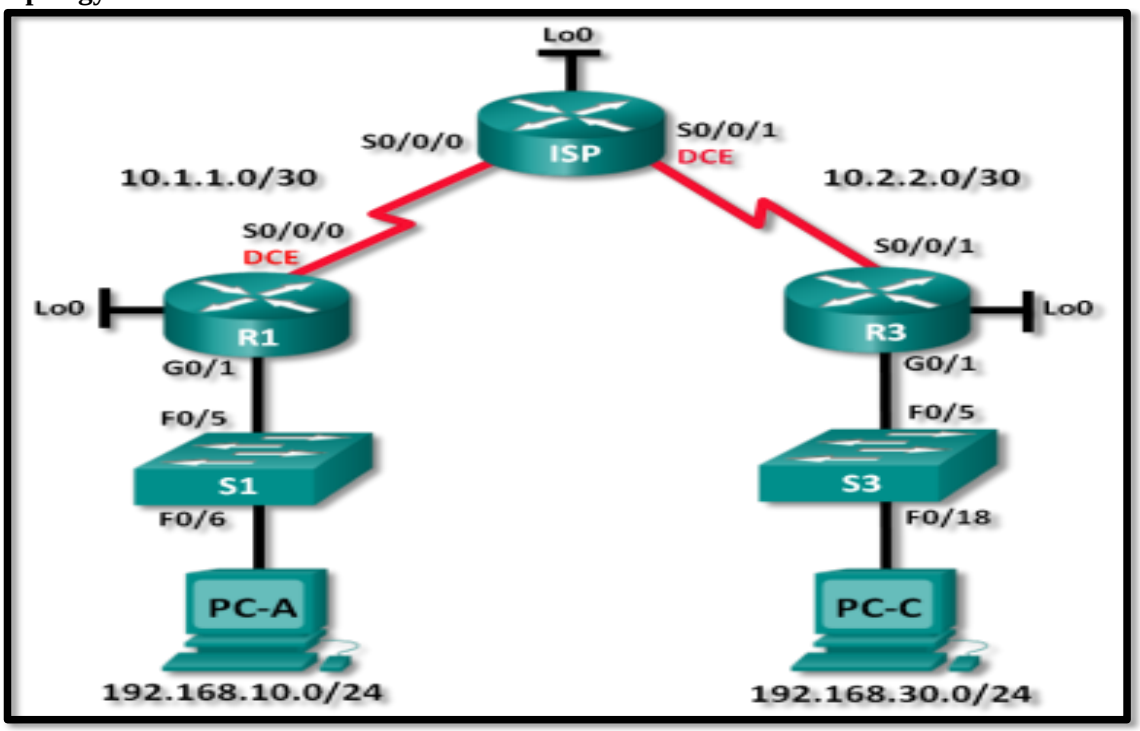
PRACTICAL 2

Lab – Configuring and Verifying Standard IPv4 ACLs :-

Topology



Lab – Configuring and Verifying Standard IPv4 ACLs

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1

PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Objectives

Part 1: Set Up the Topology and Initialize Devices · Set up equipment to match the network topology. Initialize and reload the routers and switches.

Part 2: Configure Devices and Verify Connectivity. Assign a static IP address to PCs. Configure basic settings on routers.

Configure basic settings on switches. Configure OSPF routing on R1, ISP, and R3. Verify connectivity between devices.

Part 3: Configure and Verify Standard Numbered and Named ACLs. Configure, apply, and verify a numbered standard ACL. · Configure, apply, and verify a named ACL.

Part 4: Modify a Standard ACL. Modify and verify a named standard ACL.Test the ACL.

Background / Scenario

Network security is an important issue when designing and managing IP networks. The ability to configure proper rules to filter packets, based on established security policies, is a valuable skill.

Lab – Configuring and Verifying Standard IPv4 ACLs

In this lab, you will set up filtering rules for two offices represented by R1 and R3. Management has established some access policies between the LANs located at R1 and R3, which you must implement. The ISP router sitting between R1 and R3 will not have any ACLs placed on it. You would not be allowed any administrative access to an ISP router because you can only control and manage your own equipment.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4) M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

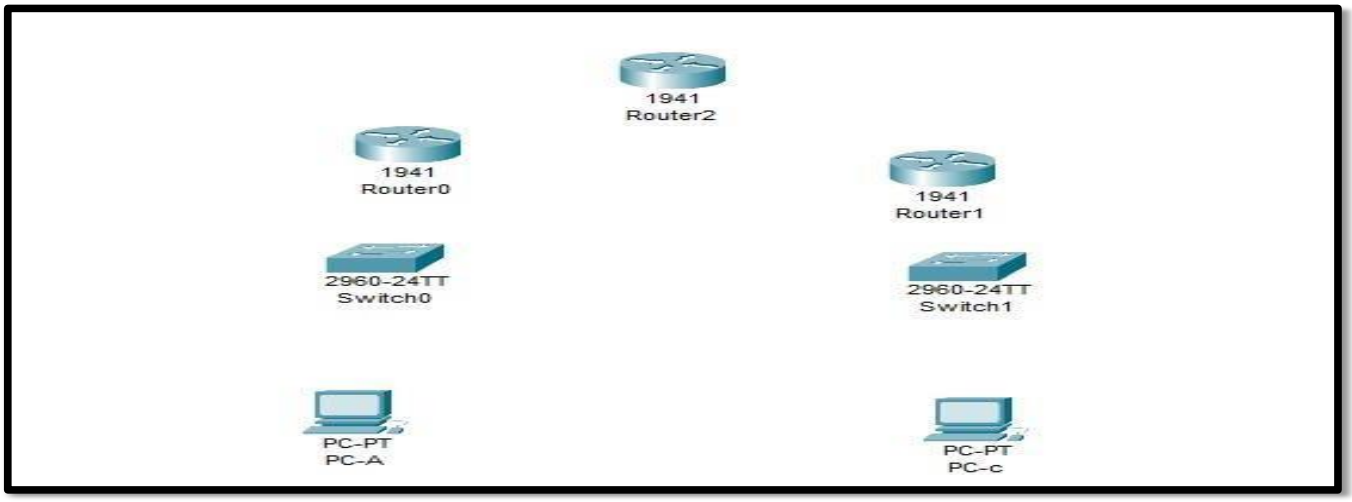
Required Resources

· 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4) M3 universal image or comparable) · 2 Switches (Cisco 2960 with Cisco IOS Release

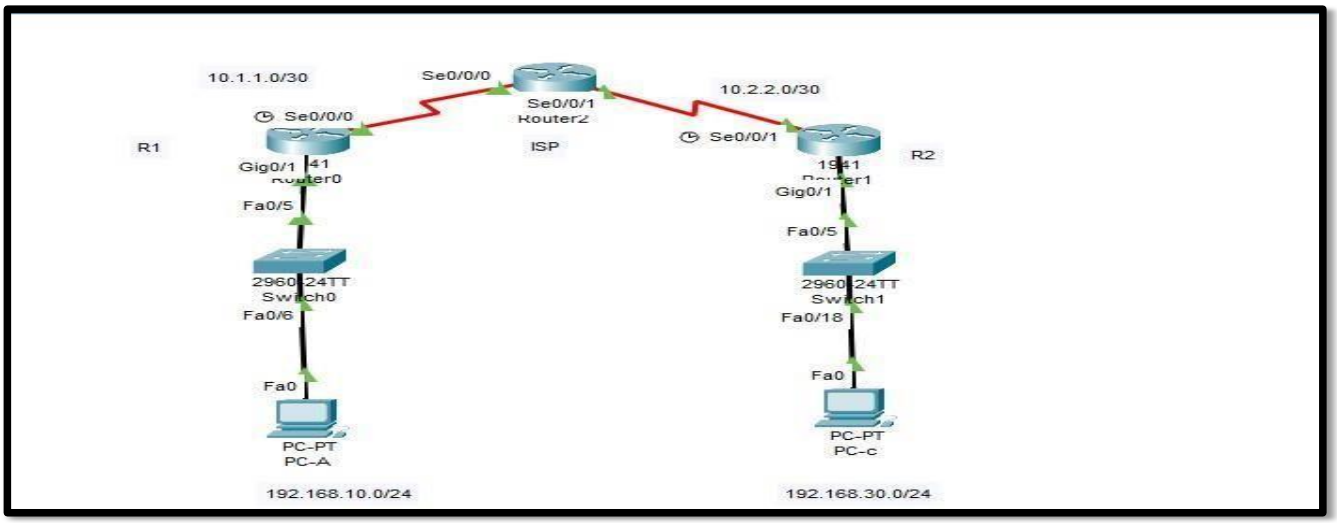
15.0(2) lanbasek9 image or comparable) · 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term) · Console cables to configure the Cisco IOS devices via the console ports · Ethernet and serial cables as shown in the topology

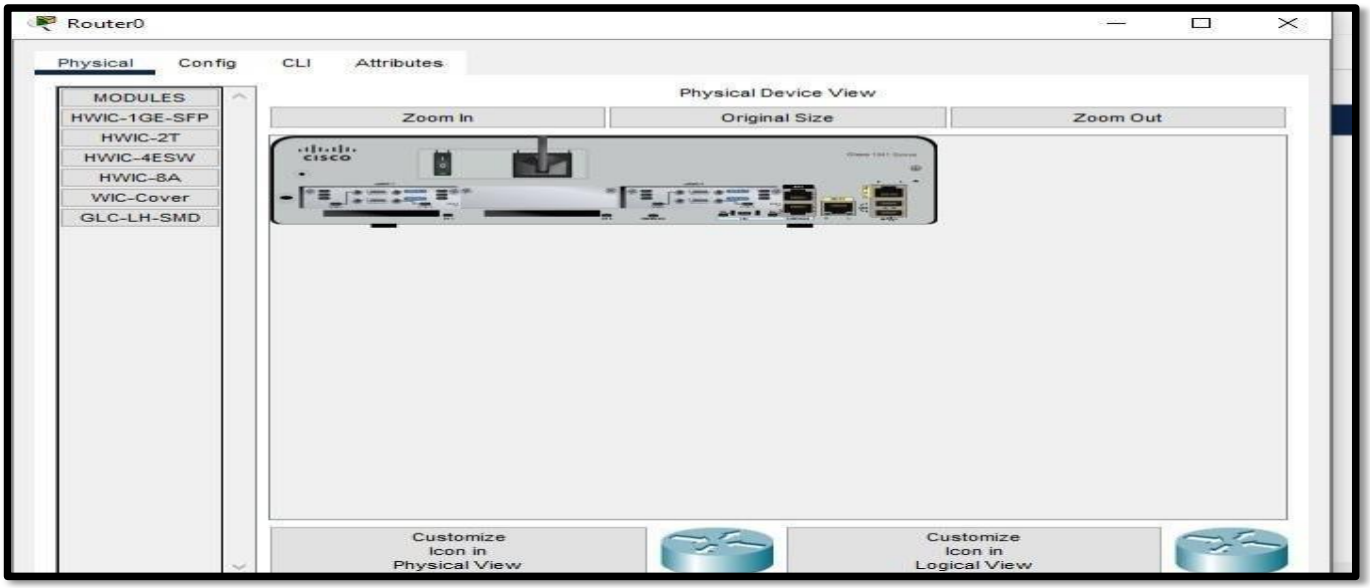
Part 1: Set Up the Topology and Initialize Devices

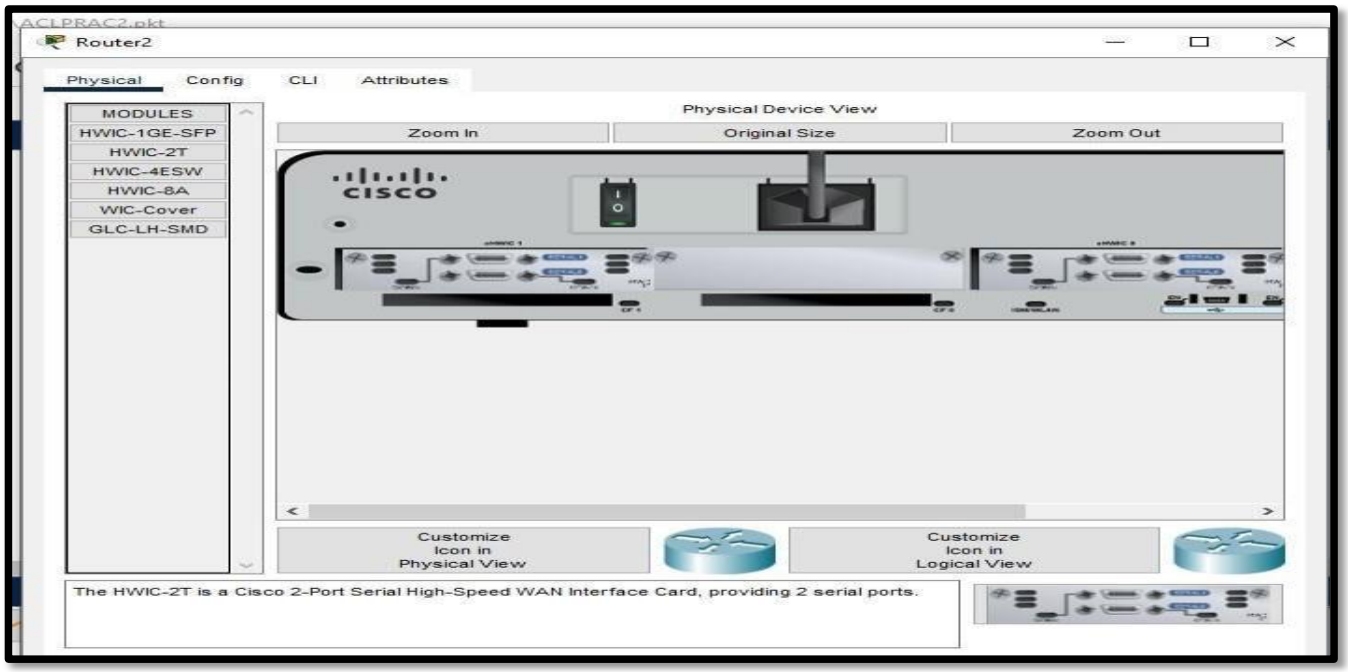
Step 1 : Cable the network as shown in the topology.

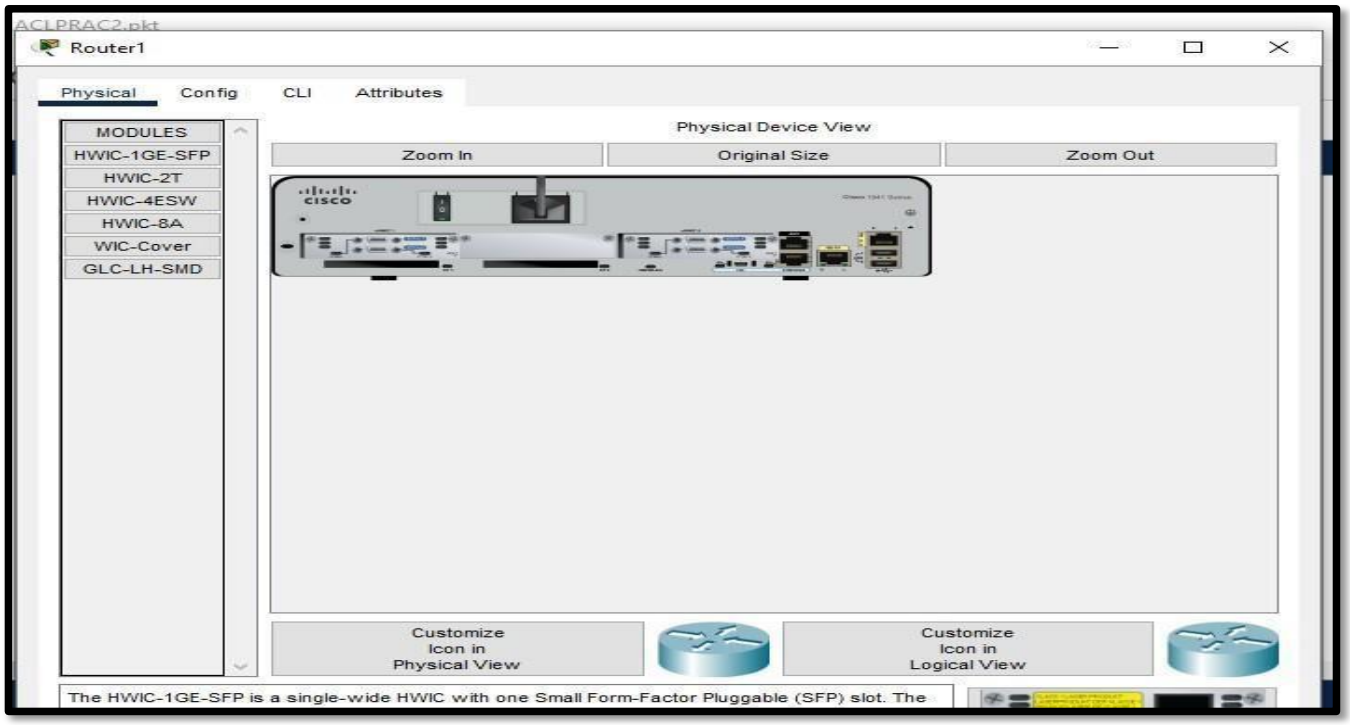


Step 2:- Initialize and reload the routers and switches.



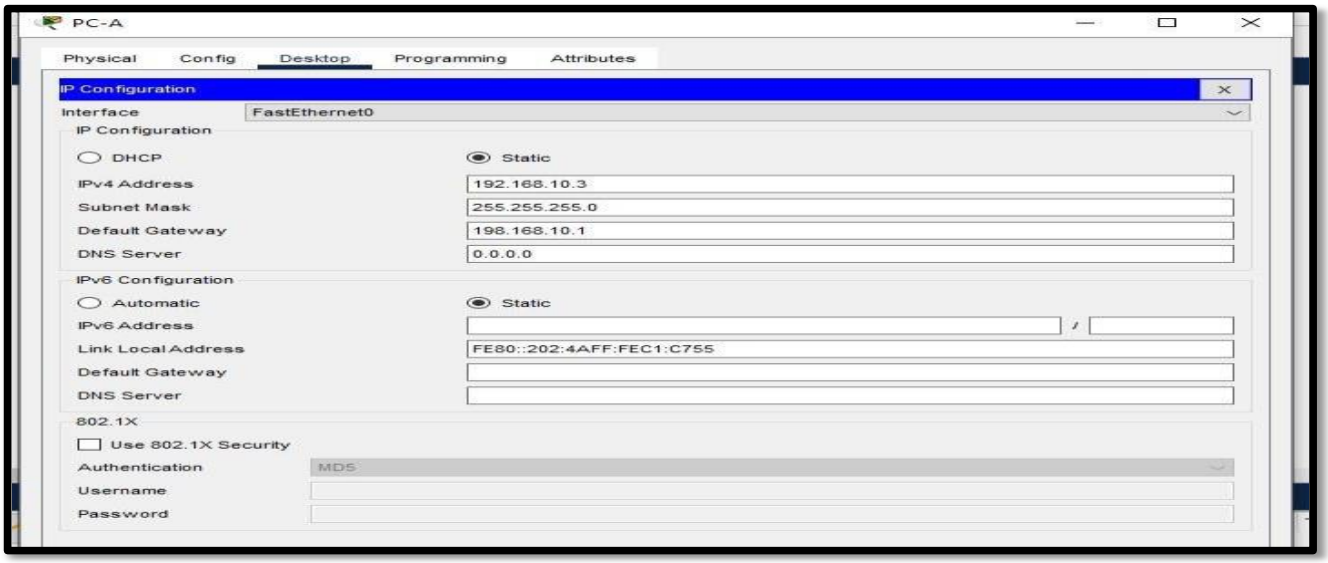


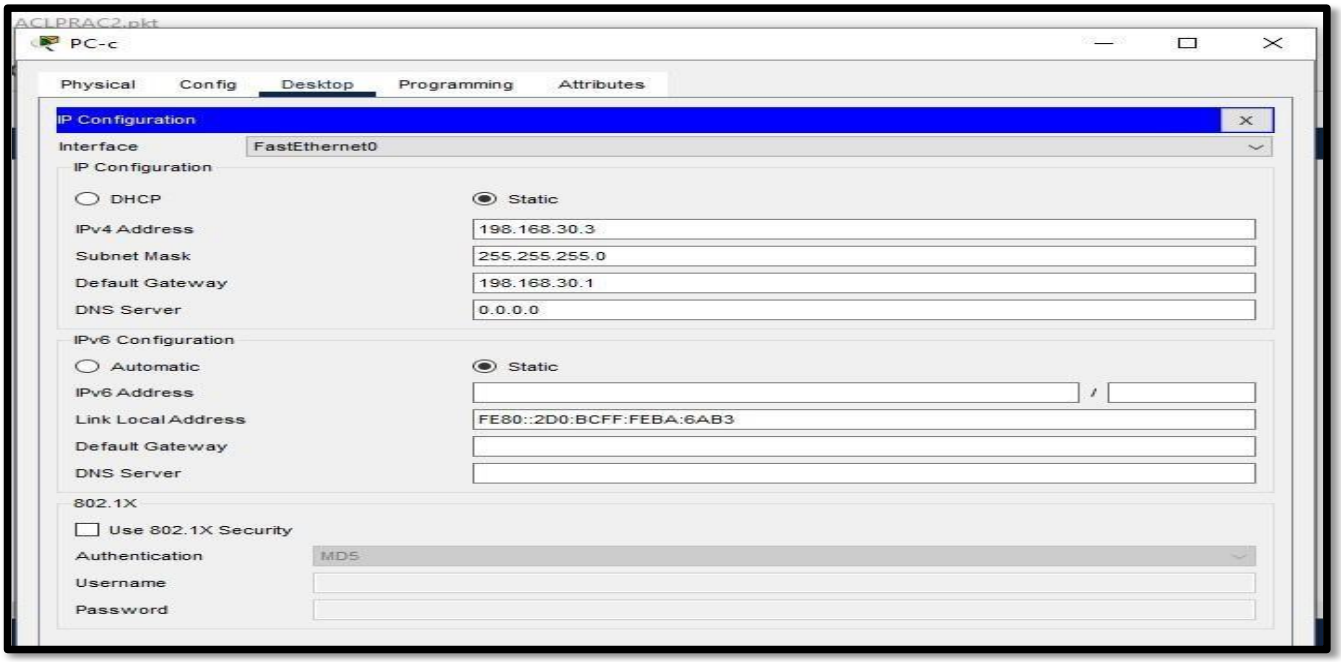




Part 2: Configure Devices and Verify Connectivity

Step 1:- Configure IP addresses on PC-A and PC-C.





Configure basic settings for the routers.

a. Console into the router and enter global configuration mode.

b. Create loopback interfaces on each router as shown in the Addressing Table.

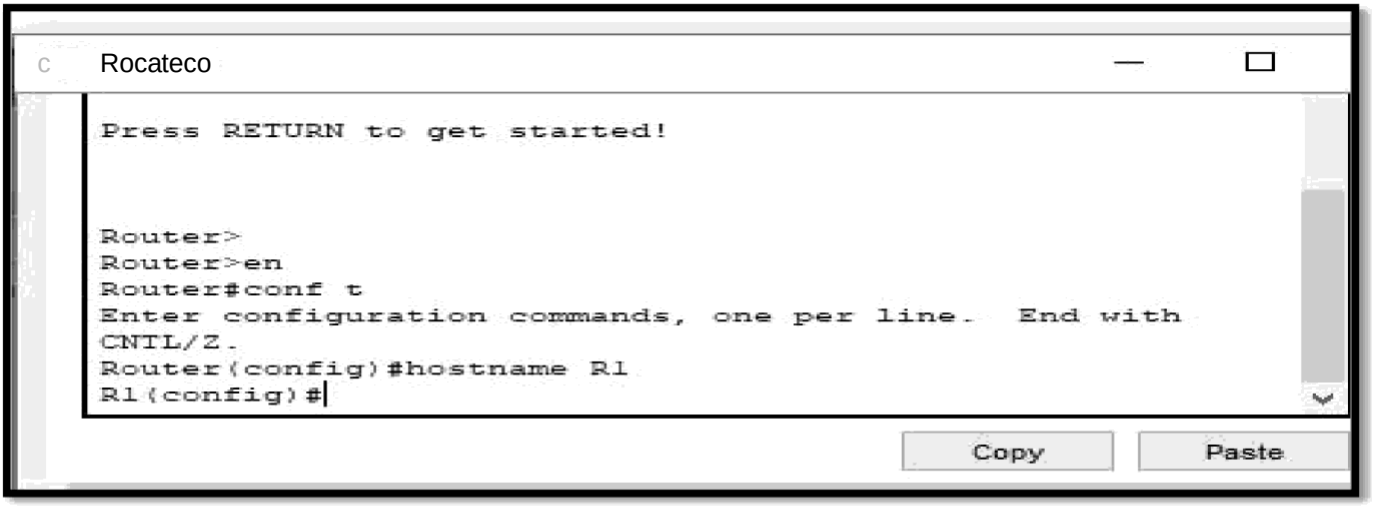
c. Configure interface IP addresses as shown in the Topology and Addressing Table.

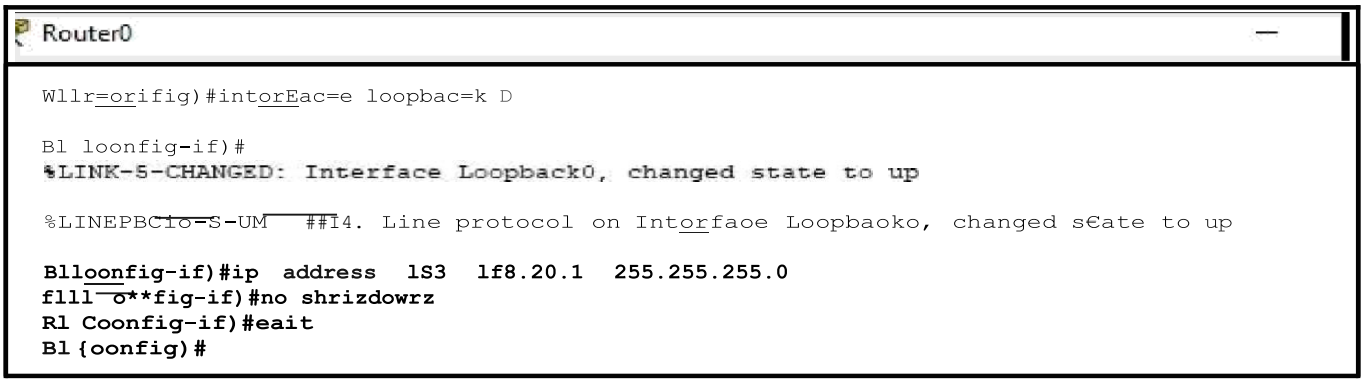
d. Assign a clock rate of 128000 to the DCE serial interfaces.

a. Router > en

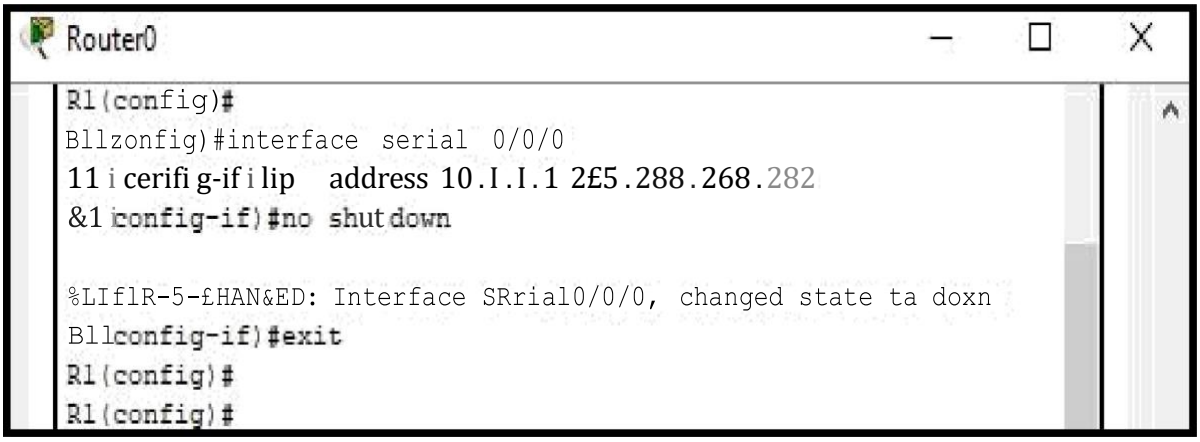
Router > conf t

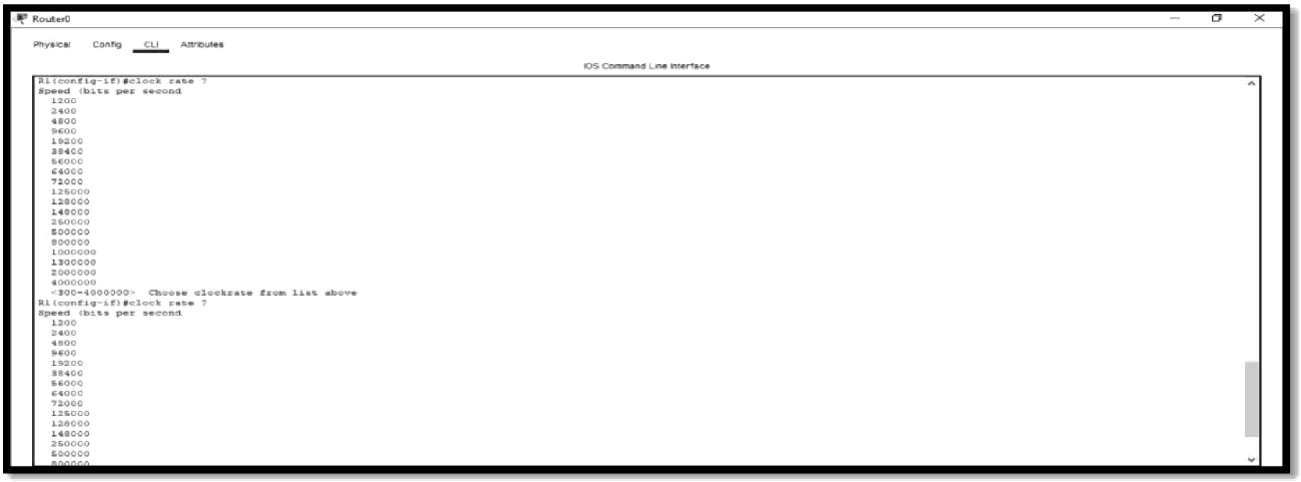
Router > hostname R1

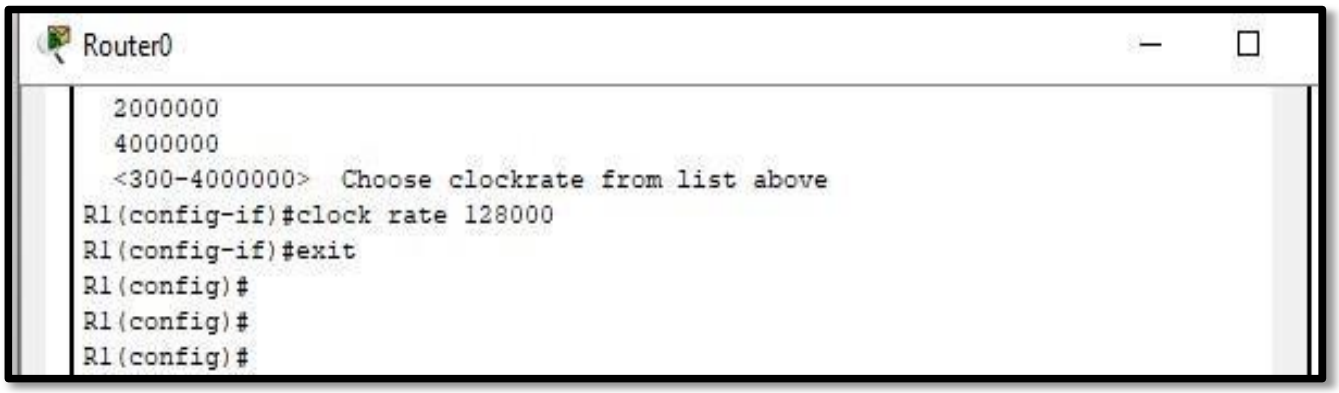

Rocateco
Press RETURN to get started!
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#hostname R1
R1(config)#
Copy
Paste

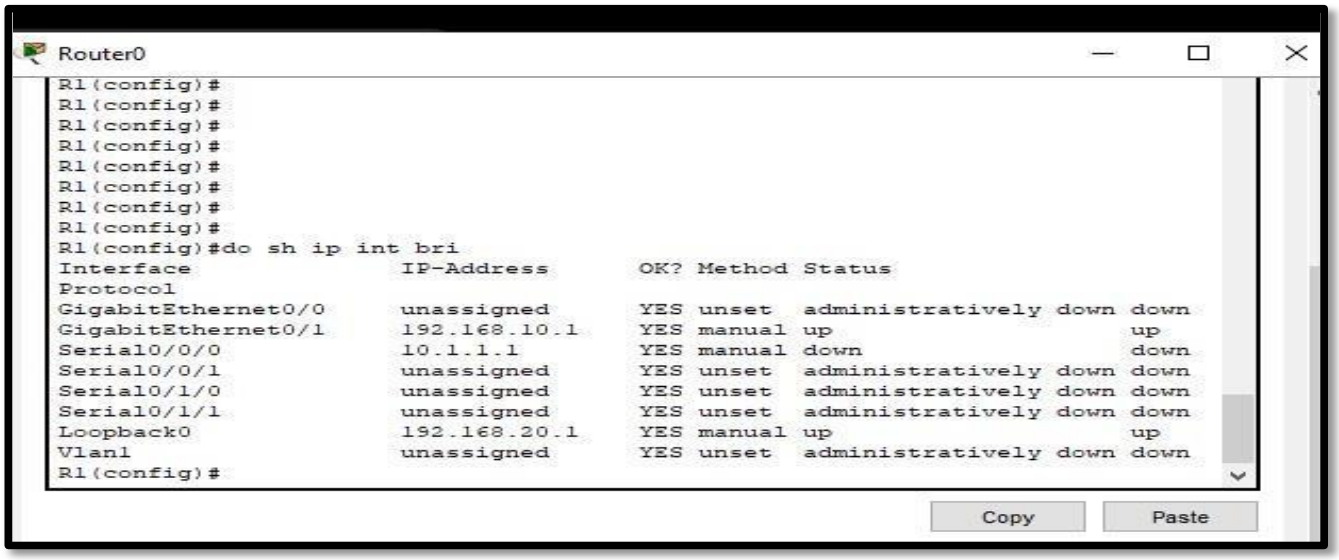

Router0
Wllr=orifig)#intorEac=e loopbac=k D
Bl loonfig-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPBClo=S-UM ##I4. Line protocol on Intorfaoe Loopbaoko, changed s€ate to up
Blloonfig-if)#ip address lS3 lf8.20.1 255.255.255.0
flll o**fig-if)#no shrizdowrz
Rl Coonfig-if)#eait
Bl{oonfig)#

```
Bl{zonfig)#interface gigabitBthernet
Blloonfig)4interface gigabitBthernet 0/1
Rl loonfig-if)#ip address I9?.148.10.1 255.255.255.0
Rlleonfig-if)#no shutdown

Rllconfig-if#
8LINK-z-CHANGED: Interface GigabitZtheznet0/l, changed state to up

8LIN9PROTO-S-UPDOHN. Line protocol on Interface GigabitEthernet0/1, changed state to


Rlloonfig-if)8exit
```







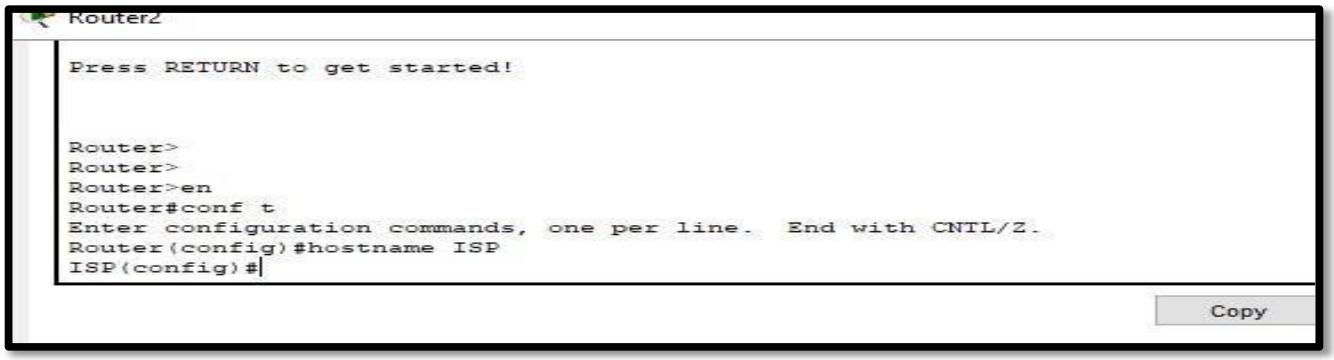


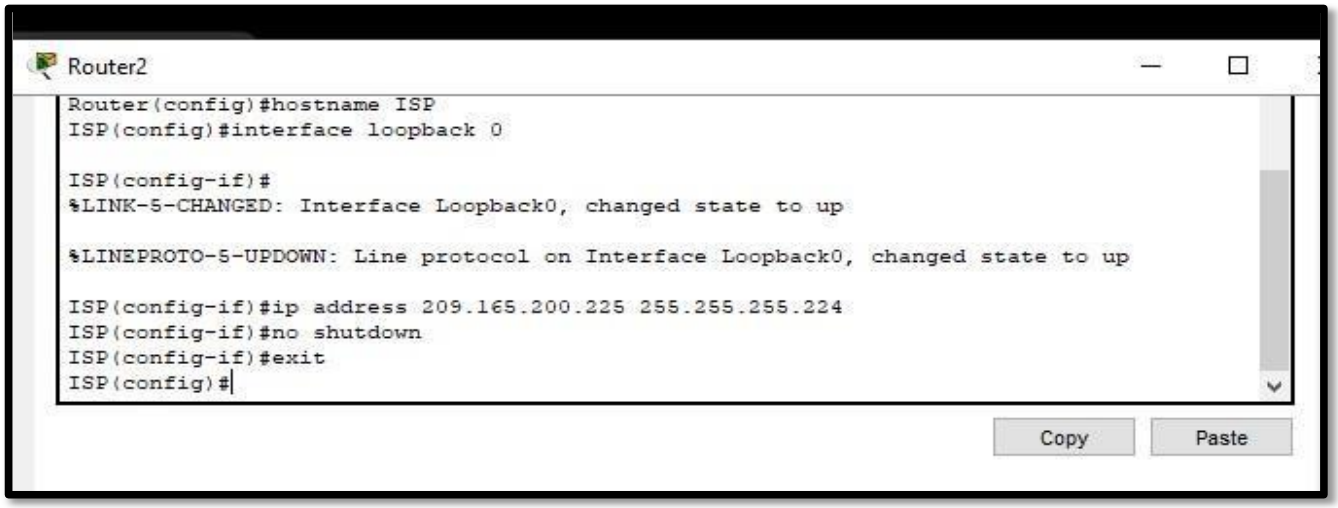
ISP

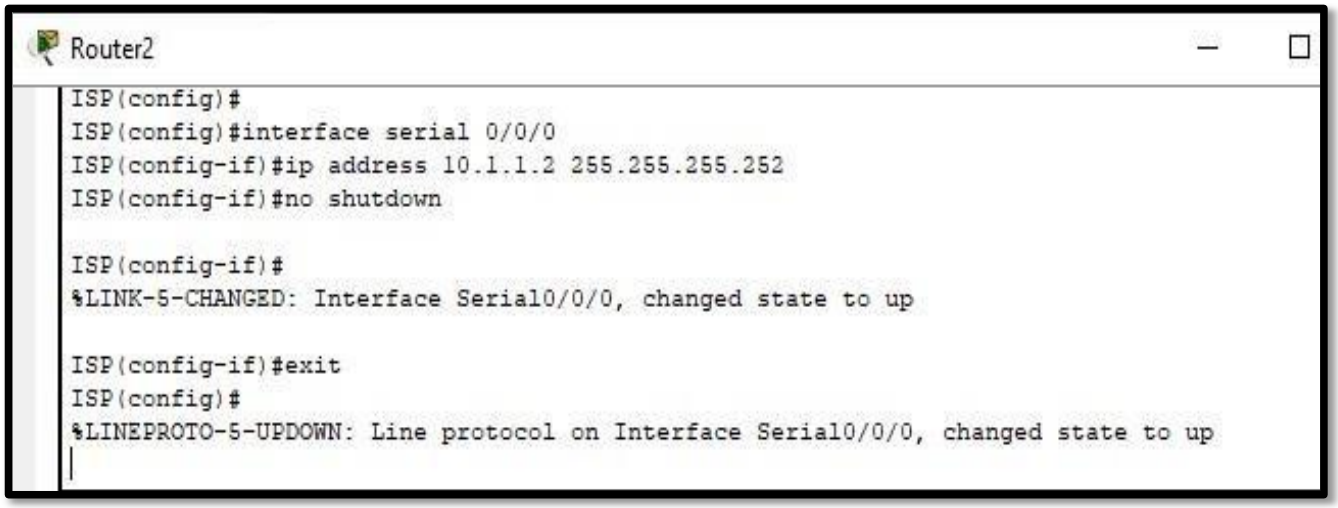
Router > en

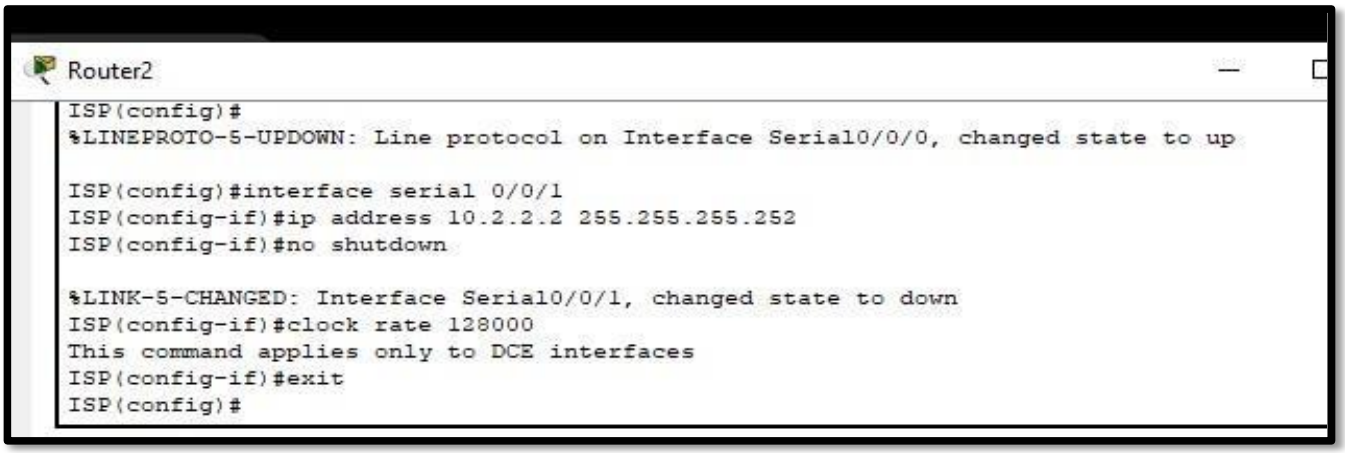
Router > conf t

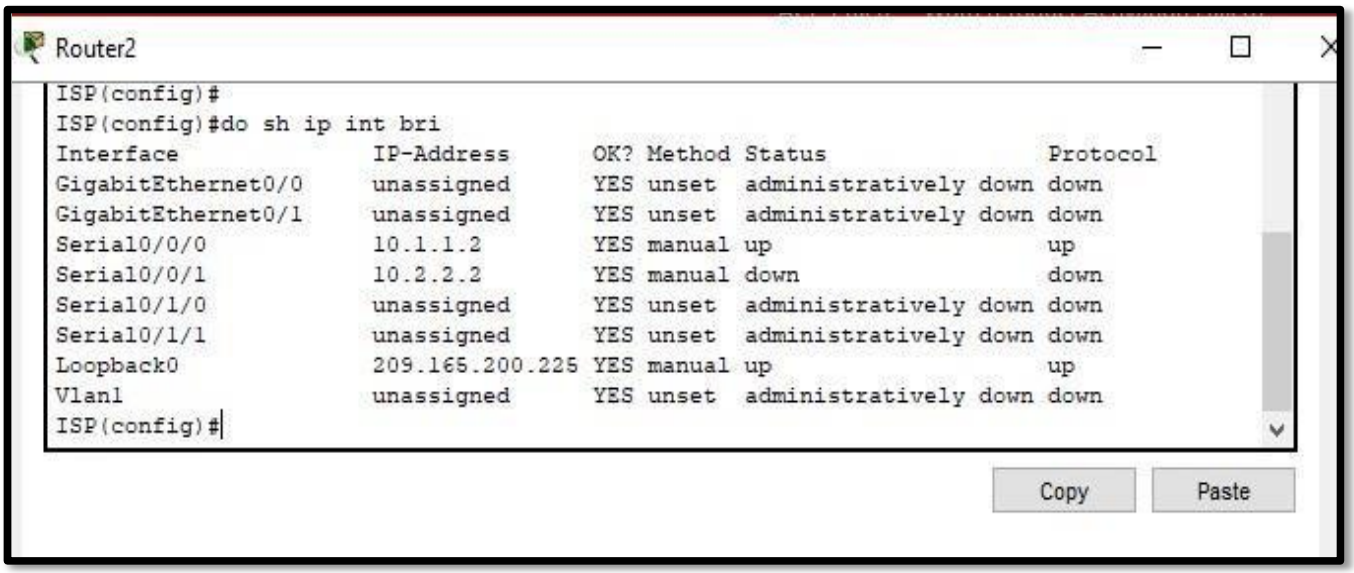
Router > hostname ISP


Router2
Press RETURN to get started!
Router>
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#
Copy


Router2
Router(config)#hostname ISP
ISP(config)#interface loopback 0
ISP(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ISP(config-if)#ip address 209.165.200.225 255.255.255.224
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#
Copy
Paste


Router2
ISP(config)#
ISP(config)#interface serial 0/0/0
ISP(config-if)#ip address 10.1.1.2 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
ISP(config-if)#exit
ISP(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up



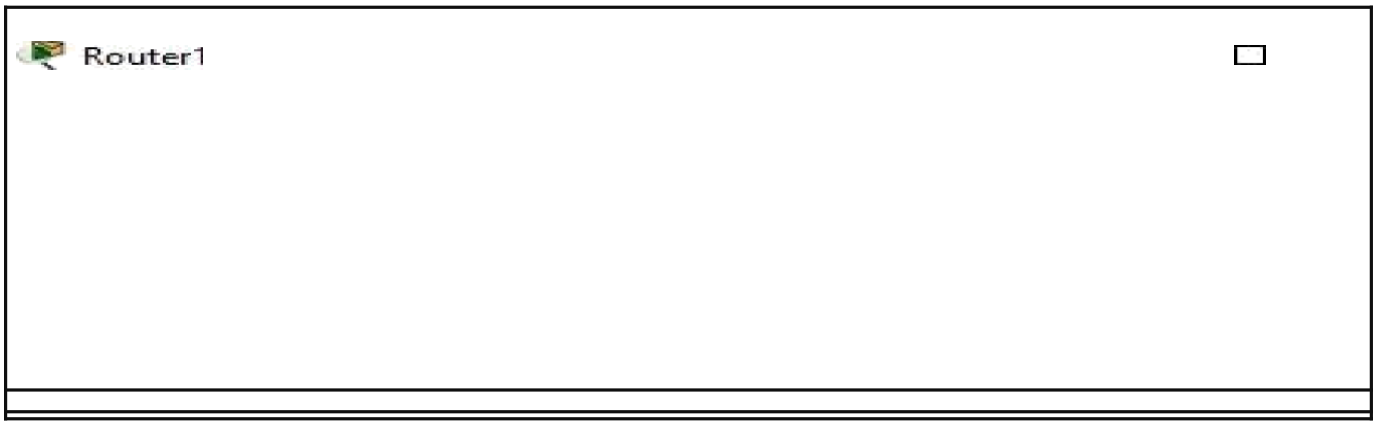


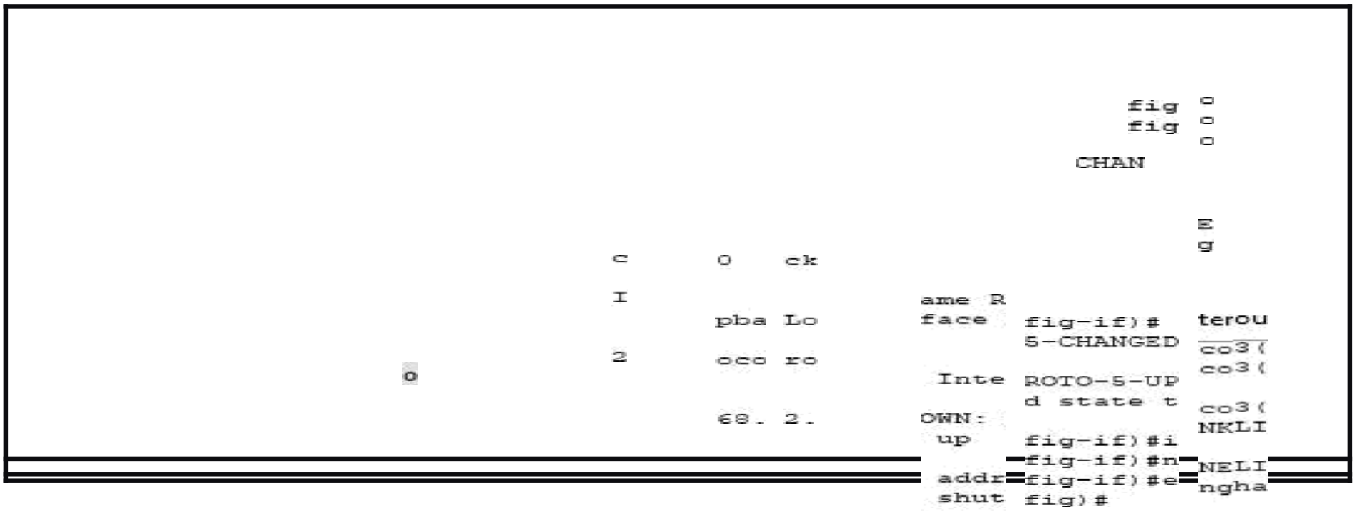
R3

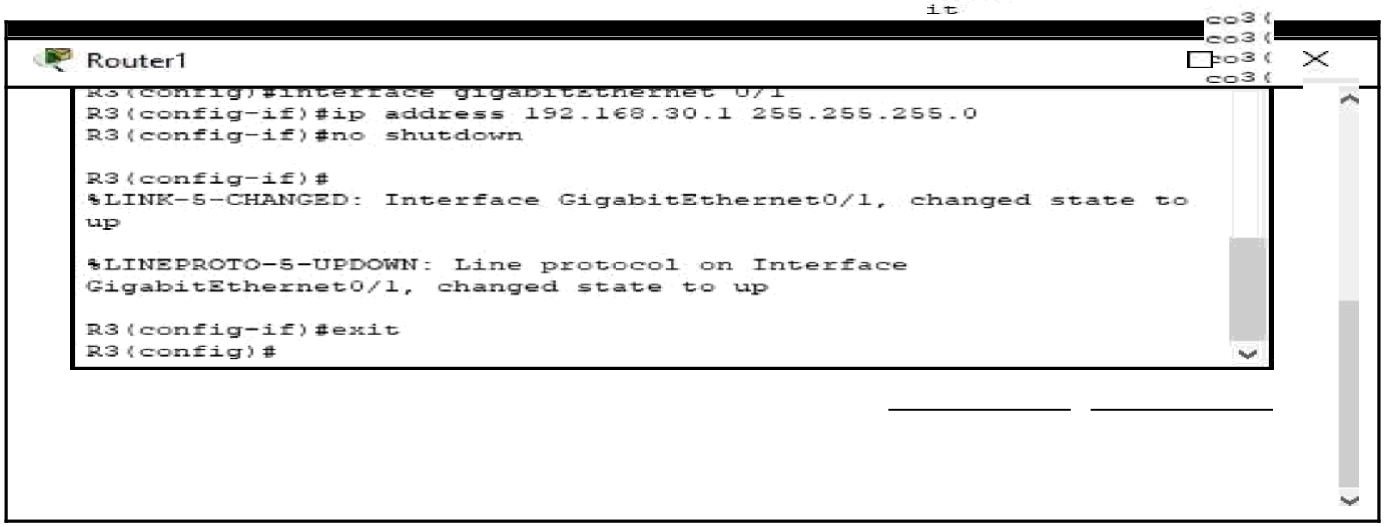
Router > en

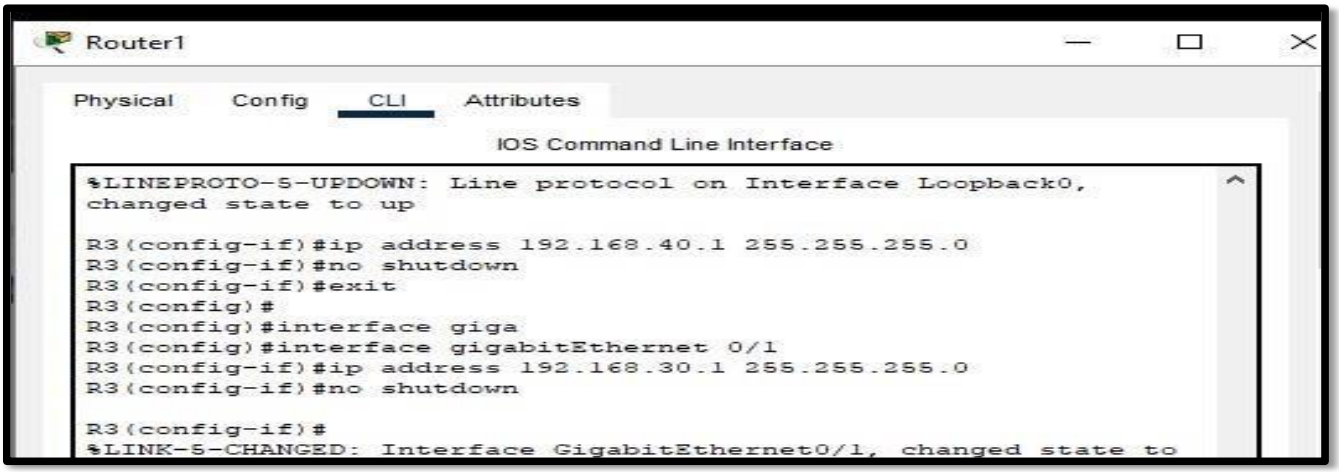
Router > conf t

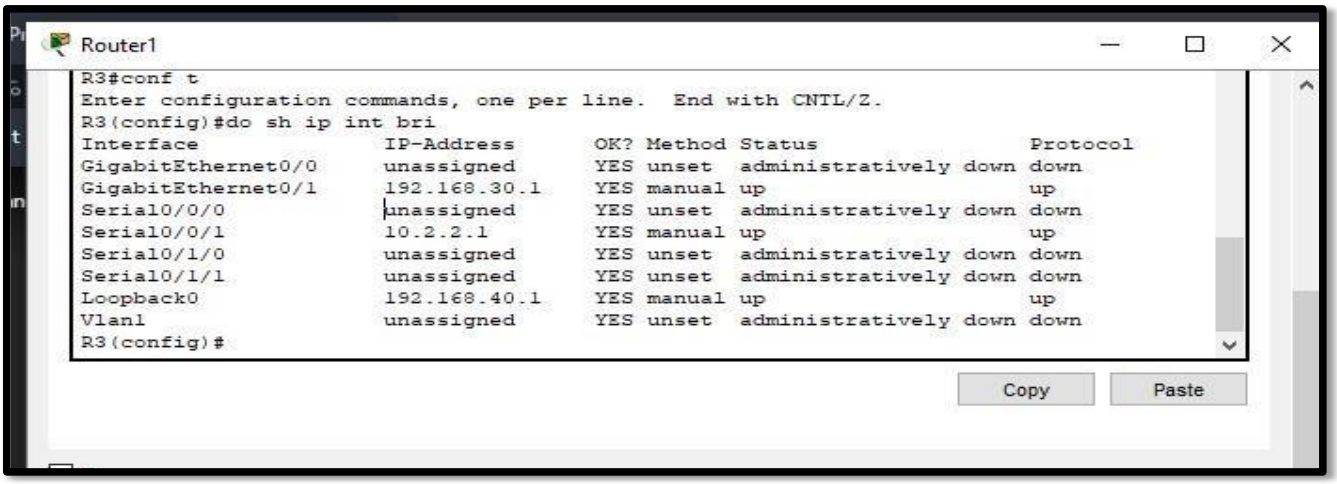
Router > hostname R3


Router1




Router1
R3(config)#interface gigabitEthernet 0/1
R3(config-if)#ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
R3(config-if)#exit
R3(config)#

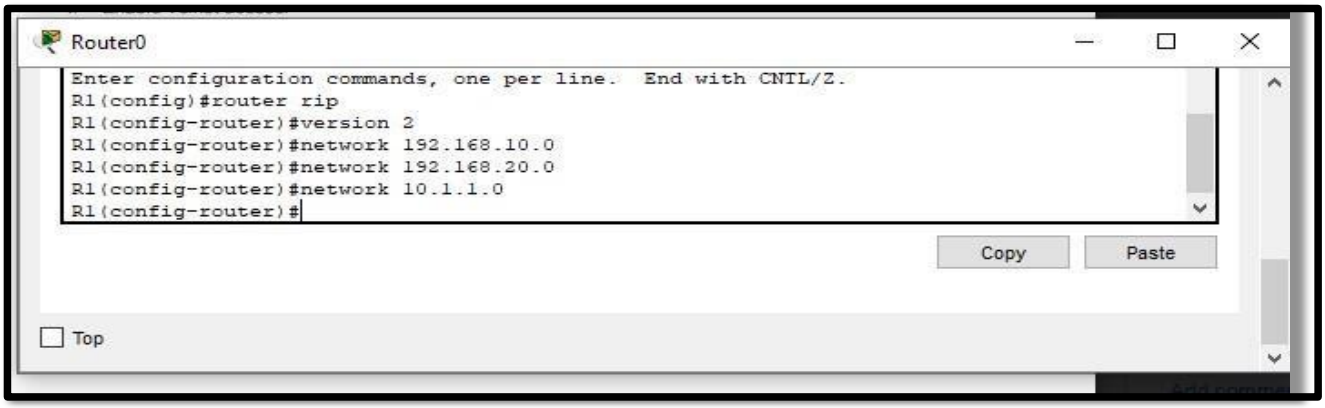




Configure Rip routing on R1, ISP, and R3.

a. Configure RIP version 2 and advertise all networks on R1, ISP, and R3. The OSPF configuration for R1 and ISP is included for reference.

R1(config)# **router rip**
R1(config-router)# **version 2**
R1(config-router)# **network 192.168.10.0**
R1(config-router)# **network 192.168.20.0**
R1(config-router)# **network 10.1.1.0**



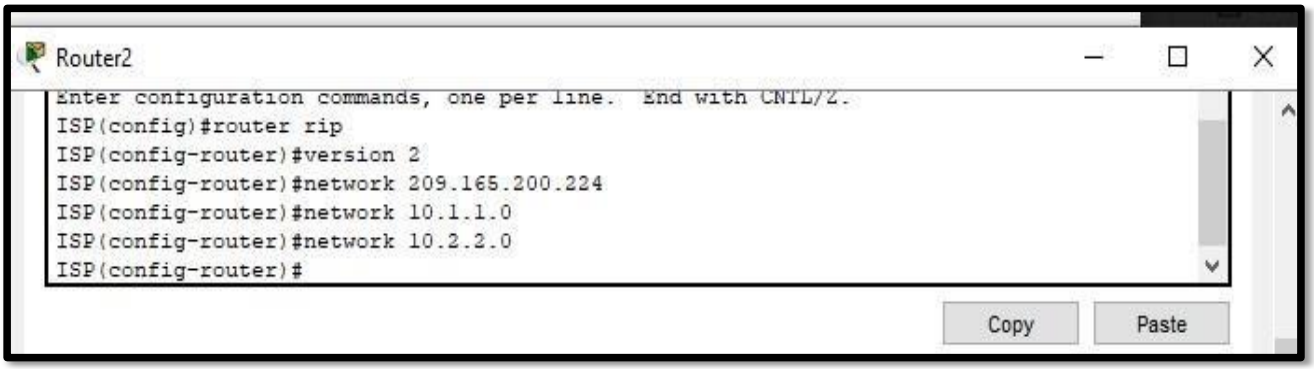
ISP(config)# **router rip**

ISP(config-router)# **version 2**

ISP(config-router)# **network 209.165.200.224**

ISP(config-router)# **network 10.1.1.0**

ISP(config -router)# **network 10.2.2.0**



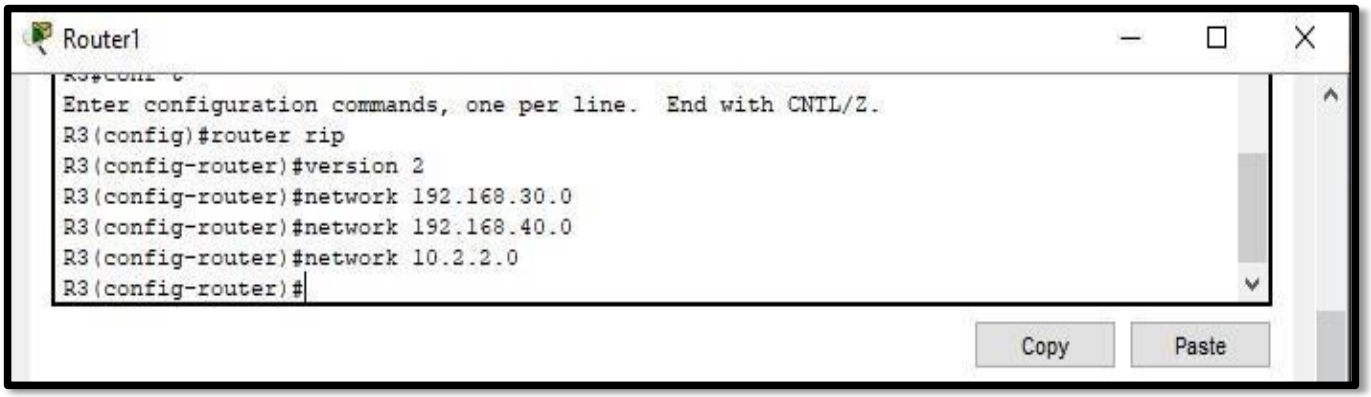
R3(config)# **router RIP**

R3(config-router)# **version 2**

R3(config-router)# **network 192.168.30.0**

R3(config-router)# **network 192.168.40.0**

R3(config-router)# **network 10.2.2.0**



Verify connectivity between devices.

Note: It is very important to test whether connectivity is working **before** you configure and apply access lists! You want to ensure that your network is properly functioning before you start to filter traffic.

a. From PC-A, ping PC-C and the loopback interface on R3. Were your pings successful? Yes

b. From R1, ping PC-C and the loopback interface on R3. Were your pings successful? Yes

c. From PC-C, ping PC-A and the loopback interface on R1. Were your pings successful? Yes

d. From R3, ping PC-A and the loopback interface on R1. Were your pings successful? Yes

Part 3: Configure and Verify Standard Numbered and Named ACLs

Step 1:- Configure a numbered standard ACL. Standard ACLs filter traffic based on the source IP address only. A typical best practice for standard ACLs is to configure and apply it as close to the destination as possible. For the first access list, create a standard numbered ACL that allows traffic from all hosts on the 192.168.10.0/24 network and all hosts on the 192.168.20.0/24 network to access all hosts on the 192.168.30.0/24 network. The security policy also states that a deny any access control entry (ACE), also referred to as an ACL statement, should be present at the end of all ACLs.

G0/1. The ACL should be applied going out. Students may answer with placing the ACL on the S0/0/1 interface on R3 going in. Emphasize to them that this would effectively block the LANs on R1 from getting to the 192.168.40.0/24 network as well!

a. **Configure the ACL on R3. Use 1 for the access list number.**

R3(config)# access-list 1 remark Allow R1 LANs Access

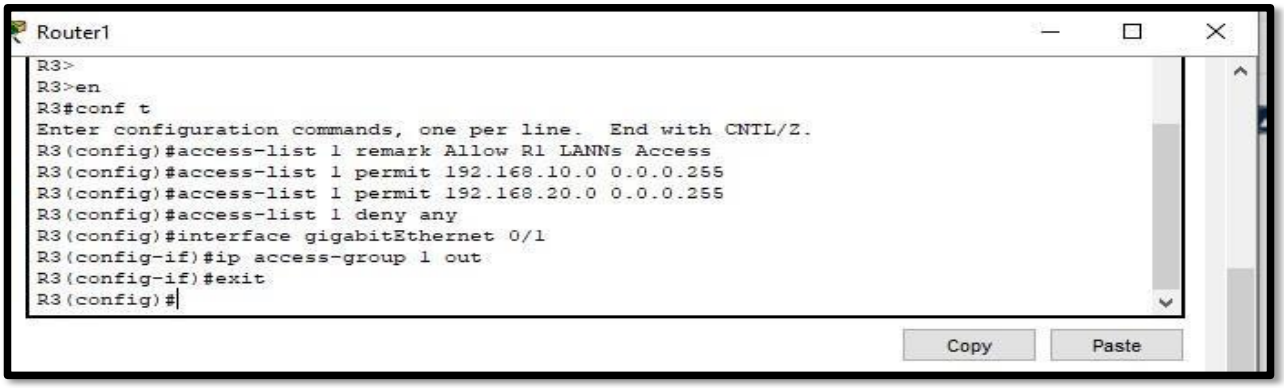
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255

R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255

R3(config)# access-list 1 deny any

b. **Apply the ACL to the appropriate interface in the proper direction. R3(config)# interface g0/1**

R3(config -if)# ip access -group 1 out



c. **Verify a numbered ACL.**

The use of various show commands can aid you in verifying both the syntax and placement of your ACLs in your router.

1) On R3, issue the show access-lists 1 command.

R3# show access-lists 1

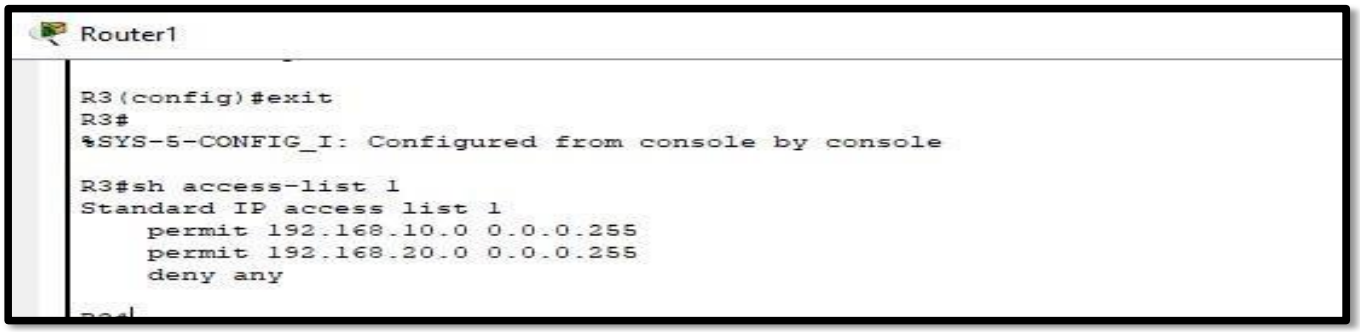
2) On R3, issue the show ip interface g0/1 command.

R3# show ip interface g0/1

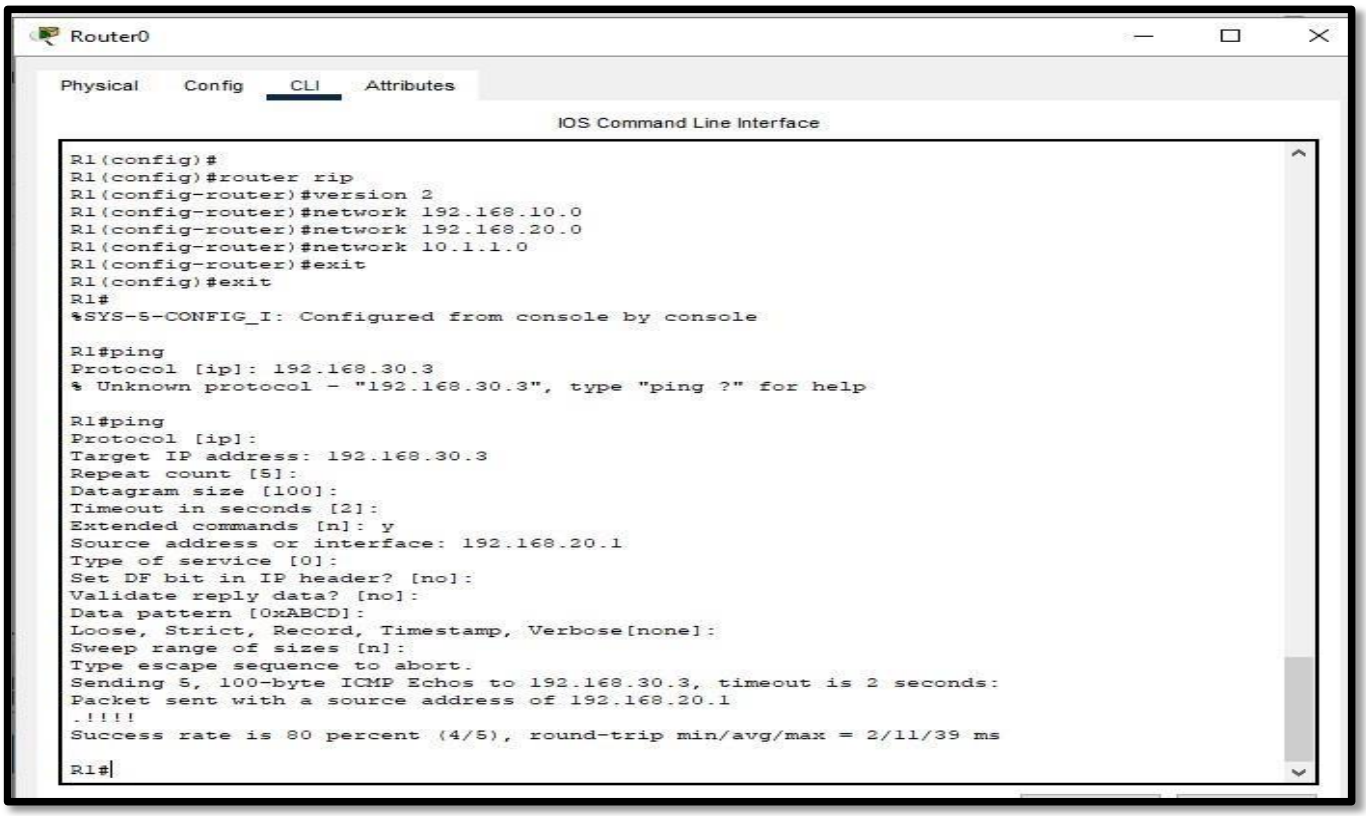
3) Test the ACL to see if it allows traffic from the 192.168.10.0/24 network access to the 192.168.30.0/24 network. From the PC-A command prompt, ping the PC-C IP address. Were the pings successful? Yes

4) Test the ACL to see if it allows traffic from the 192.168.20.0/24 network access to the 192.168.30.0/24 network. You must do an extended ping and use the loopback 0 address on

R1 as your source. Ping PC-C's IP address. Were the pings successful?_____Yes

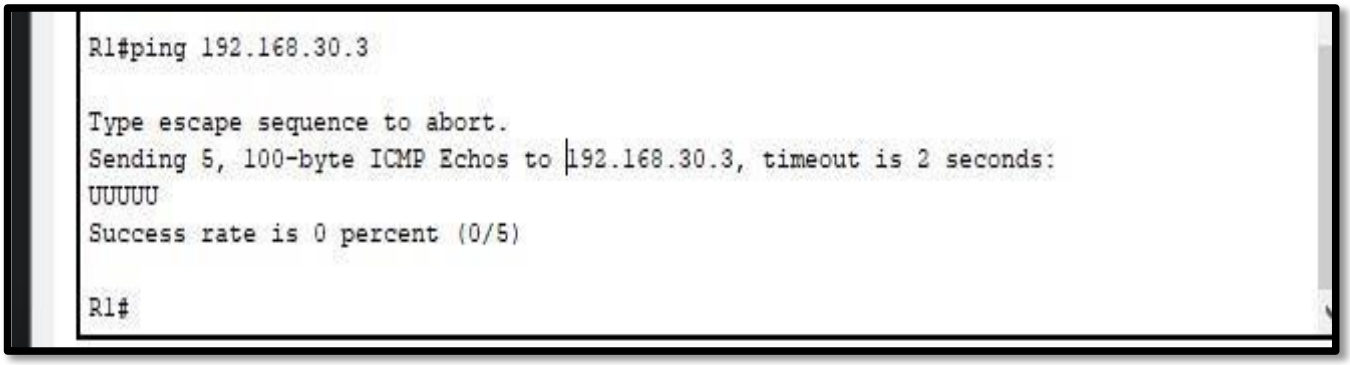


Ping :



d. **From the R1 prompt, ping PC-C's IP address again.**

R1# ping 192.168.30.3



No, the pings failed. When you ping from the router, it uses the closest interface to the destination as its source address. The pings had a source address of 10.1.1.1. The access list on R3 only allows the 192.168.10.0/24 and the 192.168.20.0/24 networks access.

Configure a named standard ACL.

Create a named standard ACL that conforms to the following policy: allow traffic from all hosts on the 192.168.40.0/24 network access to all hosts on the 192.168.10.0/24 network. Also, only allow host PC-C access to the 192.168.10.0/24 network. The name of this access list should be called BRANCH-OFFICE- POLICY.

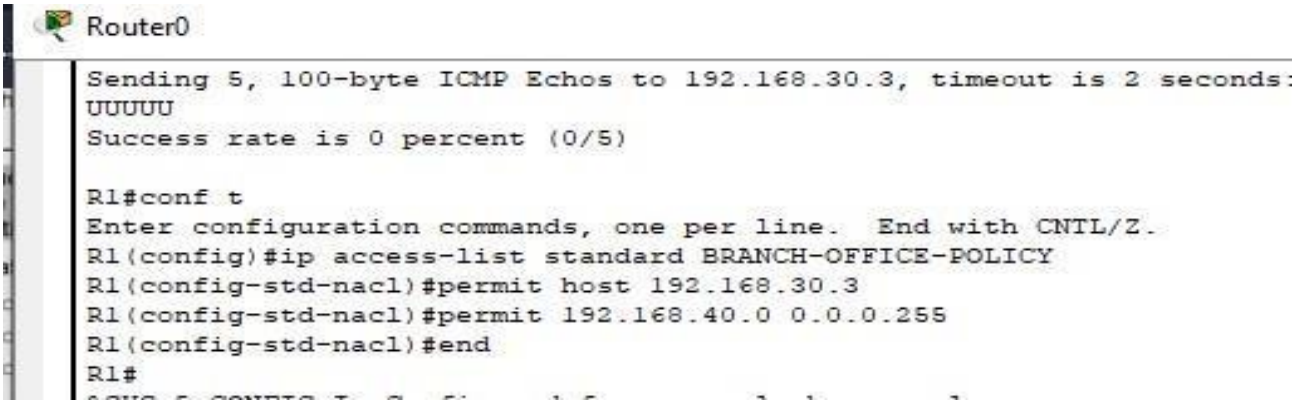
G0/1. The ACL should be applied going out. Students may answer with placing the ACL on the S0/0/0 interface on R1 going in. Emphasize to them that this would effectively block all traffic from the LANs on R3 from getting to the 192.168.20.0/24 network. a. Create the standard named ACL BRANCH-OFFICE-POLICY on R1.

R1(config)# ip access-list standard BRANCH-OFFICE-POLICY

R1(config-std-nacl)# permit host 192.168.30.3

R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255

R1(config-std-nacl)# end



b. Apply the ACL to the appropriate interface in the proper direction.

R1# config t

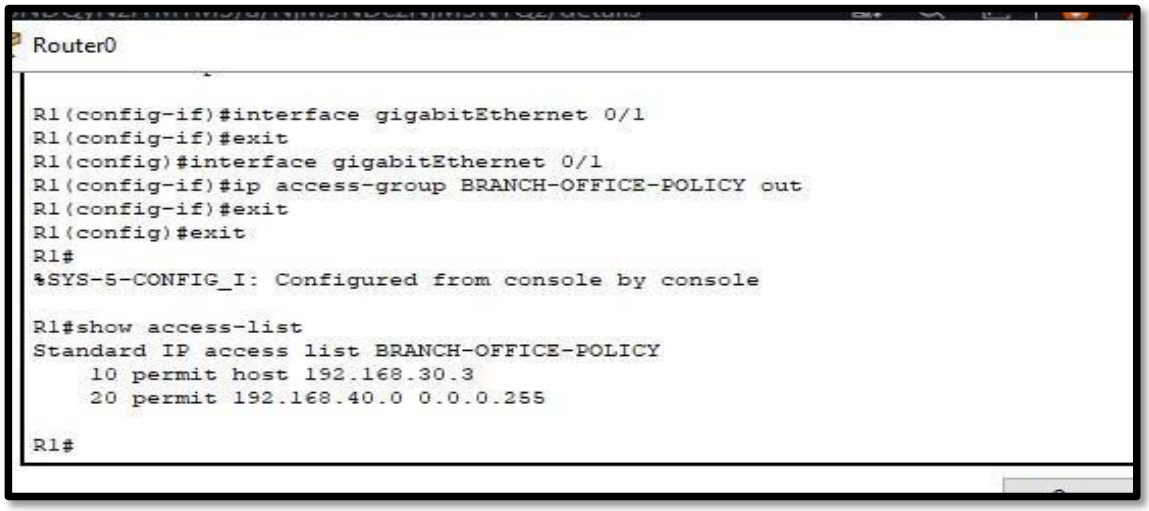
R1(config)# interface g0/1

R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out c. Verify a

named ACL.

1) On R1, issue the show access-lists command.

R1# show access-lists



Although there is no line 30 with a deny any on R1, it is implied. You may wish to emphasize this to your students. Having them actually configure the deny any ACE is a good practice and reinforces the concept as it shows up in the ACL when issuing a show access-lists command. It is easy to forget the implicit deny any when troubleshooting ACLs. This could easily result in traffic being denied that should have been allowed.

2) **On R1, issue the show ip interface g0/1 command.**

R1# show ip interface g0/1

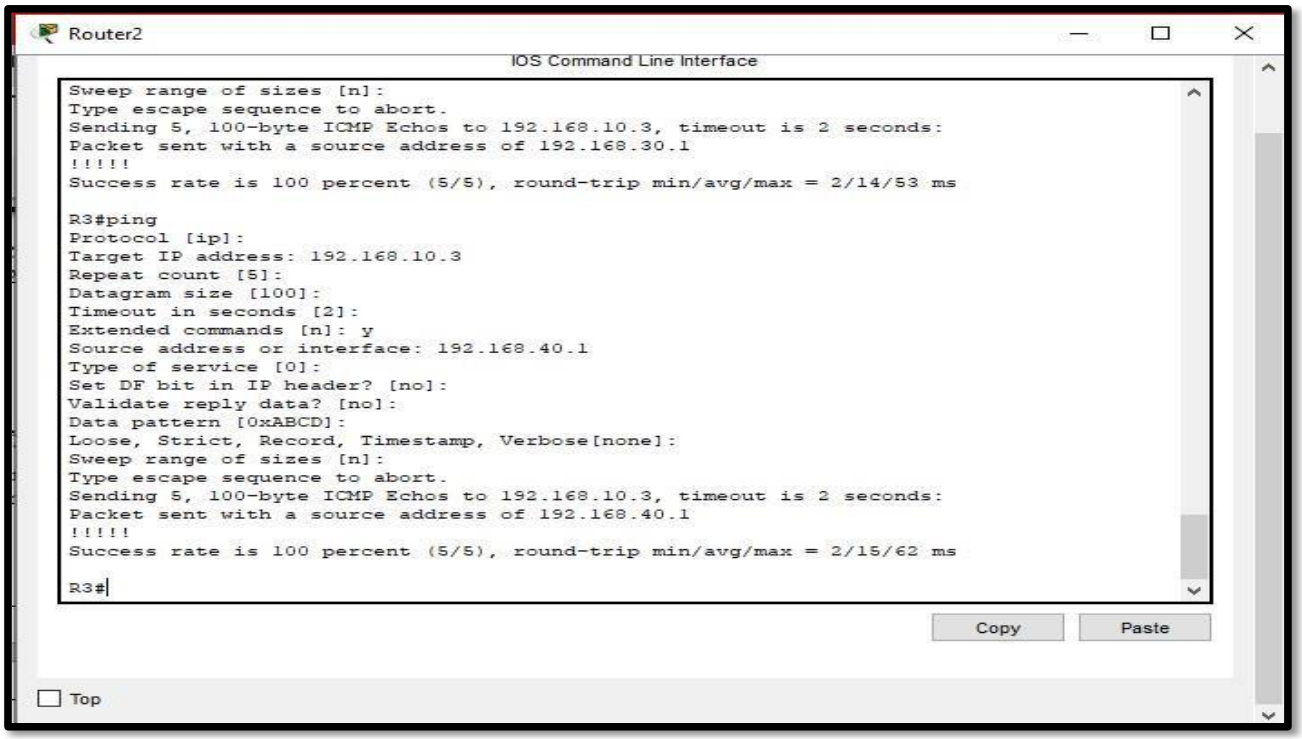
3) Test the ACL. From the command prompt on PC-C, ping PC-A's IP address. Were the pings successful? Yes

4) Test the ACL to ensure that only the PC-C host is allowed access to the 192.168.10.0/24 network. You must do an extended ping and use the G0/1 address on R3 as your source. Ping PC-A's IP address. Were the pings successful? No

R3# ping

5) Test the ACL to see if it allows traffic from the 192.168.40.0/24 network access to the 192.168.10.0/24 network. You must perform an extended ping and use the loopback 0 address on R3 as your source. Ping PC-A's IP address. Were the pings successful? Yes

R3# ping



Part 4: Modify a Standard ACL

It is common in business for security policies to change. For this reason, ACLs may need to be modified. In Part 4, you will change one of the previous ACLs you configured to match a new management policy being put in place. Management has decided that users from the 209.165.200.224/27 network should be allowed full access to the 192.168.10.0/24 network.

Management also wants ACLs on all of their routers to follow consistent rules. A deny any

ACE should be placed at the end of all ACLs. You must modify the BRANCH-OFFICE- POLICY ACL.

Step 1 :- Modify a named standard ACL.

a. From R1 privileged EXEC mode, issue a show access-lists command.

R1# show access-lists

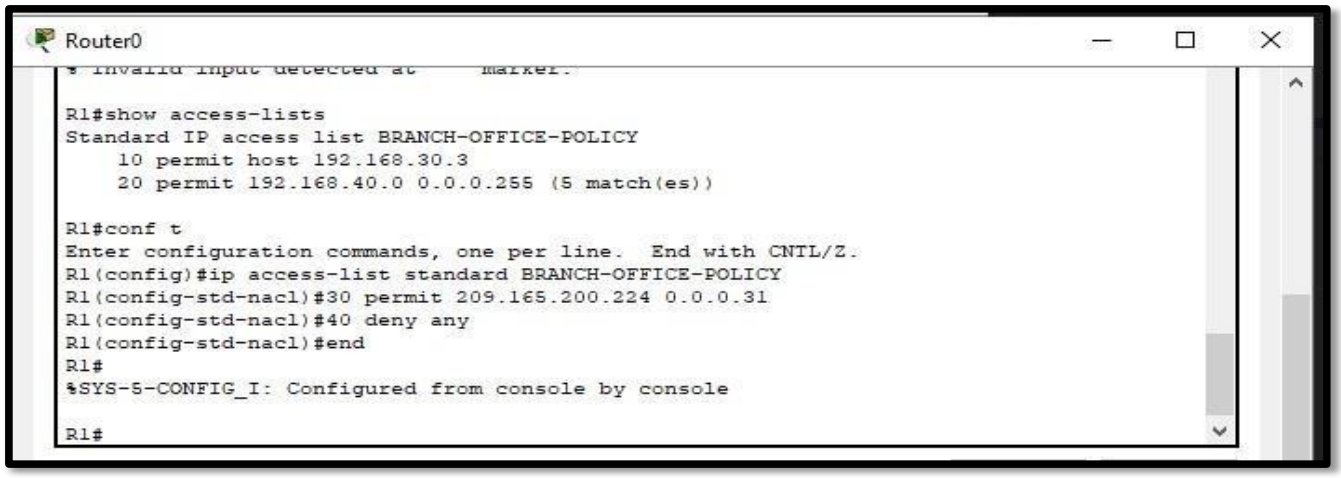
b. Add two additional lines at the end of the ACL. From global config mode, modify the ACL, BRANCH- OFFICE-POLICY.

R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY

R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31

R1(config-std-nacl)# 40 deny any

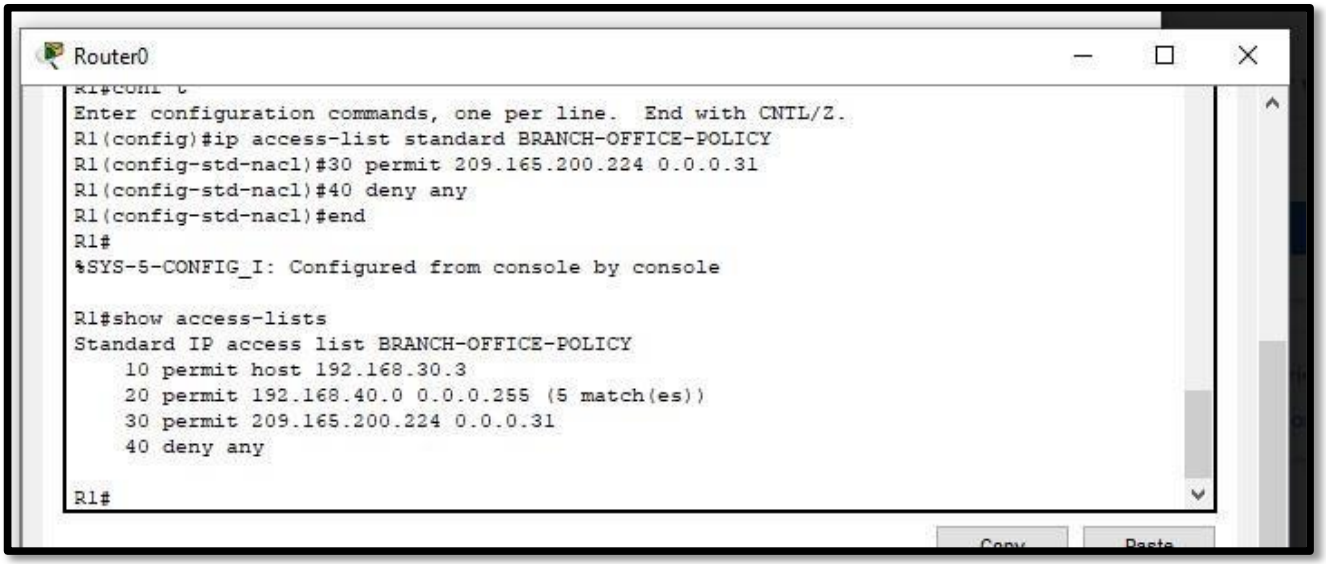
R1(config-std-nacl)# end



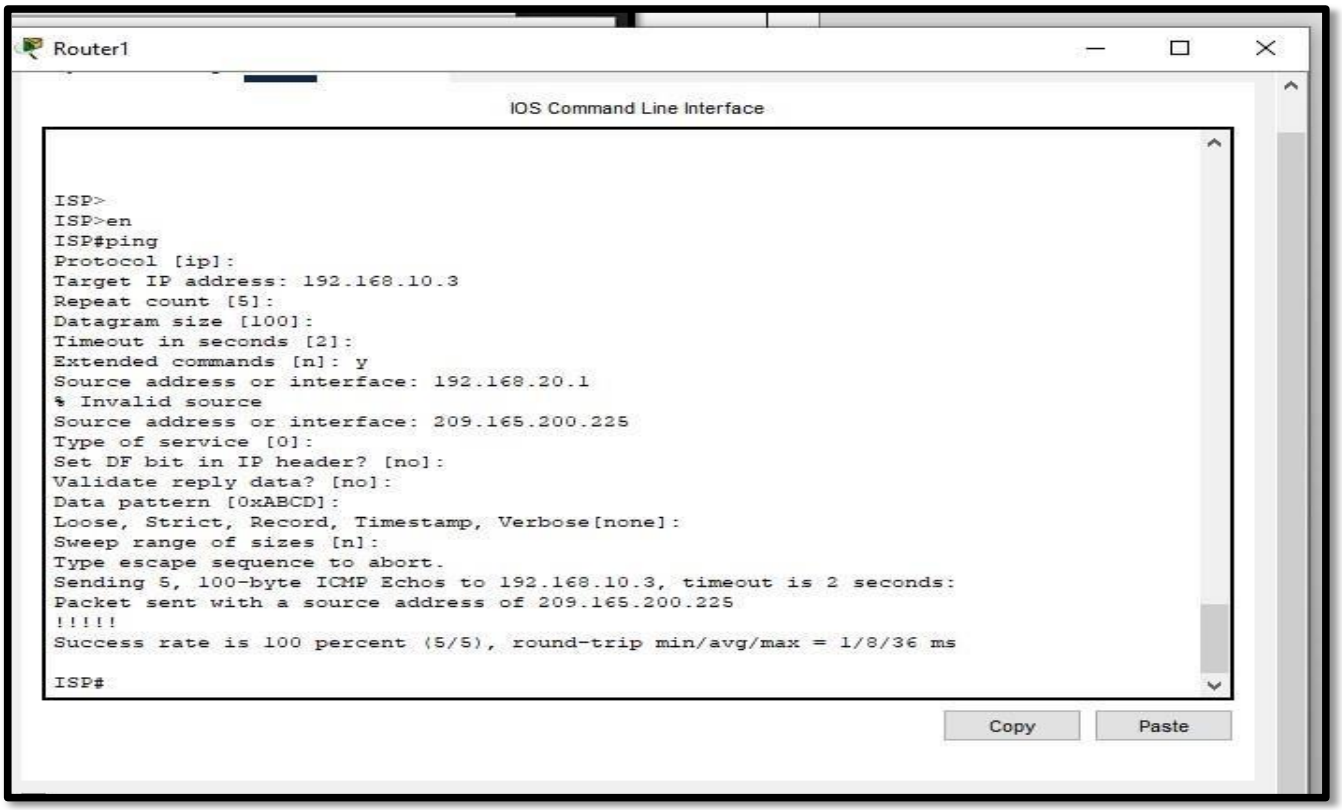
c. Verify the ACL.

1) On R1, issue the show access-lists command.

R1# show access -lists



2) From the ISP command prompt, issue an extended ping. Test the ACL to see if it allows traffic from the 209.165.200.224/27 network access to the 192.168.10.0/24 network. You must do an extended ping and use the loopback 0 address on ISP as your source. Ping PC-A's IP address. Were the pings successful? _____Yes



Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)