Department of Computer Science and Engineering

Islamic University of Technology (IUT)

A subsidiary organ of OIC

Laboratory Report

CSE 4512: Computer Networks Lab

Name: Md Farhan Ishmam

Student ID: 180041120

Section: CSE-1

Semester: Fifth

Academic Year: 2021

Date of Submission: 01-11-31

Title: Configuring numbered standard ACL in Cisco Devices

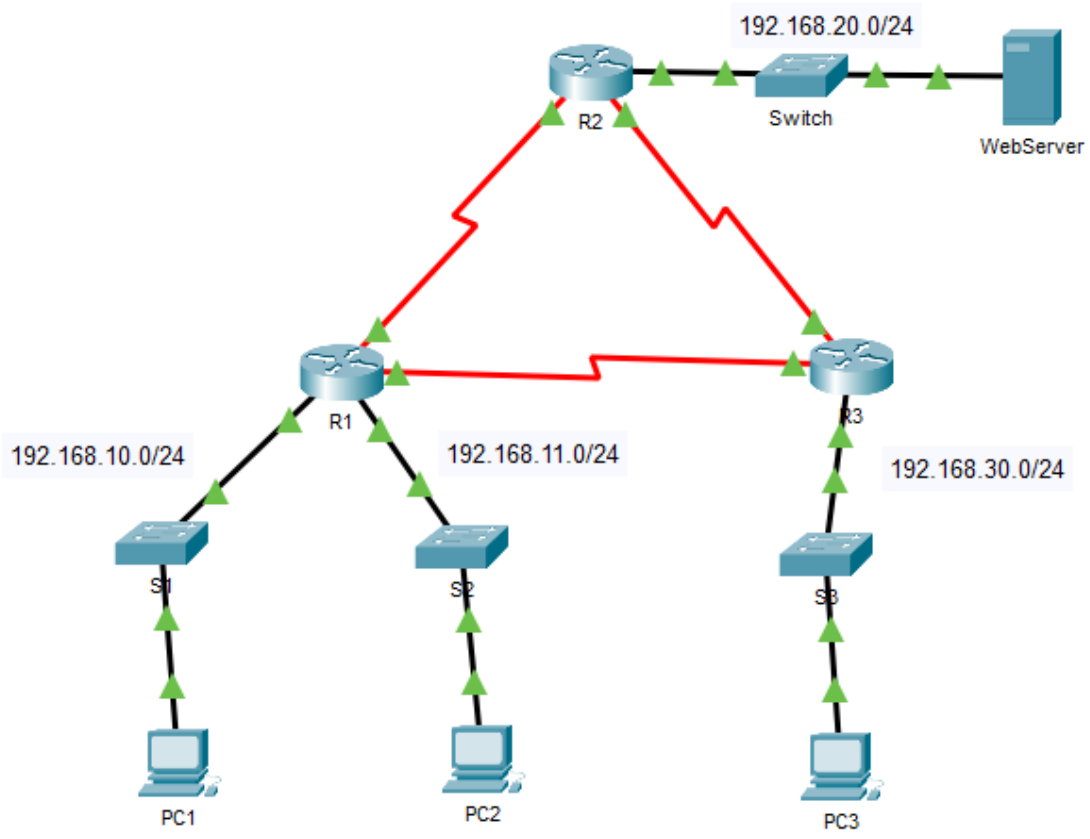
Objective:

1. Describe the concept of Access Control List (ACL)
2. Implement standard numbered ACL

Devices/ software Used:

1. Device: Windows PC
2. Software: Cisco Packet Tracer 7.3.0

Diagram of the experiment(s):

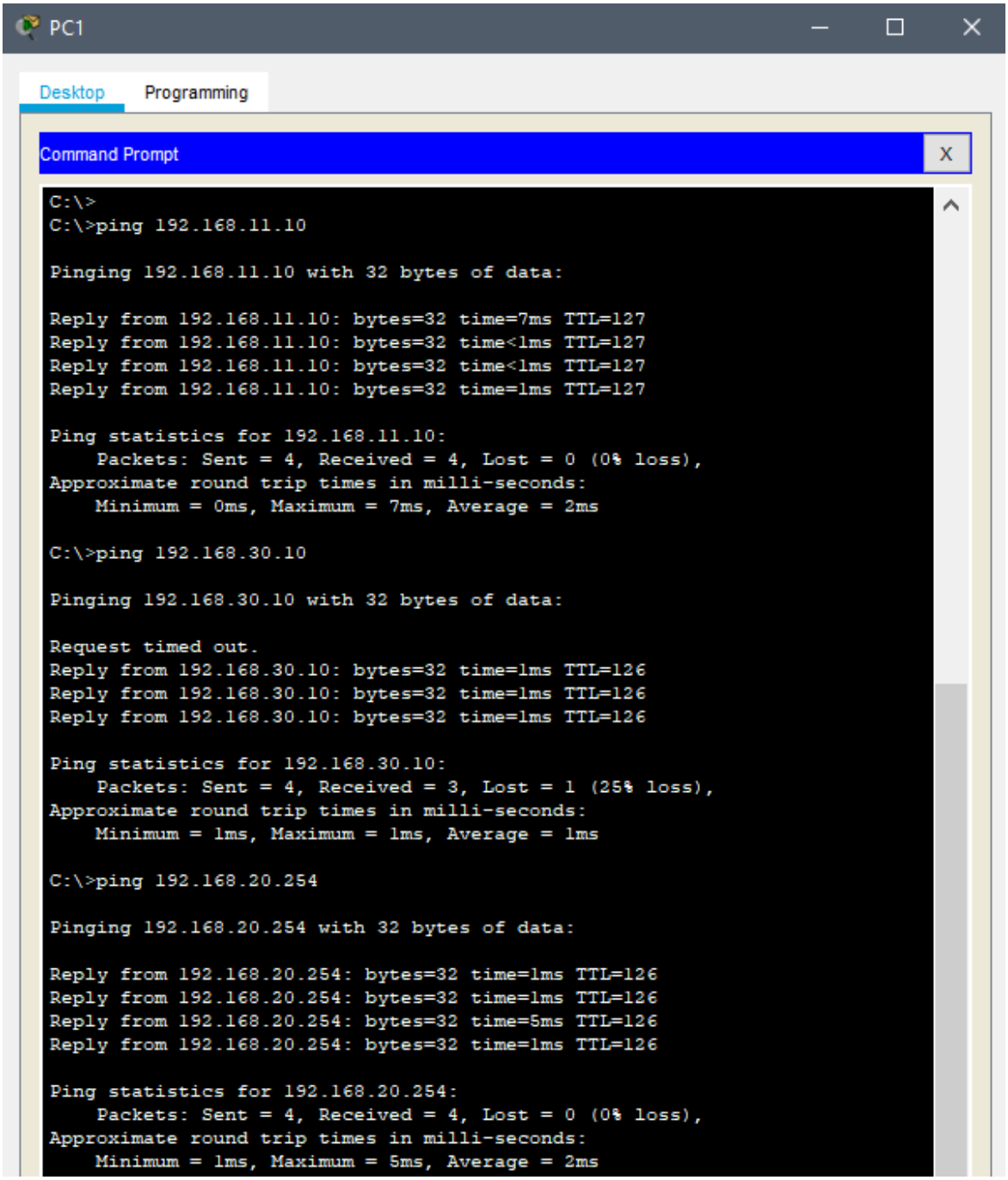


Working Procedure:

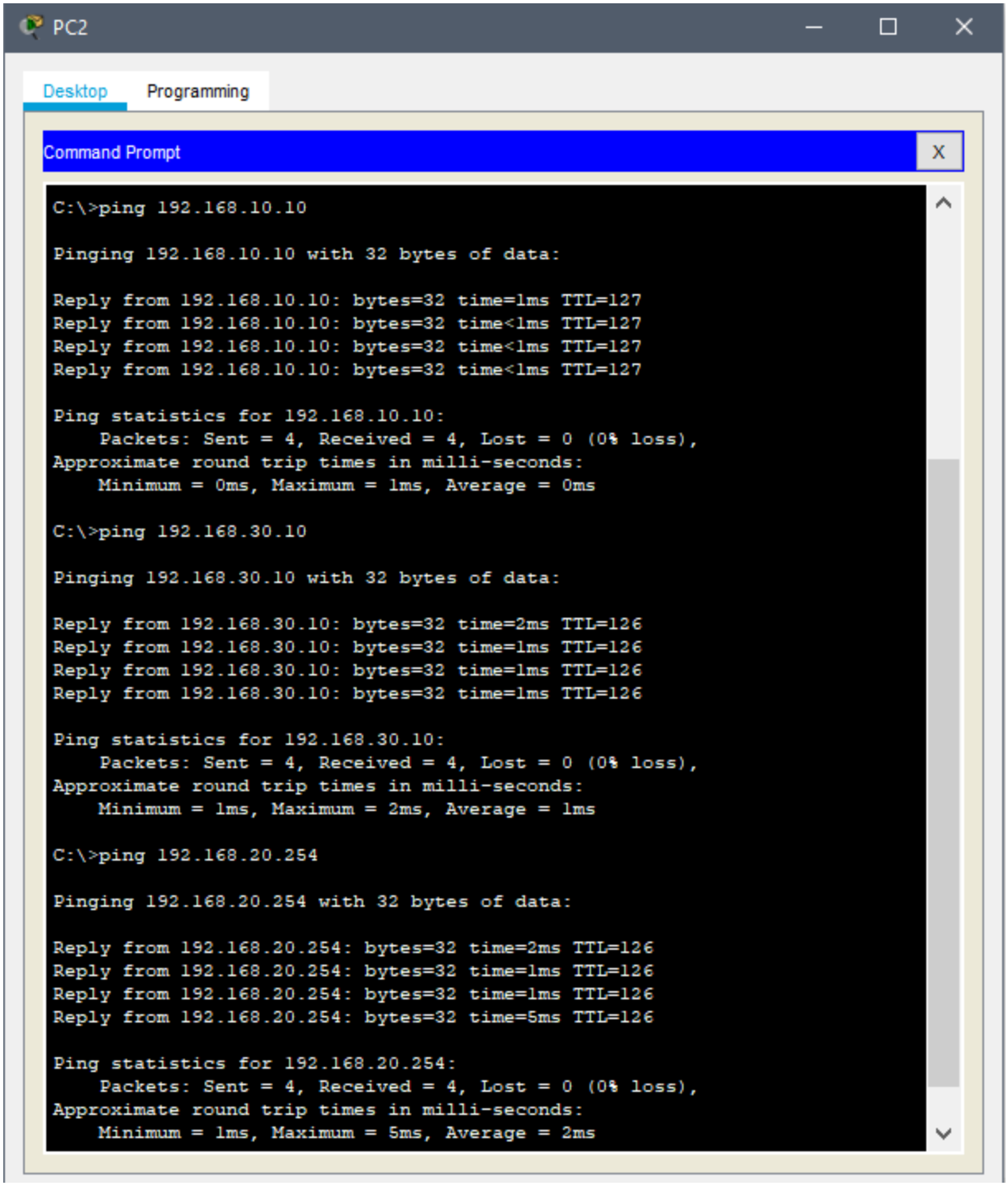
Part 1: Plan an ACL Implementation

Step 1: Investigate the current network configuration

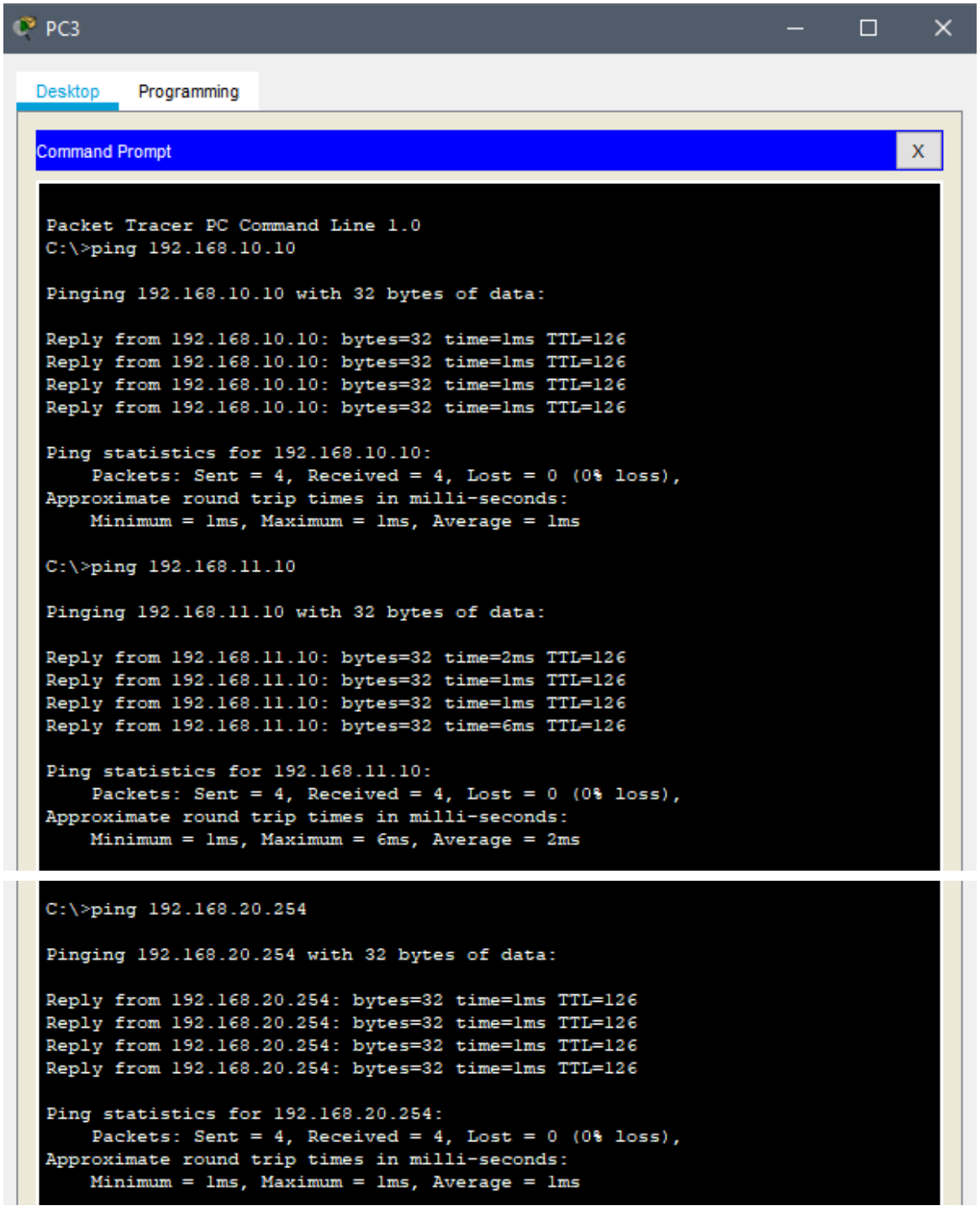
From PC-1 (192.168.10.10) to other networks:



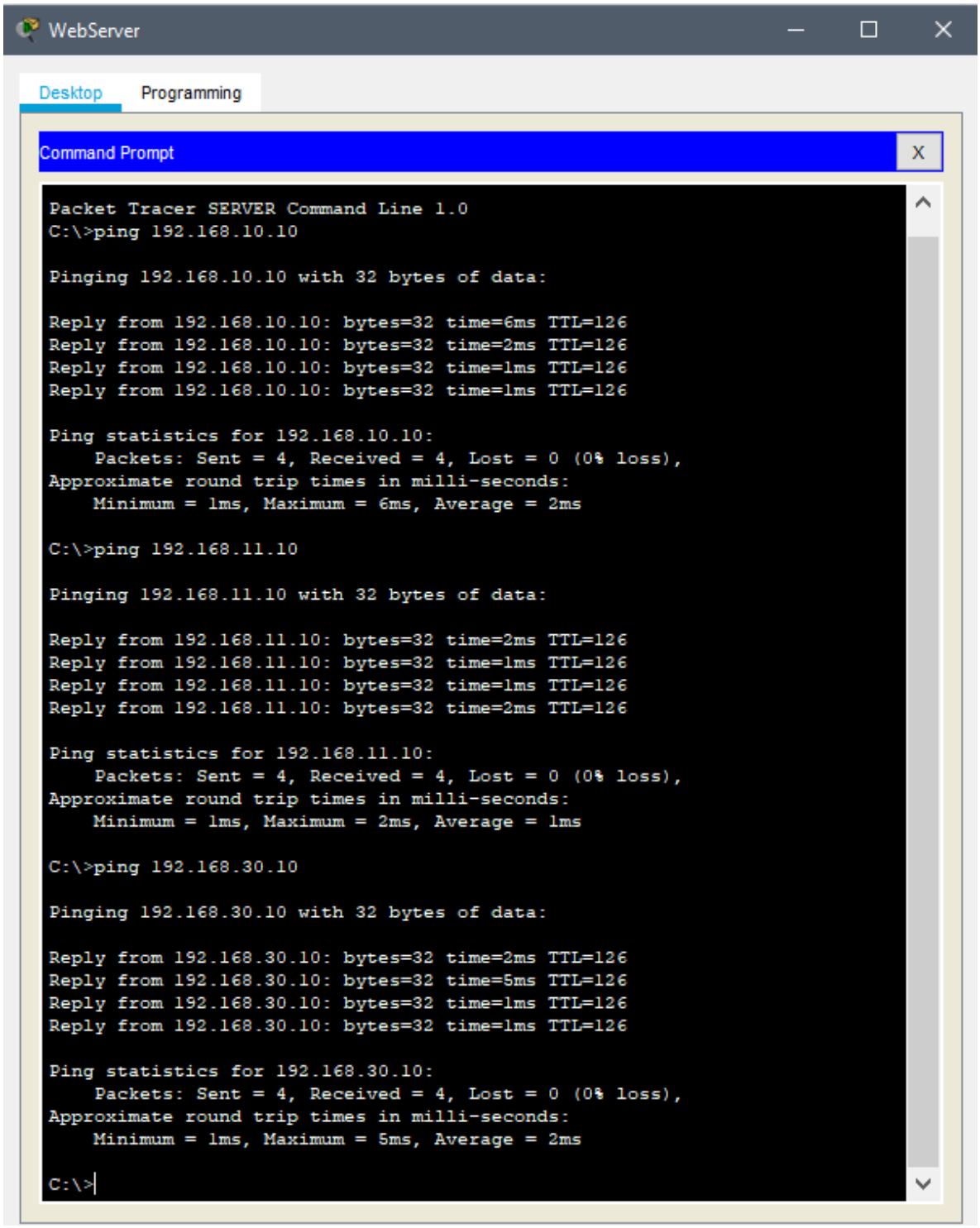
From PC-2 (192.168.11.10) to other networks:



From PC-3 (192.168.30.10) to other networks:



From WebServer (192.168.20.254) to other networks:



Step 2: Evaluate two network policies and plan ACL implementations

a. The following network policies are implemented on R2:
   - The 192.168.11.0/24 network is not allowed access to the WebServer on the 192.168.20.0/24 network
   - All other access is permitted

b. The following network policies are implemented on R3:
   - The 192.168.10.0/24 network is not allowed to communicate with the 192.168.30.0/24 network
   - All other access is permitted

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

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

a. We create an ACL using the number 1 on R2 with a statement that denies access to the 192.168.20.0/24 network from the 192.168.11.0/24 network.
b. By default, an access list denies all traffic that does not match any rules. We permit the other networks by creating a second rule in ACL 1.
c. Before applying an access list to an interface to filter traffic, it is a best practice to review the contents of the access list, in order to verify that it will filter traffic as expected.
d. For the ACL to actually filter traffic, it must be applied to some router operation. We apply the ACL by placing it for outbound traffic on the GigabitEthernet 0/0 interface.

   The following commands were used in R2:

```
R2>enable
R2#conf t
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#show access-lists
R2#conf t
R2(config)#int g0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#exit
```

The screenshot of the commands executed is given below:

```
R2>enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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
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
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

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

a. Create an ACL using the number 1 on R3 with a statement that denies access to the 192.168.30.0/24 network from the PC1 (192.168.10.0/24) network.
b. By default, an ACL denies all traffic that does not match any rules. To permit all other traffic, create a second rule for ACL 1.
c. Verify that the access list is configured correctly.
d. Apply the ACL by placing it for outbound traffic on the GigabitEthernet 0/0 interface.

The following commands were used in R3:

```
R3>en
R3#conf t
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#end
R3#show access-lists
R3#conf t
R3(config)#int g0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#exit
```

The screenshot of the commands executed is given below:

```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
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. The screenshot of the executed command in **router R2** is given below:

```
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 unreachables 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
```

The screenshot of the executed command in **router R3** is given below:

```
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 unreachables 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. The following tests are used to verify ACL implementations:

From 192.168.10.10 to 192.168.11.10, ping succeeds:

```
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 = 1ms, Average = 0ms
```

From 192.168.10.10 to 192.168.20.254, ping succeeds:

```
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=2ms 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 = 2ms, Average = 1ms
```

From 192.168.11.10 to 192.168.20.254, ping fails:

```
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),
```

From 192.168.10.10 to 192.168.30.10, ping fails:

```
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),
```

From 192.168.11.10 to 192.168.30.10, ping succeeds:

```
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=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=2ms 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 = 2ms, Average = 1ms
```

From 192.168.30.10 to 192.168.20.254, ping succeeds:

```
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=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
Reply from 192.168.20.254: bytes=32 time=5ms 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 = 5ms, Average = 2ms
```

c. Issue the **show access-lists** command again on routers **R2 and R3**. You should see an 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.

The screenshots in **Router R2** is given below:

```
R2>en
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))
```

The screenshots in **Router R3** is given below:

```
R3>en
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))
```

Questions:

Task # 01:

1. The ping from 192.168.10.10 to 192.168.11.10 is successful or not?
   Ans: Yes, the ping is successful.

2. The ping from 192.168.10.10 to 192.168.20.254 is successful or not?
   Ans: Yes, the ping is successful.

3. The ping from 192.168.11.10 to 192.168.20.254 has failed or not?
   Ans: Yes, the ping fails.

Observation:

The implementation of ACL is successful and has been verified by pinging from the devices in different networks.

Challenges (if any):

- I faced no major challenges in this lab