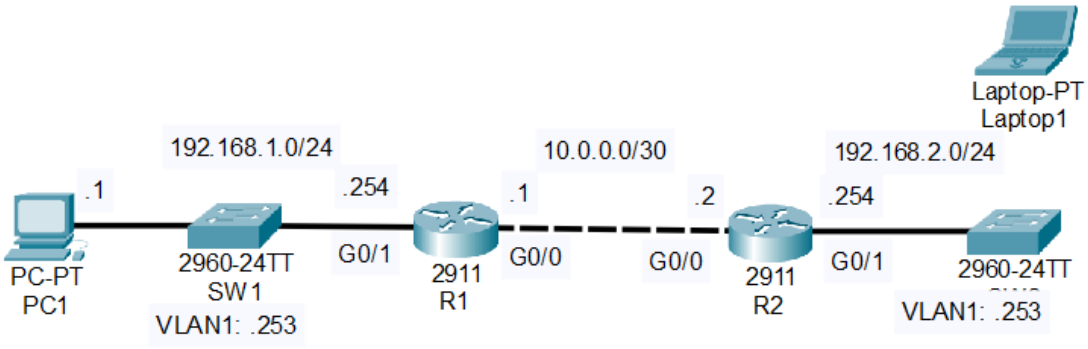
Network Topology:



Instructions and actions:

1. Connect laptop1 to SW2's console port:
   I connected the console port of the laptop with SW2 using a console cable (RS232 from laptop to console port on the switch).
2. Enable the following configurations:
   Hostname: SW2
   Enable secret: ccna
   Username/PW: jeremy/ccna
   Using the Terminal of Laptop1:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW2
SW2(config)#enable secret ccna
SW2(config)#username jeremy secret ccna
SW2(config)#line console 0
SW2(config-line)#login local
SW2(config-line)#exit
SW2(config)#exit
SW2#
%SYS-5-CONFIG_I: Configured from console by console

SW2#exit
```

3. Now, configure VLAN1 SVI: 192.168.2.253/24
   Default gateway: R2
   Commands in the global configuration mode:
   #interface vlan 1
   #ip address 192.168.2.253 255.255.255.0
   #no shutdown
   #exit
   #ip default 192.168.2.254

```
SW2(config)#interface vlan 1
SW2(config-if)#ip address 192.168.2.253 255.255.255.0
SW2(config-if)#no shutdown

SW2(config-if)#
%LINK-3-UPDOWN: Interface Vlan1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

SW2(config-if)#exit
SW2(config)#ip default gateway 192.168.2.254
                   ^
% Invalid input detected at '^' marker.

SW2(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.254
               ^
% Invalid input detected at '^' marker.

SW2(config)#ip default ?
  A.B.C.D  IP address of default gateway
SW2(config)#ip default 192.168.2.254 ?
  <cr>
SW2(config)#ip default 192.168.2.254
```

4. Configure the following console line security settings on SW2:
   Authentication: Local user
   Exec timeout: 5 minutes
   Command for authentication for the local user in the global configuration mode:
   #line console 0
   #login local
   *What do these commands do?
   They tell the switch to use its **local user database** (usernames/passwords stored on the switch) for authentication when someone connects through that line.
   For exec timeout: (user will be logged out after the configured time of inactivity)

```
SW2(config-line)#exec-timeout ?
  <0-35791>  Timeout in minutes
SW2(config-line)#exec-timeout 5
SW2(config-line)#exit
```

5. Configure SW2 for remote access via SSH:
   Domain name: jeremysitlab.com
   RSA key size: 2048 bits
   Authentication: Local user
   Exec timeout: 5 mins
   Protocols: SSH only
   +Limit access to PC1 only

```
SW2(config)#ip domain name jeremysitlab.com
SW2(config)#crypto key generate rsa
The name for the keys will be: SW2.jeremysitlab.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

SW2(config)#do sh ip ssh
*Mar 1 3:59:2.439: %SSH-5-ENABLED: SSH 1.99 has been enabled
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
SW2(config)#ip ssh version 2
SW2(config)#access-list 1 permit host 192.168.1.1
SW2(config)#line vty 0 15
SW2(config-line)#login local
SW2(config-line)#exec-timeout 5
SW2(config-line)#transport input ssh
SW2(config-line)#access-list 1 in
                            ^
% Invalid input detected at '^' marker.

SW2(config-line)#access ?
  <1-199>  IP access list
  WORD     Access-list name
SW2(config-line)#access 1 in
SW2(config-line)#no access 1 in
SW2(config-line)#access-class 1 in
```

*The difference between access-list and access-class:
An access-list is a set of rules that define who is permitted and who is not; meanwhile, an access-class is a command that applies an access-list to a management plane (Eg, VTY lines, Console port, etc)

6. Recheck:

R2 CLI:

```
R2#ping 192.168.2.253

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.253, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

R2#ssh -l 192.168.2.253
% Incomplete command.
R2#ssh -l 192.168.2.253 ?
  -v    Specify SSH Protocol Version
  WORD  IP address or hostname of a remote system
R2#ssh -l ?
  WORD  Login name
R2#ssh -l jeremy 192.168.2.253

% Connection refused by remote host
R2#
```

PC1 Command Prompt: