Lab 05

Configuring Standard and Extended IPv4 ACLs

Name: Syed Asghar Abbas Zaidi	**Student ID: 07201**

5.1 Objective

The Objectives of this lab are:

- Configure, Apply and Verify a Standard Named ACL
- Configure, Apply and Verify a Standard Numbered ACL
- Configure, Apply and Verify an Extended Numbered ACL
- Configure, Apply and Verify an Extended Numbered ACL

5.2 Introduction

Access control list (ACL) can be used to prevent a ping from reaching hosts on remote networks. In this lab, you will create a standard named ACL to prevent access to a file server. The file server contains the database for the web applications. Only the Web Manager workstation PC1 and the Web Server need to access the File Server. All other traffic to the File Server should be denied.

Topology

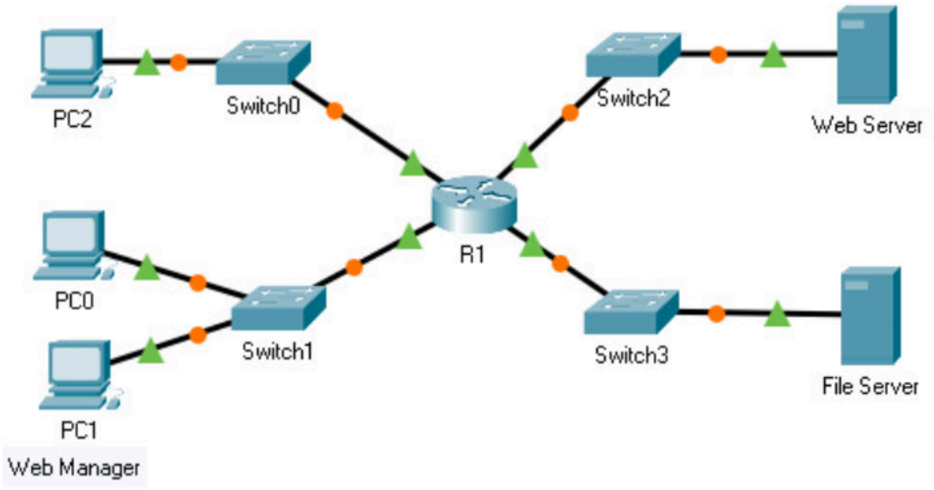
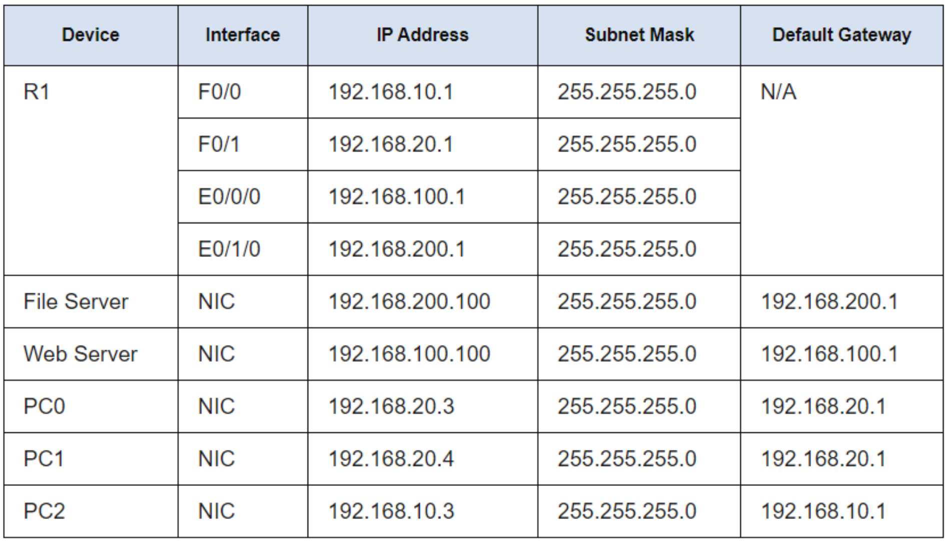


Figure 1: Topology

Addressing Table



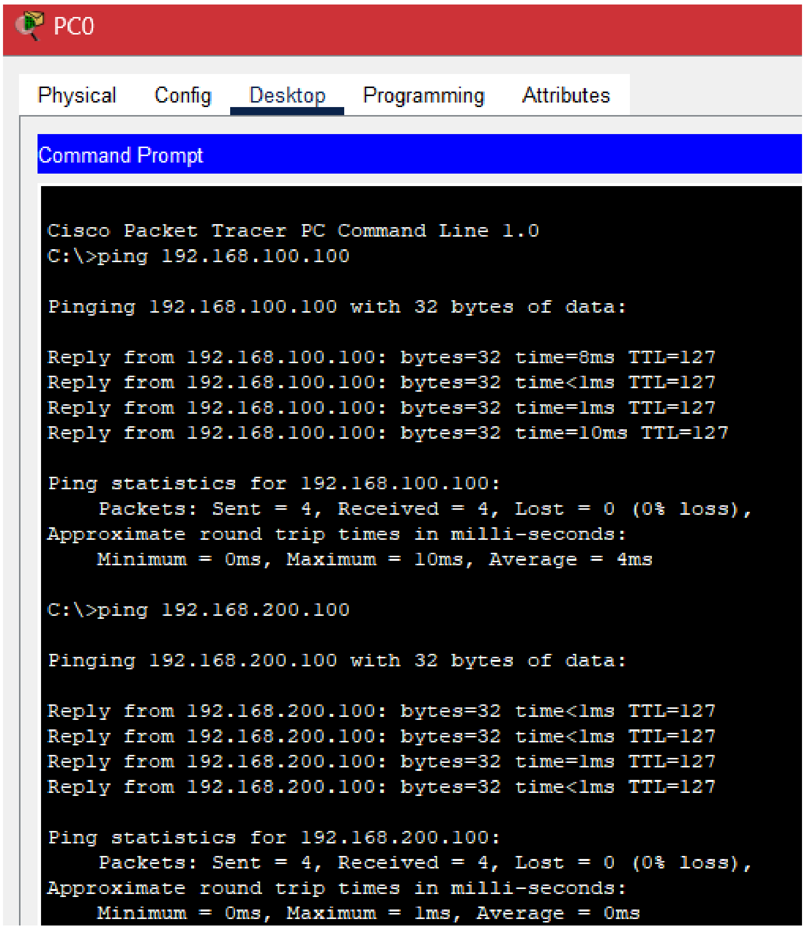
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.20.1	255.255.255.0	
	E0/0/0	192.168.100.1	255.255.255.0	
	E0/1/0	192.168.200.1	255.255.255.0	
File Server	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web Server	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Table 1: Addressing Table

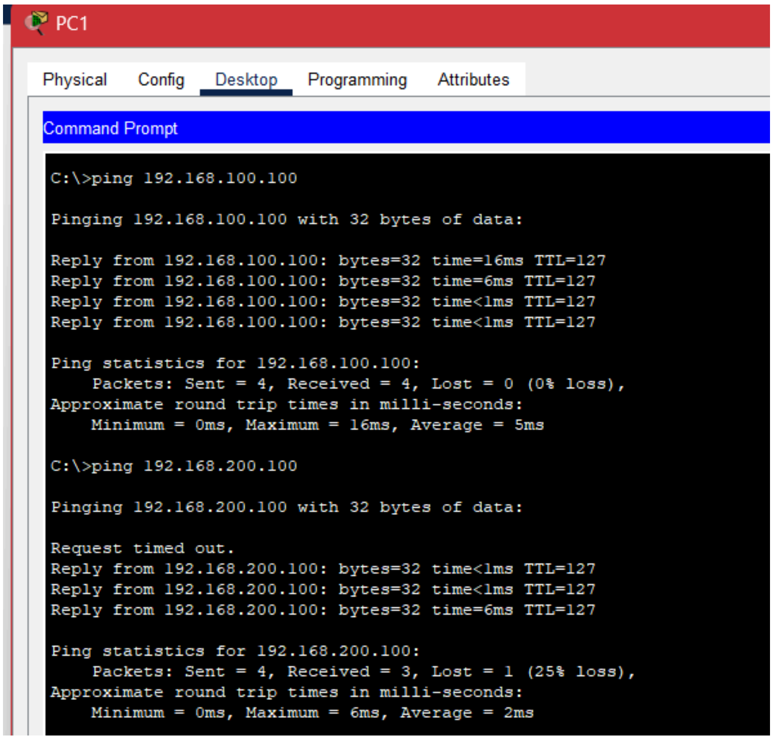
Task 1: Configure and Apply a Named Standard ACL

1. Verify connectivity before the ACL is configured and applied.

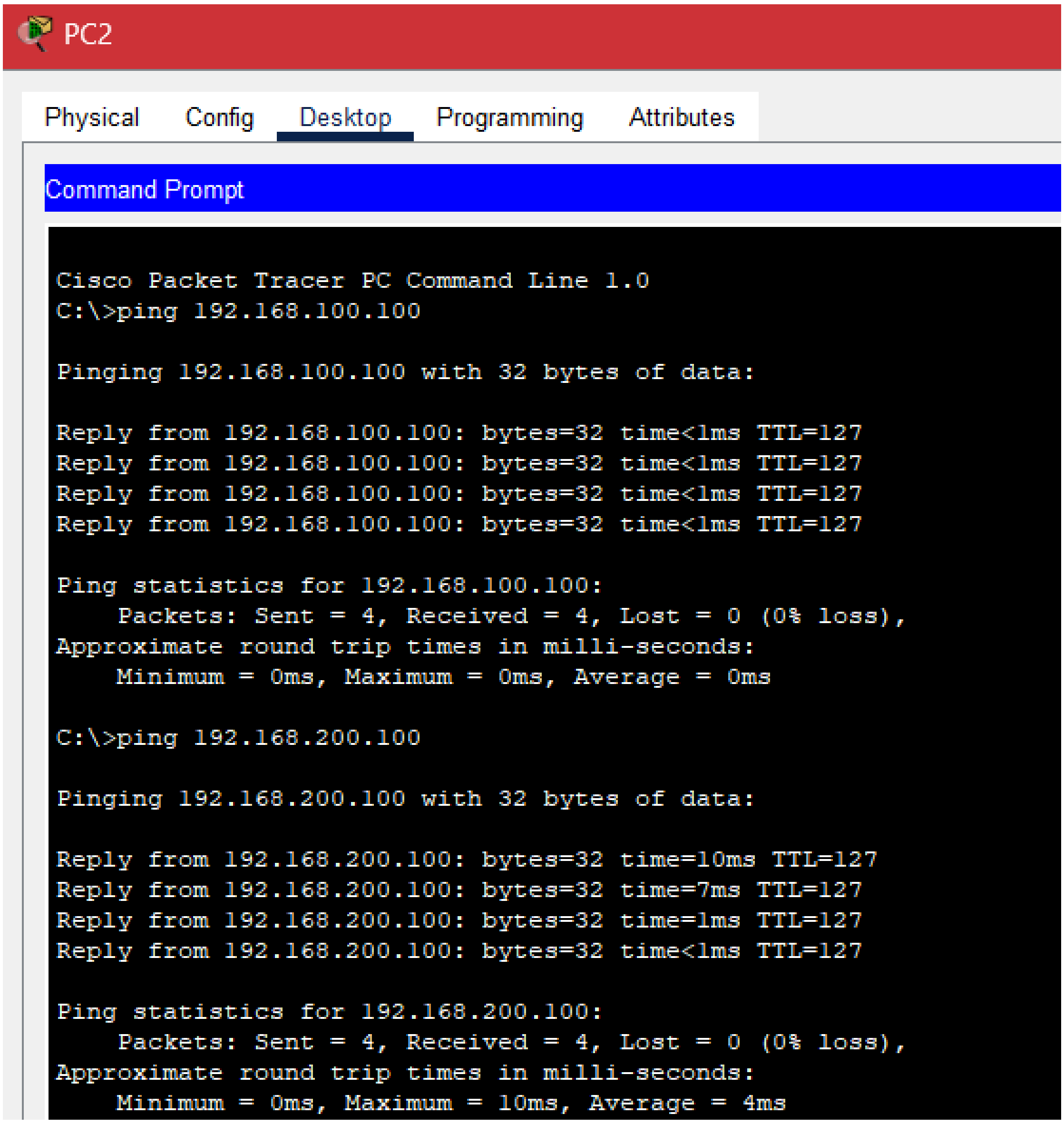
All three workstations should be able to ping the Web Server and File Server.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=8ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 4ms

C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=16ms TTL=127
Reply from 192.168.100.100: bytes=32 time=6ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 5ms

C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=6ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 2ms
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=10ms TTL=127
Reply from 192.168.200.100: bytes=32 time=7ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 4ms
```

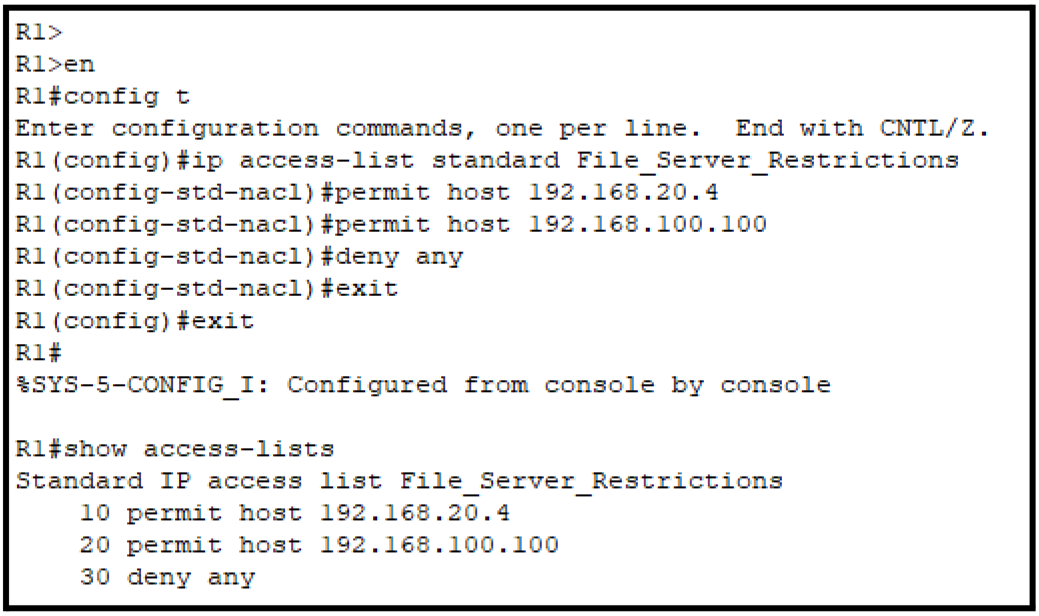
2. Configure a named standard ACL.

   a. Configure the following named ACL on **R1**.

```
R1(config)# ip access-list standard File_Server_Restrictions
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# permit host 192.168.100.100
R1(config-std-nacl)# deny any
```

Note: For scoring purposes, the ACL name is case-sensitive, and the statements must be in the same order as shown.

b. Use the **show access-lists** command to verify the contents of the access list before applying it to an interface. Make sure you have not mistyped any IP addresses and that the statements are in the correct order.



```
R1>
R1>en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard File_Server_Restrictions
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#permit host 192.168.100.100
R1(config-std-nacl)#deny any
R1(config-std-nacl)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show access-lists
Standard IP access list File_Server_Restrictions
    10 permit host 192.168.20.4
    20 permit host 192.168.100.100
    30 deny any
```

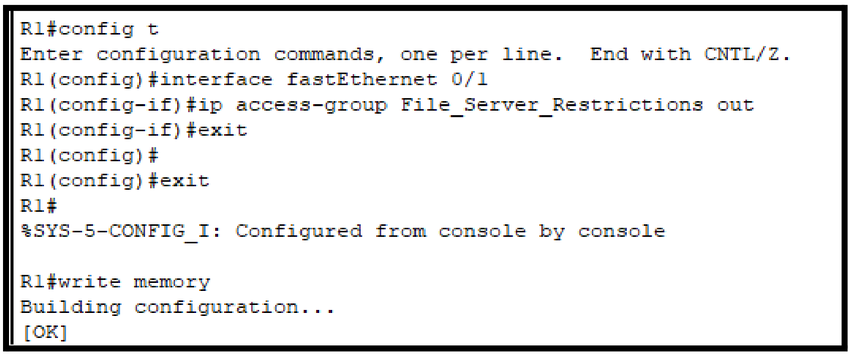
3. Apply the named ACL.

a. Apply the ACL outbound on the Fast Ethernet 0/1 interface.

Note: In an actual operational network, applying an access list to an active interface is not a good practice and should be avoided if possible.

```
R1(config-if)# ip access-group File_Server_Restrictions out
```

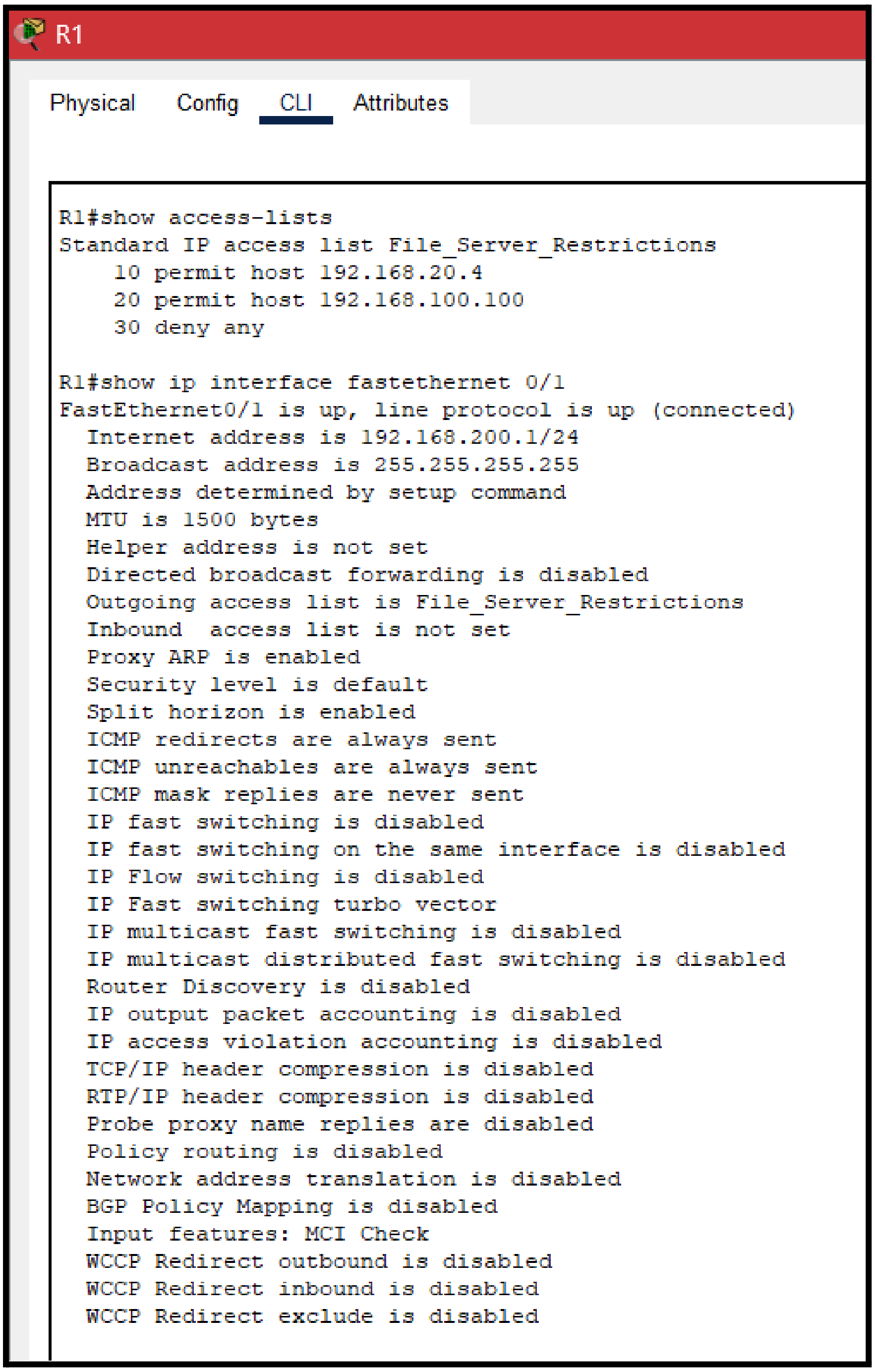
b. Save the configuration



```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fastEthernet 0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#exit
R1(config)#
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#write memory
Building configuration...
[OK]
```

4. Verify the ACL implemention
   a. Verify the ACL configuration and application to the interface.

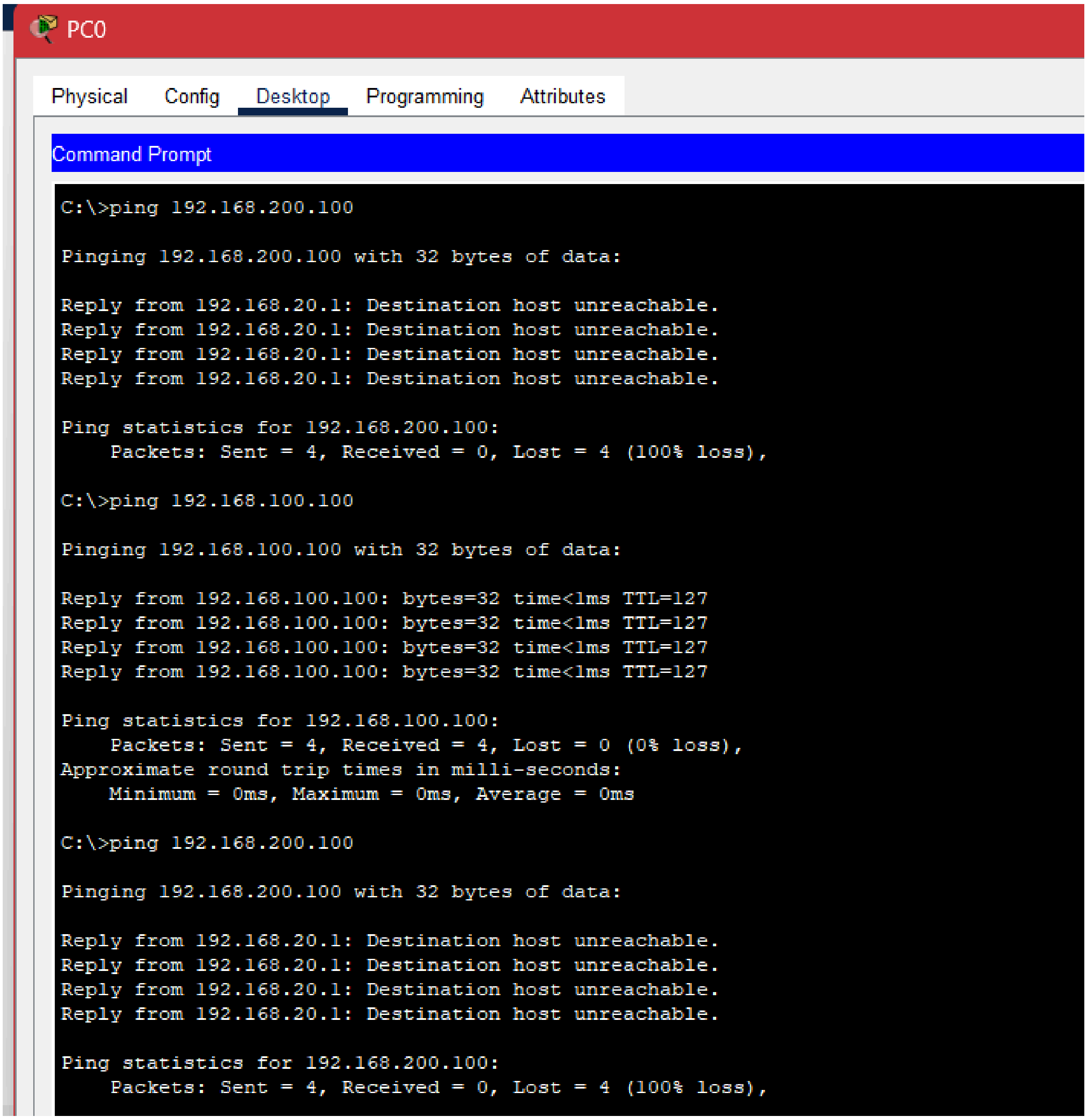
   Use the **show access-lists** command to verify the ACL configuration. Use the **show run** or **show ip interface fastethernet 0/1** command to verify that the ACL is applied correctly to the interface.



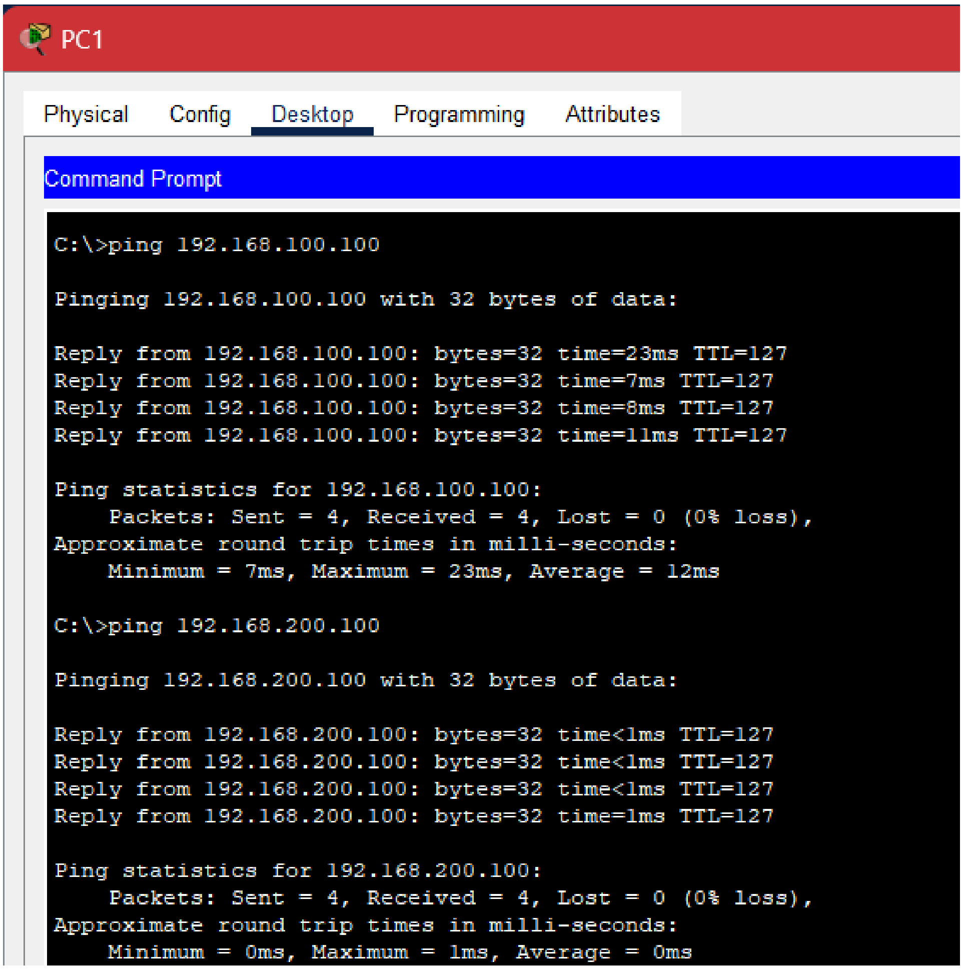
```
R1#show access-lists
Standard IP access list File_Server_Restrictions
    10 permit host 192.168.20.4
    20 permit host 192.168.100.100
    30 deny any

R1#show ip interface fastethernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.200.1/24
  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 File_Server_Restrictions
  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. Verify that the ACL is working properly.

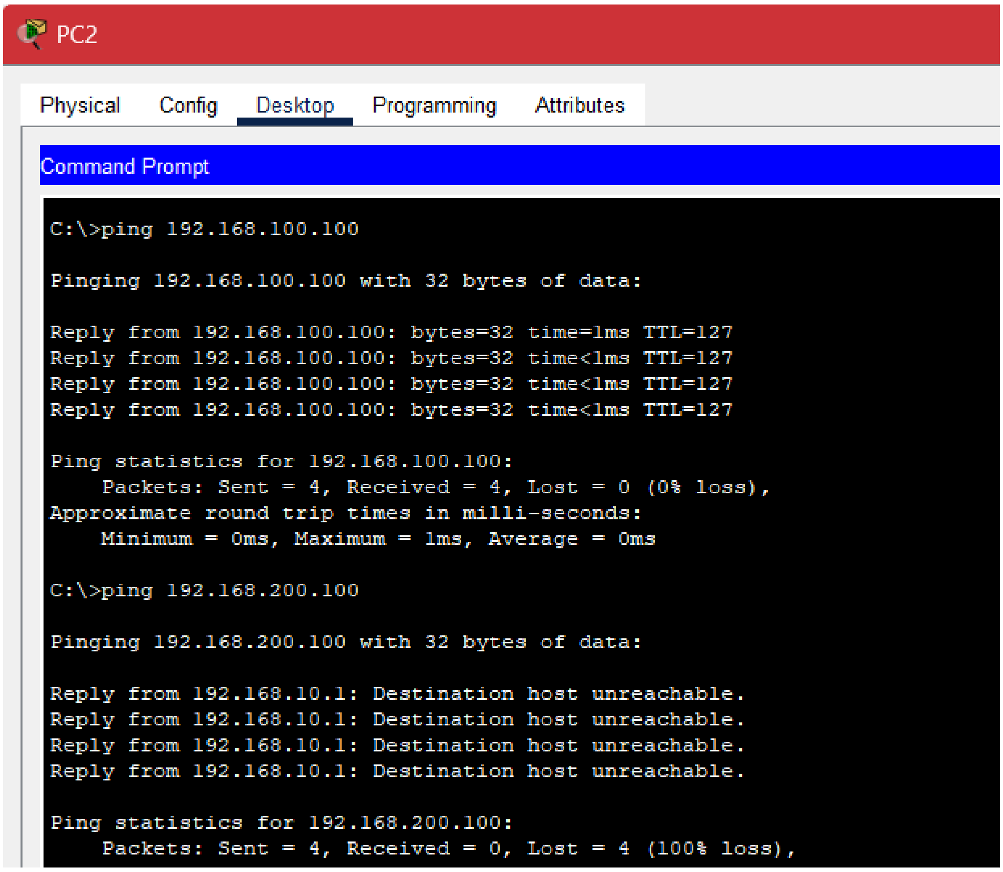
All three workstations should be able to ping the **Web Server**, but only **PC1** and the **Web Server** should be able to ping the **File Server**. Repeat the show **access-lists** command to see the number of packets that matched each statement.



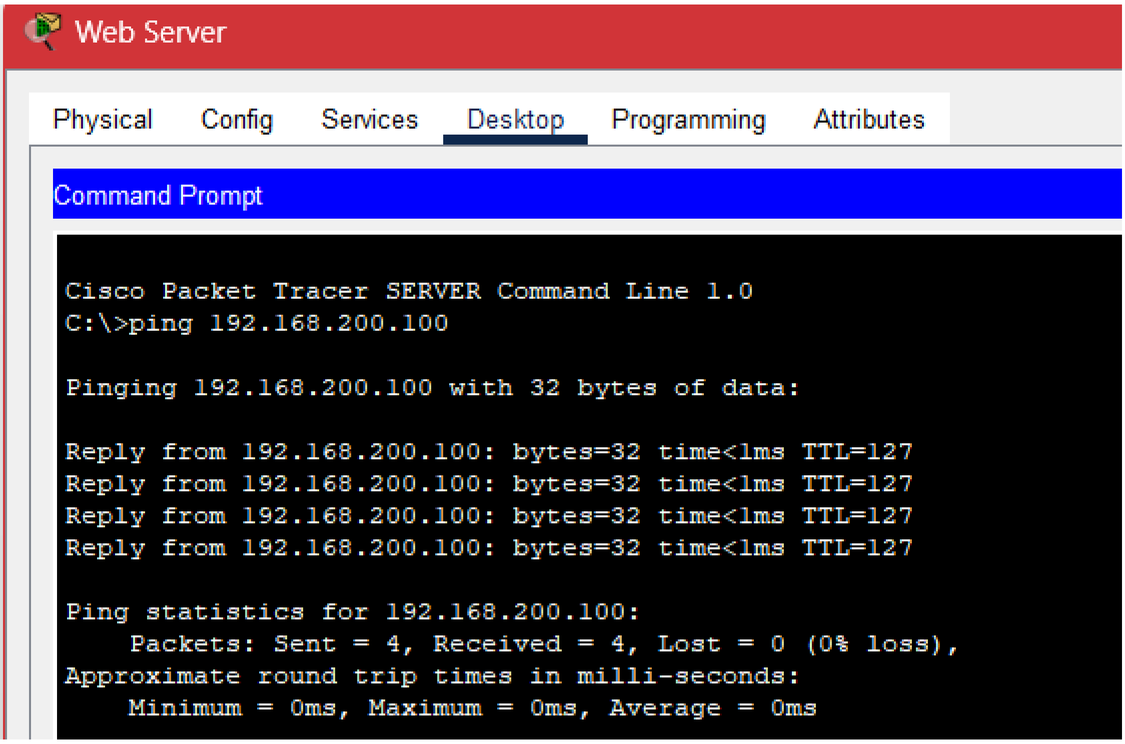
```
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



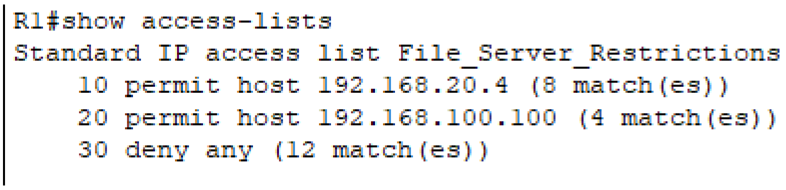
```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=23ms TTL=127
Reply from 192.168.100.100: bytes=32 time=7ms TTL=127
Reply from 192.168.100.100: bytes=32 time=8ms TTL=127
Reply from 192.168.100.100: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 23ms, Average = 12ms

C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

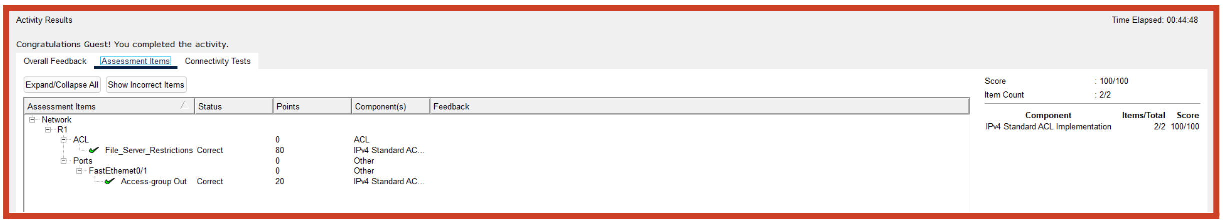


```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



```
R1#show access-lists
Standard IP access list File_Server_Restrictions
    10 permit host 192.168.20.4 (8 match(es))
    20 permit host 192.168.100.100 (4 match(es))
    30 deny any (12 match(es))
```

COMPLETION OF THIS ACTIVITY:



Activity Results

Time Elapsed: 00:44:48

Congratulations Guest! You completed the activity.

Assessment Items	Status	Points	Component(s)	Feedback
Network				
R1				
ACL		0	ACL	
✓ File_Server_Restrictions	Correct	80	IPv4 Standard AC...	
Ports		0	Other	
FastEthernet0/1		0	Other	
✓ Access-group Out	Correct	20	IPv4 Standard AC...	

Score : 100/100
Item Count : 2/2

Component	Items/Total	Score
IPv4 Standard ACL Implementation	2/2	100/100

Topology

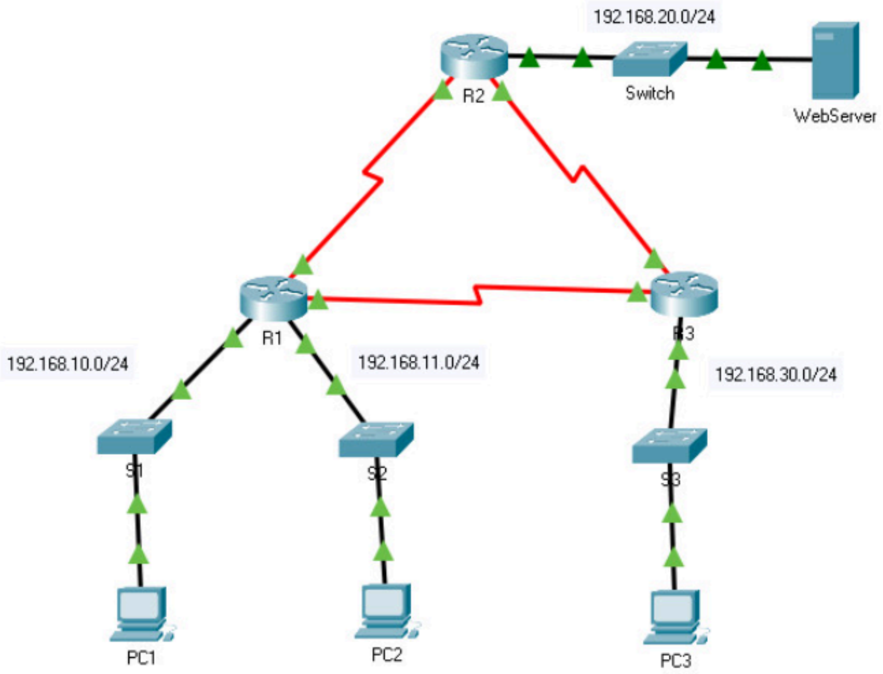
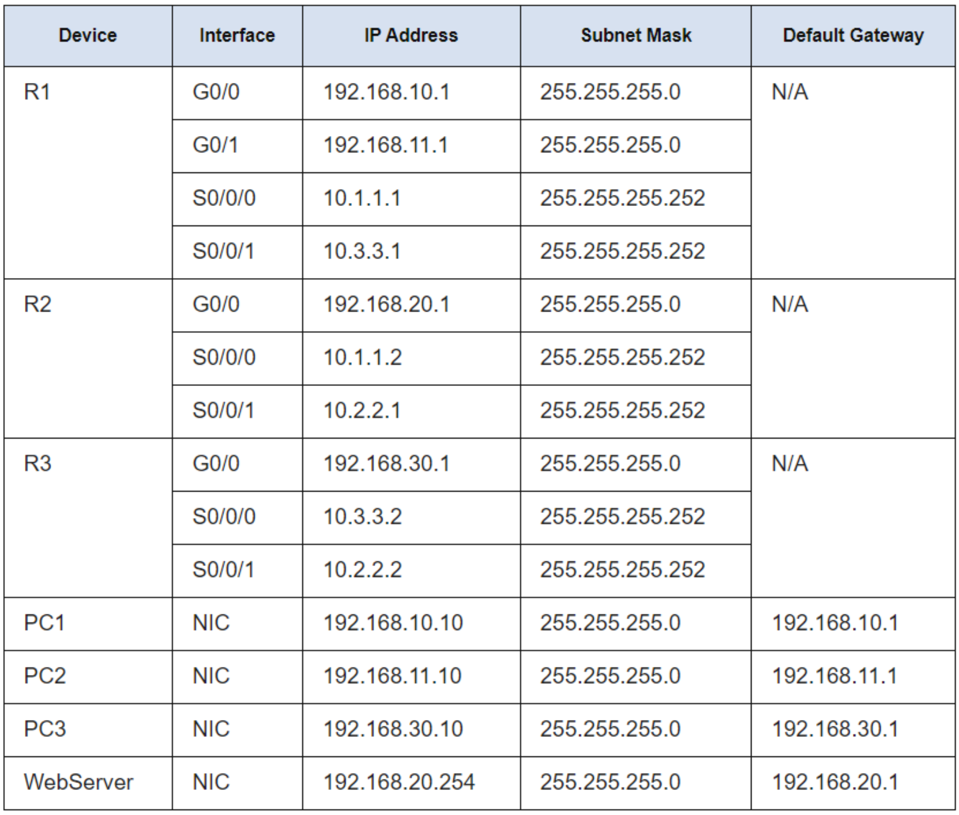


Figure 2: Topology

Addressing Table



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	
	S0/0/0	10.1.1.1	255.255.255.252	
	S0/0/1	10.3.3.1	255.255.255.252	
R2	G0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	
	S0/0/1	10.2.2.1	255.255.255.252	
R3	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	
	S0/0/1	10.2.2.2	255.255.255.252	
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

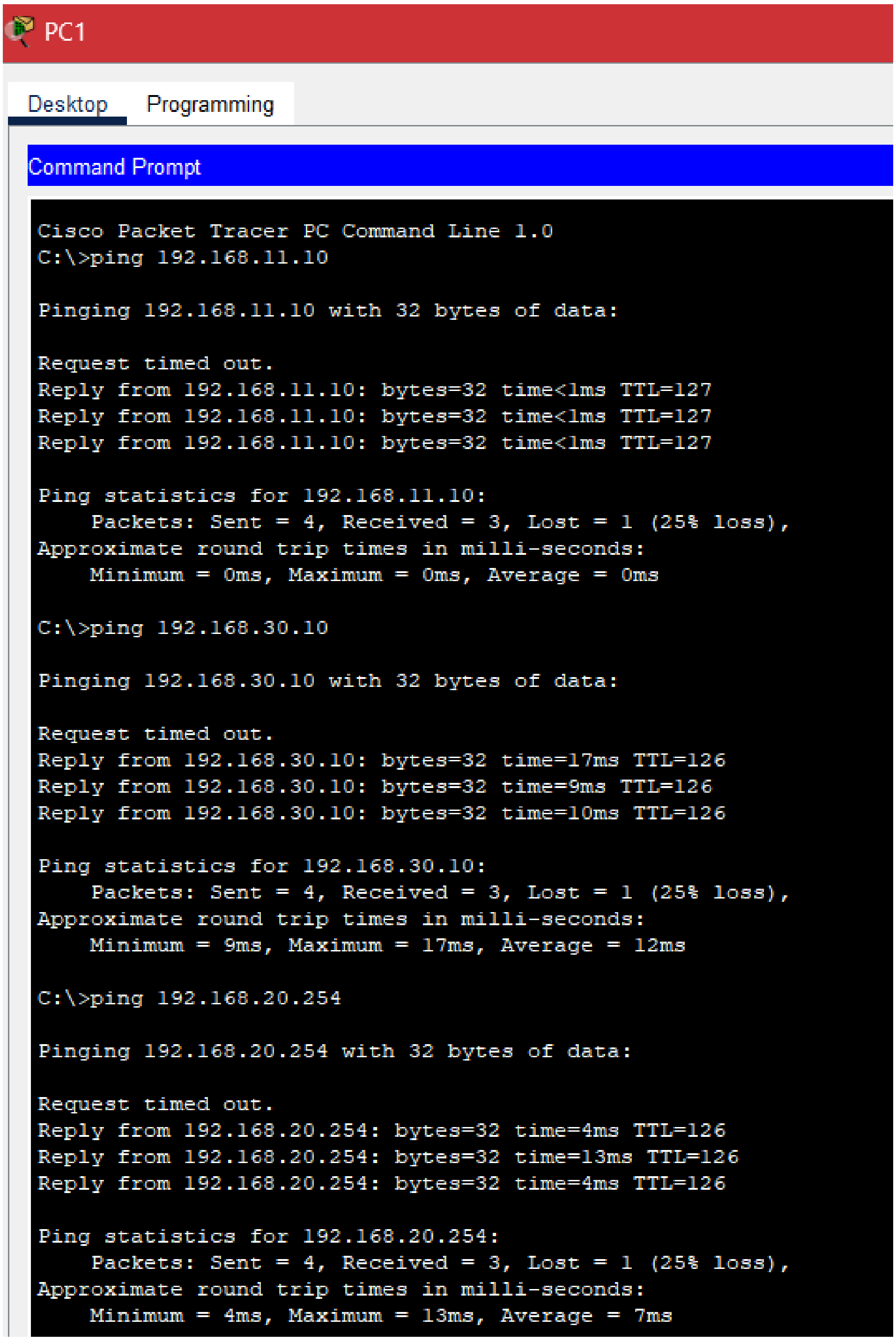
Table 2: Addressing Table

Task 2: Configure Numbered Standard IPv4 ACLs

1. Verify connectivity before the ACL is configured and applied.

Verify that the network has full connectivity by choosing a PC and pinging other devices on the network. You should be able to successfully ping every device.

Pinging from PC1 to PC2, PC3 and Web Server



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

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=17ms TTL=126
Reply from 192.168.30.10: bytes=32 time=9ms TTL=126
Reply from 192.168.30.10: bytes=32 time=10ms 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 = 9ms, Maximum = 17ms, Average = 12ms

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=4ms TTL=126
Reply from 192.168.20.254: bytes=32 time=13ms TTL=126
Reply from 192.168.20.254: bytes=32 time=4ms 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 = 4ms, Maximum = 13ms, Average = 7ms
```

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.

To restrict access from the 192.168.11.0/24 network to the WebServer at 192.168.20.254 without interfering with other traffic, an ACL must be created on **R2**. The access list must be placed on the outbound interface to the **WebServer**. A second rule must be created on **R2** to permit all other traffic.

b. The following network policies are implemented on **R3**:

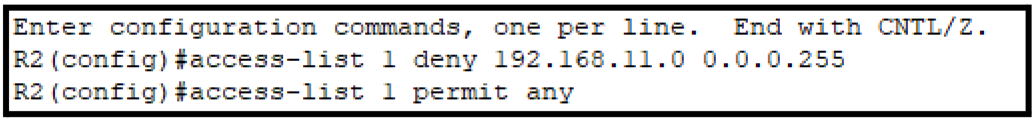
- The 192.168.10.0/24 network is not allowed to communicate with the 192.168.30.0/24 network.
- All other access is permitted.

To restrict access from the 192.168.10.0/24 network to the 192.168.30/24 network without interfering with other traffic, an access list will need to be created on **R3**. The ACL must be placed on the outbound interface to **PC3**. A second rule must be created on **R3** to permit all other traffic.

3. Configure and apply a numbered standard ACL on **R2**.

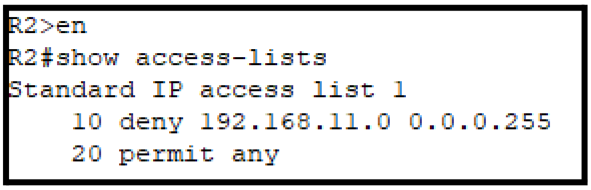
a. Create an ACL using the number **1** on **R2** with a statement that denies access to the 192.168.20.0/24 network from the PC1 (192.168.11.0/24) network.

b. By default, an access list denies all traffic that does not match any rules. To permit all other traffic, create a second rule of ACL 1.



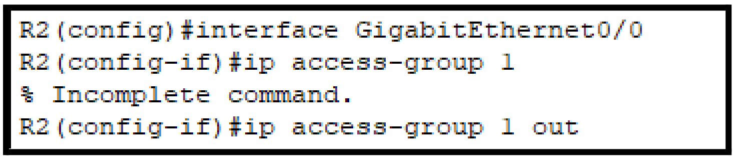
```
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
```

c. Verify that the access list is configured correctly.



```
R2>en
R2#show access-lists
Standard IP access list 1
    10 deny 192.168.11.0 0.0.0.255
    20 permit any
```

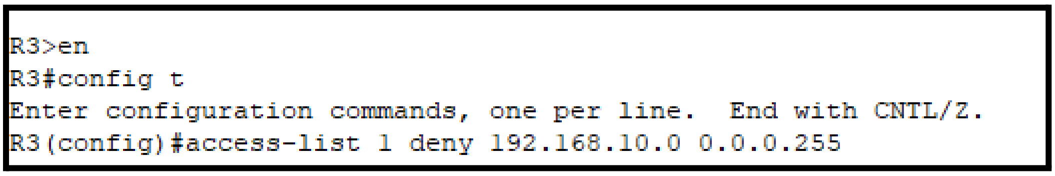
d. Apply the ACL by placing it for outbound traffic on the GigabitEthernet 0/0 interface.



```
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip access-group 1
% Incomplete command.
R2(config-if)#ip access-group 1 out
```

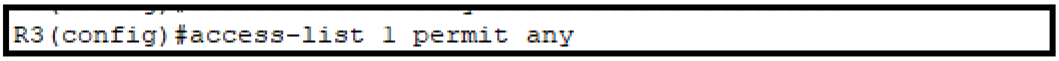
4. Configure and apply a numbered standard ACL on **R3**.

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.



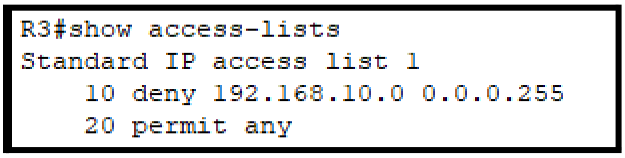
```
R3>en
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
```

b. By default, an access list denies all traffic that does not match any rules. To permit all other traffic, create a second rule of ACL 1.



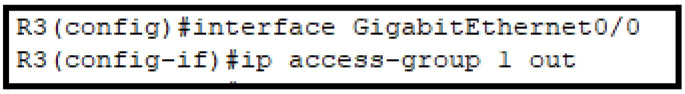
```
R3(config)#access-list 1 permit any
```

c. Verify that the access list is configured correctly.



```
R3#show access-lists
Standard IP access list 1
    10 deny 192.168.10.0 0.0.0.255
    20 permit any
```

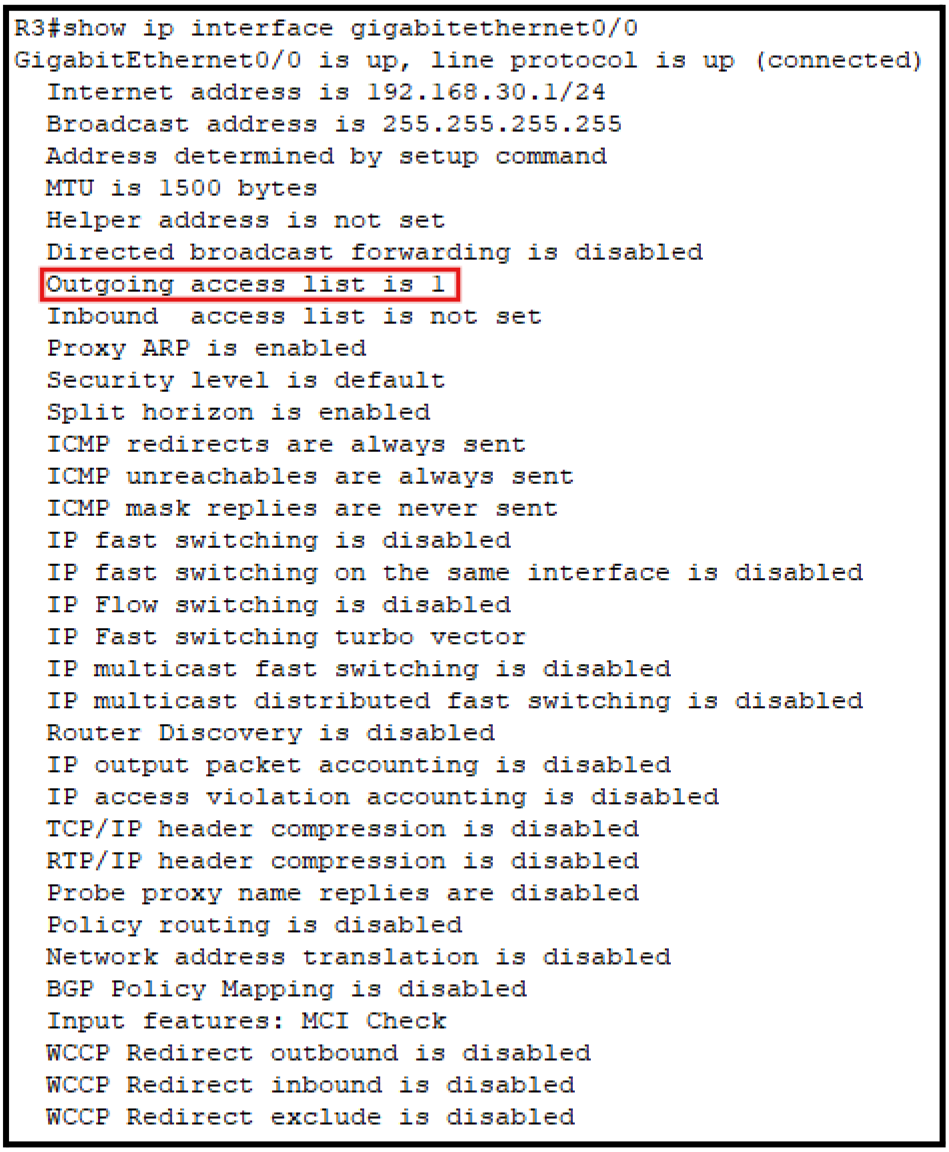
d. Apply the ACL by placing it for outbound traffic on the GigabitEthernet 0/0 interface.



```
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 1 out
```

5. Verify the ACL implementation

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

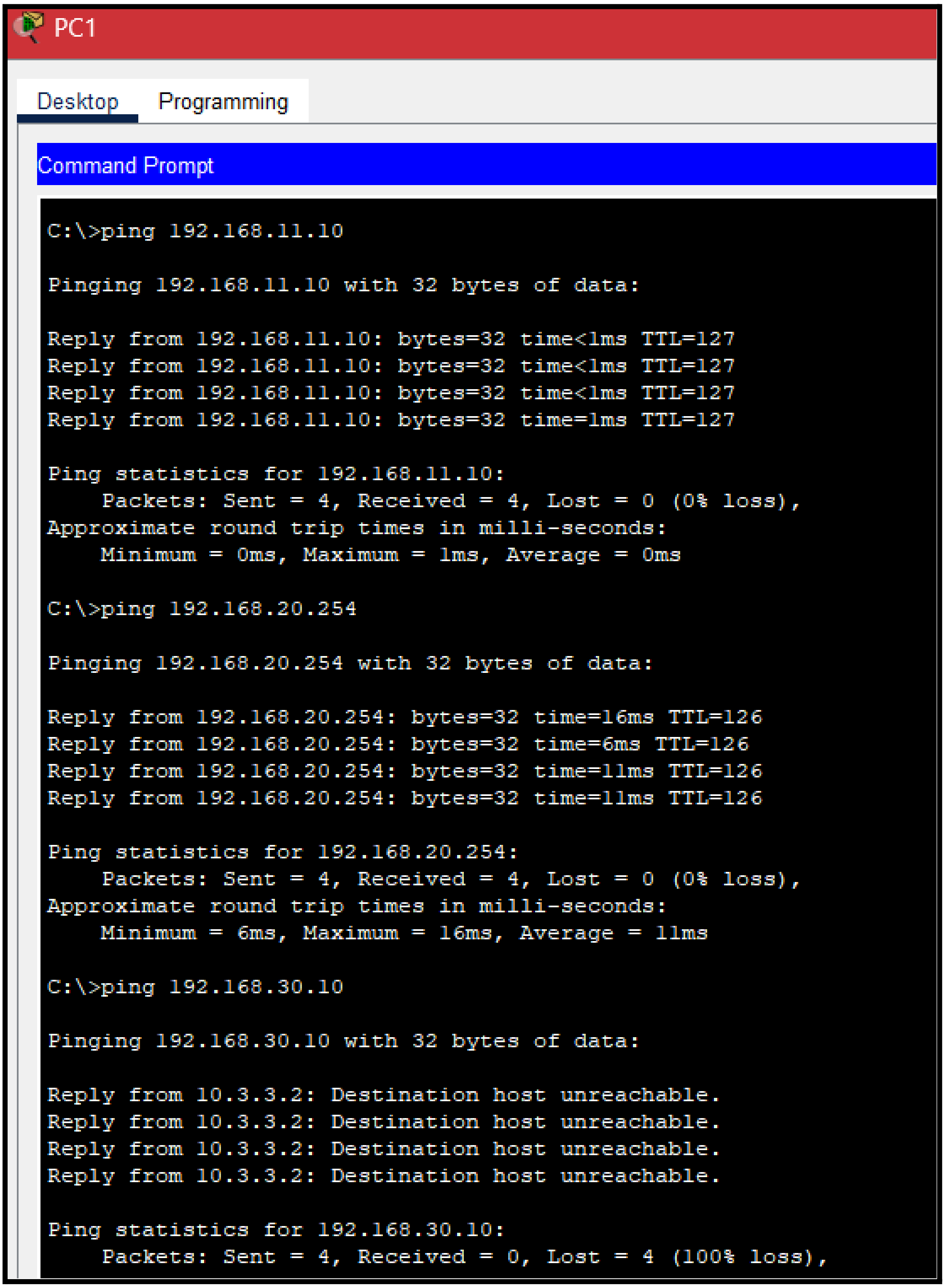


```
R3#show ip interface gigabitethernet0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  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 in Part 1. Use the following tests to verify the ACL implementations:

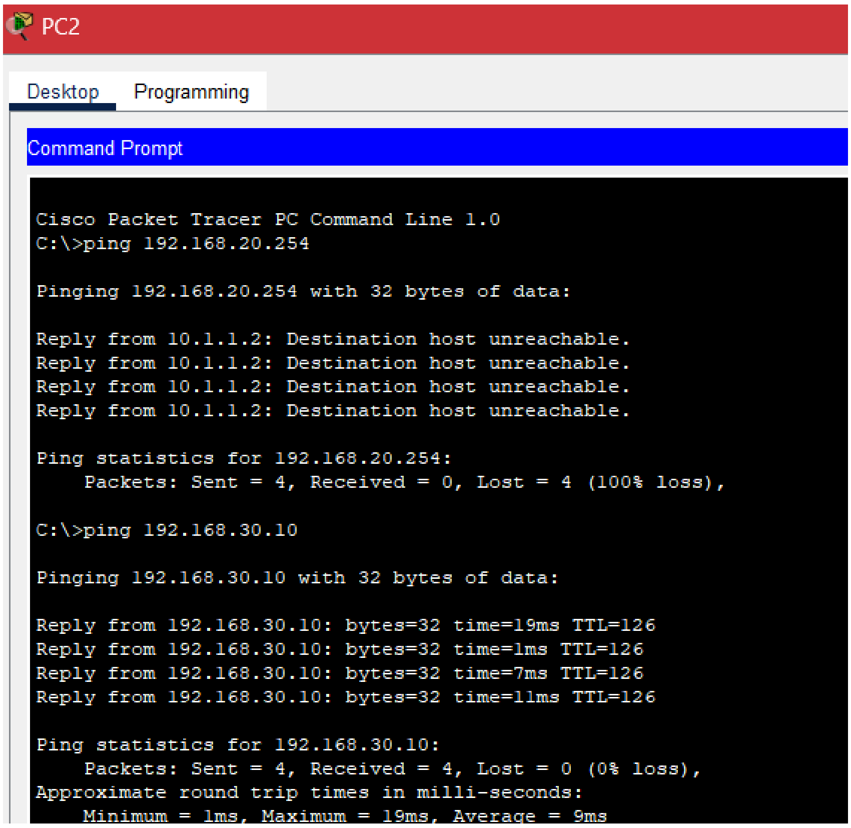
1. A ping from 192.168.10.10 to 192.168.11.10 succeeds.
2. A ping from 192.168.10.10 to 192.168.20.254 succeeds.
3. A ping from 192.168.11.10 to 192.168.20.254 fails.
4. A ping from 192.168.10.10 to 192.168.30.10 fails.
5. A ping from 192.168.11.10 to 192.168.30.10 succeeds.
6. A ping from 192.168.30.10 to 192.168.20.254 succeeds.

Verifying Condition 1,2,4 through PC0 (192.168.10.10)



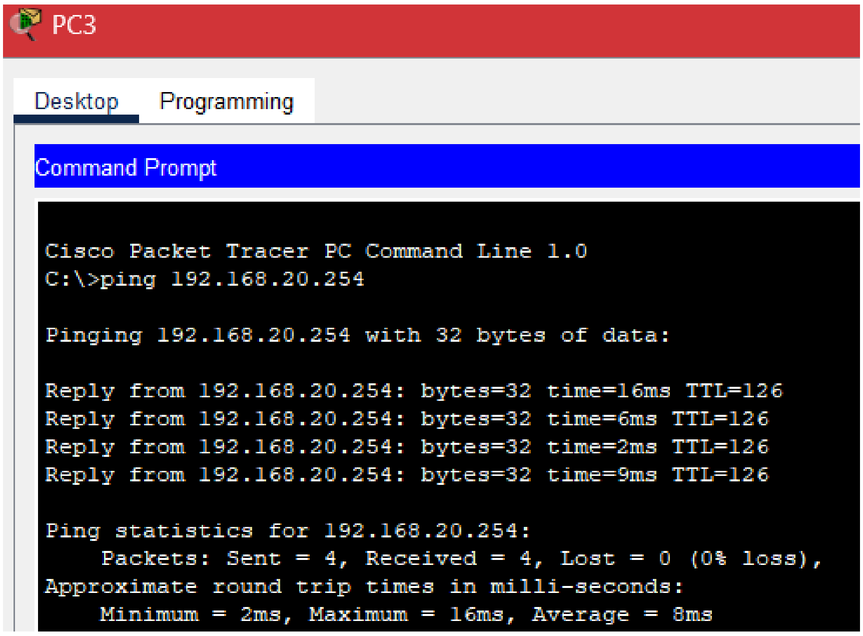
```
C:\>ping 192.168.11.10

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

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=16ms TTL=126
Reply from 192.168.20.254: bytes=32 time=6ms TTL=126
Reply from 192.168.20.254: bytes=32 time=11ms TTL=126
Reply from 192.168.20.254: bytes=32 time=11ms 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 = 6ms, Maximum = 16ms, Average = 11ms

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),
```

Verifying Condition 3,5 through PC1 (192.168.11.10)



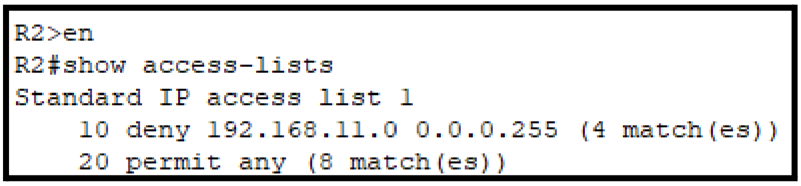
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.254

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=19ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=7ms TTL=126
Reply from 192.168.30.10: bytes=32 time=11ms 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 = 19ms, Average = 9ms
```

Verifying Condition 6 through PC1 (192.168.30.10)

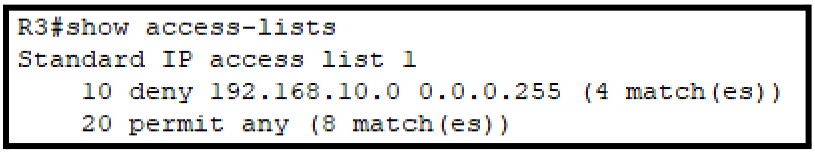


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=16ms TTL=126
Reply from 192.168.20.254: bytes=32 time=6ms TTL=126
Reply from 192.168.20.254: bytes=32 time=2ms TTL=126
Reply from 192.168.20.254: bytes=32 time=9ms 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 = 2ms, Maximum = 16ms, Average = 8ms
```

c. 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.

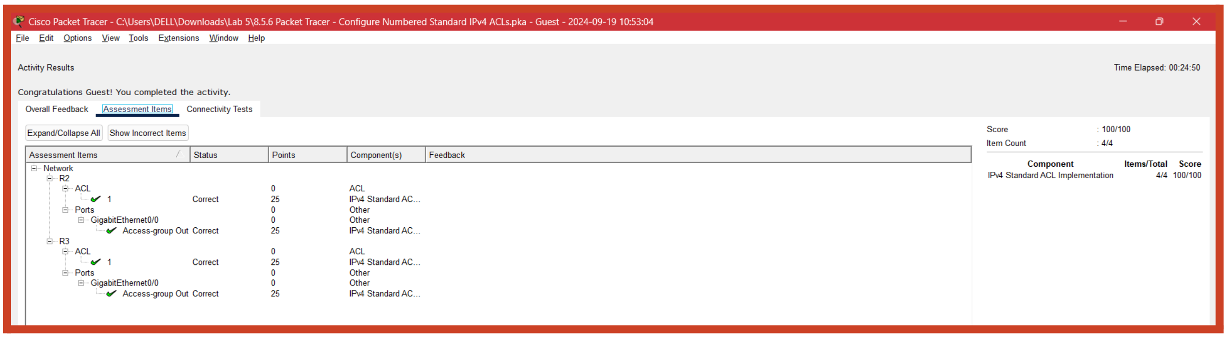


```
R2>en
R2#show access-lists
Standard IP access list 1
    10 deny 192.168.11.0 0.0.0.255 (4 match(es))
    20 permit any (8 match(es))
```



```
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))
```

COMPLETION OF THIS ACTIVITY:



Cisco Packet Tracer - C:\Users\DELL\Downloads\Lab 5\8.5.6 Packet Tracer - Configure Numbered Standard IPv4 ACLs.pka - Guest - 2024-09-19 10:53:04
File Edit Options View Tools Extensions Window Help
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items

Activity Results

Time Elapsed: 00:24:50

Congratulations Guest! You completed the activity.

Assessment Items	Status	Points	Component(s)	Feedback
Network				
R2				
ACL		0	ACL	
✓ 1	Correct	25	IPv4 Standard AC...	
Ports		0	Other	
GigabitEthernet0/0		0	Other	
✓ Access-group Out	Correct	25	IPv4 Standard AC...	
R3				
ACL		0	ACL	
✓ 1	Correct	25	IPv4 Standard AC...	
Ports		0	Other	
GigabitEthernet0/0		0	Other	
✓ Access-group Out	Correct	25	IPv4 Standard AC...	

Score : 100/100
Item Count : 4/4

Component	Items/Total	Score
IPv4 Standard ACL Implementation	4/4	100/100

Topology

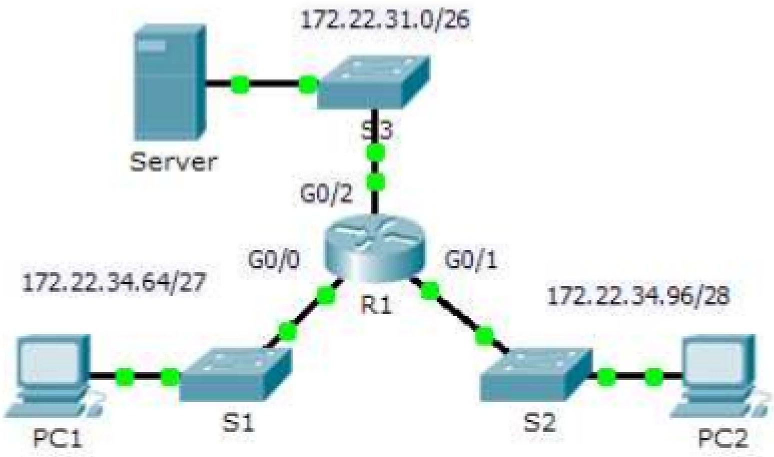
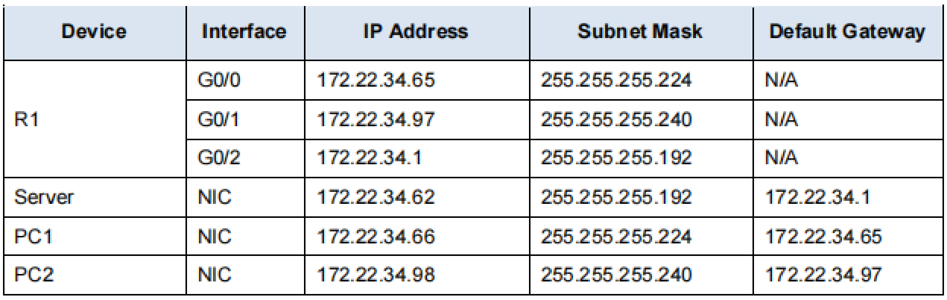


Figure 3: Topology

Addressing Table



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	N/A
	G0/2	172.22.34.1	255.255.255.192	N/A
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Table 3: Addressing Table

Background/Scenario: Two employees need access to services provided by the server. PC1 needs only FTP access while PC2 needs only web access. Both computers can ping the server, but not each other.

Task 3: Configuring Extended ACLs

1. Configure an ACL to permit FTP and ICMP.

a. From global configuration mode on **R1**, enter the following command to determine the first valid number for an extended access list.

```
R1(config)# access-list ?
```

b. Add **100** to the command, followed by a question mark.

```
R1(config)# access-list 100?
```

c. To permit FTP traffic, enter **permit,** followed by a question mark.

```
R1(config)# access-list permit?
```

d. This ACL permits FTP and ICMP. ICMP is listed above, but FTP is not, because FTP uses TCP. Therefore,enter **tcp** to further refine the ACL help.

```
R1(config)# access-list 100 permit tcp ?
```

e. Notice that we could filter just for **PC1** by using the host keyword or we could allow **any** host. In this case, any device is allowed that has an address belonging to the 172.22.34.64/27 network. Enter the network address, followed by a question mark.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 ?
```

f. Calculate the wildcard mask determining the binary opposite of a subnet mask.

11111111.11111111.11111111.11100000 = 255.255.255.224

00000000.00000000.00000000.00011111 = 0.0.0.31

g. Enter the wildcard mask, followed by a question mark.

h. Configure the destination address. In this scenario, we are filtering traffic for a single destination, which is the server. **Enter** the host keyword followed by the server's IP address.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 ?
```

i. Notice that one of the options is **<cr>** (carriage return). In other words, you can press **Enter** and the statement would permit all TCP traffic. However, we are only permitting FTP traffic; therefore, enter the **eq** keyword, followed by a question mark to display the available options. Then, enter **ftp** and press **Enter.**

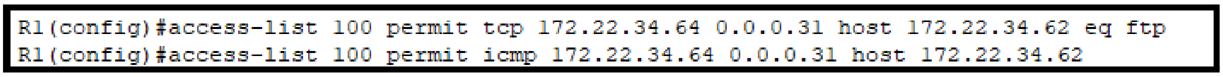
```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ?
```

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ftp
```

j. Create a second access list statement to permit ICMP (ping, etc.) traffic from **PC1** to **Server**. Note that the access list number remains the same and no particular type of ICMP traffic needs to be specified.

```
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host
172.22.34.62
```

k. All other traffic is denied, by default.

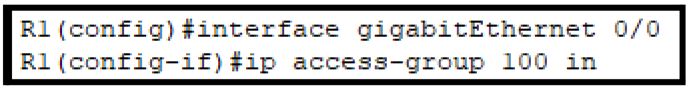


```
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
R1(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
```

2. Apply the ACL on the correct interface to filter traffic.

From **R1's** perspective, the traffic that ACL 100 applies to is inbound from the network connected to Gigabit Ethernet 0/0 interface. Enter interface configuration mode and apply the ACL.

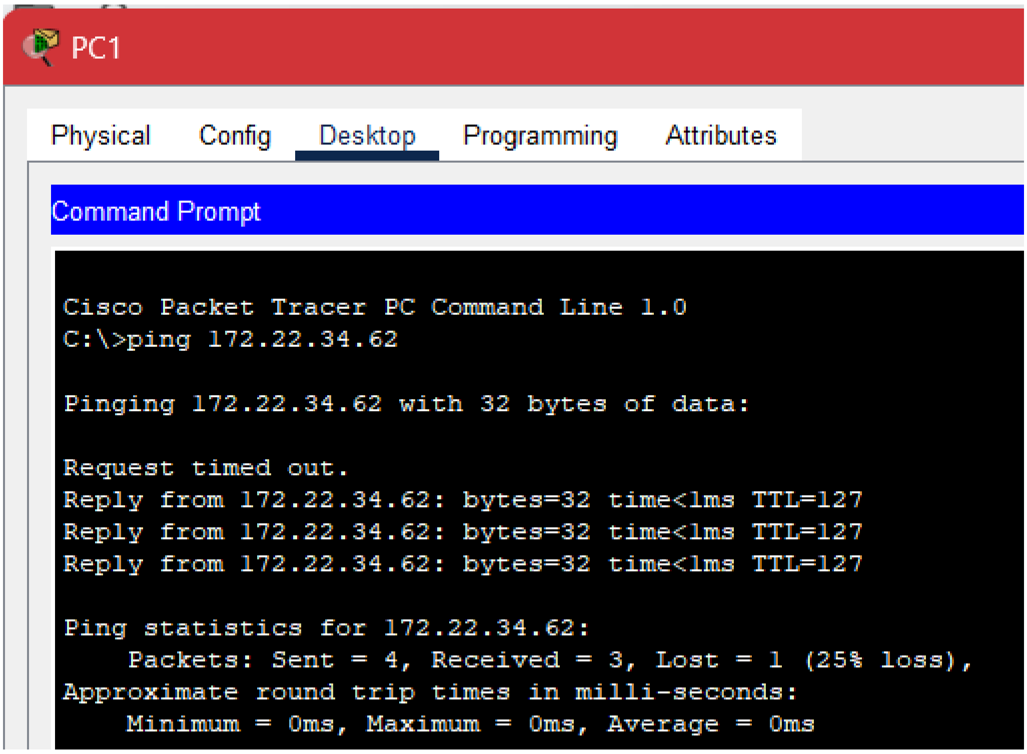
```
R1(config)# interface gigabitEthernet 0/0

R1(config-if)# ip access-group 100 in
```



```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip access-group 100 in
```

3. Verify the ACL implementation.

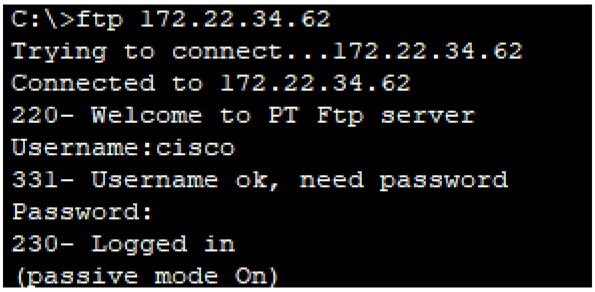
a. Ping from **PC1** to **Server**. If the pings are unsuccessful, verify the IP addresses before continuing.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Request timed out.
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

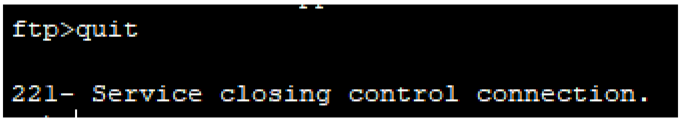
b. FTP from **PC1** to **Server**. The username and password are both **cisco.**

```
PC> ftp 172.22.34.62
```



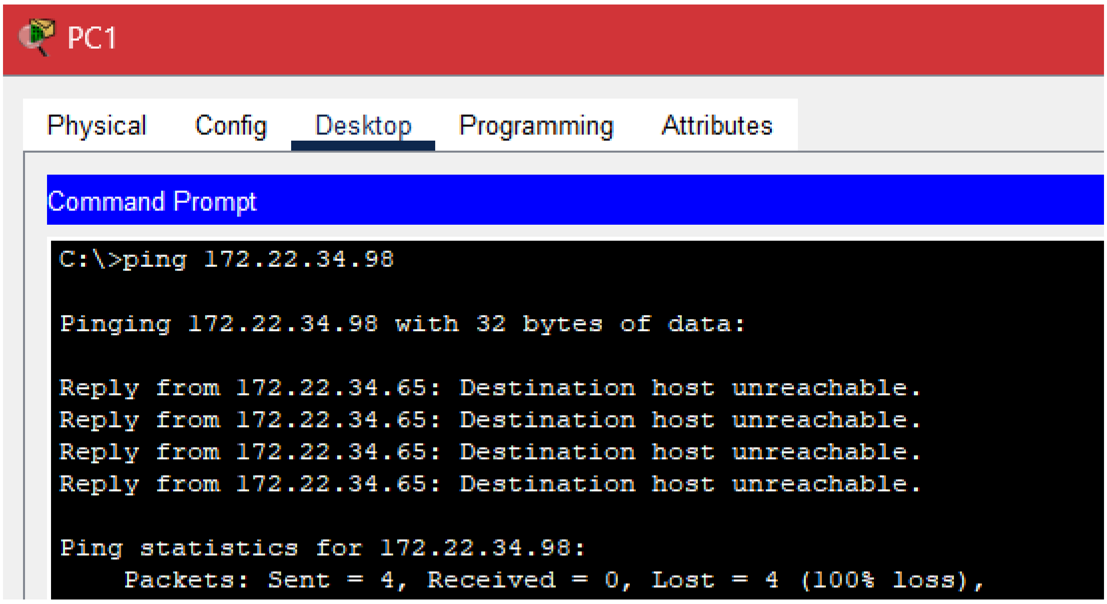
```
C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
```

c. Exit the FTP service of the **Server.**



```
ftp>quit

221- Service closing control connection.
```

d. Ping from **PC1** to **PC2**. The destination host should be unreachable, because the traffic was not explicitly permitted.



```
C:\>ping 172.22.34.98

Pinging 172.22.34.98 with 32 bytes of data:

Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.

Ping statistics for 172.22.34.98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Task 4: Configure, Apply and Verify an Extended Named ACL

1. Configure an ACL to permit HTTP access and ICMP.

a. Named ACLs start with the **ip** keyword. From global configuration mode of **R1**, enter the following command, followed by a question mark.

```
R1(config)# access-list ?
```

b. You can configure named standard and extended ACLs. This access list filters both source and destination IP addresses; therefore, it must be extended. Enter HTTP_ONLY as the name.

```
R1(config)# ip access-list extended HTTP_ONLY
```

c. The prompt changes. You are now in extended named ACL configuration mode. All devices on the PC2 LAN need TCP access. Enter the network address, followed by a question mark.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 ?

A.B.C.D Source wildcard bits
```

d. An alternative way to calculate a wildcard is to subtract the subnet mask from 255.255.255.255.

```
255.255.255.255 - 255.255.255.240 = 0. 0. 0. 15
```

e. Finish the statement by specifying the server address as you did in Part 1 and filtering **www** traffic.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62
eq www
```

f. Create a second access list statement to permit ICMP (ping, etc.) traffic from PC2 to Server. Note: The prompt remains the same and a specific type of ICMP traffic does not need to be specified.

g. All other traffic is denied, by default. Exit out of extended named ACL configuration mode.

2. Apply the ACL on the correct interface to filter traffic.

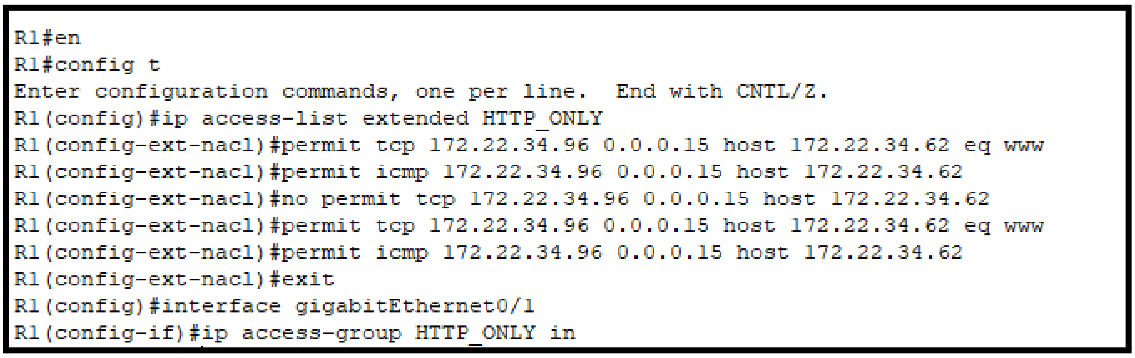
From **R1**'s perspective, the traffic that access list **HTTP_ONLY** applies to is inbound from the network connected to Gigabit Ethernet 0/1 interface. Enter the interface configuration mode and apply the ACL.

```
R1(config)# interface gigabitEthernet 0/1
```

```
R1(config-if)# ip access-group HTTP_ONLY in
```

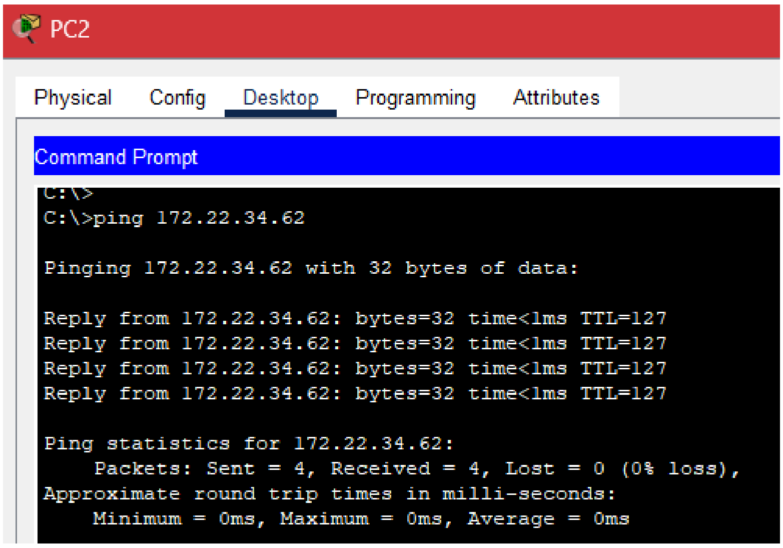
3. Verify the ACL implementation.

Setting Up:



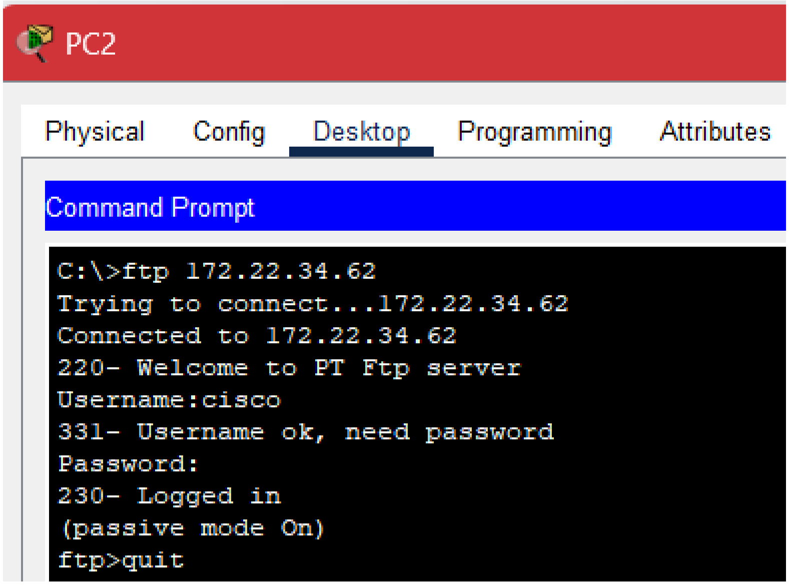
```
R1#en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list extended HTTP_ONLY
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
R1(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
R1(config-ext-nacl)#no permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
R1(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
R1(config-ext-nacl)#exit
R1(config)#interface gigabitEthernet0/1
R1(config-if)#ip access-group HTTP_ONLY in
```

a. Ping from **PC2** to **Server**. If the pings are unsuccessful, verify the IP addresses before continuing.



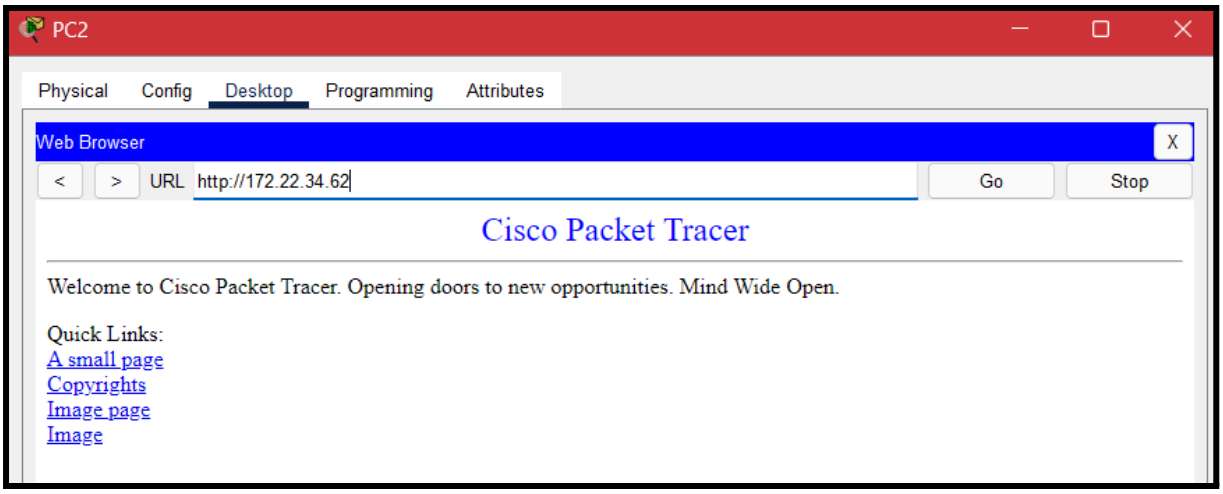
```
C:\>
C:\>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

b. FTP from **PC2** to **Server**.



```
C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit
```

c. Open the web browser on PC2 and enter the IP address of Server as the URL. The connection should be successful.



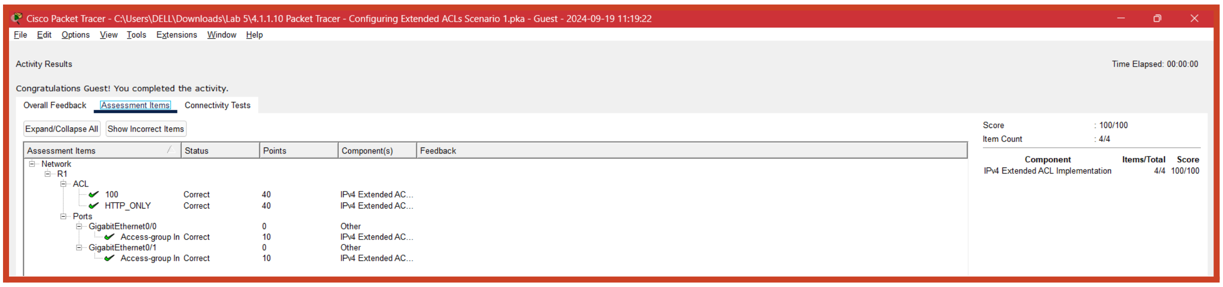
http://172.22.34.62

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

COMPLETED THE ACTIVITY PROOF!



Cisco Packet Tracer - C:\Users\DELL\Downloads\Lab 5\4.1.1.10 Packet Tracer - Configuring Extended ACLs Scenario 1.pka - Guest - 2024-09-19 11:19:22

Activity Results

Time Elapsed: 00:00:00

Congratulations Guest! You completed the activity.

Assessment Items	Status	Points	Component(s)	Feedback
Network				
R1				
ACL				
✓ 100	Correct	40	IPv4 Extended AC...	
✓ HTTP_ONLY	Correct	40	IPv4 Extended AC...	
Ports				
GigabitEthernet0/0		0	Other	
✓ Access-group In	Correct	10	IPv4 Extended AC...	
GigabitEthernet0/1		0	Other	
✓ Access-group In	Correct	10	IPv4 Extended AC...	

Score : 100/100
Item Count : 4/4

Component	Items/Total	Score
IPv4 Extended ACL Implementation	4/4	100/100

Assessment Rubric

Lab 05

Configuring Standard and Extended IPv4 ACLs

Name: Syed Asghar Abbas Zaidi	**Student ID: 07201**

<u>Points Distribution</u>

Task No.	**LR 2 Simulation**	**LR3 Troubleshooting**	**LR5 Results/Plots**	**LR9 Report**
Task 1	10	5	5	
Task 2	10	5	5	
Task 3	15	5	5	
Task 4	15	5	5	
Total	/50	/20	/20	/10
CLO Mapped	CLO 1	CLO 1	CLO 1	CLO1

Affective Domain Rubric		**Points**	**CLO Mapped**
AR 7	Report Submission	/10	CLO 1

CLO	**Total Points**	**Points Obtained**
1	90	
1	10	
Total	**100**	

For description of different levels of the mapped rubrics, please refer the provided Lab Evaluation Assessment Rubrics and Affective Domain Assessment Rubrics.

Lab Evaluation Assessment Rubric

#	Assessment Elements	Level 1: Unsatisfactory Points 0-1	Level 2: Developing Points 2	Level 3:Good Points 3	Level 4:Exemplary Points 4
LR2	**Program/Code / Simulation Model/ Network Model**	Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software.	Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software.	Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine.	Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software.
LR3	**Troubleshooting**	Unable to identify the fault/minimal effort show in troubleshooting.	Able to identify the fault but unable to remove it.	Able to identify the fault but partially removes it.	Able to identify the fault and takes necessary steps and actions to correct it.
LR5	**Results & Plots**	Figures/ graphs / tables are not developed or are poorly constructed with erroneous results. Titles, captions, units are not mentioned. Data is presented in an obscure manner.	Figures, graphs and tables are drawn but contain errors. Titles, captions, units are not accurate. Data presentation is not too clear.	All figures, graphs, tables are correctly drawn but contain minor errors or some of the details are missing.	Figures / graphs / tables are correctly drawn and appropriate titles/captions and proper units are mentioned. Data presentation is systematic.
LR9	**Report**	All the in-lab tasks are not included in report and / or the report is submitted too late.	Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. Report is submitted after due date.	Good summary of most the in-lab tasks is included in report. The work is supported by figures and plots with explanations. The report is submitted timely.	Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables.