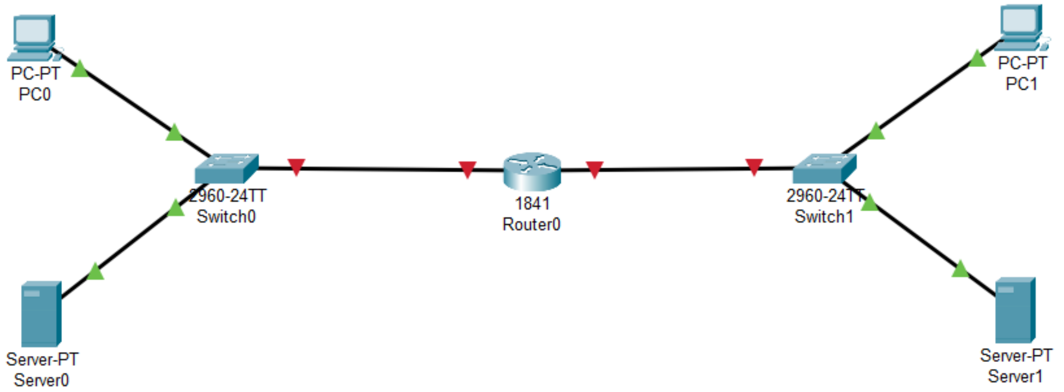
CS-342 Computer Networks Lab

Assignment #5: Cisco Packet Tracer

Group #4: Aditya Patidar, 200101009
Advaita Mallik, 200101010
Akshat Mittal, 200101011
Aman Soni, 200101012

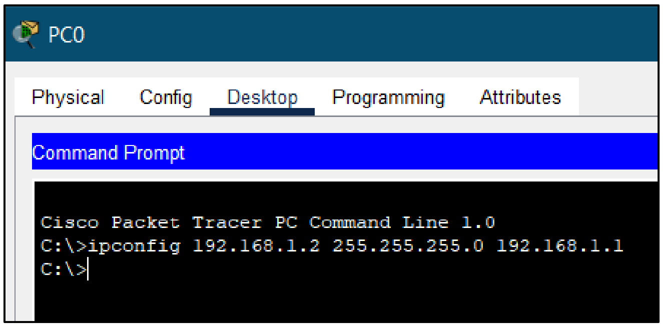
We installed the cisco packet tracer from netacad.com in Windows operating system. After successful installation, first we constructed the required network structure using the available components.



The network consists of two VLANs. Each VLAN consists of a PC, server and a router connecting each of the VLANs via switches.

A. Assign IP address, subnet mask, default gateway to the PC and Server as described in the above table.

For this, we selected each PC/server one by one and from the desktop tab, opened Command Prompt and using *ipconfig <ip-add> <subnet> <gateway>*, added the IP address, subnet and default gateway to them. The corresponding screenshot for PC0 is shown (*rest other were exactly same, no screenshots attached*).



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 192.168.1.2 255.255.255.0 192.168.1.1
C:\>
```

Similarly, the IP address, subnet and gateway were also assigned for PC1, server0 and server1 as per the table.

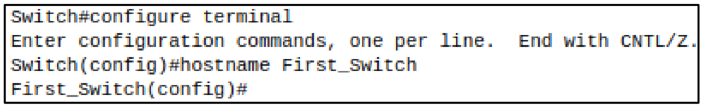
Device	Interface	IP address	Subnet mask	Default Gateway
Router0	fa0/0	192.168.1.1	255.255.255.0	-
Router0	fa0/1	209.165.201.1	255.255.255.0	-
Switch0	VLAN1	192.168.1.5	255.255.255.0	192.168.1.1
Switch1	VLAN2	209.165.201.11	255.255.255.0	209.165.201.1
PC0	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC1	NIC	209.165.201.10	255.255.255.0	209.165.201.1
Server0	NIC	192.168.1.3	255.255.255.0	192.168.1.1
Server1	NIC	209.165.201.13	255.255.255.0	209.165.201.1

B. Configure both the Switches in global configuration mode

Select the switch and open CLI tab. Use *enable* to enter Privileged EXEC mode. Change to Global configuration mode using *configure terminal* command. (*Screenshots attached only for switch0, configuration of switch1 is similar*).

1. Configure Switch hostname: <YourShortName>_Switch

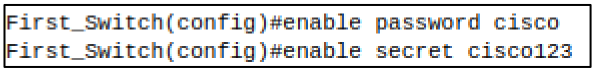
Use the command hostname <name> to change the hostname of the switch. We are using First_Switch for switch0 and Second_Switch for switch1.



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

2. Configure password and secret for privileged mode

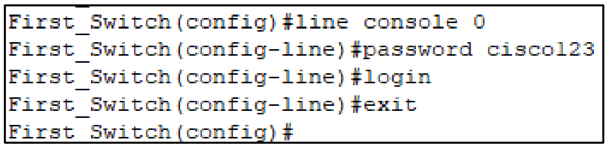
In global configuration mode, use *enable password cisco* and *enable secret cisco123* to achieve the task.



```
First_Switch(config)#enable password cisco
First_Switch(config)#enable secret cisco123
```

- **Configure the console password for global configuration mode**

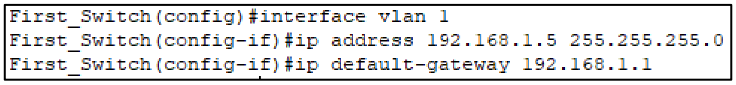
From global configuration mode, switch to line configuration mode using *line console 0* and use *password cisco123* to set console password and *login* to enable password checking at login.



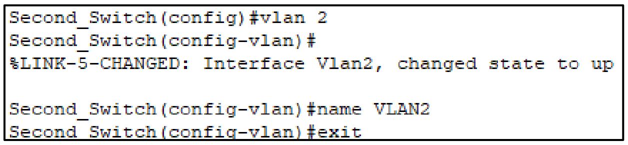
```
First_Switch(config)#line console 0
First_Switch(config-line)#password cisco123
First_Switch(config-line)#login
First_Switch(config-line)#exit
First_Switch(config)#
```

3. Assign given IP addresses to VLANs and default gateways for the switches

In the global configuration mode, first use *interface vlan <vlan_id>* to change to VLAN and then use *ip address <ip-add> <subnet>* to assign IP address and subnet to VLAN. Use *ip default-gateway <gateway>* to set default gateway for the switch. Also use *no shutdown* to change state of vlan to UP. In case of switch1, we first have to create VLAN2 using *vlan 2* command and then assign IP address, subnet and default gateway.



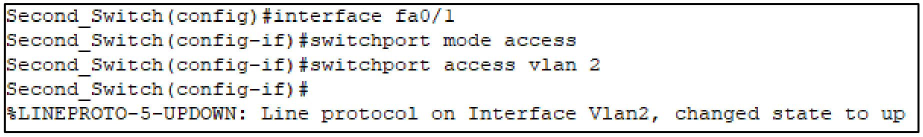
```
First_Switch(config)#interface vlan 1
First_Switch(config-if)#ip address 192.168.1.5 255.255.255.0
First_Switch(config-if)#ip default-gateway 192.168.1.1
```



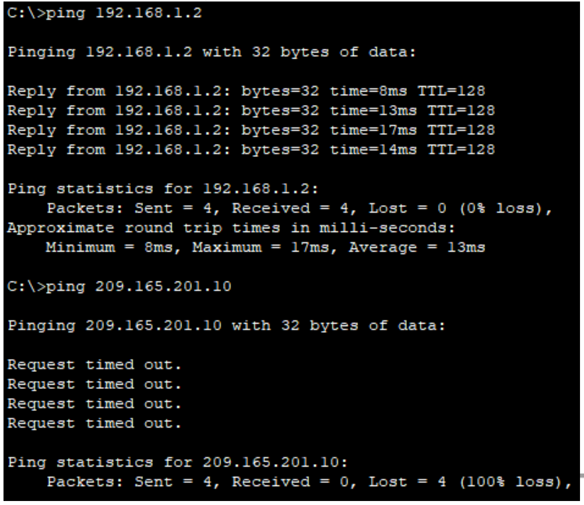
```
Second_Switch(config)#vlan 2
Second_Switch(config-vlan)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

Second_Switch(config-vlan)#name VLAN2
Second_Switch(config-vlan)#exit
```

4. Add corresponding devices to VLANs as show in the diagram

In global configuration mode, change to *interface fa0/1* (one connected to PC1, in switch1) and use *switchport mode access* and *switchport access vlan 2* to add PC1 to this VLAN. Repeat for other ports and similar for switch0 (vlan 1) as well.



```
Second_Switch(config)#interface fa0/1
Second_Switch(config-if)#switchport mode access
Second_Switch(config-if)#switchport access vlan 2
Second_Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
```



```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=13ms TTL=128
Reply from 192.168.1.2: bytes=32 time=17ms TTL=128
Reply from 192.168.1.2: bytes=32 time=14ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 17ms, Average = 13ms

C:\>ping 209.165.201.10

Pinging 209.165.201.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.201.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

After doing this, we were able to ping server0 from PC0 but not able to ping PC1, i.e., we are able to perform intra-vlan communications but not able to perform inter-vlan communications.

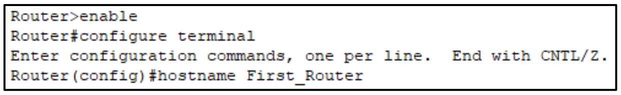
Note: We were also able to ping server1 from PC1, i.e., an intra-vlan communication.

C. Configure Router in global configuration mode

Select the router and open CLI tab. Configuration of router is almost similar to that of switches.

1. Configure router hostname: <YourShortName>_Router

   Use the command hostname <name> to change the hostname of the router. We are using First_Router.



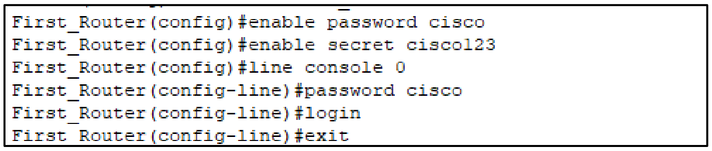
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname First_Router
```

2. Configure the password and secret for privileged mode

   In global configuration mode, use *enable password cisco* and *enable secret cisco123* to achieve the task.

- Configure the console password for global configuration mode

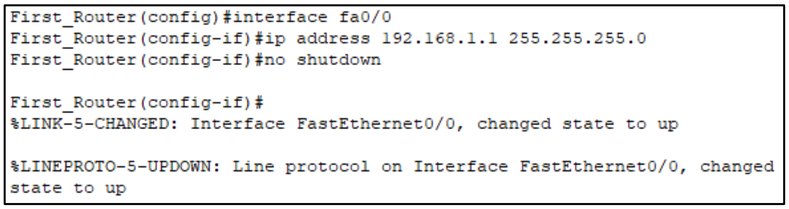
  From global configuration mode, switch to line configuration mode using *line console 0* and use *password cisco* to set console password and *login* to enable password checking at login.



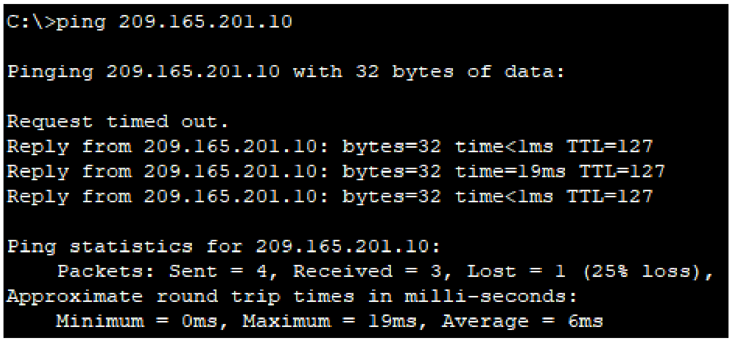
```
First_Router(config)#enable password cisco
First_Router(config)#enable secret cisco123
First_Router(config)#line console 0
First_Router(config-line)#password cisco
First_Router(config-line)#login
First_Router(config-line)#exit
```

3. Assign given IP address, subnet mask to interface fa0/0 and fa0/1 as mentioned in the table

   In the global configuration mode, first use *interface <interface-id>* to change to fa0/0 and then use *ip address <ip-add> <subnet>* to assign IP address and subnet mask to that interface. Use *no shutdown* to change state of the link to UP. Repeat for interface fa0/1.



```
First_Router(config)#interface fa0/0
First_Router(config-if)#ip address 192.168.1.1 255.255.255.0
First_Router(config-if)#no shutdown

First_Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
```



```
C:\>ping 209.165.201.10

Pinging 209.165.201.10 with 32 bytes of data:

Request timed out.
Reply from 209.165.201.10: bytes=32 time<1ms TTL=127
Reply from 209.165.201.10: bytes=32 time=19ms TTL=127
Reply from 209.165.201.10: bytes=32 time<1ms TTL=127

Ping statistics for 209.165.201.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 6ms
```

After doing this, we were able to ping PC1 as well from PC0, i.e., we are able to perform inter-vlan communications successfully.

D. Configure port security in the switch

1. Configure port security for the port used by PC0.

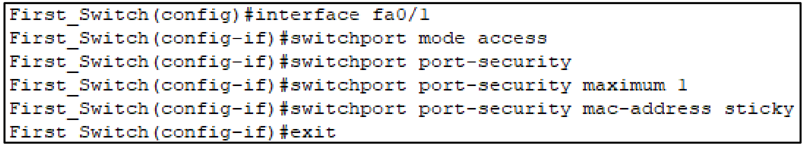
   From global configuration mode, enter *interface fa0/1* to select the port used by PC0 and enter *switchport mode access* to change to access mode of that port.

   I. Enable port security

   Use *switchport port-security* to enable security.

   II. Allow only one MAC address.

   Using *switchport port-security maximum <num>*, we can set maximum number of MAC addresses allowed to num.



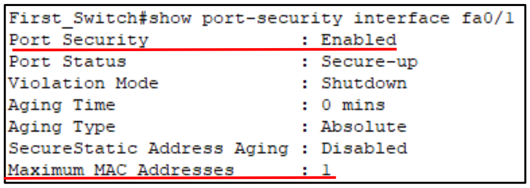
```
First_Switch(config)#interface fa0/1
First_Switch(config-if)#switchport mode access
First_Switch(config-if)#switchport port-security
First_Switch(config-if)#switchport port-security maximum 1
First_Switch(config-if)#switchport port-security mac-address sticky
First_Switch(config-if)#exit
```

   III. Configure the first learned MAC address to “stick” to the configuration

   Using *switchport port-security mac-address sticky*, we can achieve this task.

2. Verify port security enabled for fa0/1.

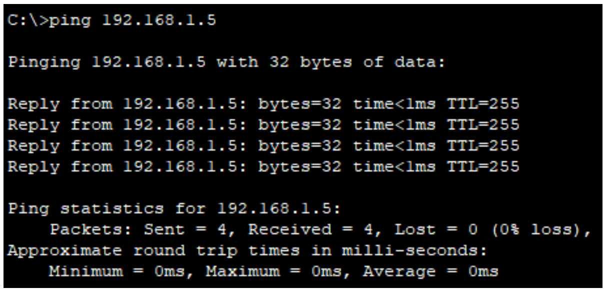
In privileged mode, enter *show port-security interface fa0/1* to see details of fa0/1 interface. We can see that port security is now enabled and maximum MAC address is set to 1.



```
First_Switch#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
```

3. Send ping PC0 to Switch0

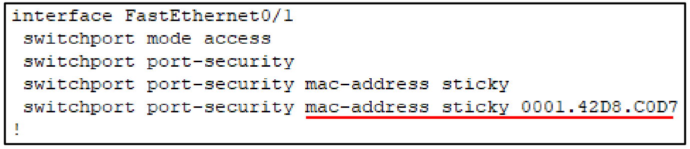
Ping sent to switch0 from pc0 using *ping 192.168.1.5*, i.e., IP address of switch0.



```
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=255
Reply from 192.168.1.5: bytes=32 time<1ms TTL=255
Reply from 192.168.1.5: bytes=32 time<1ms TTL=255
Reply from 192.168.1.5: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4. Now verify whether Switch0 added the MAC address for PC0 to the running configuration

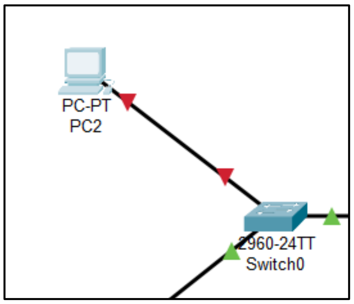
Use *show running-config* in privileged mode to see details of each port. We can clearly see that MAC address of PC0 (i.e., 0001.42D8.C0D7) has been added as sticky mac-address in interface fa0/1.



```
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.42D8.C0D7
!
```

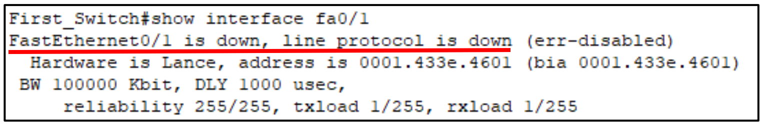
5. Remove connection fa0/1 between Switch0 and PC0 using GUI and connect PC2 to port fa0/1 to cause the port to shut down.

We removed PC0 and attached PC2 to the same port fa0/1 of switch0. Assigned new IP address (192.168.1.4), subnet (255.255.255.0) and default-gateway (192.168.1.2) to it. We can see that the link turned DOWN.



6. Viewing the fa0/1 interface shows that line protocol is down, which indicates the security violation

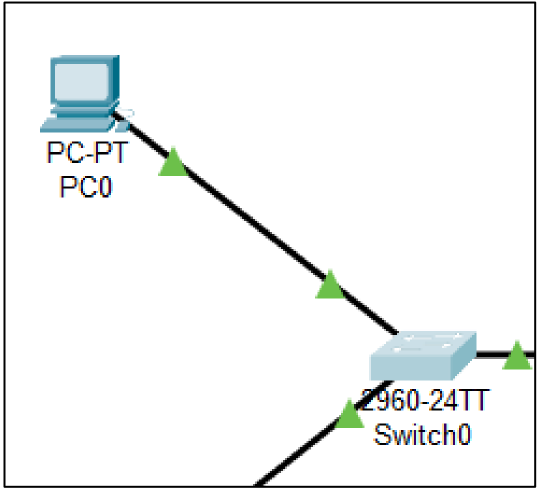
On running *show interface fa0/1*, we can see that the line protocol is down due to different MAC address of the PC2 attached at this port.

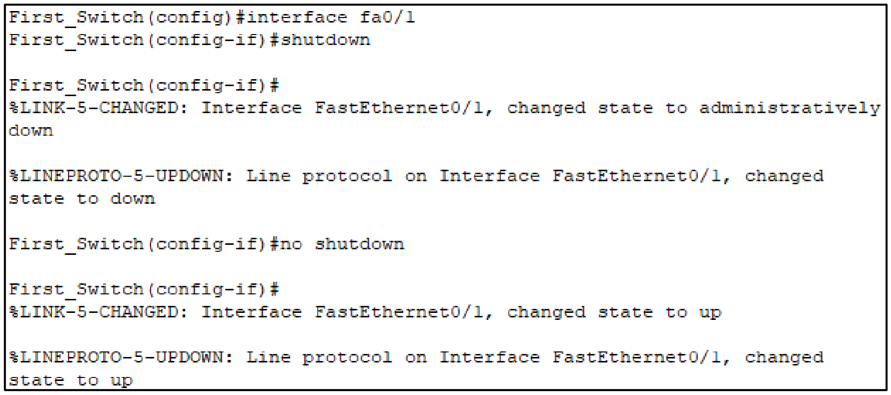


```
First_Switch#show interface fa0/1
FastEthernet0/1 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 0001.433e.4601 (bia 0001.433e.4601)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

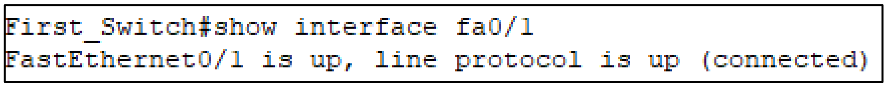
7. Re-connect PC0 with port fa0/1 of Switch 0 using GUI and re-enable the port

We reconnected PC0 back to fa0/1 interface of switch0 and using *no shutdown* command inside this interface, re-enabled the port. Also, we can see that line protocol is UP again.





```
First_Switch(config)#interface fa0/1
First_Switch(config-if)#shutdown

First_Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down

First_Switch(config-if)#no shutdown

First_Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
```

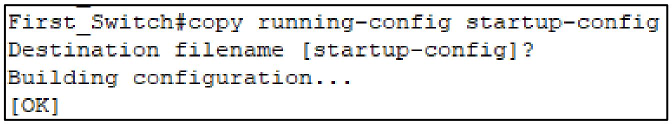


```
First_Switch#show interface fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
```

E. Manage Configuration files

1. Save the current configuration for Switch0 and Router0 to NVRAM.

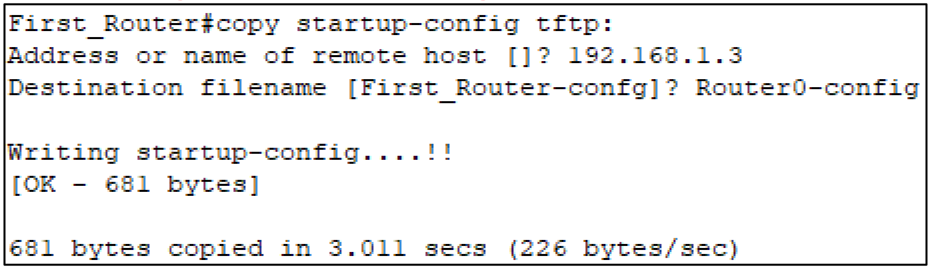
   In privilege mode, use *copy running-config startup-config* to save the current running configuration of device to NVRAM inside the device only.



```
First_Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

2. Back up the startup configuration file on Switch0 and Router0 by uploading them to Server0. (While uploading use file name as Router0-config and Switch0-config).

   After saving to NVRAM, use *copy startup-config tftp:* to backup the file using TFTP server. Enter IP address of server0 and rename the file as required. The file will be copied to server0 within some time.

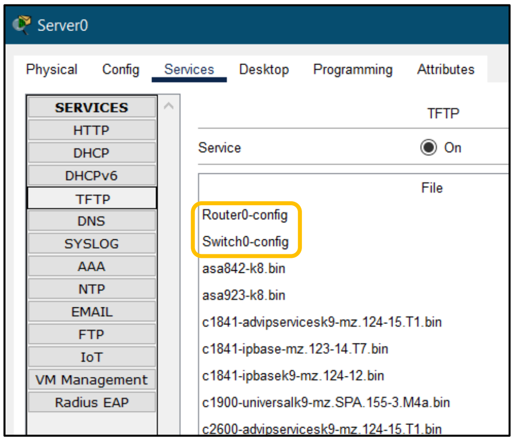


```
First_Router#copy startup-config tftp:
Address or name of remote host []? 192.168.1.3
Destination filename [First_Router-confg]? Router0-config

Writing startup-config....!!
[OK - 681 bytes]

681 bytes copied in 3.011 secs (226 bytes/sec)
```

3. Verify that server has Router0-config and Switch0-config file.

   Select server0 and under Services tab, select TFTP. We can clearly see both the files successfully backed up to server.

   TFTP- Trivial File Transfer Protocol



Service ● On

Router0-config
Switch0-config
asa842-k8.bin
asa923-k8.bin
c1841-advipservicesk9-mz.124-15.T1.bin
c1841-ipbase-mz.123-14.T7.bin
c1841-ipbasek9-mz.124-12.bin
c1900-universalk9-mz.SPA.155-3.M4a.bin
c2600-advipservicesk9-mz.124-15.T1.bin