



Department of Computer Science and Engineering
Islamic University of Technology (IUT)
A subsidiary organ of OIC

Laboratory Report

CSE 4512: Computer Networks Lab

Name: Namisa Najah Raisa

Student ID: 210042112

Section: B(Even)

Semester: 4th

Academic Year: 2022-2023

Date of Submission: April 7, 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. Implement standard numbered ACL
4. Describe the concept of Network Address Translation (NAT)
5. Explain different types of NAT configuration
6. Implement NAT in a given topology

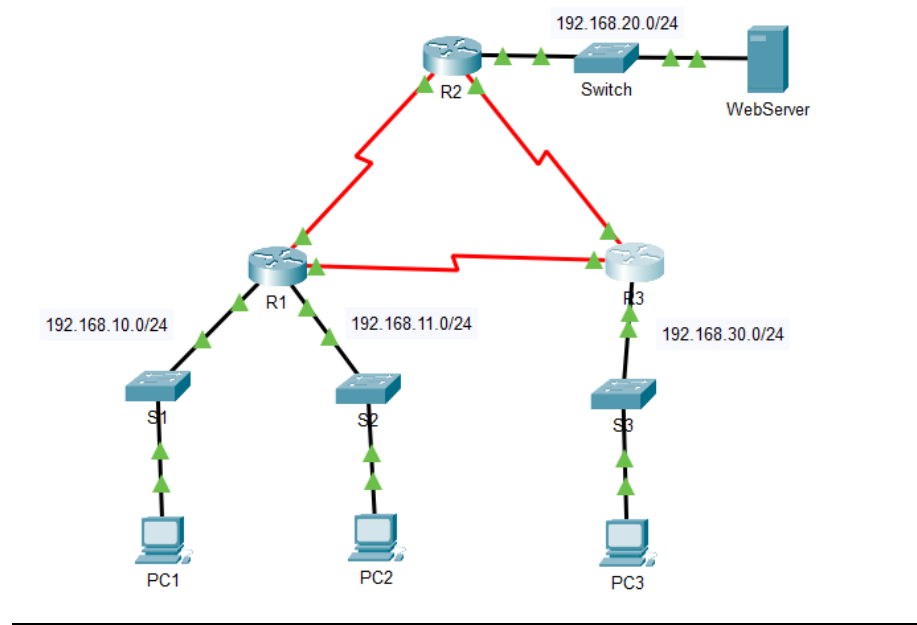
Devices/ software Used:

1. Cisco Packet Tracer

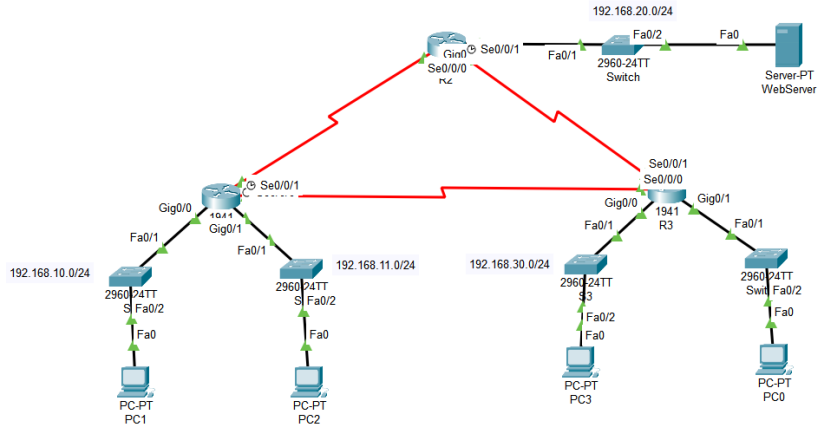
Diagram of the experiment(s):

(Provide screenshot of the final network topology. Make sure to label the network components.)

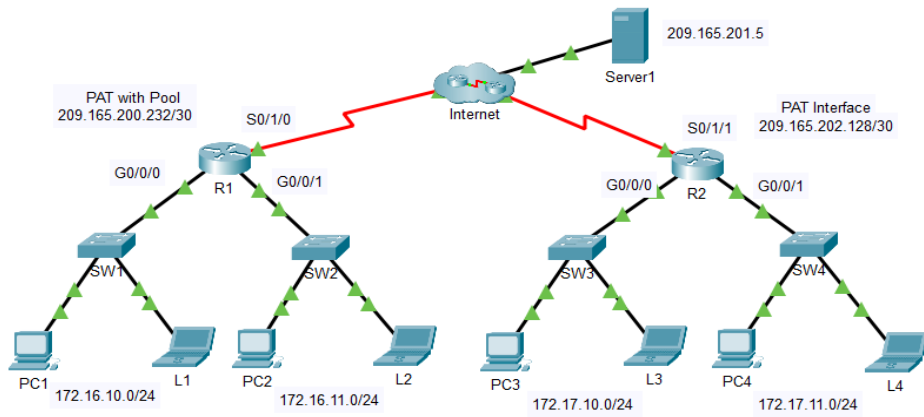
Task-1:



Task-1(part-3)



Task-2:



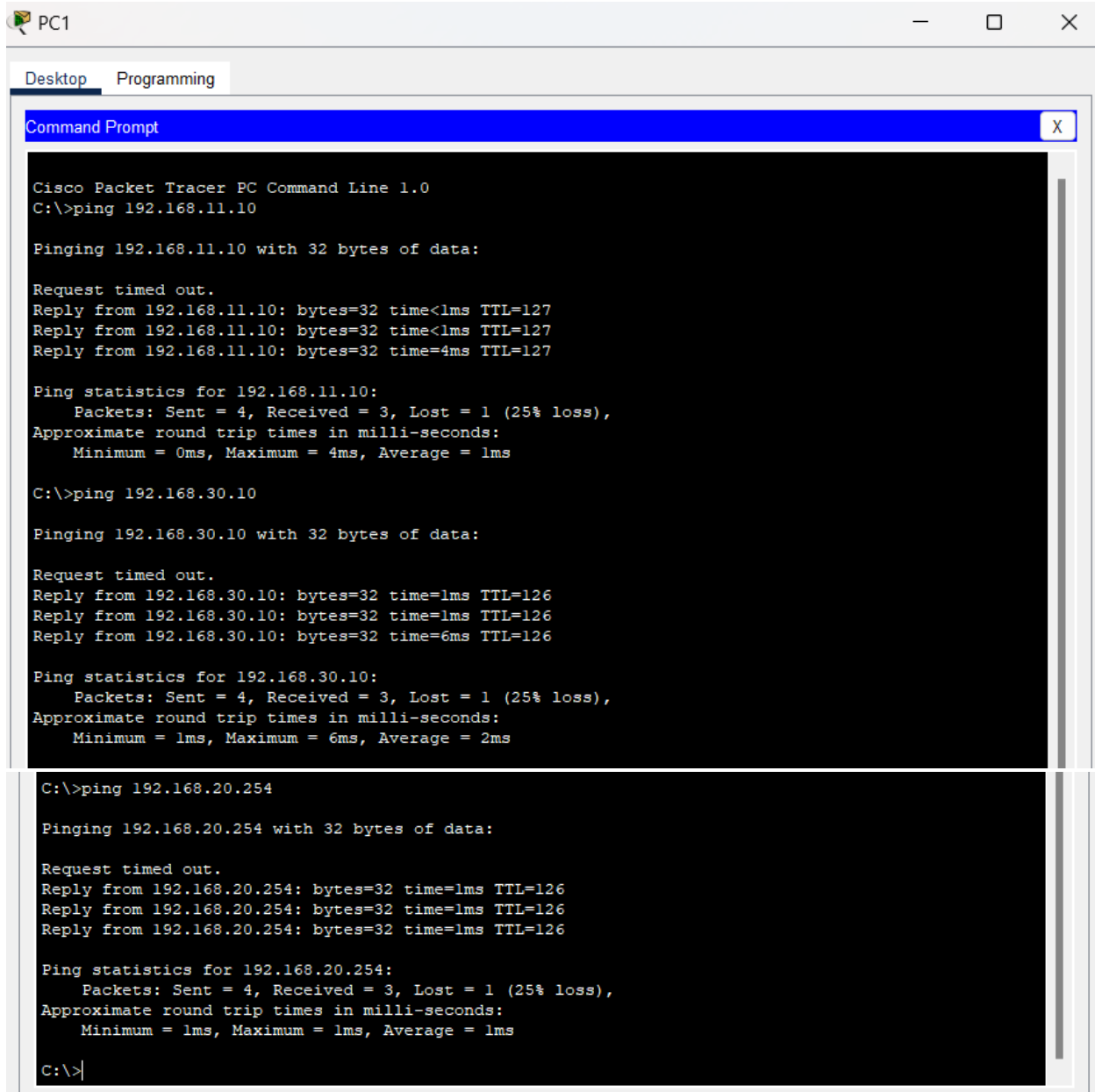
Working Procedure:

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

Task-1:

Part 1: Plan an ACL Implementation

Step 1: Investigate the current network configuration.



The screenshot shows a PC1 window with a Command Prompt open. The Command Prompt has a blue title bar and a black background with white text. It displays the output of three ping commands. The first command is 'ping 192.168.11.10', which shows a 25% loss. The second command is 'ping 192.168.30.10', which also shows a 25% loss. The third command is 'ping 192.168.20.254', which shows a 25% loss. The output for each command includes the number of bytes, time, TTL, and statistics for packets sent, received, and lost, as well as approximate round trip times.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time=4ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=6ms TTL=126

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 6ms, Average = 2ms

C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>|
```

Step 2: Evaluate two network policies and plan ACL implementations.

Part 2: Configure, Apply, and Verify a Standard ACL

Step 1: Configure and apply a numbered standard ACL on R2.

```
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show access lists
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 g0/0
R2(config-if)#ip access-group 1 out
```

Step 2: Configure and apply a numbered standard ACL on R3.

```
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
                        ^
% Invalid input detected at '^' marker.

R3(config)#access-list 1 permit any
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

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)#int g0/0
R3(config-if)#ip access-group 1 out
```

Step 3: Verify ACL configuration and functionality.

- a. Enter the **show run** or **show ip interface gigabitethernet 0/0** command to verify the ACL placements.

```
R2#show ip int g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.20.1/24
  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#show ip int g0/0
GigabitEthernet0/0 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
```

b. With the two ACLs in place, network traffic is restricted according to the policies detailed in Part 1. Use the following tests to verify the ACL implementations:

- A ping from 192.168.10.10 to 192.168.11.10 succeeds.
- A ping from 192.168.10.10 to 192.168.20.254 succeeds.
- A ping from 192.168.10.10 to 192.168.30.10 fails.

```

C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=18ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 18ms, Average = 5ms

C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

- A ping from 192.168.11.10 to 192.168.20.254 fails.
- A ping from 192.168.11.10 to 192.168.30.10 succeeds.


```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=6ms TTL=126
Reply from 192.168.30.10: bytes=32 time=10ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 4ms

```

- A ping from 192.168.30.10 to 192.168.20.254 succeeds.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=10ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 3ms

```

- Issue the **show access-lists** command again on routers **R2** and **R3**. You should see output that indicates the number of packets that have matched each line of the access list. Note: The number of matches shown for your routers may be different, due to the number of pings that are sent and received.

```

R2#show access-lists
Standard IP access list 1
 10 deny 192.168.11.0 0.0.0.255 (4 match(es))
 20 permit any (8 match(es))

R3#show access-lists
Standard IP access list 1
 10 deny 192.168.10.0 0.0.0.255 (4 match(es))
 20 permit any (8 match(es))

```

Task-2(part-3)

Step 1: Add a PC with a switch on R3

Step 2: The network for the new PC should be 192.168.X.0/24 a. Here X = last 3 digits of your student ID

Step 3: Apply ACL on the new PC a. Apply the ACL on the new PC such that it can only be accessed by PC2.

```

R3(config)#access-list 1 permit 192.168.11.0 0.0.0.255
R3(config)#access-list 1 deny any
R3(config)#int g0/1
R3(config-if)#ip access-group 1 out
R3(config-if)#end

```

Task-2:

Part 1: Configure Dynamic NAT with Overload

Step 1: Configure traffic that will be permitted.

Step 2: Configure a pool of address for NAT.

Step 3: Associate ACL 1 with the NAT pool and allow addresses to be reused.

Step 4: Configure the NAT interfaces.

```

R1(config)#access-list 1 permit 172.16.0.0 0.0.255.255
R1(config)#ip nat pool MY_POOL 209.165.200.233 209.165.200.234 netmask 255.255.255.252
R1(config)#ip nat inside source list 1 pool MY_POOL overload
R1(config)#int s0/1/0
R1(config-if)#ip nat outside
R1(config-if)#int g0/0/0
R1(config-if)#ip nat inside
R1(config-if)#int g0/0/1
R1(config-if)#ip nat inside
R1(config-if)#

```

Part 2: Verify Dynamic NAT with Overload Implementation

Step 1: Access services across the internet.

Step 2: View NAT translations.

```
R1#  
%SYS-5-CONFIG_I: Configured from console by console  
show ip nat translations  
Pro Inside global      Inside local      Outside local      Outside global  
tcp 209.165.200.233:1024 172.16.10.11:1025 209.165.201.5:80 209.165.201.5:80  
tcp 209.165.200.233:1025 172.16.10.10:1025 209.165.201.5:80 209.165.201.5:80  
tcp 209.165.200.233:1026 172.16.11.10:1025 209.165.201.5:80 209.165.201.5:80  
tcp 209.165.200.233:1027 172.16.11.11:1025 209.165.201.5:80 209.165.201.5:80
```

Part 3: Configure PAT using an Interface

Step 1: Configure traffic that will be permitted.

Step 2: Associate ACL 2 with the NAT interface and allow addresses to be reused.

Step 3: Configure the NAT interfaces.

```
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 inside source list 2 int s0/1/1 overload  
R2(config)#int s0/1/1  
R2(config-if)#ip nat outside  
R2(config-if)#int g0/0/0  
R2(config-if)#ip nat inside  
R2(config-if)#int g0/0/1  
R2(config-if)#ip nat inside  
R2(config-if)#
```

Part 4: Verify PAT Interface Implementation

Step 1: Access services across the internet.

Step 2: View NAT translations.

```
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
```

Step 3: Compare NAT statistics on R1 and R2.

Compare the NAT statistics on the two devices.

```

R1#show ip nat statistics
Total translations: 4 (0 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: GigabitEthernet0/0/0 , GigabitEthernet0/0/1
Hits: 29 Misses: 4
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool MY_POOL refCount 4
  pool MY_POOL: netmask 255.255.255.252
    start 209.165.200.233 end 209.165.200.234
    type generic, total addresses 2 , allocated 1 (50%), misses 0

R2#show ip nat statistics
Total translations: 4 (0 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/1/1
Inside Interfaces: GigabitEthernet0/0/0 , GigabitEthernet0/0/1
Hits: 28 Misses: 4
Expired translations: 0
Dynamic mappings:

```

Questions:

Task # 01:

1. The ping from 192.168.10.10 to 192.168.11.10 is successful or not? Explain.
Ans: Successful; because the ACL in R3 doesn't allow traffic only between 192.168.10.0/24 and 192.168.30.0/24 but everything else is permitted.
2. The ping from 192.168.10.10 to 192.168.20.254 is successful or not? Explain.
Ans: Successful; because the ACL in R3 doesn't allow traffic only between 192.168.10.0/24 and 192.168.30.0/24 but everything else is permitted.
3. The ping from 192.168.11.10 to 192.168.20.254 failed or not? Explain.
Ans: Failed; because the ACL in R2 doesn't allow traffic from 192.168.11.10 to 192.168.20.254.

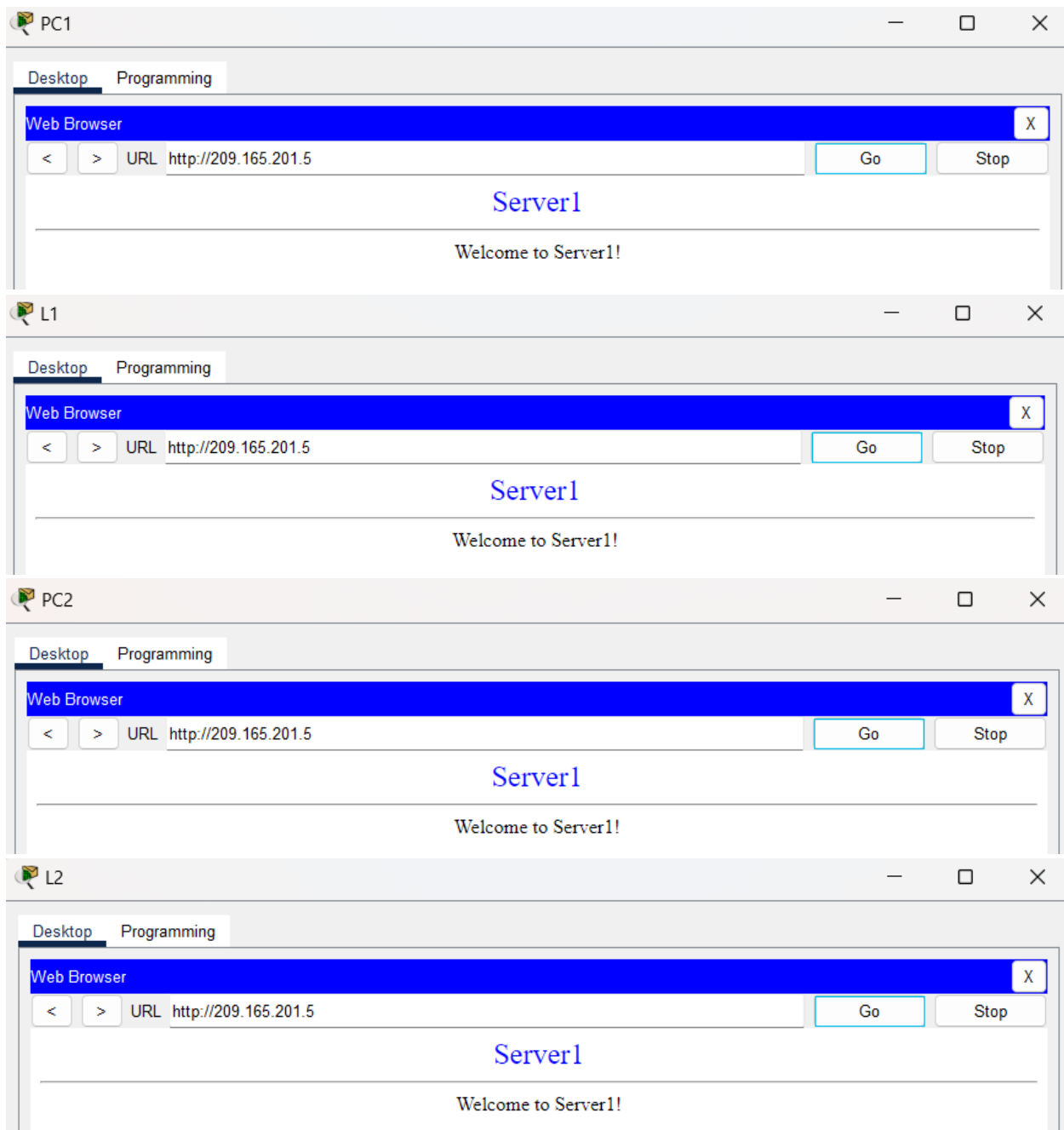
Task # 02:

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

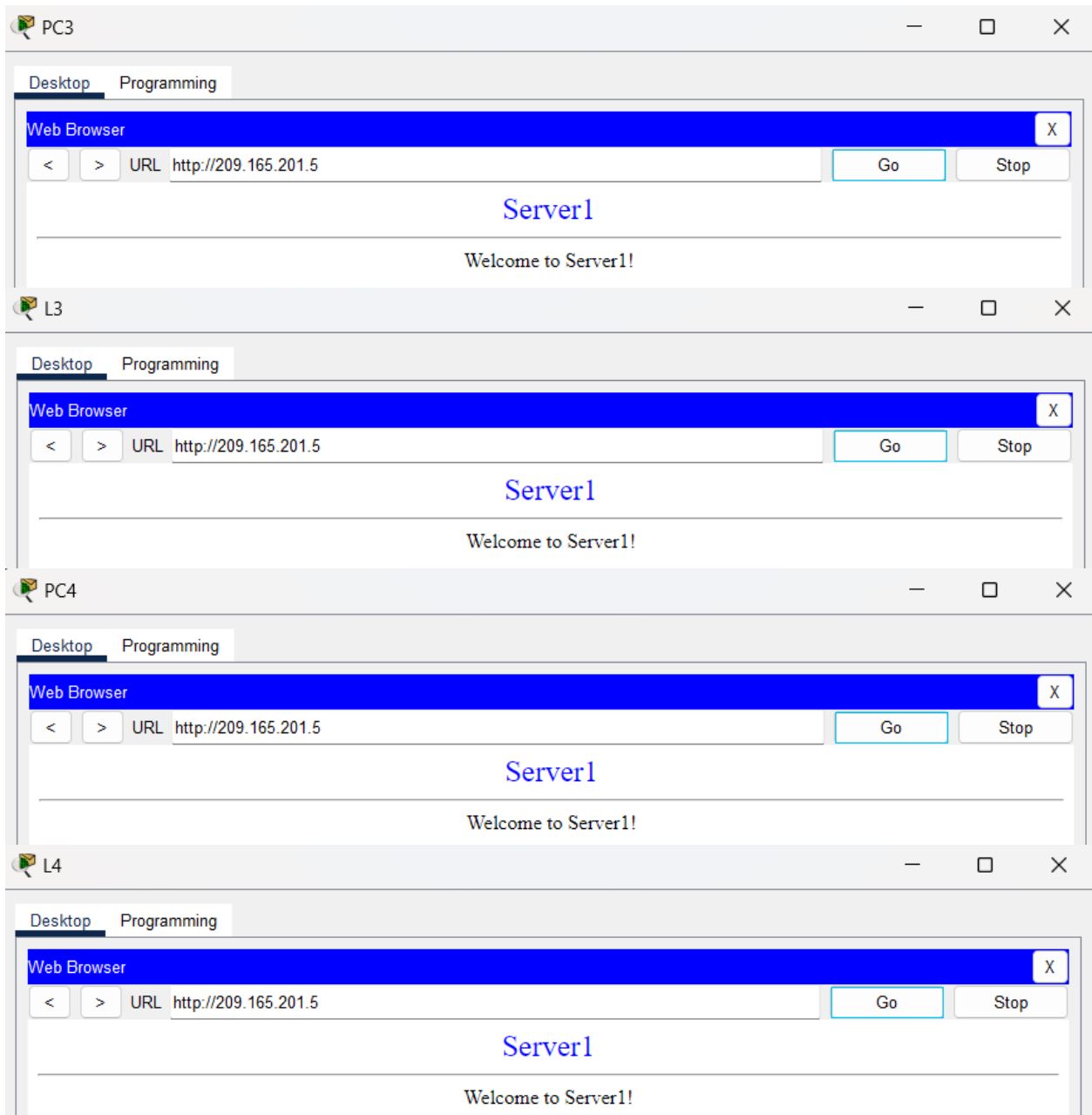


- From the web browser of each of the PCs that use R2 as their gateway (PC3, L3, PC4, and L4), access the web page for Server1.

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: R1 lists dynamic mappings for the pool of addresses that has been configured. R2 is only using the outside interface as the address to translate internal addresses to so there is no dynamic mapping.

Observation:

Challenges (if any):