Department of Computer Science and Engineering

Islamic University of Technology (IUT)

A subsidiary organ of OIC

Laboratory Report

CSE 4512: Computer Networks Lab

Name: Tahsin Islam

Student ID: 210042137

Section: SWE (Group – A)

Semester: Summer (4^{th})

Academic Year: 2022-2023

Date of Submission: 10/04/2024

Title: Configuring ACL and NAT in Cisco Devices

Objective:

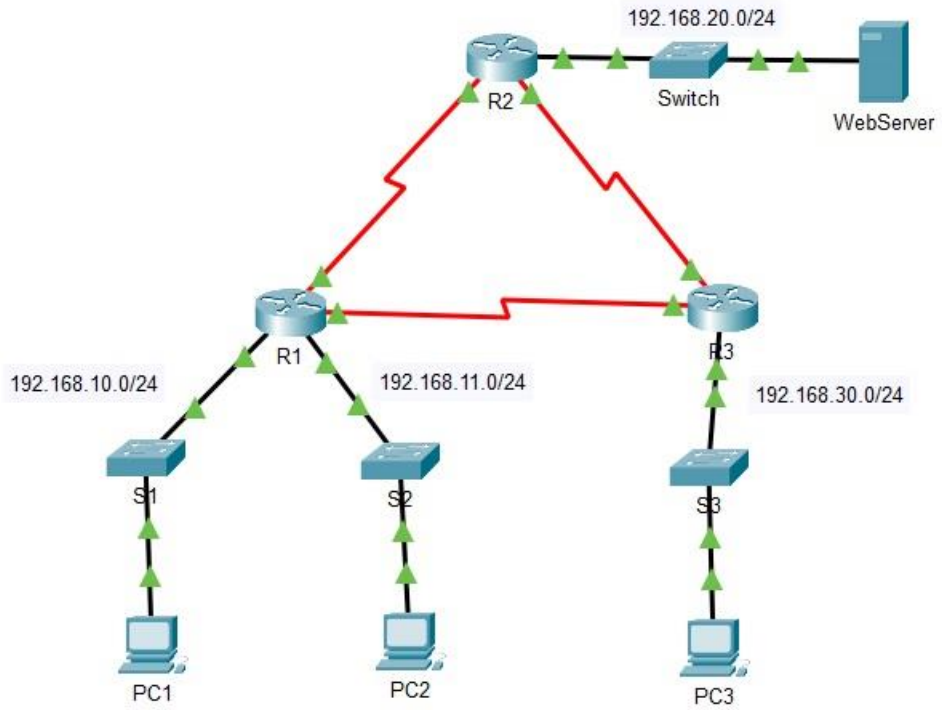
1. Describe the concept of Access Control List (ACL)
2. Implement standard numbered ACL
3. Describe the concept of Network Address Translation (NAT)
4. Explain different types of NAT configuration
5. Implement NAT in a given topology

Devices/ software Used:

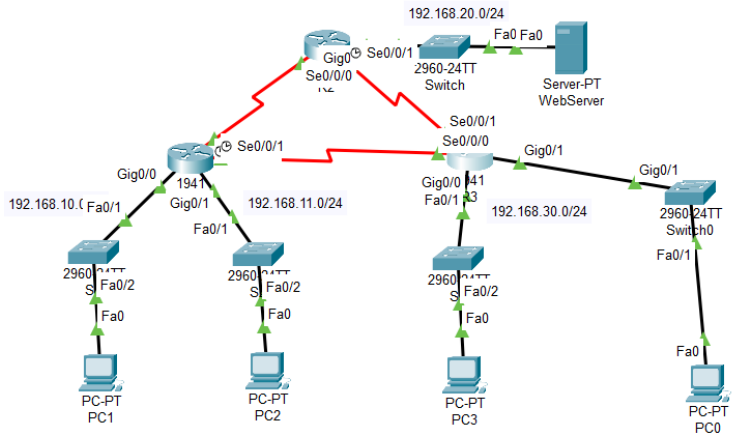
1. Cisco Packet Tracer
2. Laptop / PC

Diagram of the experiment(s):

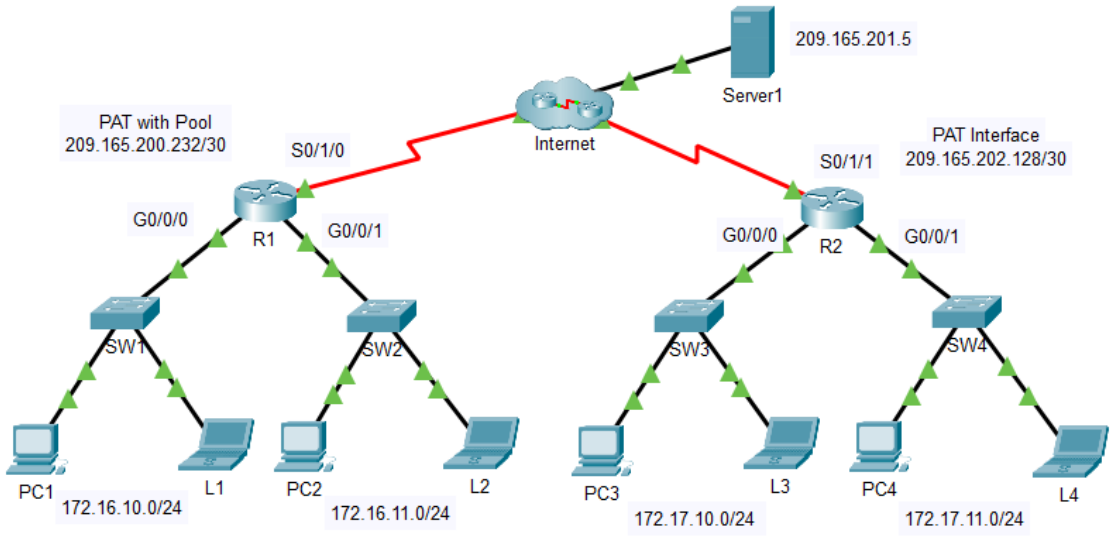
Task-1 (A)



Task-1 (B)



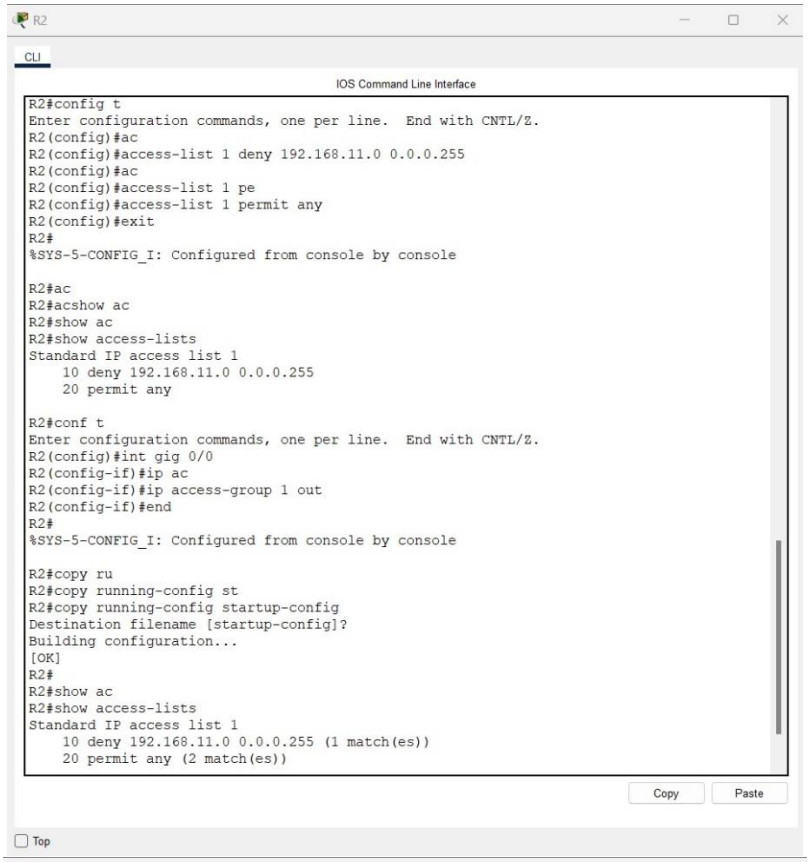
Task-2

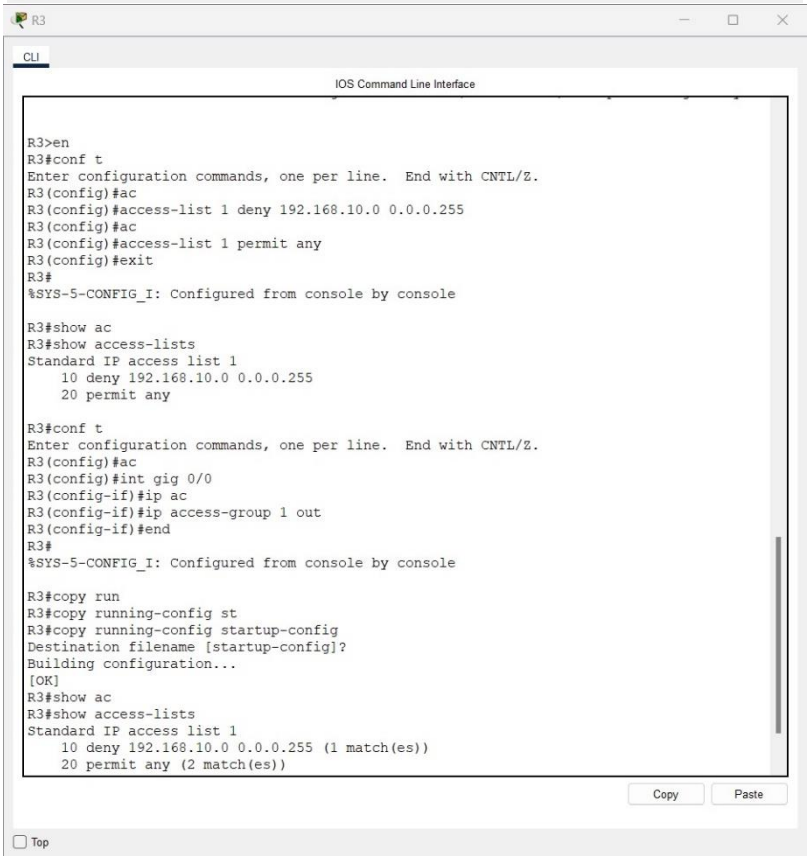


Working Procedure:

(Explain in brief how you completed the tasks. Provide necessary screenshots of used commands for each task.)

Task-1


R2
CLI
IOS Command Line Interface
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ac
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#ac
R2(config)#access-list 1 pe
R2(config)#access-list 1 permit any
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#ac
R2#acshow ac
R2#show ac
R2#show access-lists
Standard IP access list 1
10 deny 192.168.11.0 0.0.0.255
20 permit any
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int gig 0/0
R2(config-if)#ip ac
R2(config-if)#ip access-group 1 out
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#copy ru
R2#copy running-config st
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
R2#show ac
R2#show access-lists
Standard IP access list 1
10 deny 192.168.11.0 0.0.0.255 (1 match(es))
20 permit any (2 match(es))
Copy
Paste
Top


R3
CLI
IOS Command Line Interface
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ac
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#ac
R3(config)#access-list 1 permit any
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#show ac
R3#show access-lists
Standard IP access list 1
10 deny 192.168.10.0 0.0.0.255
20 permit any
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ac
R3(config)#int gig 0/0
R3(config-if)#ip ac
R3(config-if)#ip access-group 1 out
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#copy run
R3#copy running-config st
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#show ac
R3#show access-lists
Standard IP access list 1
10 deny 192.168.10.0 0.0.0.255 (1 match(es))
20 permit any (2 match(es))
Copy
Paste
Top

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC2	ICMP		0.000	N	0	(edit)	
	Successful	PC1	WebServer	ICMP		0.000	N	1	(edit)	
	Failed	PC2	WebServer	ICMP		0.000	N	2	(edit)	
	Failed	PC1	PC3	ICMP		0.000	N	3	(edit)	
	Successful	PC2	PC3	ICMP		0.000	N	4	(edit)	
	Successful	PC3	WebServer	ICMP		0.000	N	5	(edit)	

Task-2

R1

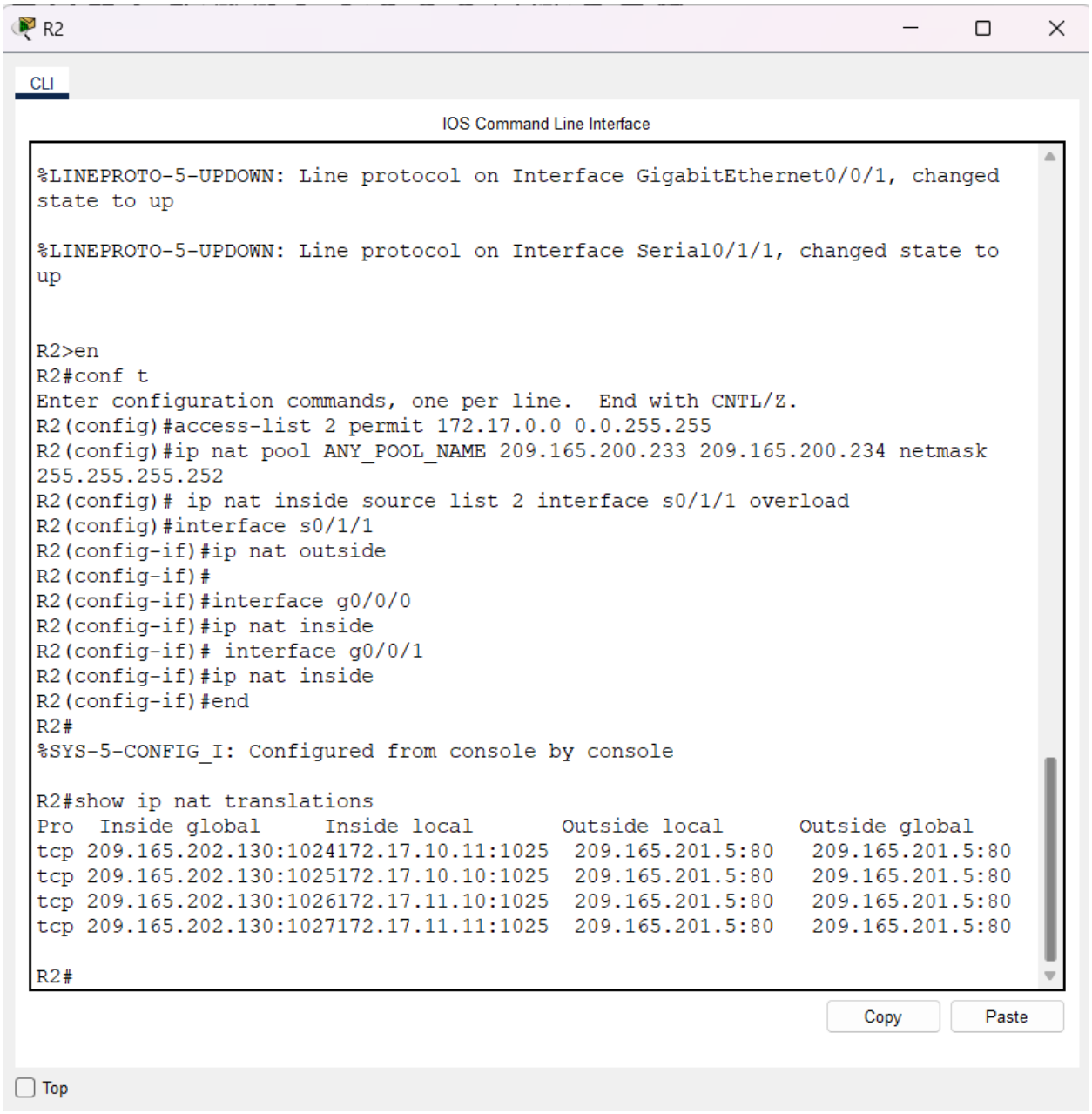
CLI

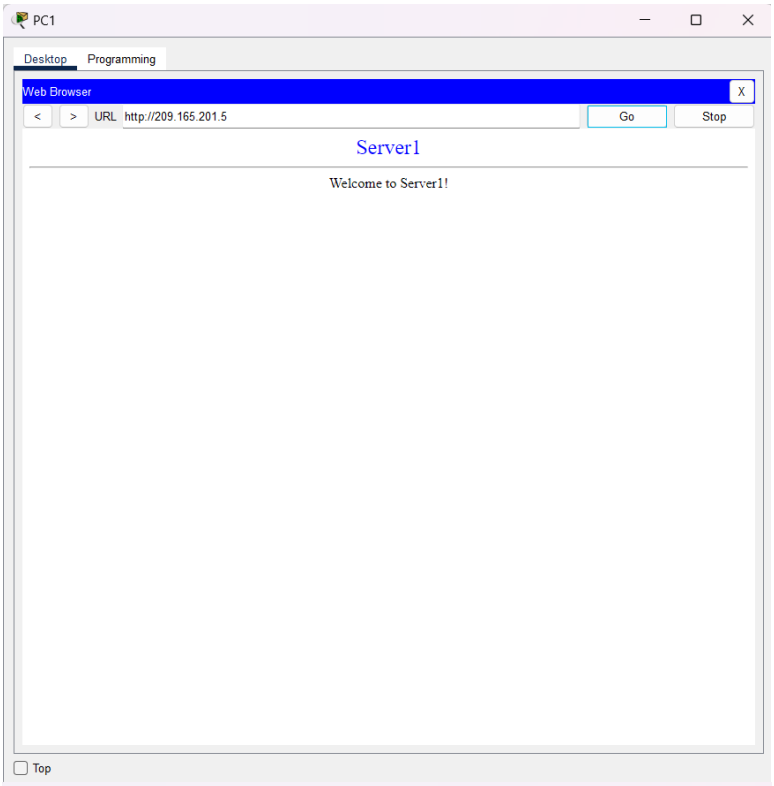
IOS Command Line Interface

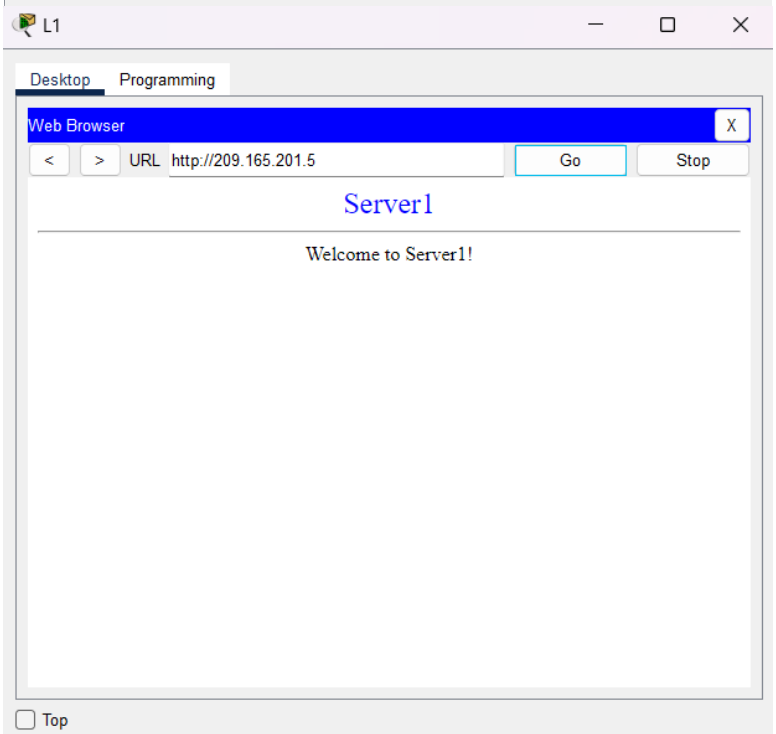
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up


R1>en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 1 permit 172.16.0.0 0.0.255.255
R1(config)#ip nat pool ANY_POOL_NAME 209.165.200.233 209.165.200.234 netmask
255.255.255.252
R1(config)#ip nat inside source list 1 pool ANY_POOL_NAME overload
R1(config)#interface s0/1/0
R1(config-if)#ip nat outside
R1(config-if)#interface g0/0/0
R1(config-if)#ip nat inside
R1(config-if)#interface g0/0/1
R1(config-if)#ip nat inside
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 209.165.200.233:1024172.16.10.11:1025  209.165.201.5:80   209.165.201.5:80
tcp 209.165.200.233:1025172.16.10.10:1025  209.165.201.5:80   209.165.201.5:80
tcp 209.165.200.233:1026172.16.11.10:1025  209.165.201.5:80   209.165.201.5:80
tcp 209.165.200.233:1027172.16.11.11:1025  209.165.201.5:80   209.165.201.5:80

R1#
```

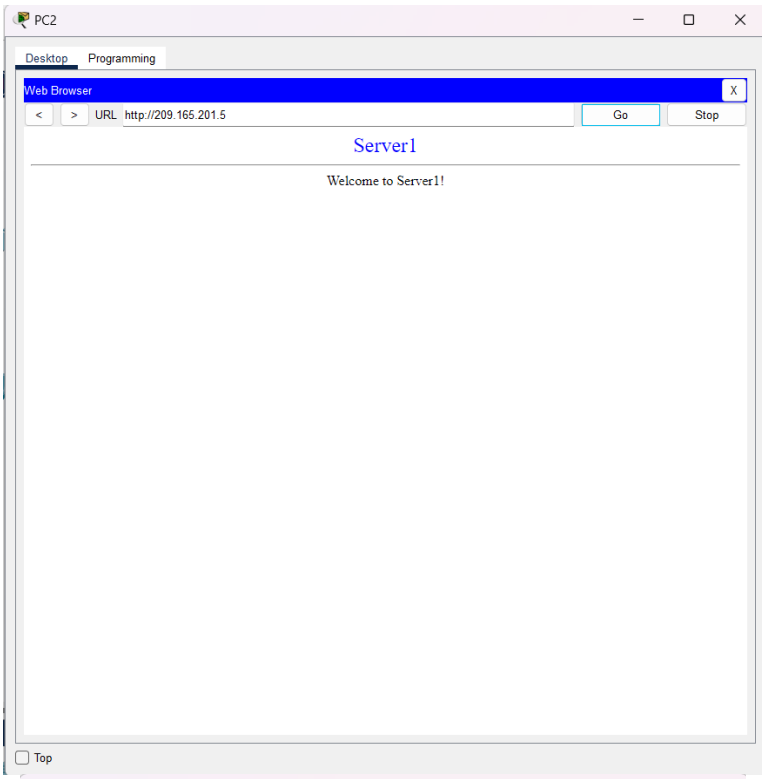
Copy Paste

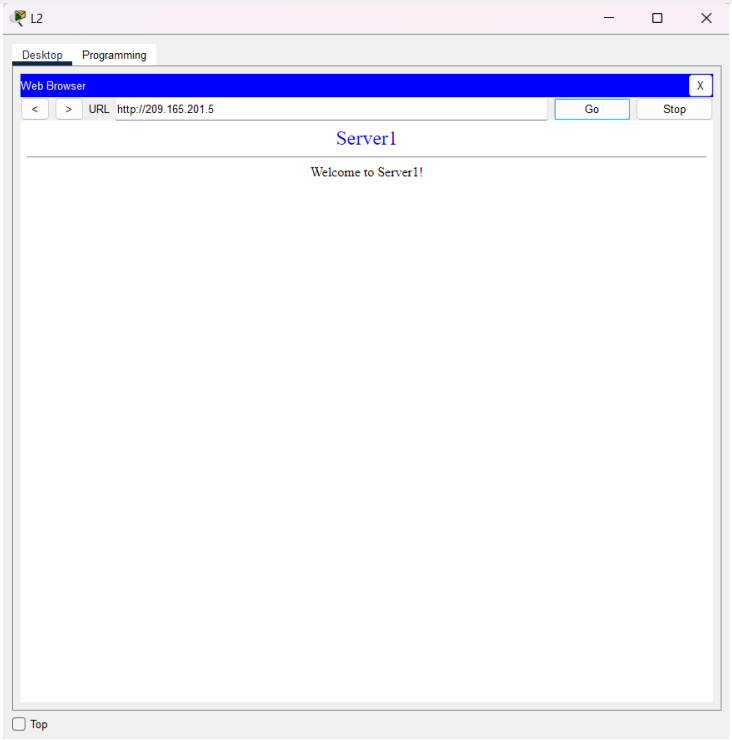
Top

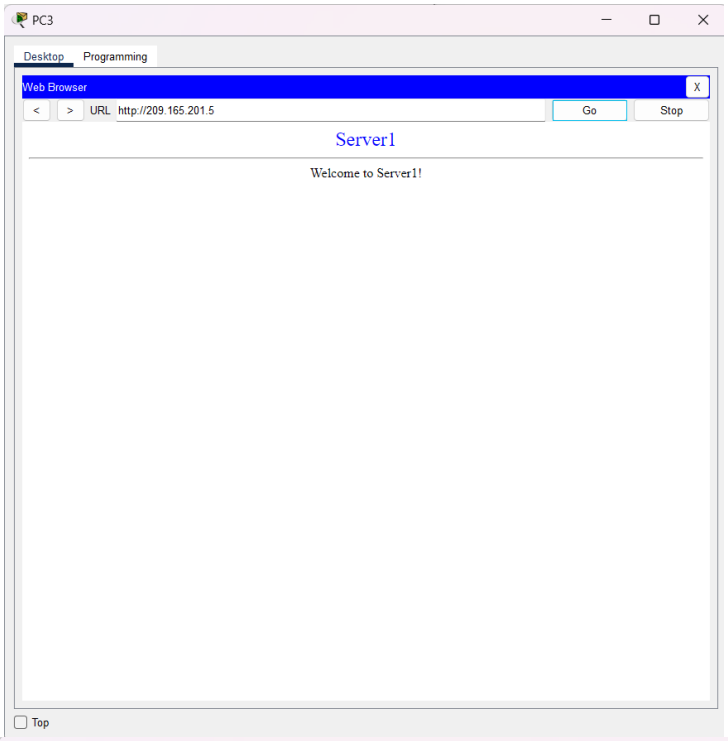

R2
CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 2 permit 172.17.0.0 0.0.255.255
R2(config)#ip nat pool ANY_POOL_NAME 209.165.200.233 209.165.200.234 netmask 255.255.255.252
R2(config)# ip nat inside source list 2 interface s0/1/1 overload
R2(config)#interface s0/1/1
R2(config-if)#ip nat outside
R2(config-if)#
R2(config-if)#interface g0/0/0
R2(config-if)#ip nat inside
R2(config-if)# interface g0/0/1
R2(config-if)#ip nat inside
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 209.165.202.130:1024 172.17.10.11:1025 209.165.201.5:80 209.165.201.5:80
tcp 209.165.202.130:1025 172.17.10.10:1025 209.165.201.5:80 209.165.201.5:80
tcp 209.165.202.130:1026 172.17.11.10:1025 209.165.201.5:80 209.165.201.5:80
tcp 209.165.202.130:1027 172.17.11.11:1025 209.165.201.5:80 209.165.201.5:80
R2#
Copy
Paste
Top

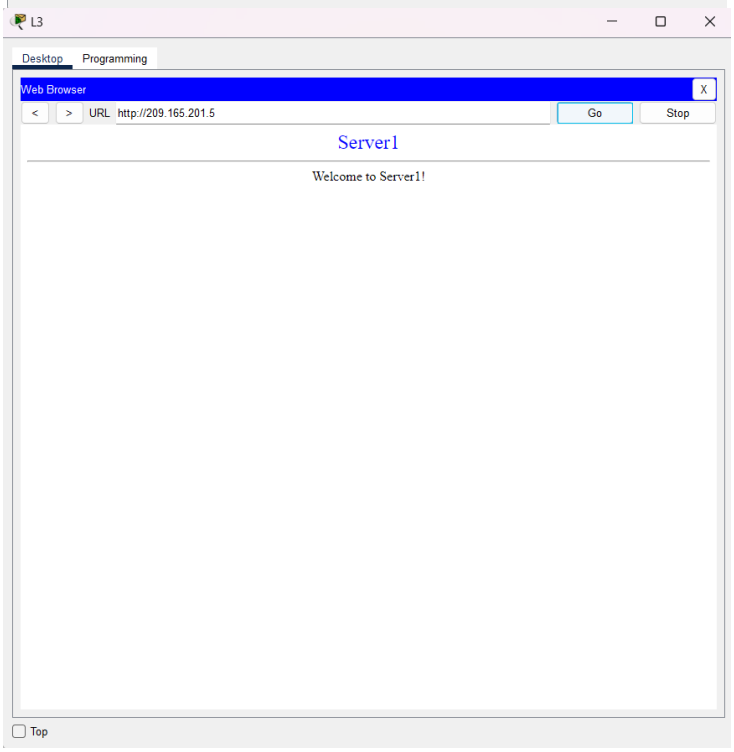

PC1
Desktop
Programming
Web Browser
X
<
>
URL
http://209.165.201.5
Go
Stop
Server1
Welcome to Server1!
Top

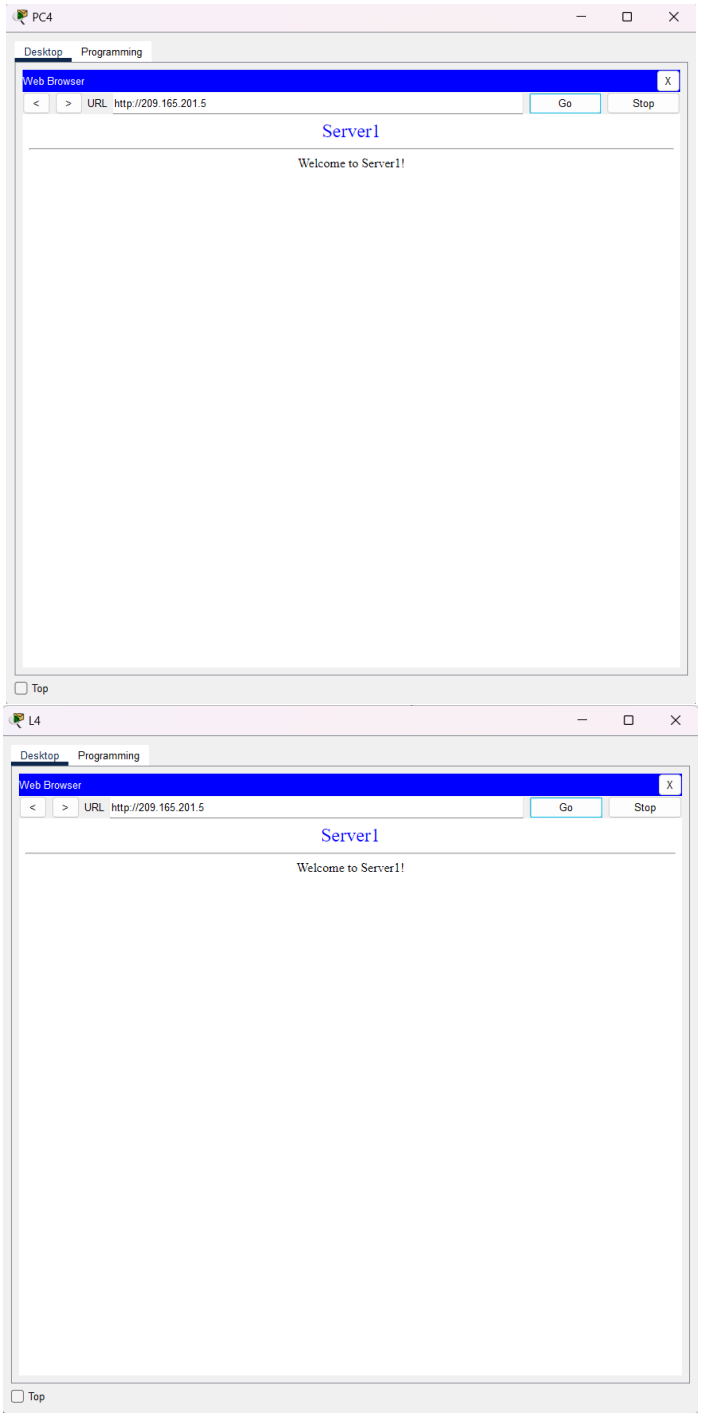

L1
Desktop
Programming
Web Browser
X
<
>
URL
http://209.165.201.5
Go
Stop
Server1
Welcome to Server1!
Top


PC2
Desktop
Programming
Web Browser
X
<
>
URL
http://209.165.201.5
Go
Stop
Server1
Welcome to Server1!
Top


L2
Desktop
Programming
Web Browser
X
<
>
URL
http://209.165.201.5
Go
Stop
Server1
Welcome to Server1!
Top


PC3
Desktop
Programming
Web Browser
X
<
>
URL
http://209.165.201.5
Go
Stop
Server1
Welcome to Server1!
Top


L3
Desktop
Programming
Web Browser
X
<
>
URL
http://209.165.201.5
Go
Stop
Server1
Welcome to Server1!
Top



Questions:

Task # 01:

1. The ping from 192.168.10.10 to 192.168.11.10 is successful or not? Explain.

Ans: Successful. The 192.168.10.0/24 network is not allowed to communicate with the 192.168.30.0/24 network. But it can communicate with 192.168.11.0/24 network.

2. The ping from 192.168.10.10 to 192.168.20.254 is successful or not? Explain.
   Ans: : **Successful.** The 192.168.10.0/24 network is not allowed to communicate with the 192.168.30.0/24 network. But it can communicate with 192.168.20.0/24 network. 192.168.11.0/24 was restricted to communicate with 192.168.20.0/24 network.

3. The ping from 192.168.11.10 to 192.168.20.254 failed or not? Explain.
   Ans: Failed. The 192.168.11.0/24 network is not allowed to communicate with 192.168.20.0/24 network.

Task # 02:

1. From the web browser of each of the PCs that use R1 as their gateway (PC1, L1, PC2, and L2), access the web page for Server1.
   Question: Were all connections successful?
   Ans: YES

2. From the web browser of each of the PCs that use R2 as their gateway (PC3, L3, PC4, and L4), access the web page for Server1.
   Question: Were all connections successful?
   Ans: Yes

3. Compare the NAT statistics on the two devices.
   Question: Why doesn't R2 list any dynamic mappings?
   Ans: PAT establishes many-to-one mapping between multiple local hosts and a single global IP address. It uses the Port (TCP/UDP port) information to distinguish between different internal hosts and assign a single global IP to all those addresses thus greatly conserving the global address pool. We implemented PAT on R2 so R2 doesn't list any dynamic mappings

Observation:

Challenges (if any):