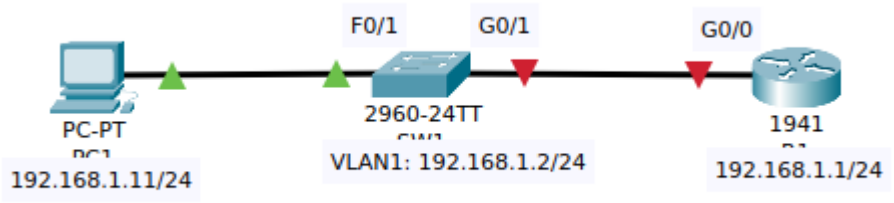
# ACTIVITY 22: Telnet




1: Configure R1's G0/0 interface and SW1's VLAN1 interface with the indicated IP addresses.

--- R1

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

--- To verify it:

```
R1(config-if)#exit
R1(config)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.1.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
R1(config)#
```

--- SW1

```
SW1(config)#interface vlan 1
SW1(config-if)#ip address 192.168.1.2 255.255.255.0
SW1(config-if)#no shutdown
SW1#show ip interface brief
...
Vlan1          192.168.1.2          YES          manual          up      up
```

2: Configure the following user account on SW1 and R1:
username: cisco / password: CCNA

```
R1(config)#username cisco password CCNA
```

3: Configure VTY lines 0 through 15 on SW1 and R1 as follows:

```
R1(config)#line vty 0 15
```

-require the use of the local user database to connect to the vty lines

```
R1(config-line)#login local
```

-allow only telnet connections to the vty lines

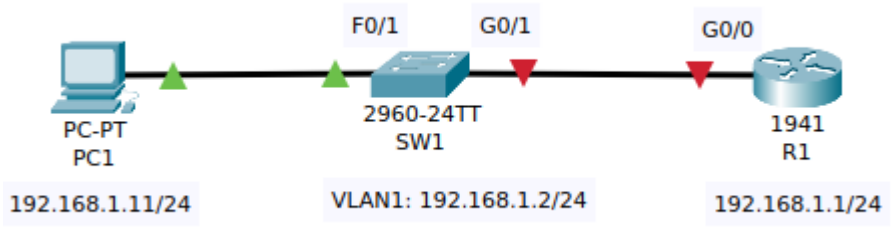
```
R1(config-line)#transport input telnet
```

4: Attempt to telnet to each device from PC1.

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Username: cisco
Password:
R1>
```

```
C:\>telnet 192.168.1.2
Trying 192.168.1.2 ...Open


User Access Verification

Username: cisco
Password:
SW1>
```

## ACTIVITY 23: SSH




- Configure the user account on SW1 and R1: username: cisco / password: CCNA

R1(config)#username cisco password CCNA

- Configure a DNS domain name of cisco.com on SW1 and R1.

R1(config)#ip domain-name cisco.com

- Generate keys to encrypt the SSH packets on each device, with a modulus size of 1024.

R1(config)#crypto key generate rsa
The name for the keys will be: R1.cisco.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]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

- Configure VTY lines 0 through 15 on SW1 and R1 as follows:

R1(config)#line vty 0 15
-- require the use of the local user database to connect to the vty lines
R1(config-line)#login local

-- allow only SSH connections to the vty lines
R1(config-line)#transport input ssh
-- terminate connections after 5 minutes of inactivity
R1(config-line)#exec-timeout 5

- Enable SSH version 2 on each device.

R1(config)#ip ssh version 2

- Attempt to connect to each device using SSH from PC1.