Final Project DEPI

Implemented by:

Menna Elgamel

Ahmed Abdslam

Fatma Elzhraa Adhem

Abanoub Mores

Hanaa Marzouk

Ahmed Emad

Topology Diagram

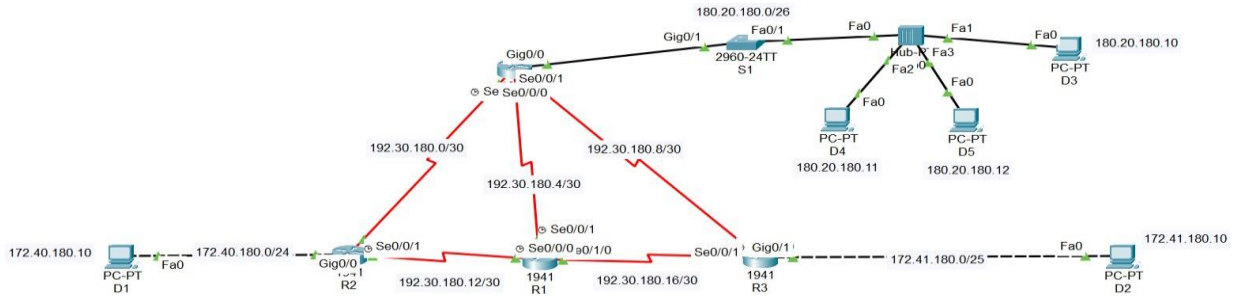

Figure 1 *– Topology Diagram.*

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	S0/0/0	192.30.180.14	255.255.255.252	N/A
	S0/0/1	192.30. 180.6	255.255.255.252	N/A
	S0/1/0	192.30. 180.17	255.255.255.252	N/A
R2	G0/0	172.40. 180.1	255.255.255.0	N/A
	S0/0/0	192.30. 180.1	255.255.255.252	N/A
	S0/0/1	192.30. 180.13	255.255.255.252	N/A
R3	G0/1	172.41. 180.1	255.255.255.128	N/A
	S0/0/0	192.30. 180.18	255.255.255.252	N/A
	S0/0/1	192.30. 180.10	255.255.255.252	N/A
R4	G0/0	180.20. 180.1	255.255.255.192	N/A
	S0/0/0	192.30. 180.2	255.255.255.252	N/A
	S0/0/1	192.30. 180.5	255.255.255.252	N/A
	S0/1/0	192.30. 180.9	255.255.255.252	N/A
S1	VLAN1	180.20. 180.5	255.255.255.192	180.20.XXX.1
D1	NIC	172.40. 180.10	255.255.255.0	172.40.XXX.1
D2	NIC	172.41. 180.10	255.255.255.128	172.41.XXX.1
D3	NIC	180.20.XXX.10	255.255.255.192	180.20.XXX.1

Table 1 *– Addressing table.*

Learning Objectives

Configure Device Basic Settings

Switch Security Configuration

Configure OSPF Dynamic Routing Protocol

Standard ACL configuration

Verify Network Connectivity

Document the configuration.

Scenario

You are asked to configure the routers to support IPv4 connectivity, and LAN redundancy using HSRP. You will also configure OSPF and verify connectivity.

1) **Router interfaces configuration**

Step 1. Configure R1 interfaces

1. Set the Router name as mentioned in table A

2. Configure the interfaces of R1.

- Access each interface.
- Configure the layer 3 IPv4 address (refer to table A for the IP address).
- Set the clock rate on the serial interfaces S0/0/0 and S0/1/0 to 800000.
- Activate the interface.

```
R1(config-if)#int s0/0/0
R1(config-if)#clock
R1(config-if)#clock rate 800000
R1(config-if)#ex
R1(config)#int s0/0/1
R1(config-if)#clock rate 800000
R1(config-if)#ex
R1(config)#int s0/1/0
R1(config-if)#clock rate 800000
This command applies only to DCE interfaces
R1(config-if)#int s0/1/0
R1(config-if)#clock rate 800000
This command applies only to DCE interfaces
R1(config-if)#ex
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#cop
R1#copy r
R1#copy running-config s
R1#copy running-config sta
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figure 2

Step 2. Configure R2 interfaces

1. Set the Router name as mentioned in table A
2. Configure the Interfaces
    - Access each interface.
    - Configure the layer 3 IPv4 address (refer to table A for the IP address) .
    - Set the description on interface G0/0 to "Interface connected to LAN 172.40.180.0/24".
    - Activate the interface

Step 3. Configure R3 interfaces

1. Set the Router name as mentioned in table A
2. Configure the Interfaces
    - Access each interface.
    - Configure the layer 3 IPv4 address (refer to table A for the IP address).
    - Set the description on interface G0/1 to "Interface connected to LAN 172.41.180.0/25".
    - Activate the interface.

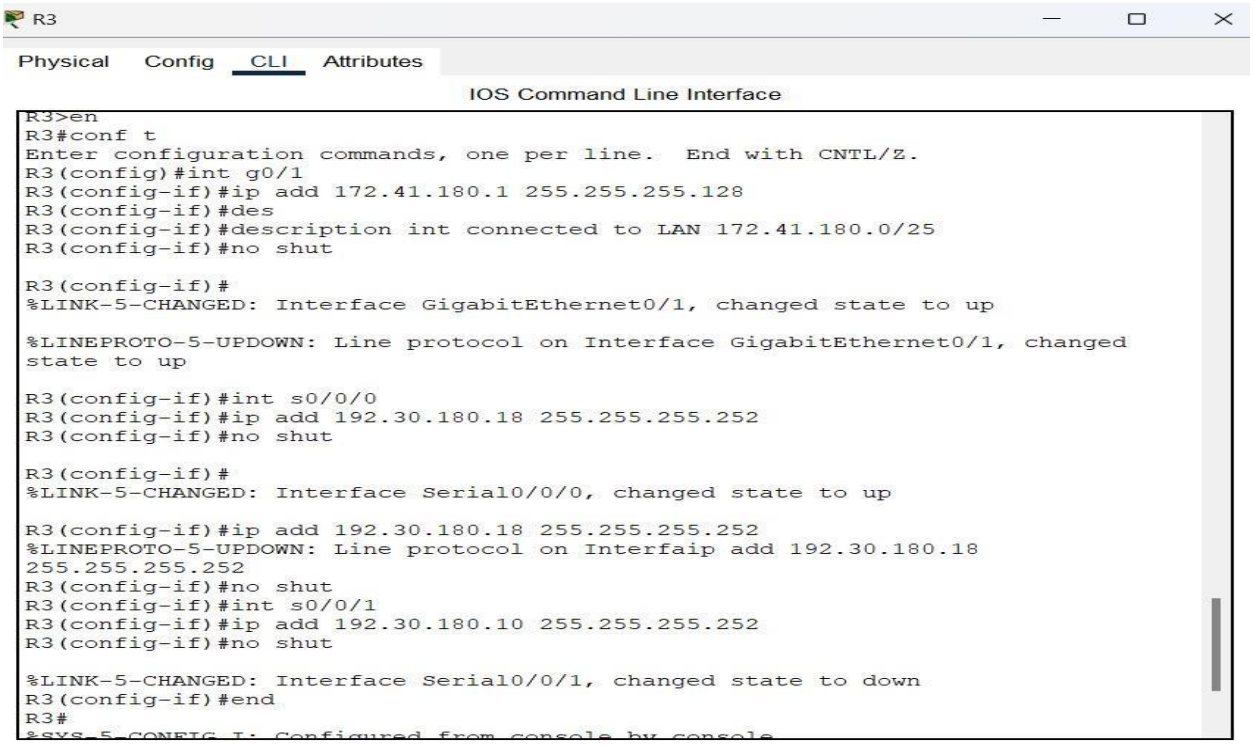

Figure 3

Step 4. Configure R4 interfaces

1. Set the Router name as mentioned in table A
2. Configure the Interfaces
    - Access each interface.
    - Configure the layer 3 IPv4 address (refer to table A for the IP address).
    - Set the description on interface G0/0 to "Interface connected to LAN 180.20.180.0/26".
    - Set the clock rate on the serial interfaces to 800000.
    - Activate the interface.

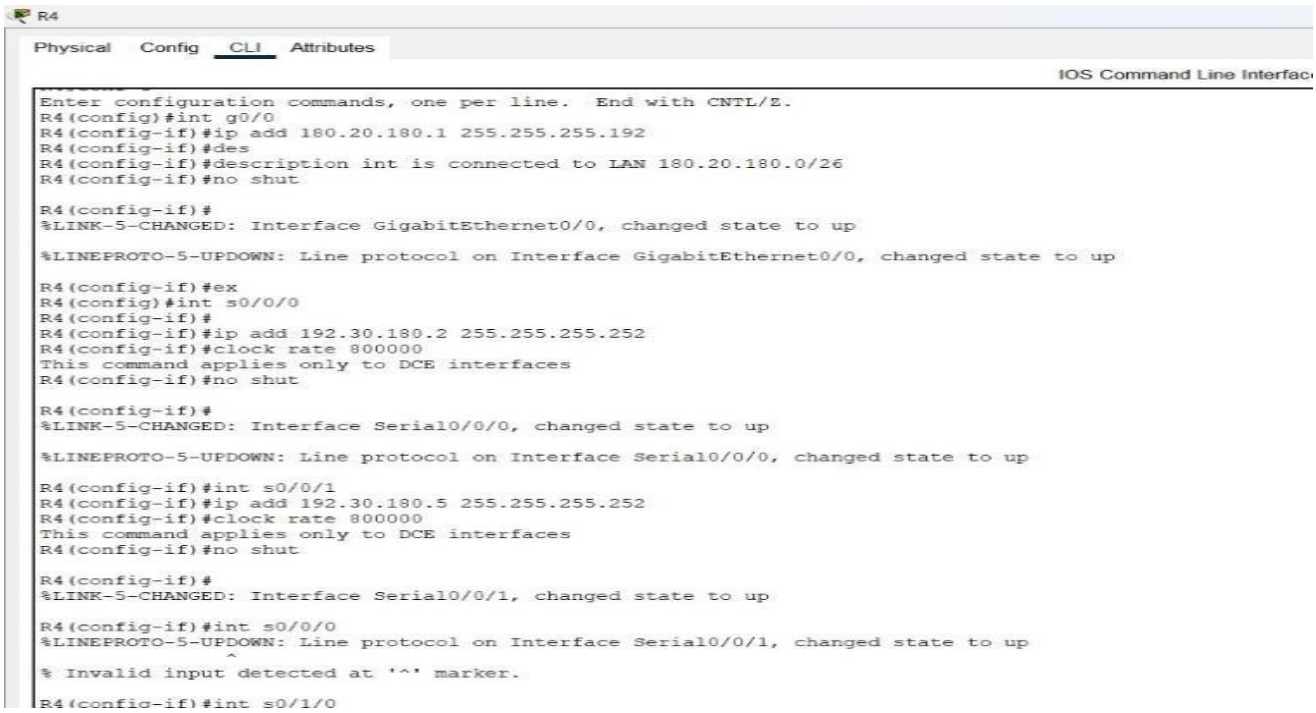

Figure 4

2) PCs' interface configuration

Configure the IPv4 address on the Ethernet interface of the PCs using the "*IP configuration*" mode under the Desktop tab List (Refer to table A).

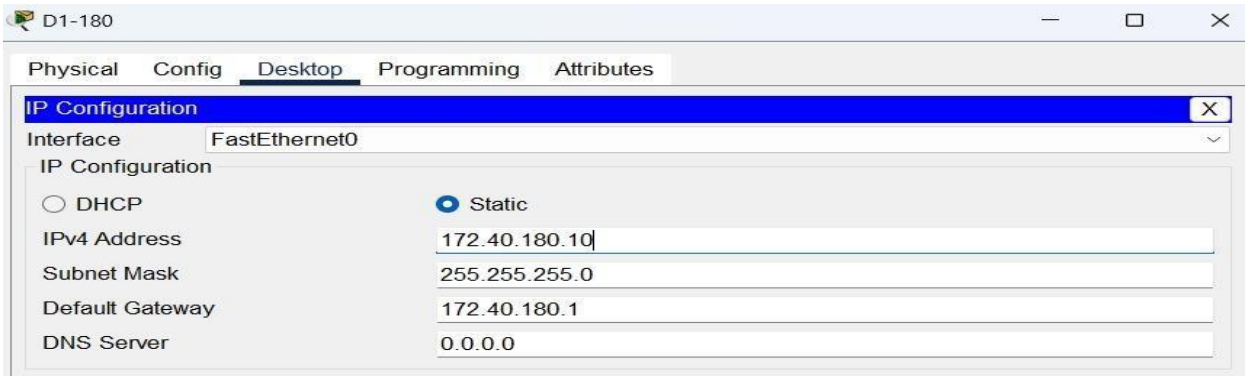

Figure 5

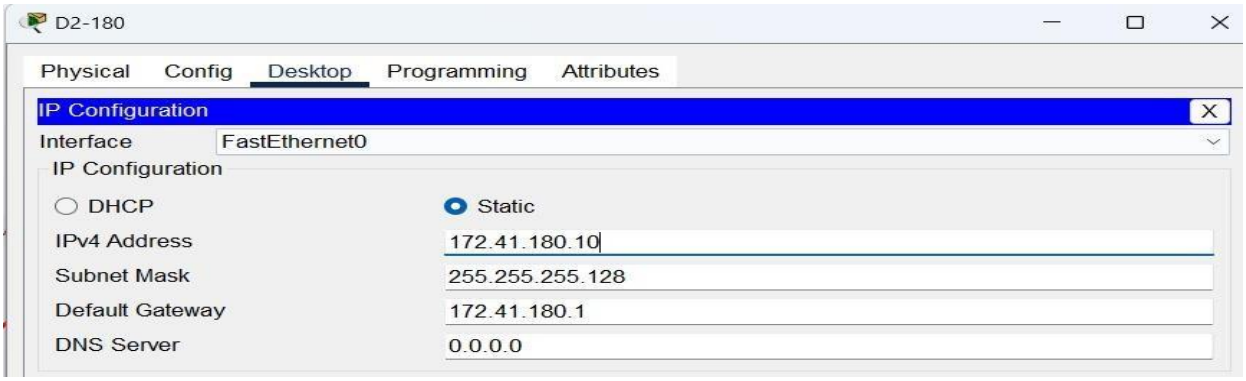

Figure C

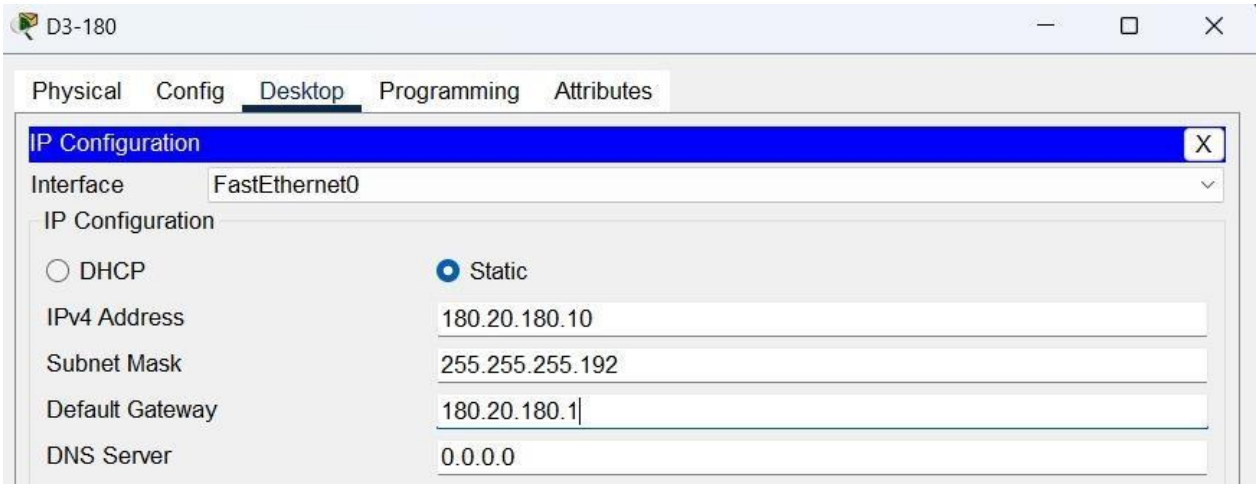

Figure 7

3) **Test the connectivity between all the devices**

- From R4 you need to ping:
  - D3
  - R2 interface S0/0/0
  - R1 interface S0/0/1
  - R3 interface S0/0/1

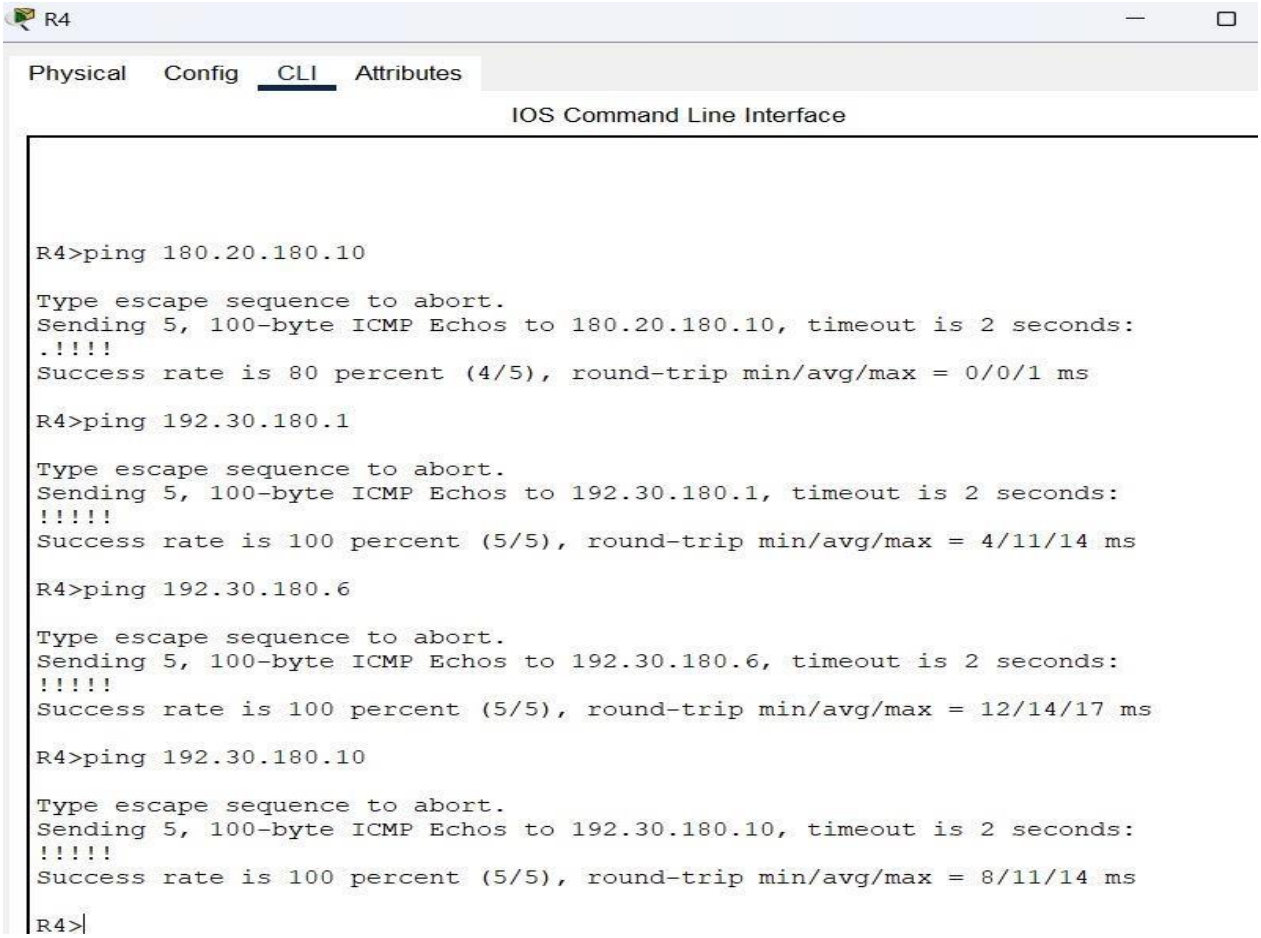

Figure 8

- From R2 you need to ping:
  - D1
  - R1 interface S0/0/0

```
R2>ping 172.40.180.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.40.180.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

R2>ping 192.30.180.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.30.180.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/9/13 ms
```

Figure 3

- From R3 you need to ping:
  - D2
  - R1 interface S0/1/0

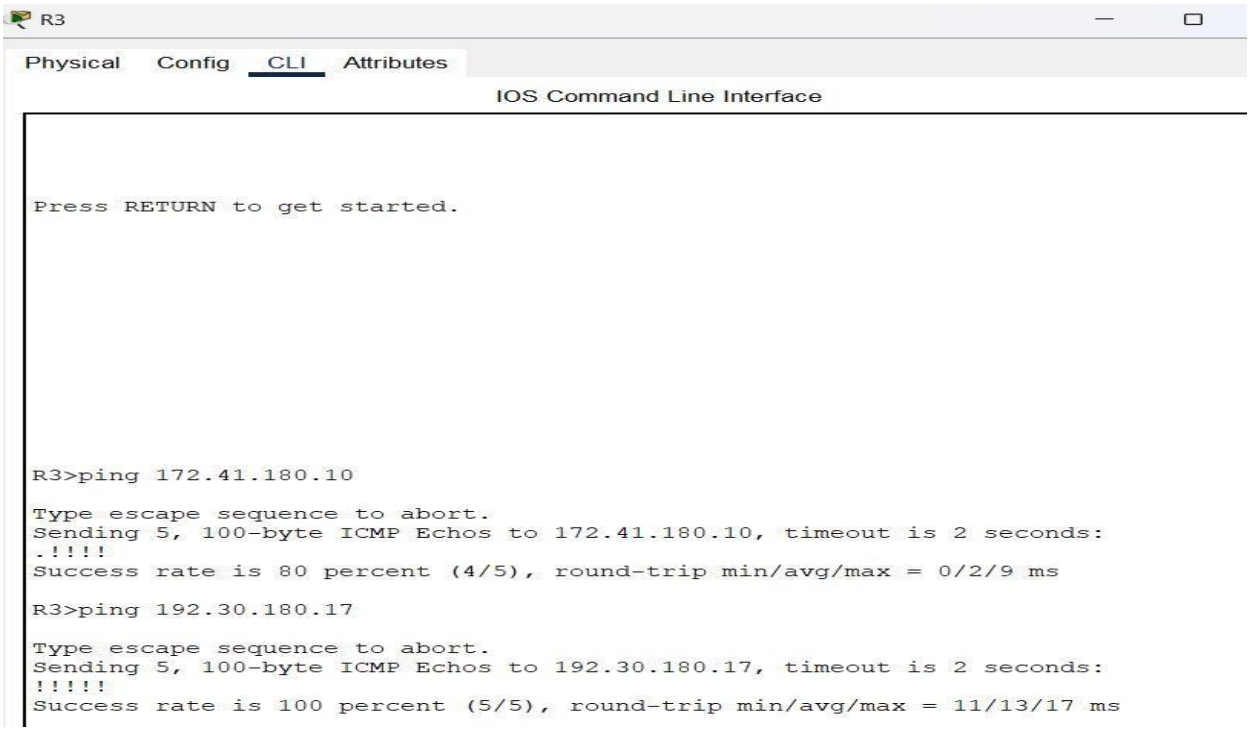

Figure 10

4) **Switch Security**

Step 1. Configure switch security on S1

1. Set the Switch name as mentioned in table A.

2. Enable port security on interface Fa0/1.

3. Display the current port security settings for Fa0/1.

4. Set the maximum number of MAC addresses allowed to 2.

5. Enable the switch to dynamically learn the MAC address and stick them to the running configuration.

C. Set the port security violation mode to *restrict*.

7. Display the current port security settings for G0/1.

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/1
S1(config-if)#switchport port-security max 2
S1(config-if)#switchport port-security mac
S1(config-if)#switchport port-security mac-address ST
S1(config-if)#switchport port-security mac-address STicky
S1(config-if)#switchport port-security viol
S1(config-if)#switchport port-security violation r
S1(config-if)#switchport port-security violation restrict
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Figure 11

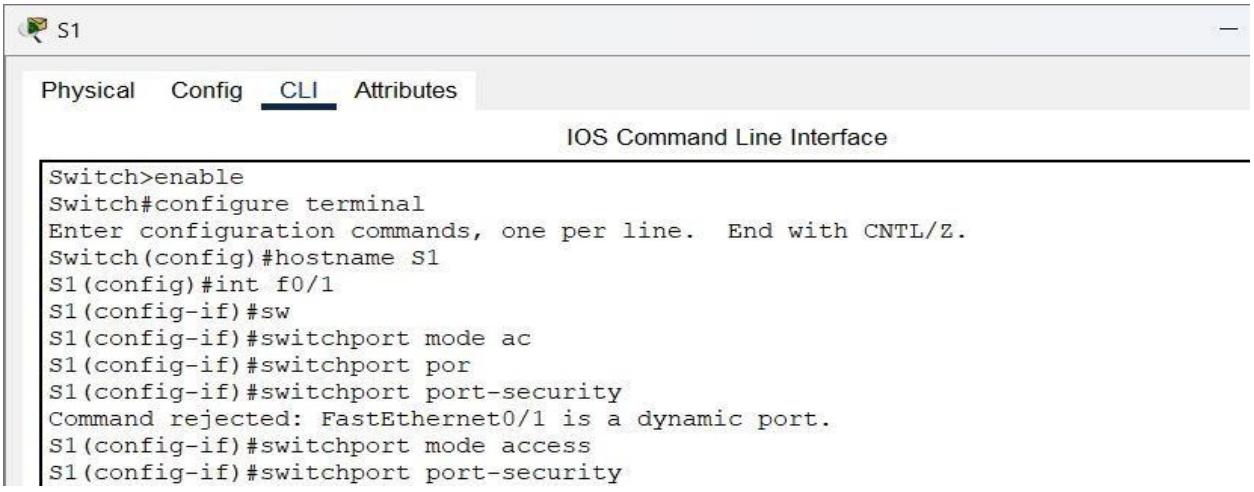

Figure 12

Step 2. Testing the Switch Security

1. Add 2 more PCs (respectively D4 and D5) to the hub using a copper Straight-Through cable and assign to each one an IP address from the network 180.20.180.0/26 (respectively .11 and .12)
2. From D3 ping R4 interface G0/0 (180.20. 180.1)
3. From D4 ping R4 interface G0/0 (180.20. 180.1)
4. From D5 ping R4 interface G0/0 (180.20. 180.1)
5. In one snapshot include the ping of each of the 3 PCs.
6. Verify that MAC addresses are "sticking" to the configuration using the ***show run*** command
7. Include a snapshot of the running configuration that display the mac addresses that are "sticking"
8. Include a snapshot of the packet tracer showing all the devices connected

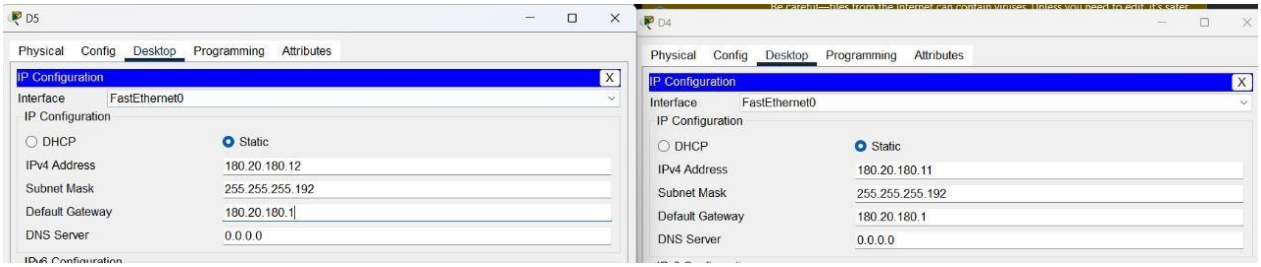

Figure 13

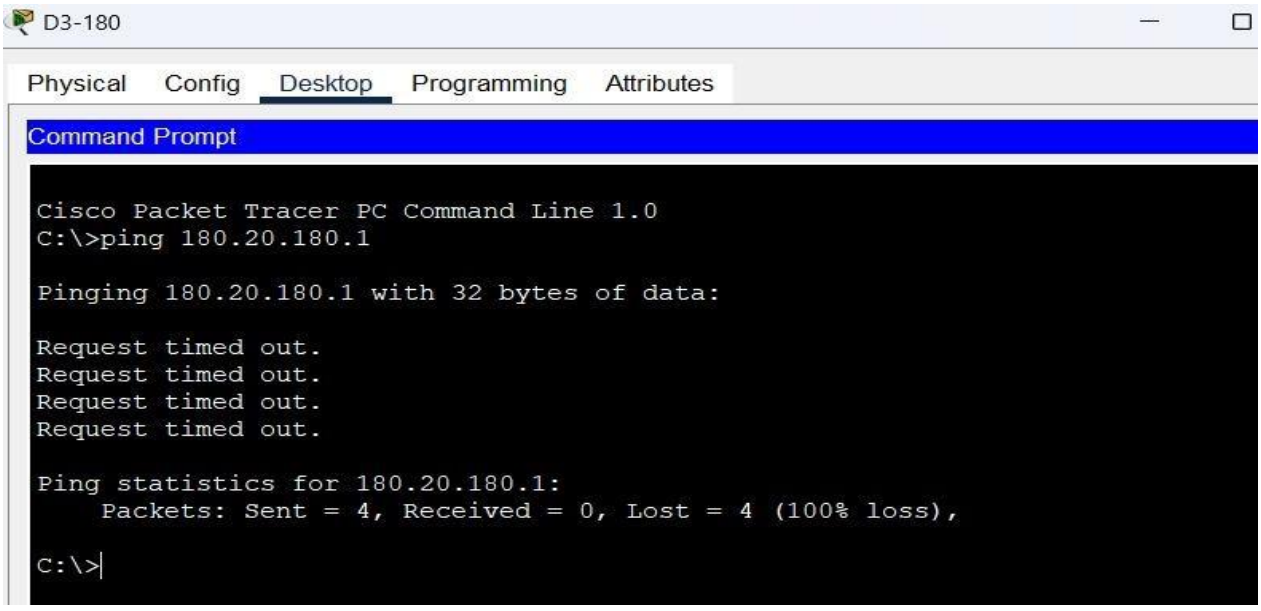

Figure 14

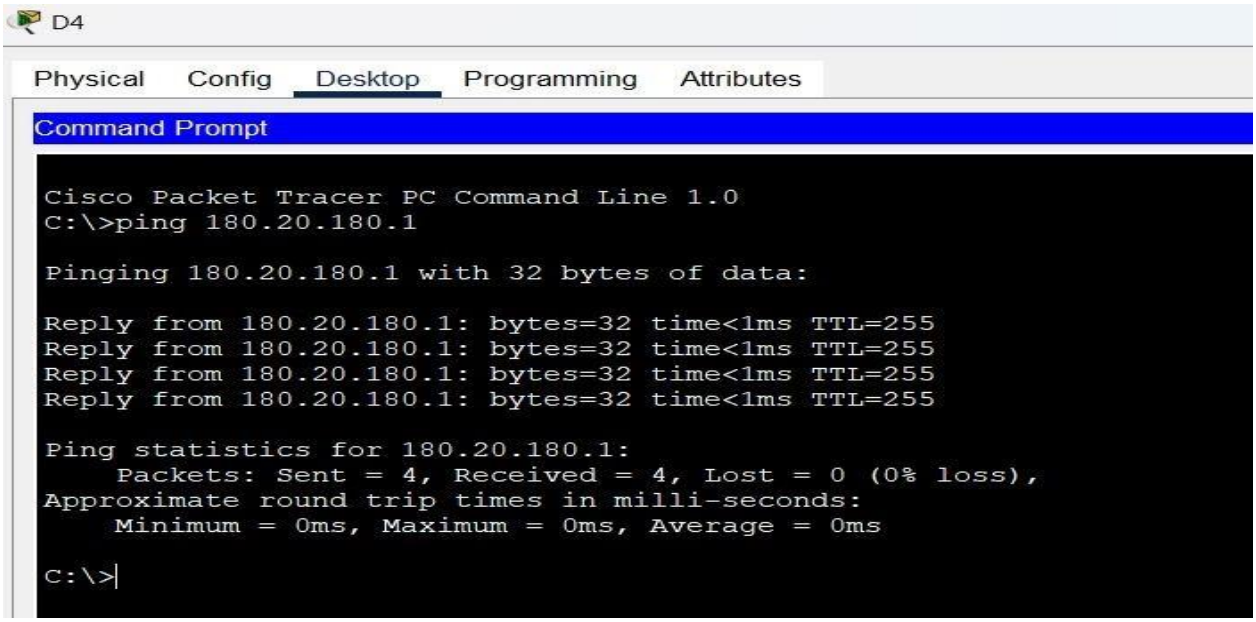

Figure 15

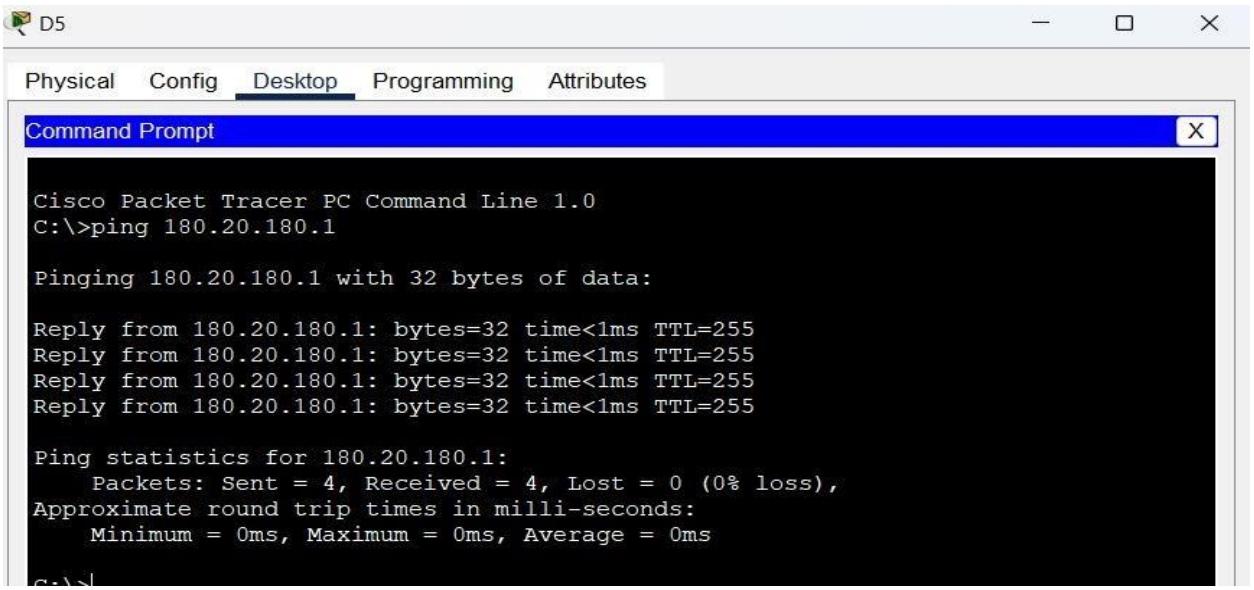

Figure 1C

5) Configure OSPF Dynamic Routing Protocol

Step 1. Configure OSPF on R1

1. Configure OSPF on R1
2. Advertise all the directly connected networks in area 0.
    - Use classless network addresses.

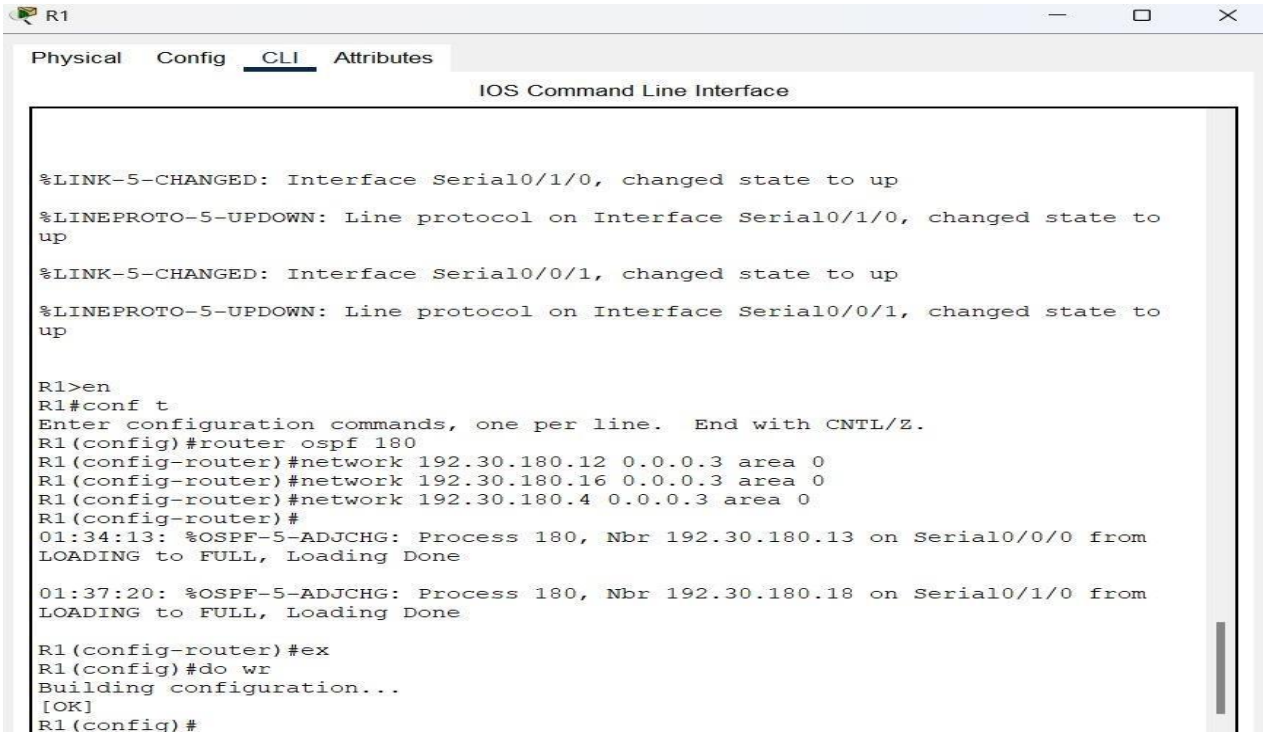

Figure 17

Step 2. Configure OSPF on R2

1. Configure OSPF on R2
2. Advertise all the directly connected networks in area 0.
    - Use classless network addresses.
3. Set only interface G0/0 as passive.

Step 3. Configure OSPF on R3

1. Configure OSPF on R3
2. Advertise all the directly connected networks in area 0.
    - Use classless network addresses.
3. Set interface G0/1 as passive.

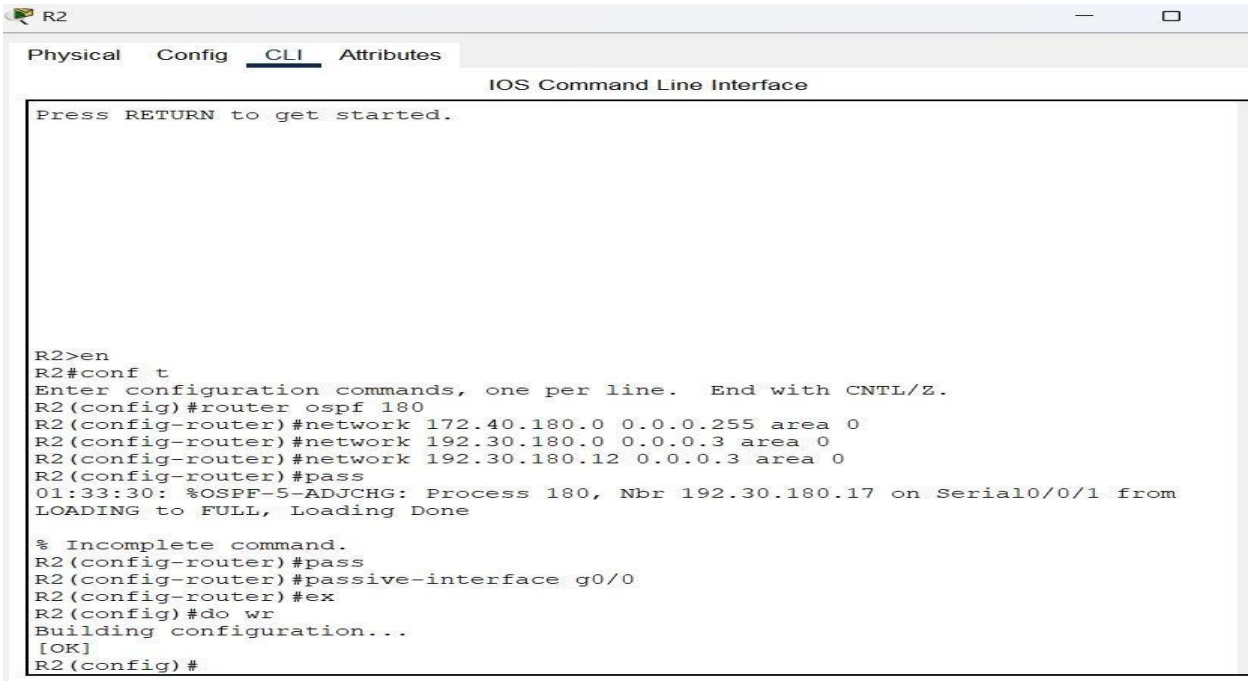

Figure 18

Step 4. Configure OSPF on R4

1. Configure OSPF on R4
2. Advertise all the directly connected networks in area 0.
    - Use classless network addresses.
3. Set interface G0/0 as passive.

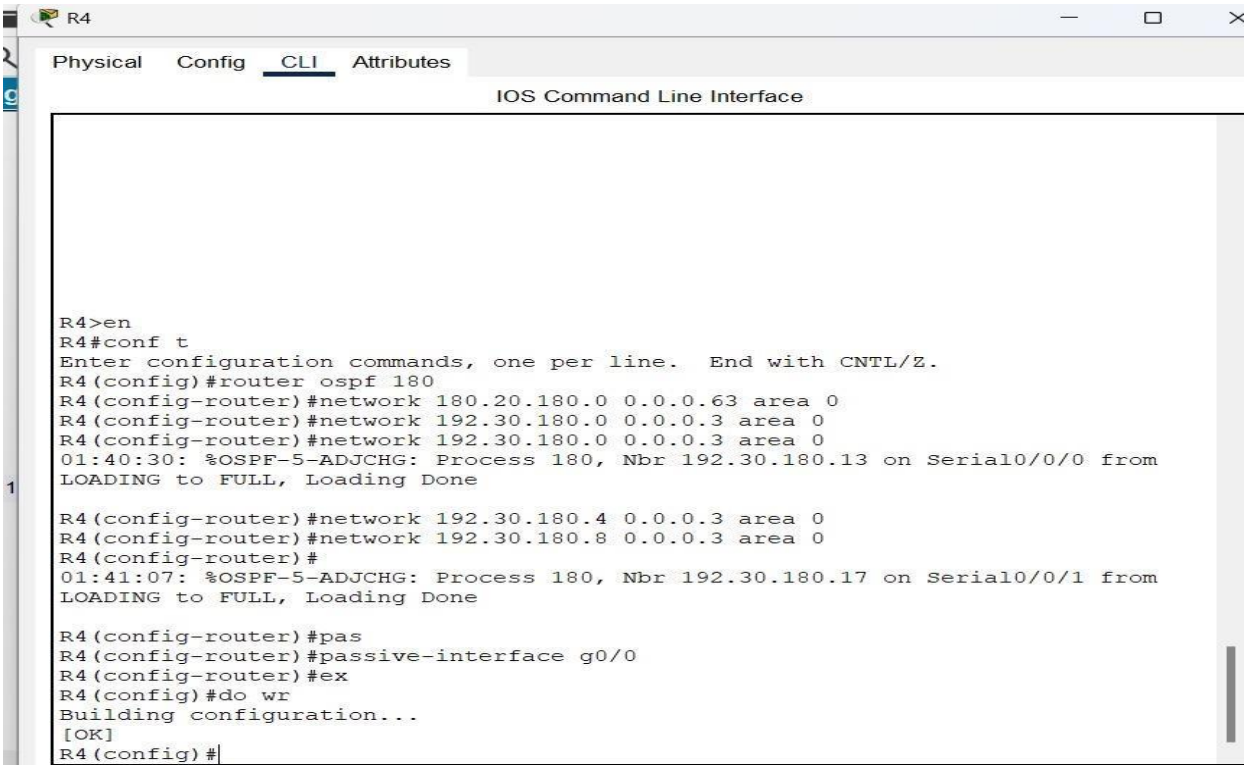

Figure 13

6) Verify OSPF configuration

A) Display the routing table on router R1. Include a screenshot of the routing table (use the ***show ip route ospf*** command to display the routing table)

```
R1#show ip route ospf
     172.40.0.0/24 is subnetted, 1 subnets
O       172.40.180.0 [110/65] via 192.30.180.13, 00:08:51, Serial0/0/0
     172.41.0.0/25 is subnetted, 1 subnets
O       172.41.180.0 [110/65] via 192.30.180.18, 00:05:44, Serial0/1/0
     180.20.0.0/26 is subnetted, 1 subnets
O       180.20.180.0 [110/65] via 192.30.180.5, 00:01:25, Serial0/0/1
     192.30.180.0/24 is variably subnetted, 8 subnets, 2 masks
O       192.30.180.0 [110/128] via 192.30.180.13, 00:01:25, Serial0/0/0
                     [110/128] via 192.30.180.5, 00:01:25, Serial0/0/1
O       192.30.180.8 [110/128] via 192.30.180.5, 00:01:25, Serial0/0/1
```

Figure 22

B) From D1 ping:

- D2 (172.41. 180.10)
- D3 (180.20. 180.10)
- D4 (180.20. 180.11)
- D5 (180.20. 180.12)

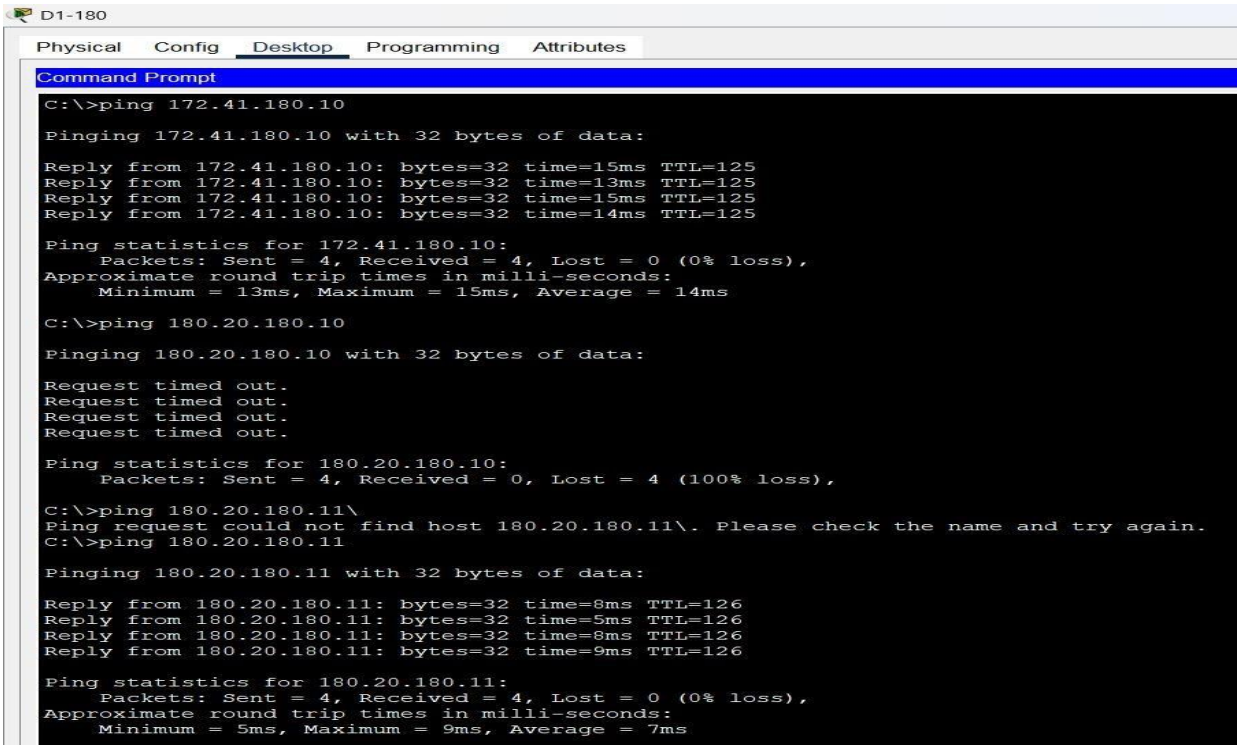

Figure 21

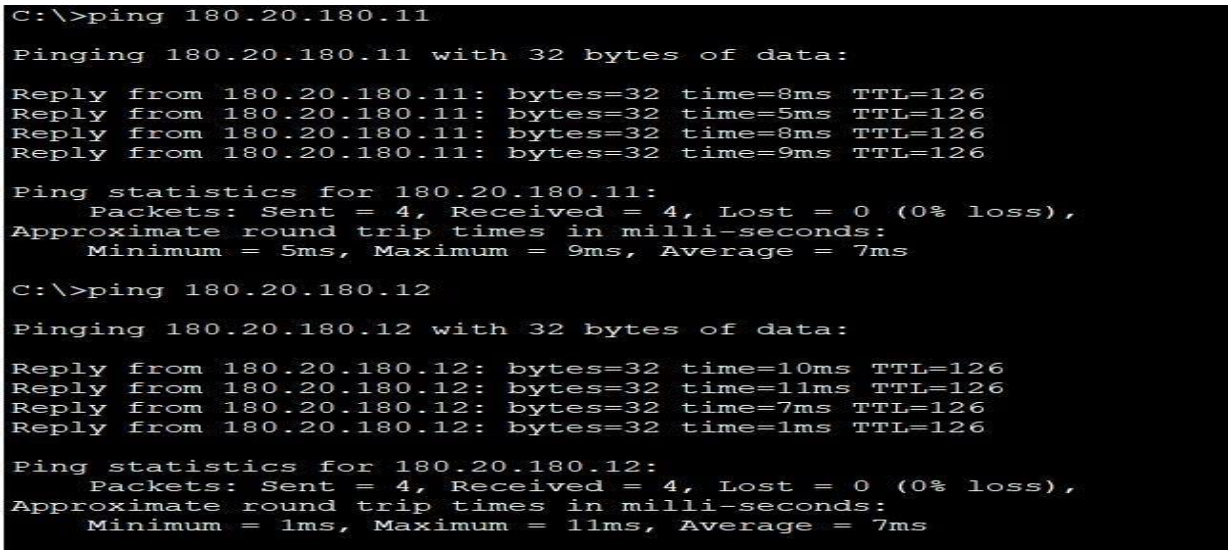

Figure 22

7) Configure a standard ACL on R4

Step 1. Configure the standard ACL on R4

The ACL should perform the following issues:

- Allow all devices on network 172.40. 180.0/24 to access network 172.41. 180.0/25 except D1 (172.40. 180.10).
- Allow only 2 devices from network 180.20. 180.0/26 (the one that D1 successfully pinged them in part 6), to access network 172.41. 180.0/25.
    - Permit all other traffic network

      172.41.180.0/25.
    - the access list number →80

Step 2. Apply the ACL

Apply the ACL to Router R3 interface G0/1 for traffic exiting the interface

Step 3. Test the ACL

a) From D1 and the two hosts from network 180.20. 180.0/26 (D3, D4 or D5) ping D2.
Note: ping should not be successful from D1.

b) Change the IP of D1 (172.40.180.20) and one of the two hosts of network 180.20.180.0/26 and ping D2
Note: ping should be only successful for D1.