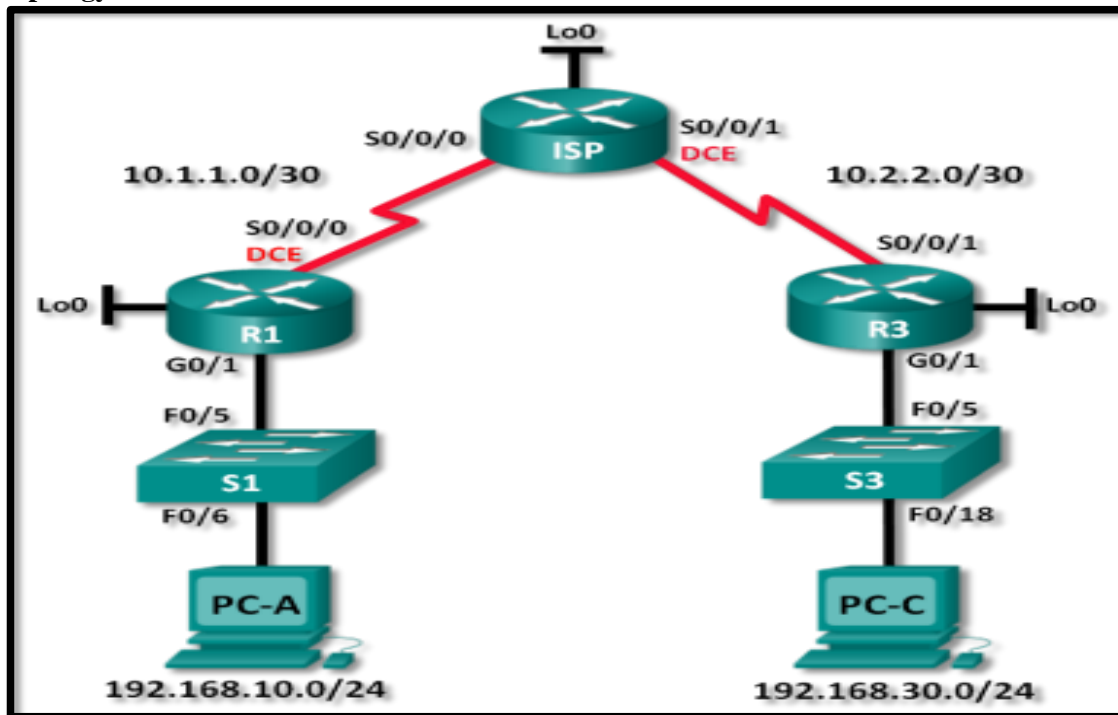


## PRACTICAL 2

### 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.

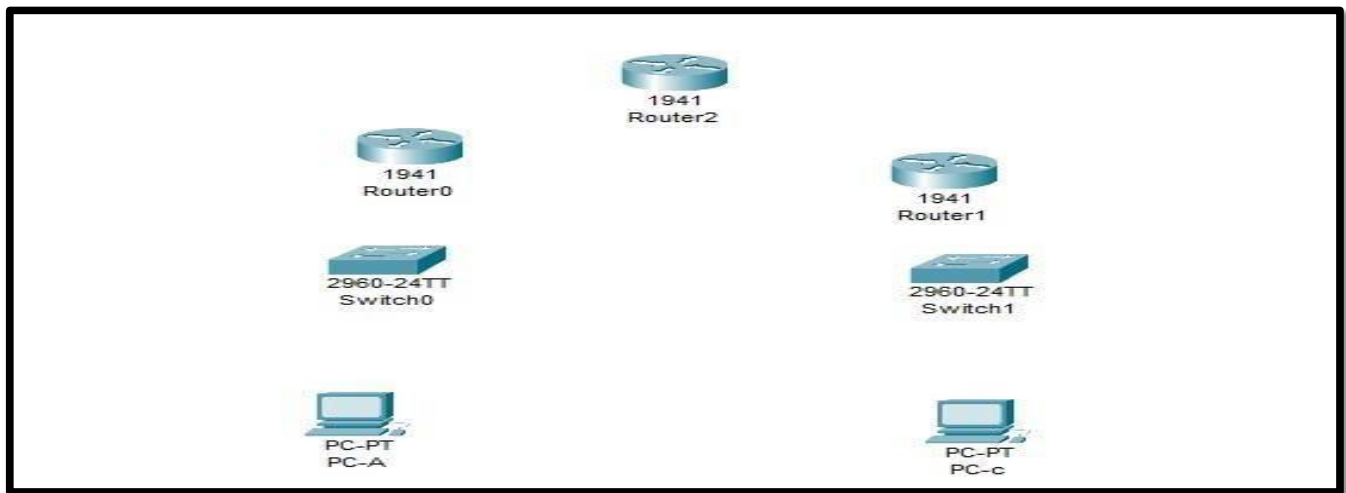
## Required Resources

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

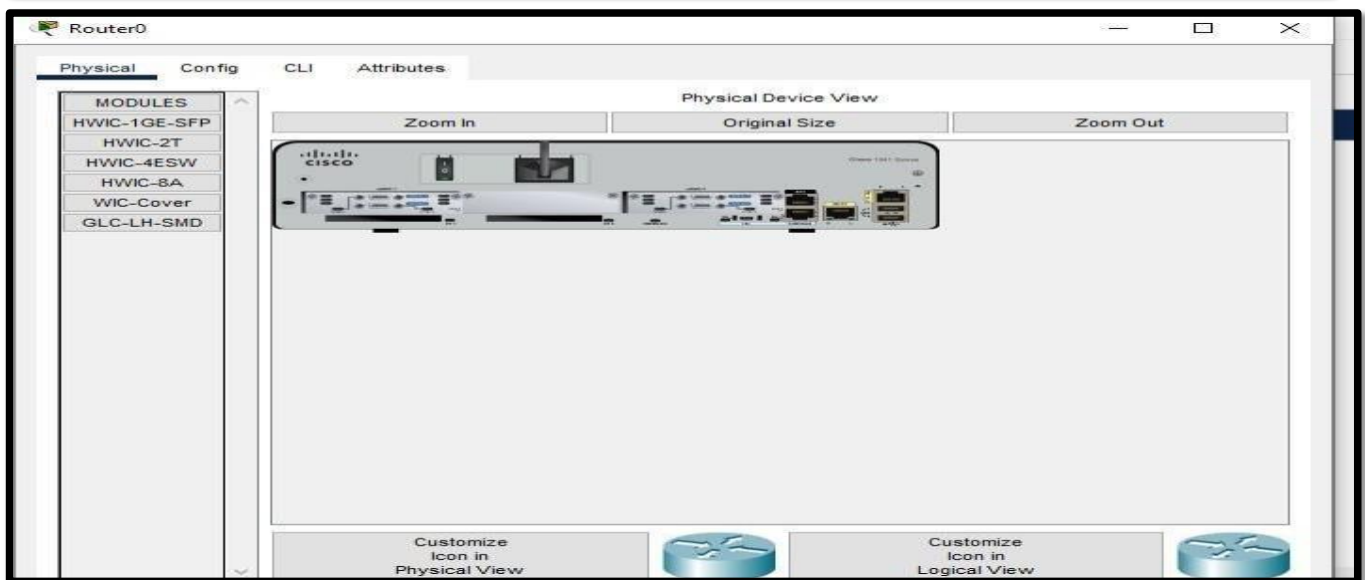
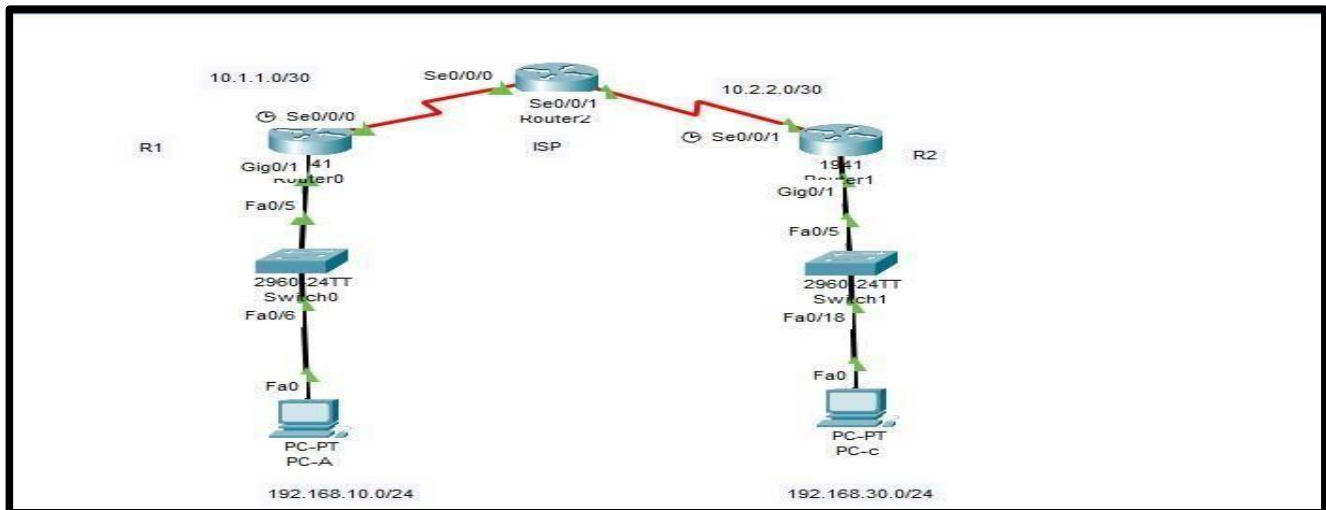
15.0(2) lanbasek9 image or comparable) · 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term) · Console cables to configure the Cisco IOS devices via the console ports · Ethernet and serial cables as shown in the topology

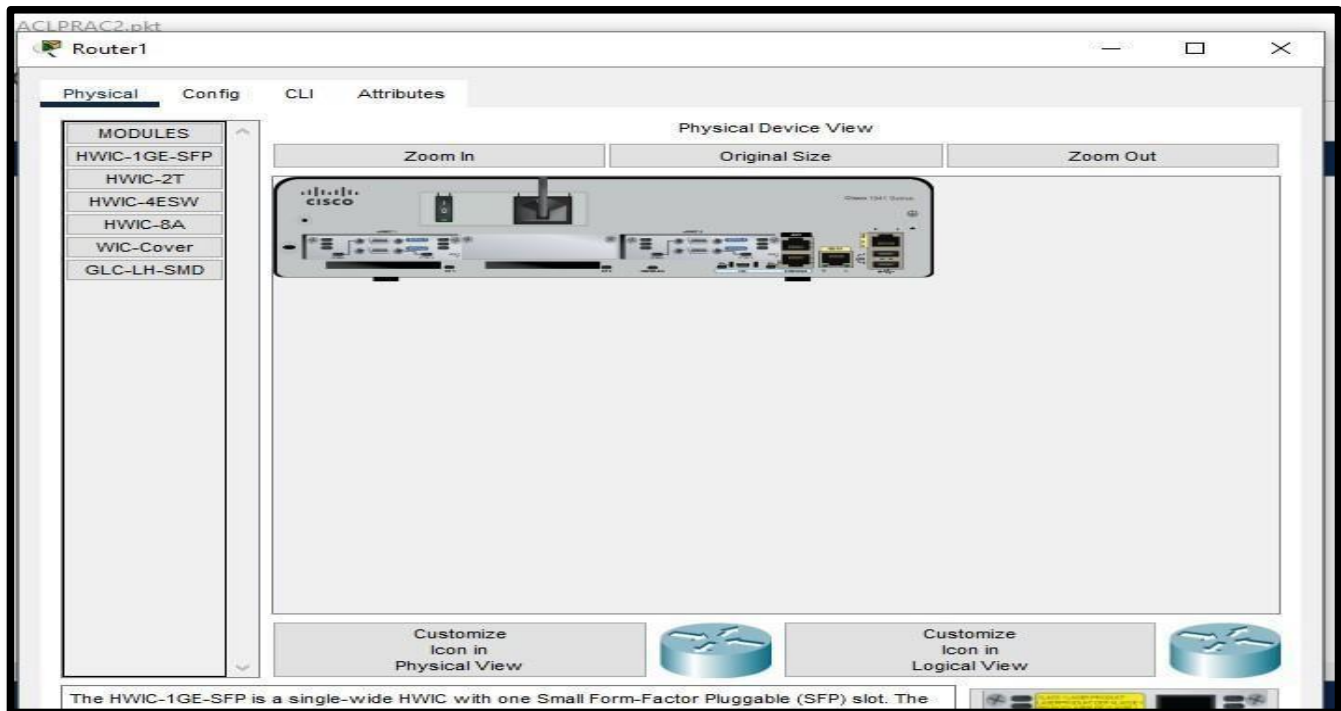
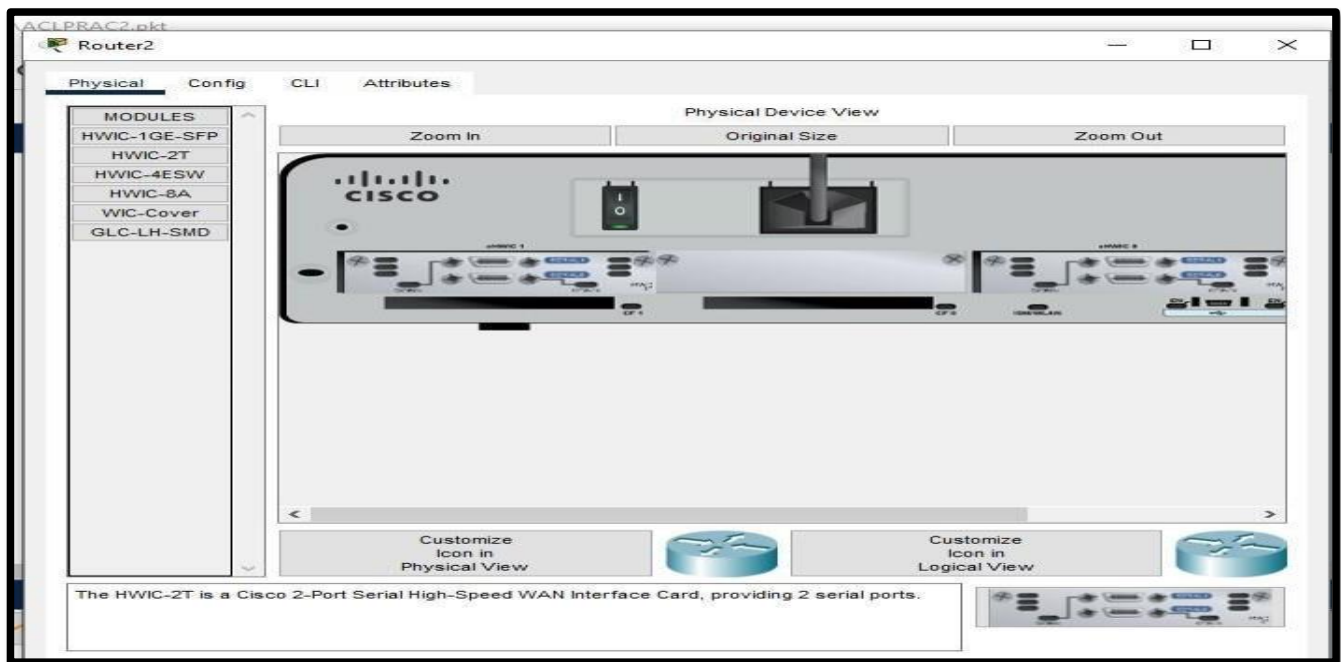
### Part 1: Set Up the Topology and Initialize Devices

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



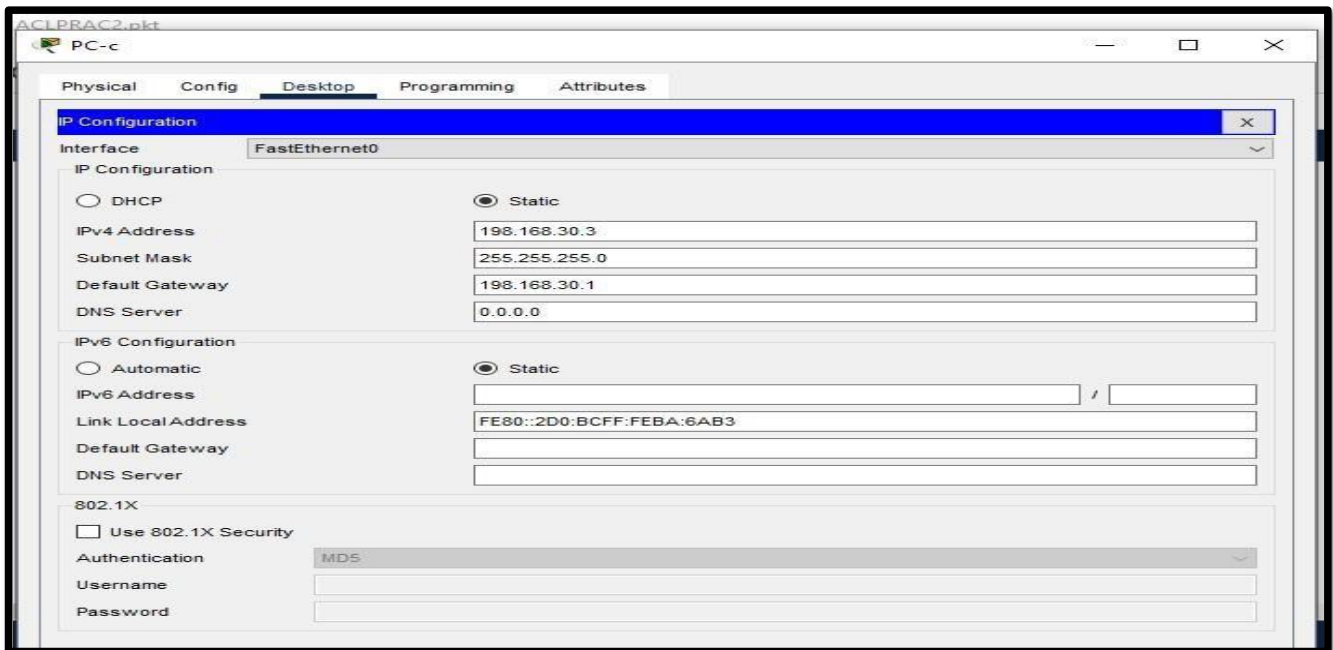
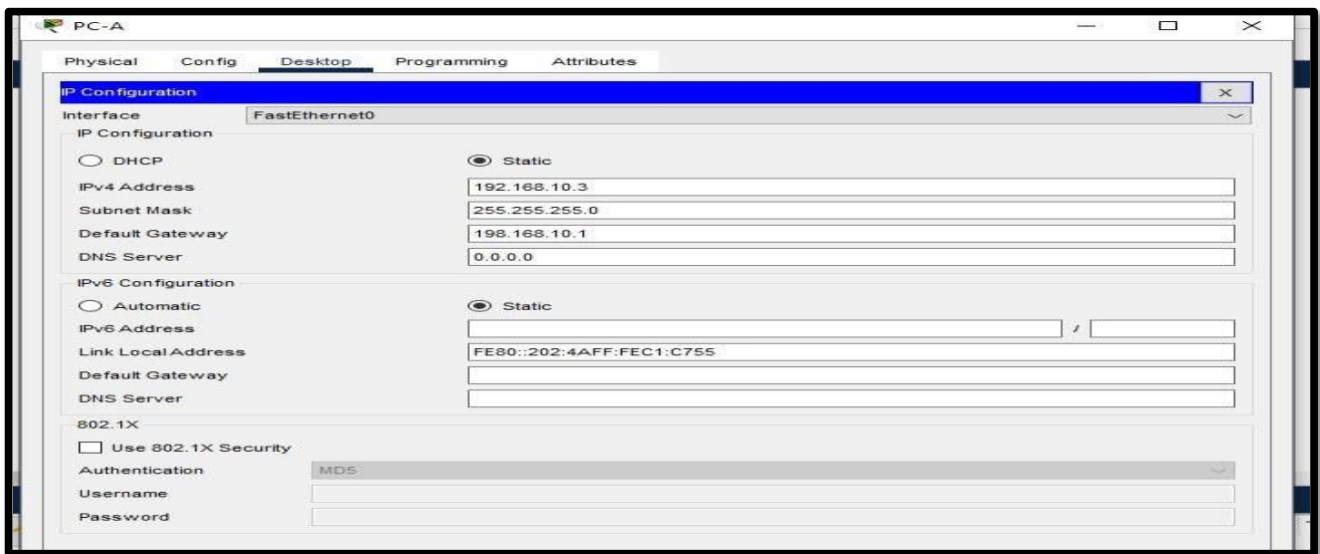
Step 2:- Initialize and reload the routers and switches.





## Part 2: Configure Devices and Verify Connectivity

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



Configure basic settings for the routers.

- Console into the router and enter global configuration mode.
- Create loopback interfaces on each router as shown in the Addressing Table.
- Configure interface IP addresses as shown in the Topology and Addressing Table.
- Assign a clock rate of 128000 to the DCE serial interfaces.

**a. Router > en**

**Router > conf t**

**Router > hostname R1**

```
c  Rocateco

Press RETURN to get started!

Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with
CNTIL/Z.
Router(config)#hostname R1
R1(config)#|
```

Copy Paste

```
Router0

Wllr=orifig)#intorEac=e loopbac=k D

B1 loonfig-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPBCto=S-UM##I4. Line protocol on Intorfae Loopbaoko, changed sEate to up

Blloonfig-if)#ip address 1S3 1f8.20.1 255.255.255.0
flll-o**fig-if)#no shrizdowrz
Rl Coonfig-if)#eait
B1 {oonfig)#
```

```

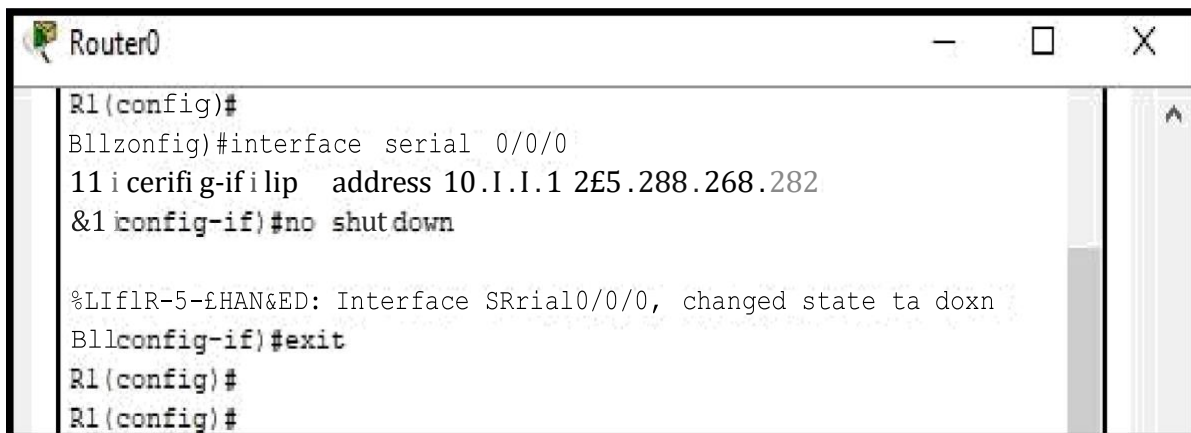
Bl(zonfig)#interface gigabitBthernet
Blloonfig)4interface gigabitBthernet 0/1
Rlloonfig-if)#ip address I9?.148.10.1 255.255.255.0
Rlleonfig-if)#no shutdown

Rllconfig-if#
8LINK-z-CHANGED: Interface GigabitZtheznet0/1, changed state to up

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

Rlloonfig-if)8exit

```

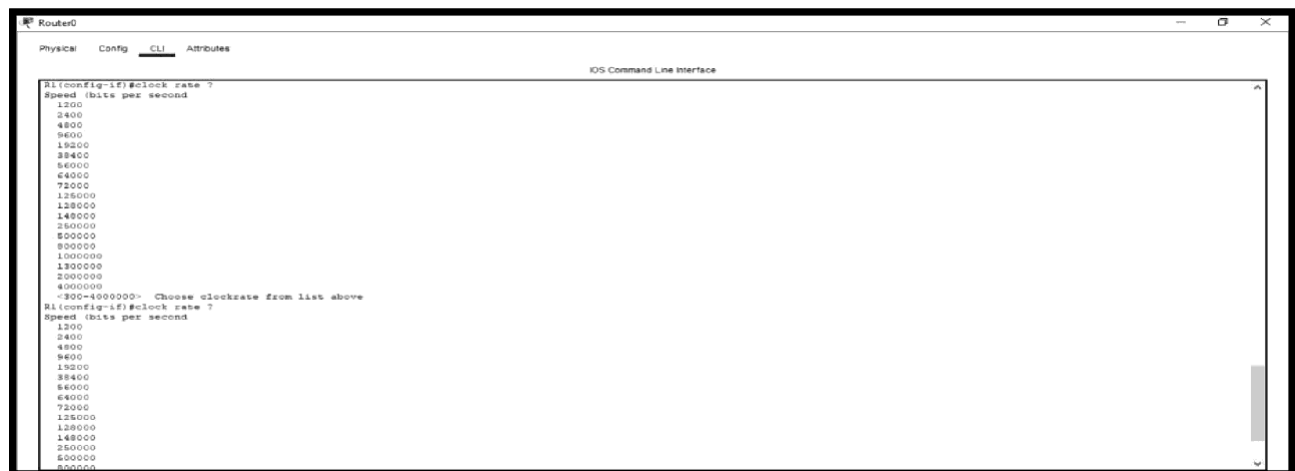


```

Router0
R1(config)#
Bl(zonfig)#interface serial 0/0/0
11 i cerifig-if ilip address 10.I.I.1 2£5.288.268.282
&1 config-if)#no shutdown

%LIflR-5-£HAN&ED: Interface SRrial0/0/0, changed state ta doxn
Bl(lconfig-if)#exit
R1(config)#
R1(config)#

```



```

Router0
Physical Config CLI Attributes
IOS Command Line Interface
R1(config-if)#clock rate ?
Speed (bits per second)
1200
2400
4800
9600
19200
38400
56000
64000
72000
125000
128000
148000
200000
250000
300000
312500
320000
400000
480000
>300-4000000> Choose clockrate from list above
R1(config-if)#clock rate ?
Speed (bits per second)
1200
2400
4800
9600
19200
38400
56000
64000
72000
125000
128000
148000
200000
250000
300000
312500
320000

```

```
Router0
2000000
4000000
<300-4000000> Choose clockrate from list above
R1(config-if)#clock rate 128000
R1(config-if)#exit
R1(config)#
R1(config)#
R1(config)#
```

```
Router0
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#do sh ip int bri
Interface          IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/1 192.168.10.1    YES manual    up
Serial0/0/0         10.1.1.1        YES manual    down
Serial0/0/1         unassigned      YES unset  administratively down down
Serial0/1/0         unassigned      YES unset  administratively down down
Serial0/1/1         unassigned      YES unset  administratively down down
Loopback0          192.168.20.1    YES manual    up
Vlan1              unassigned      YES unset  administratively down down
R1(config)#
```

Copy Paste

## 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
```

```
Router2
ISP(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

ISP(config)#interface serial 0/0/1
ISP(config-if)#ip address 10.2.2.2 255.255.255.252
ISP(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
ISP(config-if)#clock rate 128000
This command applies only to DCE interfaces
ISP(config-if)#exit
ISP(config)#
```

```
Router2
ISP(config)#
ISP(config)#do sh ip int bri
Interface                IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0       unassigned      YES unset  administratively down down
GigabitEthernet0/1       unassigned      YES unset  administratively down down
Serial0/0/0              10.1.1.2        YES manual  up              up
Serial0/0/1              10.2.2.2        YES manual  down            down
Serial0/1/0              unassigned      YES unset  administratively down down
Serial0/1/1              unassigned      YES unset  administratively down down
Loopback0                209.165.200.225 YES manual  up              up
Vlan1                    unassigned      YES unset  administratively down down
ISP(config)#
```

Copy Paste

### R3

Router > en

Router > conf t

Router > hostname R3

Router1



fig 0  
fig 0  
CHAN

E  
g

C O ck

I

pba Lo

ame R

face fig-if)#

terou

S-CHANGED

co3(

2

oco ro

Inte

ROTO-S-Up

co3(

OWN: d state t

co3(

68. 2.

up

fig-if)#i

NKLI

fig-if)#n

NELI

addr fig-if)#e

ngha

shut fig)#

it

co3(

co3(

co3(

co3(

Router1

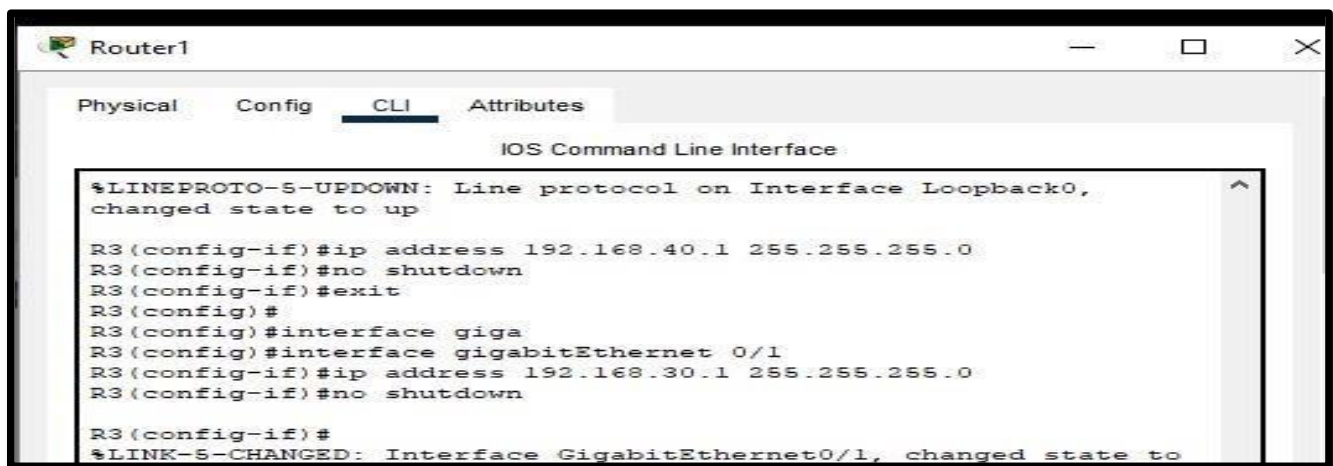


```
R3(config)#interface gigabitEthernet 0/1
R3(config-if)#ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown
```

```
R3(config-if)#
%LINK-S-CHANGED: Interface GigabitEthernet0/1, changed state to
up
```

```
%LINEPROTO-S-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
```

```
R3(config-if)#exit
R3(config)#
```



Router1

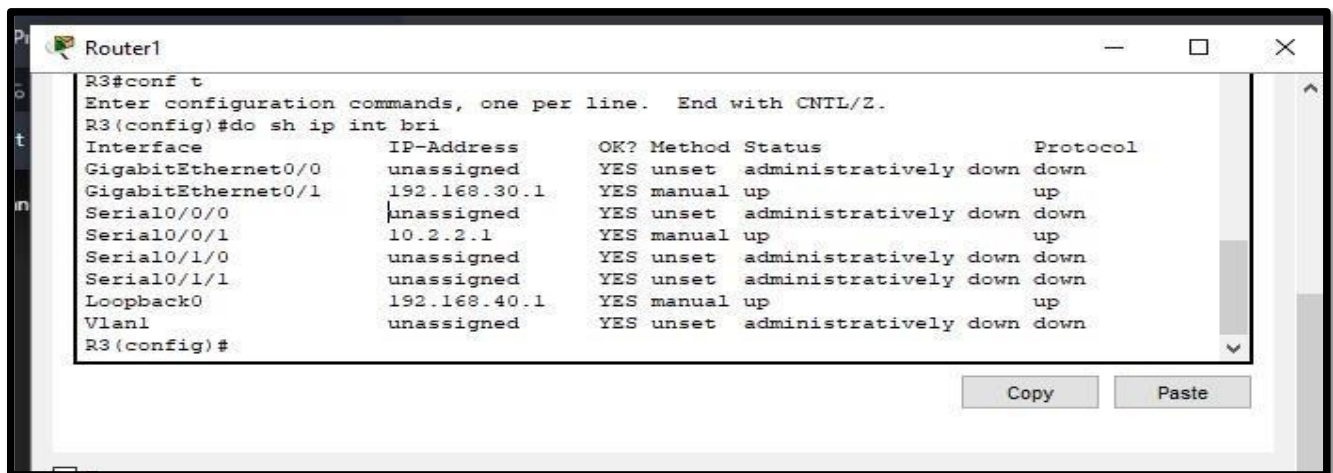
Physical Config **CLI** Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up

R3(config-if)#ip address 192.168.40.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
R3(config)#interface giga
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
```



Router1

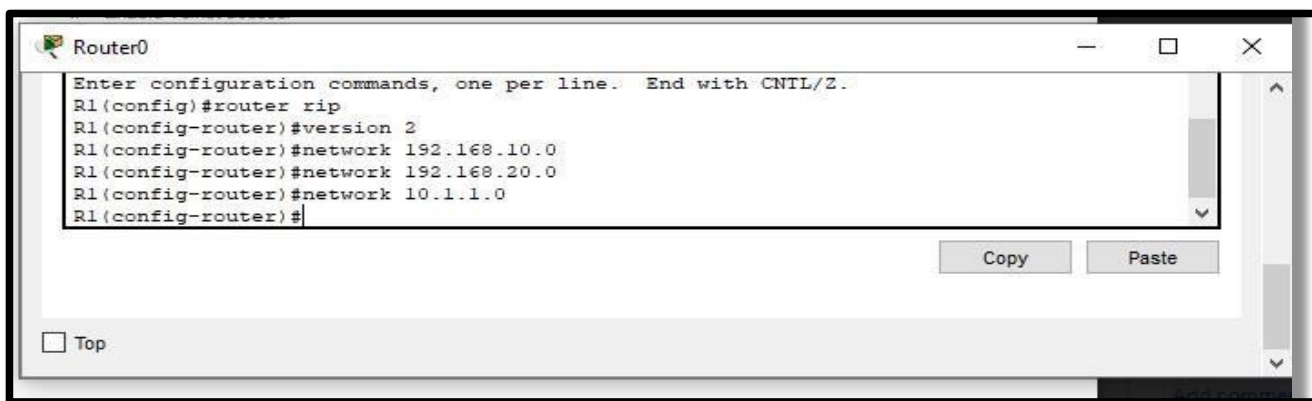
```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#do sh ip int bri
Interface                IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0       unassigned      YES unset    administratively down down
GigabitEthernet0/1       192.168.30.1    YES manual    up            up
Serial0/0/0              unassigned      YES unset    administratively down down
Serial0/0/1              10.2.2.1        YES manual    up            up
Serial0/1/0              unassigned      YES unset    administratively down down
Serial0/1/1              unassigned      YES unset    administratively down down
Loopback0                192.168.40.1    YES manual    up            up
Vlan1                    unassigned      YES unset    administratively down down
R3(config)#
```

Copy Paste

### 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.

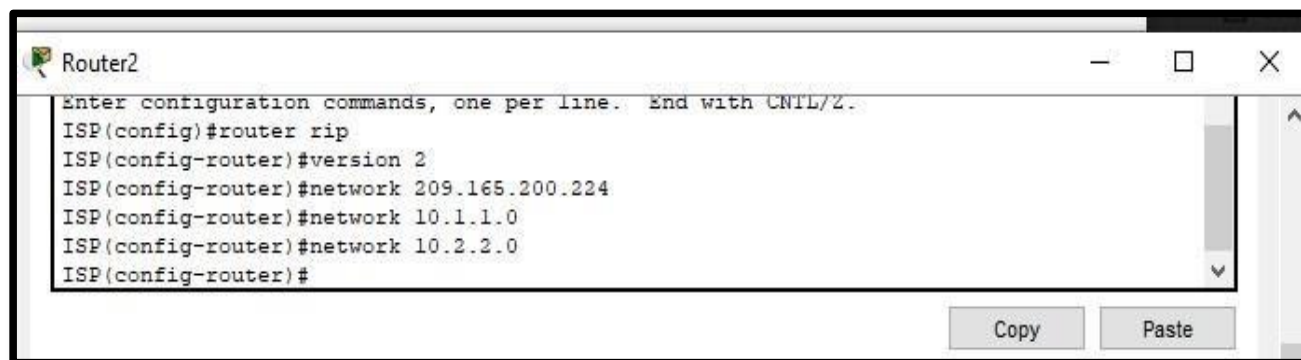
```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.10.0
R1(config-router)# network 192.168.20.0
R1(config-router)# network 10.1.1.0
```

A screenshot of a terminal window titled "Router0". The window contains a series of configuration commands for a router. The prompt is "Enter configuration commands, one per line. End with CNTL/Z." The commands entered are: "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", and "R1(config-router)#network 10.1.1.0". The prompt "R1(config-router)#" is visible at the end of the last line. There are "Copy" and "Paste" buttons at the bottom right of the terminal area. A "Top" button is at the bottom left.

```
Router0
Enter configuration commands, one per line. End with CNTL/Z.
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
R1(config-router)#
```

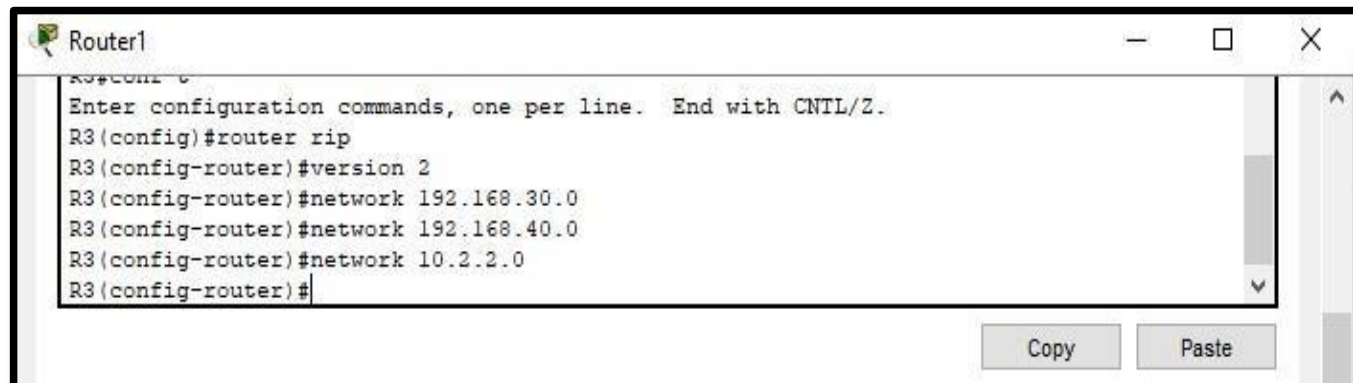
```
ISP(config)#  router rip
ISP(config-router)# version 2
ISP(config-router)# network 209.165.200.224
ISP(config-router)# network 10.1.1.0

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

A screenshot of a terminal window titled "Router2". The window contains a series of configuration commands for a router. The prompt is "Enter configuration commands, one per line. End with CNTL/Z." The commands entered are: "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", and "ISP(config-router)#". The prompt "ISP(config-router)#" is visible at the end of the last line. There are "Copy" and "Paste" buttons at the bottom right of the terminal area.

```
Router2
Enter configuration commands, one per line. End with CNTL/Z.
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
ISP(config-router)#
```

```
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
```

A screenshot of a terminal window titled "Router1". The window contains a series of configuration commands for a router. The prompt is "Enter configuration commands, one per line. End with CNTL/Z." The commands entered are: "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", and "R3(config-router)#". The prompt "R3(config-router)#" is visible at the end of the last line. There are "Copy" and "Paste" buttons at the bottom right of the terminal area.

```
Router1
Enter configuration commands, one per line. End with CNTL/Z.
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
R3(config-router)#
```

### 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.

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

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

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

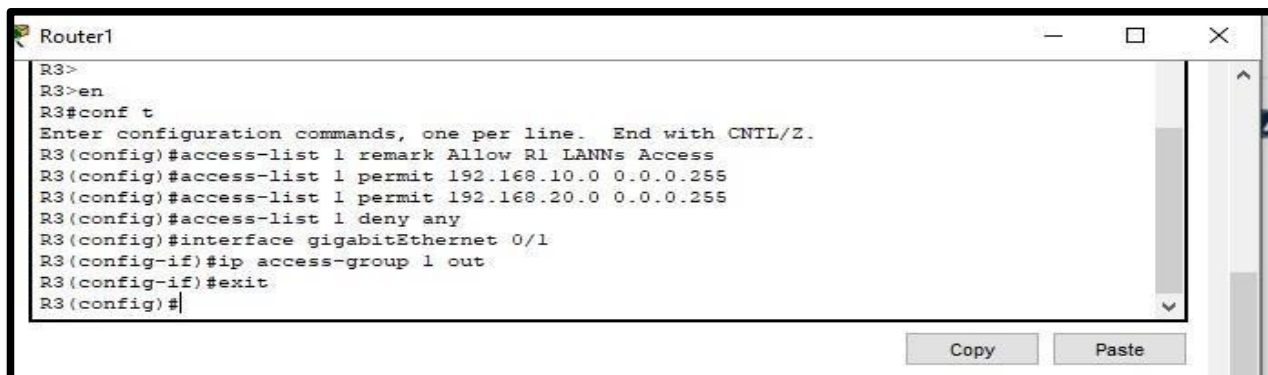
```
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```

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

```
R3(config)# access-list 1 deny any
```

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

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



```
Router1
R3>
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 1 remark Allow R1 LANNs 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
R3(config)#interface gigabitEthernet 0/1
R3(config-if)#ip access-group 1 out
R3(config-if)#exit
R3(config)#
```

- 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

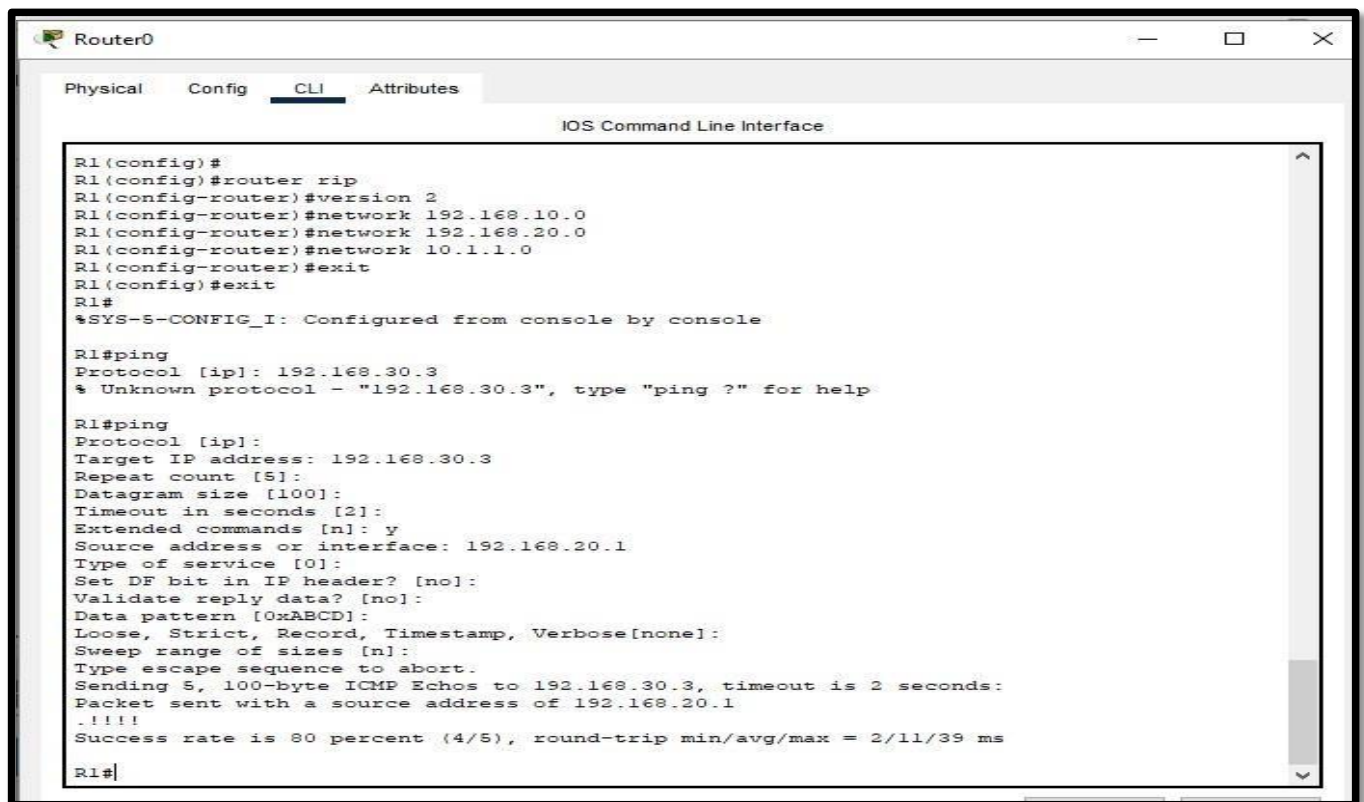
R1 as your source. Ping PC-C's IP address. Were the pings successful? \_\_\_\_\_ Yes

```
Router1
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#sh access-list 1
Standard IP access list 1
  permit 192.168.10.0 0.0.0.255
  permit 192.168.20.0 0.0.0.255
  deny any
```

```
Router1
Physical Config CLI Attributes
R3#sh ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
R3#
```

**Ping :**



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface

R1(config)#
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
R1(config-router)#exit
R1(config)#exit
R1#
*SYS-S-CONFIG_I: Configured from console by console

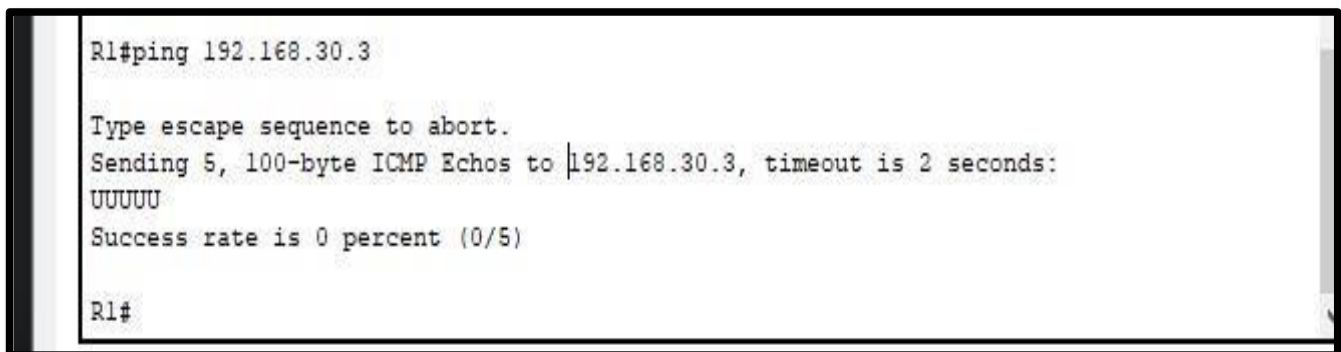
R1#ping
Protocol [ip]: 192.168.30.3
* Unknown protocol - "192.168.30.3", type "ping ?" for help

R1#ping
Protocol [ip]:
Target IP address: 192.168.30.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
.....
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/11/39 ms

R1#
```

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

R1# ping 192.168.30.3



```
R1#ping 192.168.30.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)

R1#
```

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.

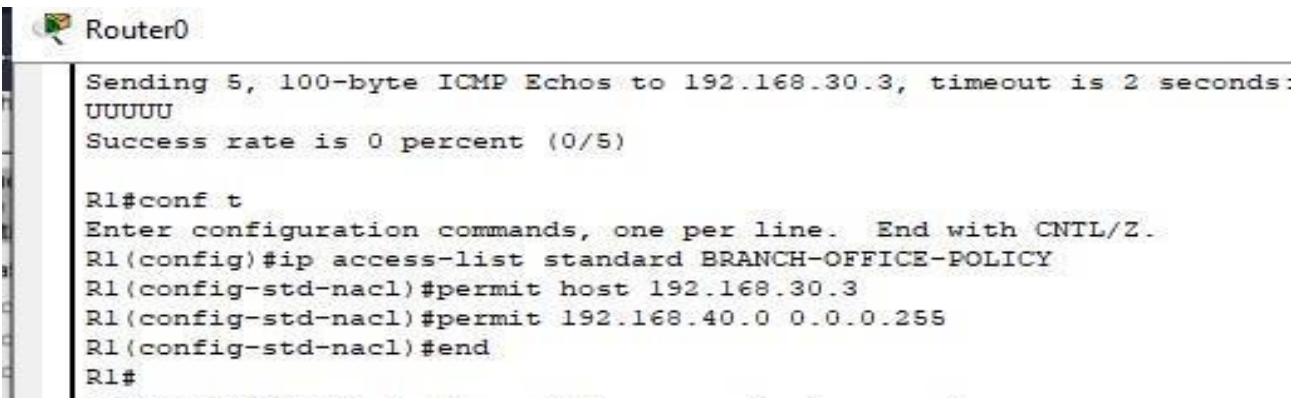


```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
```

```
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
```



```
Router0
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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
R1#
```

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
```



```
Router0

R1(config-if)#interface gigabitEthernet 0/1
R1(config-if)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip access-group BRANCH-OFFICE-POLICY out
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

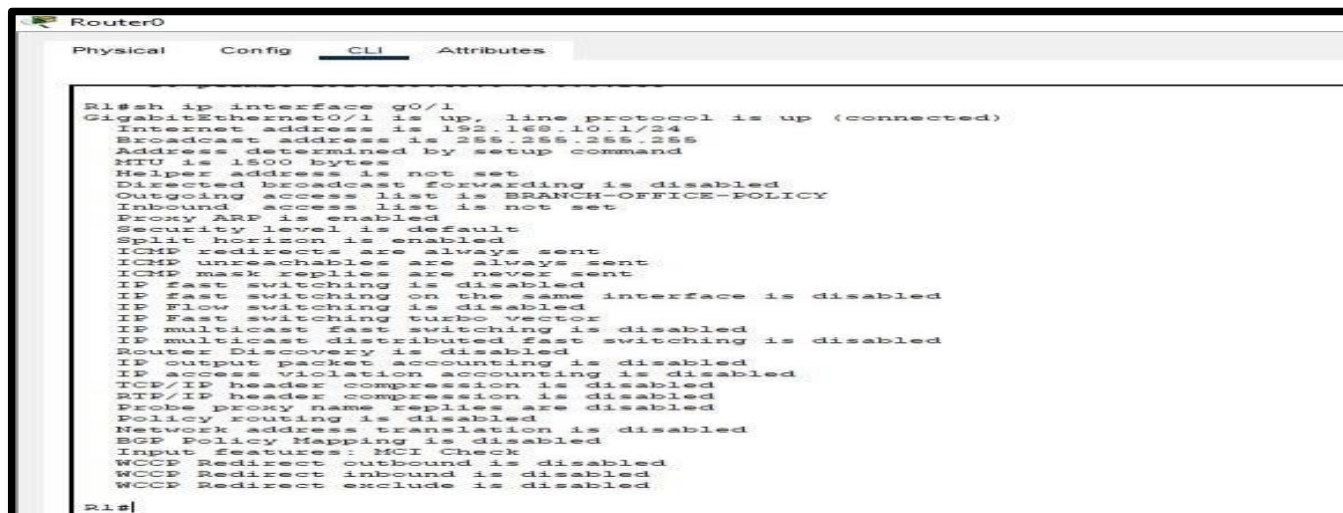
R1#show access-list
Standard IP access list BRANCH-OFFICE-POLICY
 10 permit host 192.168.30.3
 20 permit 192.168.40.0 0.0.0.255

R1#
```

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**



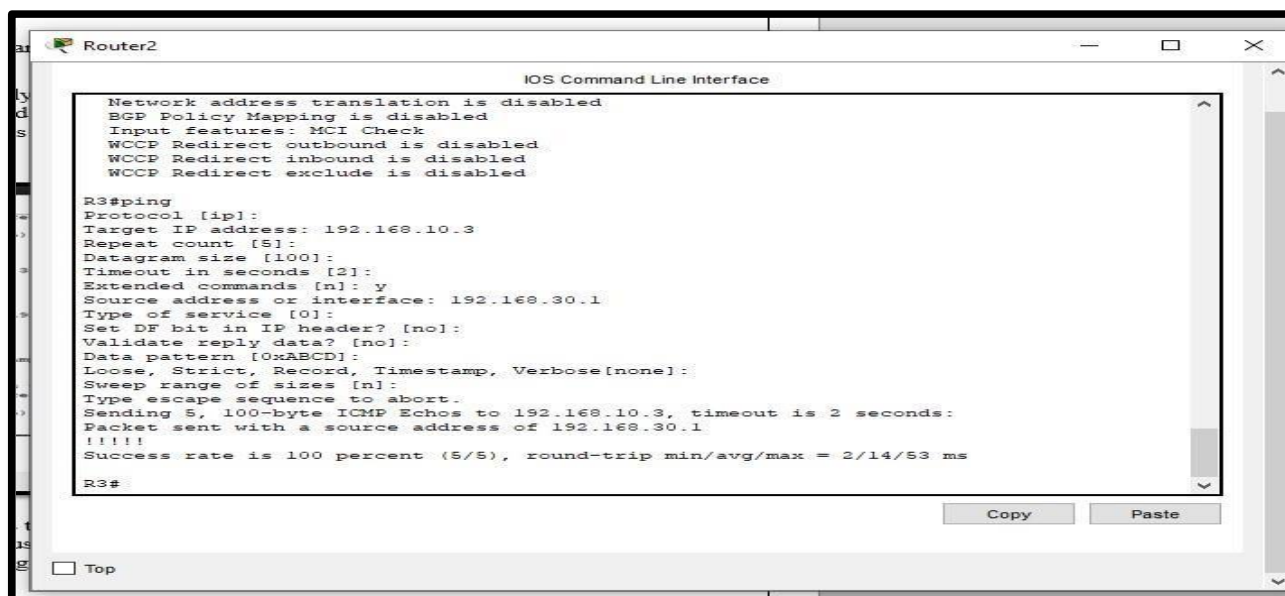
```
Router0
Physical Config CLI Attributes
R1#sh ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
Internet address is 192.168.10.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is BRANCH-OFFICE-POLICY
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
R1#
```

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**

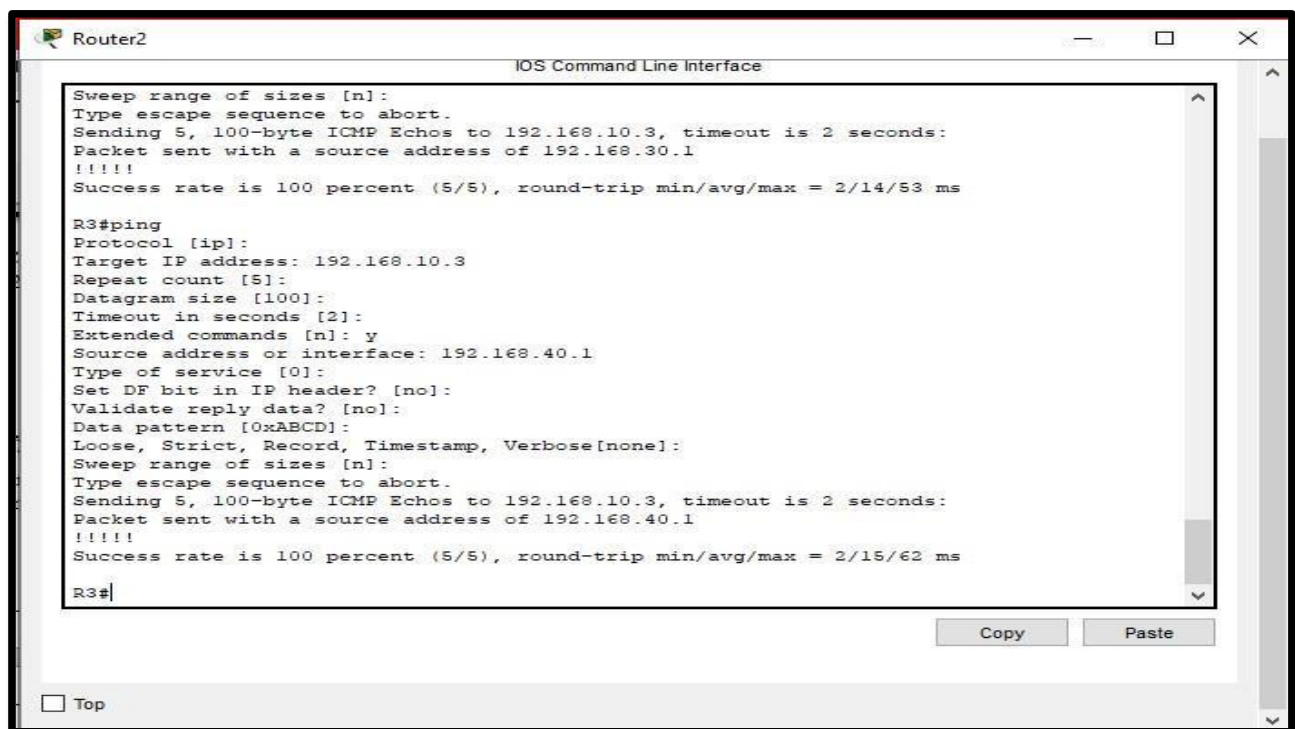


```
Router2
IOS Command Line Interface
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled

R3#ping
Protocol [ip]:
Target IP address: 192.168.10.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.30.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.10.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/14/53 ms
R3#
```

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**



```
Router2
IOS Command Line Interface

Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/14/53 ms

R3#ping
Protocol [ip]:
Target IP address: 192.168.10.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.40.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.40.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/15/62 ms

R3#
```

#### 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
```

```
Router0
* Invalid input detected at ... marker ...

R1#show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
 10 permit host 192.168.30.3
 20 permit 192.168.40.0 0.0.0.255 (5 match(es))

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

c. Verify the ACL.

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

R1# show access -lists

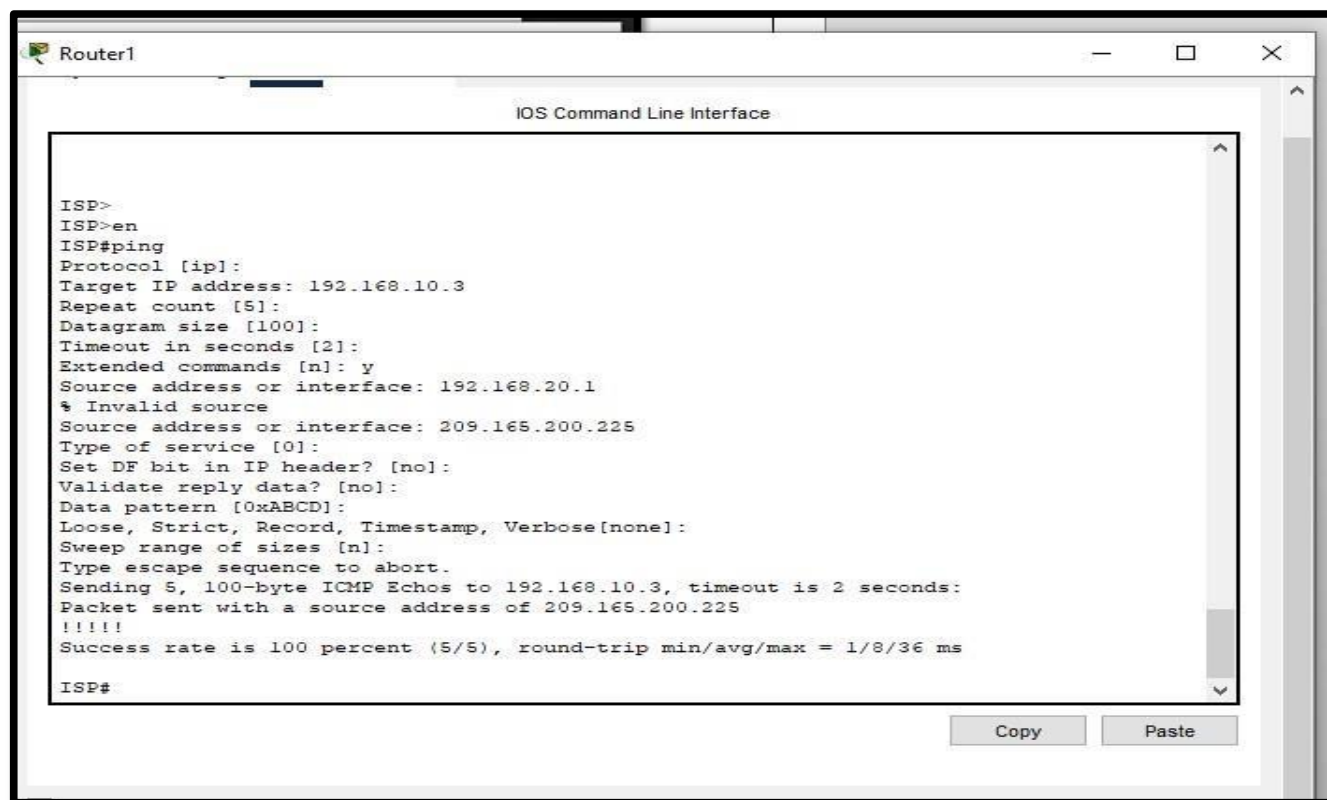
```
Router0
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)#30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)#40 deny any
R1(config-std-nacl)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
 10 permit host 192.168.30.3
 20 permit 192.168.40.0 0.0.0.255 (5 match(es))
 30 permit 209.165.200.224 0.0.0.31
 40 deny any

R1#
```

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)