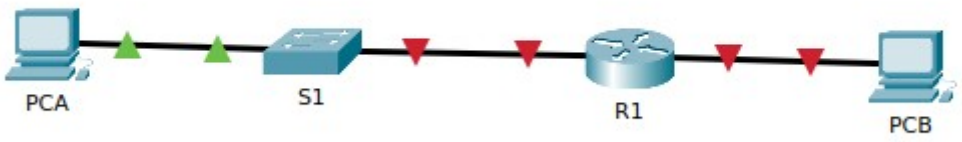
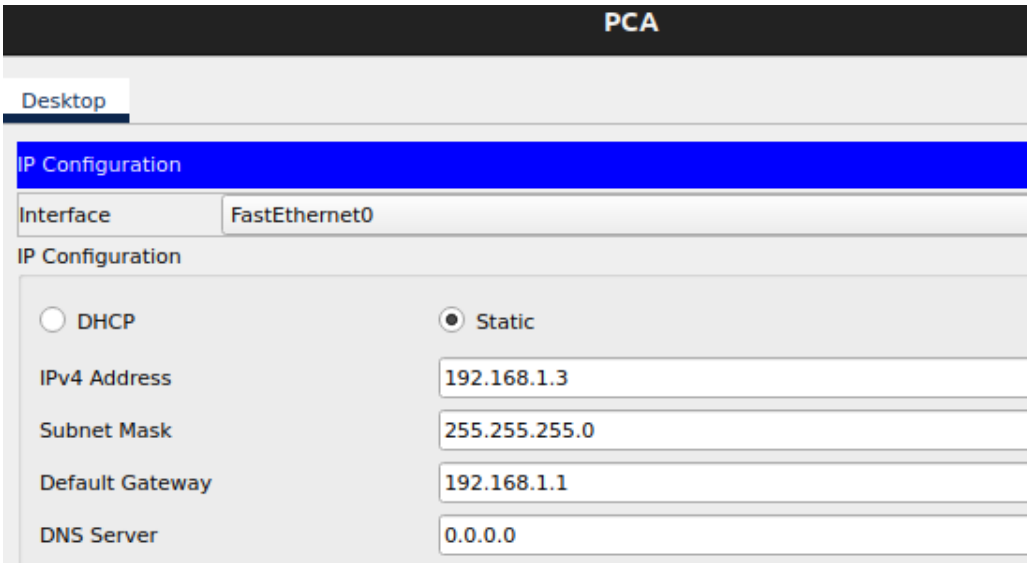
# Packet Tracer - Build a Switch and Router Network

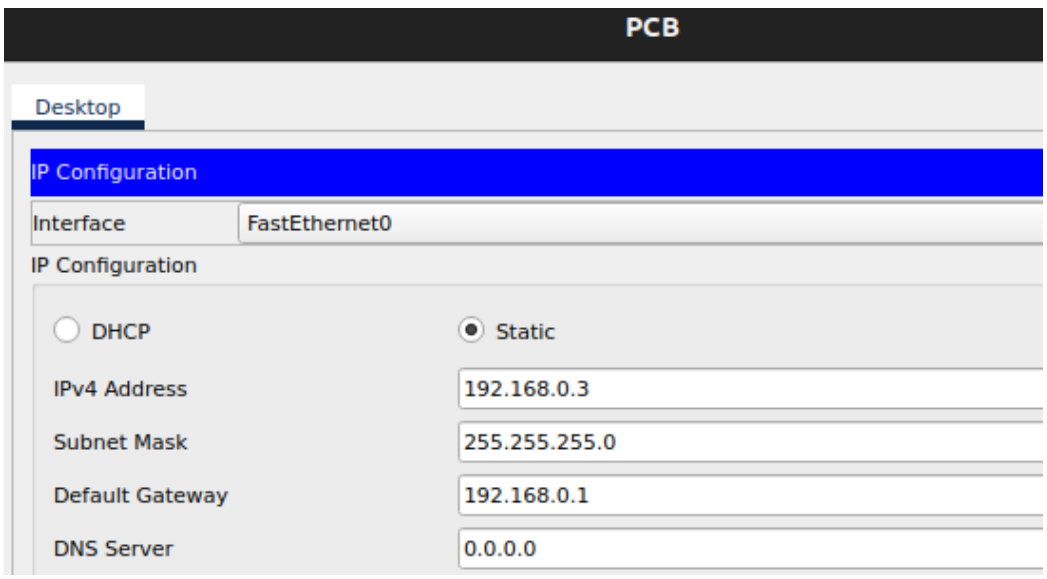



| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| R1 | G0/0/0 | 192.168.0.1 | 255.255.255.0 | N/A |
| | G0/0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
| S1 | VLAN 1 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 |
| PCA | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PCB | NIC | 192.168.0.3 | 255.255.255.0 | 192.168.0.1 |

- Configure the IPv4 address, subnet mask, and default gateway settings on PCA .




- Configure the IPv4 address, subnet mask, and default gateway settings on PCB .



-- On R1:

- Assign a hostname according to the Addressing Table.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

- Assign class as the privileged EXEC encrypted password.

```
R1(config)#enable secret class
```

- Assign cisco as the console password and enable login.

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

- Encrypt the plaintext passwords.

```
R1(config)#service password-encryption
```

- Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

```
R1(config)#banner motd "Unauthorized access is prohibited."
```

- Configure IP addressing of G0/0/0 and activate the interface.

```
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown
```

- Configure IP addressing of G0/0/1 and activate the interface.

```
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

- Save the running configuration to the startup configuration file.

```
R1#write
Building configuration...
[OK]
```

- Ping between PCA and PCB.

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

-- On S1:

- Assign a hostname according to the Addressing Table.

```
Switch>enable
```

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#
```

- Assign class as the privileged EXEC encrypted password.

```
S1(config)#enable secret class
```

- Assign cisco as the console password and enable login.

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

- Encrypt the plaintext passwords.

```
S1(config)#service password-encryption
```

- Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

```
S1(config)#banner motd "Unauthorized access is prohibited."
```

- Configure IP addressing of Vlan 1 and activate the interface.

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.2 255.255.255.0
S1(config-if)#no shutdown
```

- Configure the default gateway according to the Addressing Table.

```
S1(config)#ip default-gateway 192.168.1.1
```

- Save the running configuration to the startup configuration file.

```
S1#write
Building configuration...
[OK]
```

-- On R1:

- Configure the domain name as academy.net.

```
R1(config)#ip domain-name academy.net
```

- Generate RSA keys with a 1024 key length.

```
R1(config)#crypto key generate rsa
The name for the keys will be: R1.academy.net
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]
```

- Create a user with SSHuser as the username and cisco as the secret password.

```
R1(config)#username SSHuser secret cisco
```

- Configure the VTY lines to use the local username database for login credentials. The VTY lines should only allow SSH for remote access.

```
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
```

- Enable ssh version 2
R1(config)#ip ssh version 2

- From PCA or PCB, use the Command Prompt to establish a secure session with R1. At the prompt, use the ssh command.