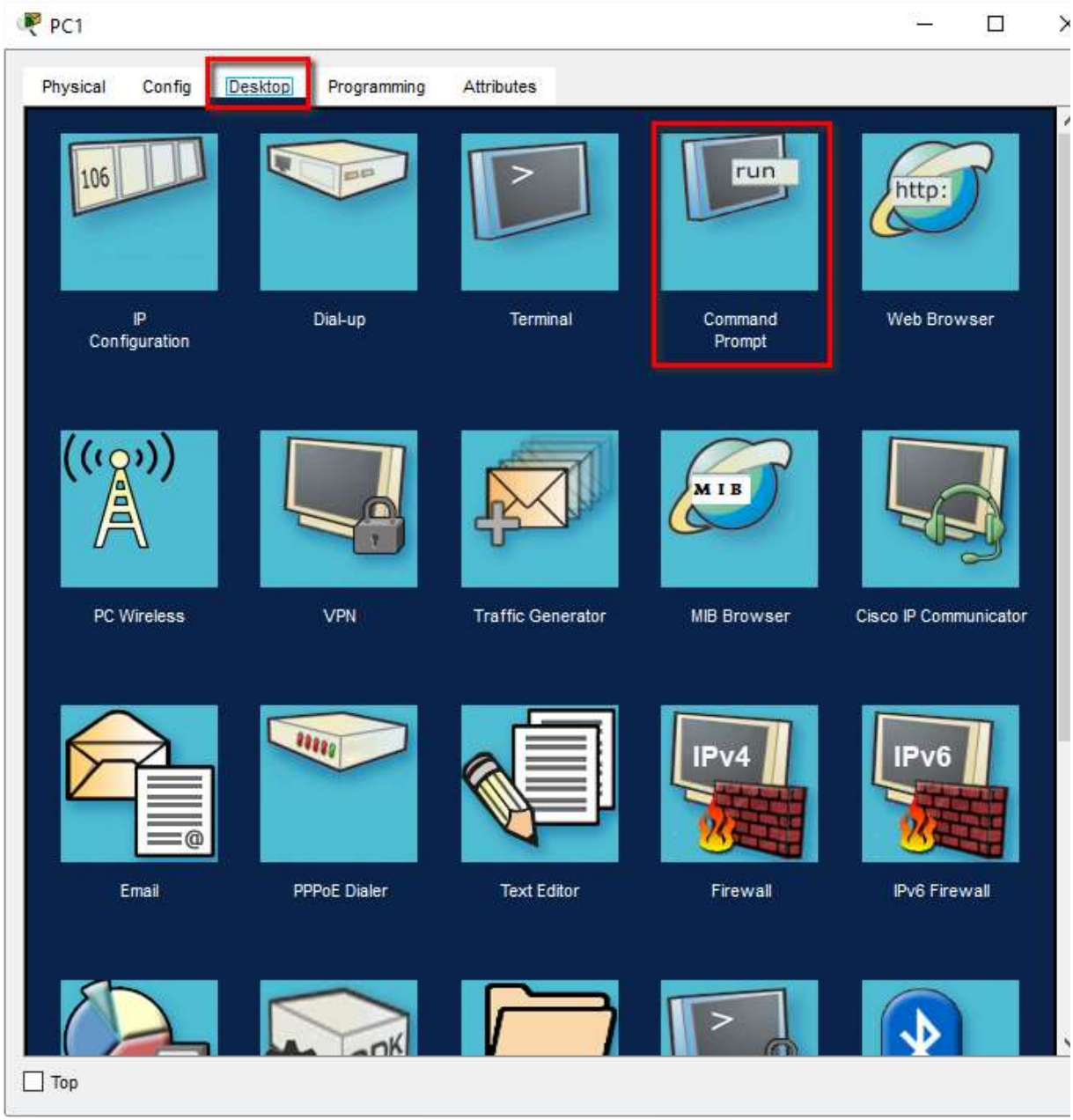
*SW2 has been new ly added to the netw ork, but has not yet been configured.
1.Connect Laptop1 to SW2's console port to perform the follow ing configurations:
Host name: SW2
Enable secret: ccna
Username/PW: aaron/ccna
VLAN1 SVI: 192.168.2.253/24
Default gatew ay: R2

2. Configure the follow ing console line security settings on SW2:
Authentication: Local user
Exec timeout: 5 minutes

3. Configure SW2 for remote access via SSH:
Domain name: aaronguild.net
RSA key size: 2048 bits
Authentication: Local user
Exec timeout: 5 minutes
Protocols: SSH only
+Limit access to PC1 ONLY

`Switch>enable`	Moves you into privileged mode.
`Switch#conf t`	Moves you into global configuration mode on.
`Switch(config)#hostname SW2`	Changes the hostname from Switch to SW2.
`SW2(config)#enable secret ccna`	Configure an enable password in the most secure method supported with a password of **ccna**
`SW2(config)#username aaron secret ccna`	Configure a user named **aaron** with a secret password of **ccna**
`SW2(config)#interface vlan 1`	Create an SVI for remote access
`SW2(config-if)#ip address 192.168.2.253 255.255.255.0`	Config an IP address and mask for SVI
`SW2(config-if)#no shut`	Enable the SVI
`SW2(config-if)#exit`	Exit to global config mode
`SW2(config)#ip default-gateway 192.168.2.254`	Give the Switch a default gateway
`SW2(config)#line console 0` `SW2(config-line)#login local`	Move into console line configuration mode and configure it to require login using the local user database.
`SW2(config-line)#exec-timeout 5`	Config the console to disconnect if idle 5 min
`SW2(config)#ip domain-name aaronguild.net`	Configure a domain-name of **aaronguild.net**
`SW2(config)#crypto key generate rsa`	Generate an RSA key pair using a 2048 bit key.
`SW2(config)#ip ssh version 2`	Enable SSH version 2
`SW2(config)#access-list 1 permit 192.168.1.1`	Configure a standard ACL 1 permitting the management server IP address 192.168.1.1
`SW2(config-line)#line vty 0 15` `SW2(config-line)#login local`	Move into terminal line configuration mode and also configure it to require a login using the local user database
`SW2(config-line)#exec-timeout 5`	Config the VTY lines to disconnect if idle 5 min
`SW2(config-line)#transport input ssh`	Configure the lines to only support SSH logins
`SW2(config-line)#access-class 1 in`	Configure the lines to only allow access from the address specified in ACL 1.

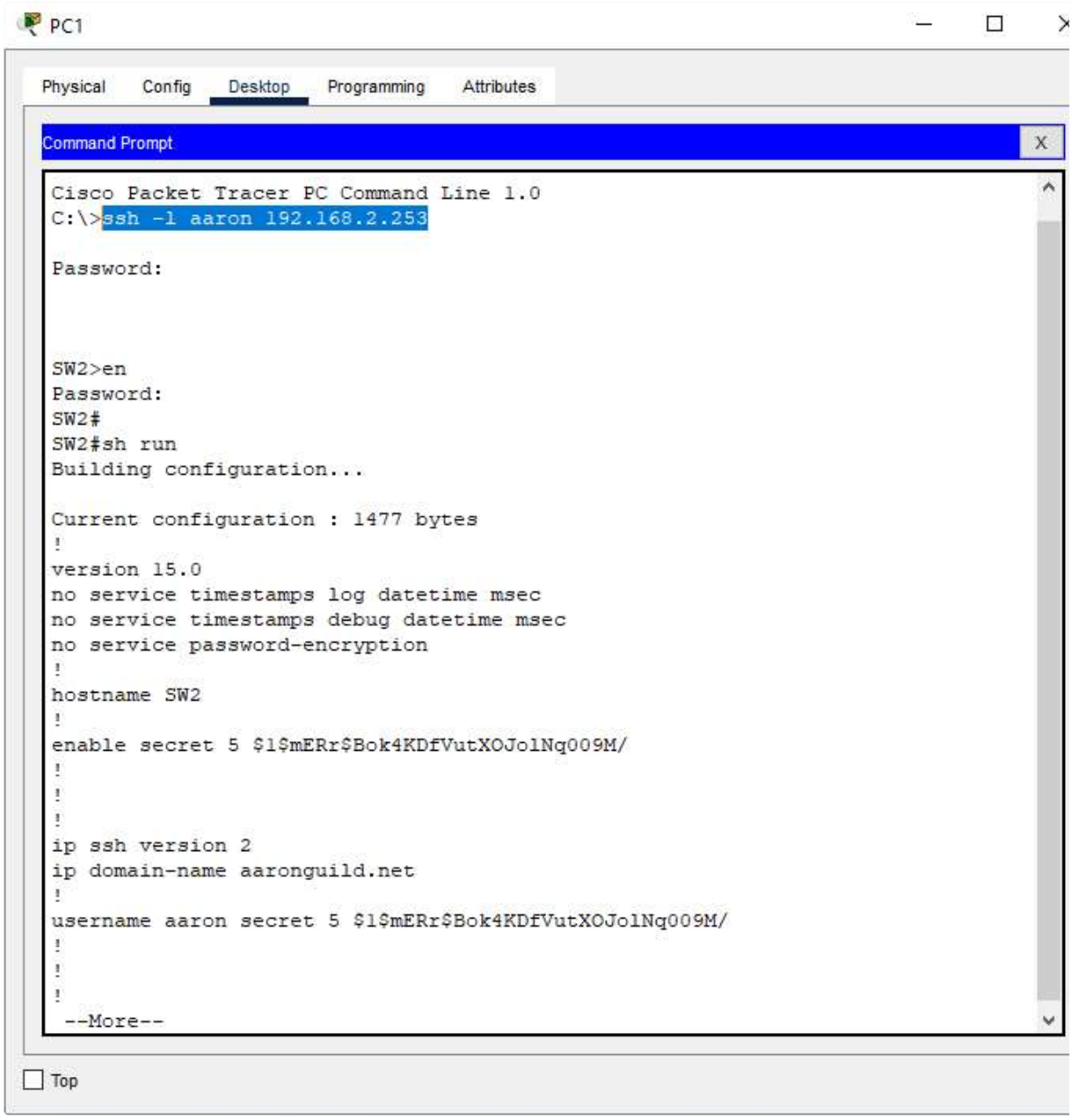
Test the configuration by connecting to SW2 via SSH from PC1 > Desktop > Command Prompt:



In PC1s command prompt issue the following command:

ssh -l aaron 192.168.2.253

Enter the password: **ccna**



And it works! You're now remotely connected to SW2 over the Secure Shell protocol.