Packet Tracer - Configure Named Standard IPv4 ACLs

Nombre: Luis Enrique Pérez Señalin

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.100.1	255.255.255.0	N/A
	F0/1	192.168.200.1	255.255.255.0	
	E0/0/0	192.168.10.1	255.255.255.0	
	E0/1/0	192.168.20.1	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

Objectives

Part 1: Configure and Apply a Named Standard ACL

Part 2: Verify the ACL Implementation

Background / Scenario

The senior network administrator has asked you to create a standard named ACL to prevent access to a file server. The file server contains the data base 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.

Instructions

Part 1: Configure and Apply a Named Standard ACL

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

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

Step 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# 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
```

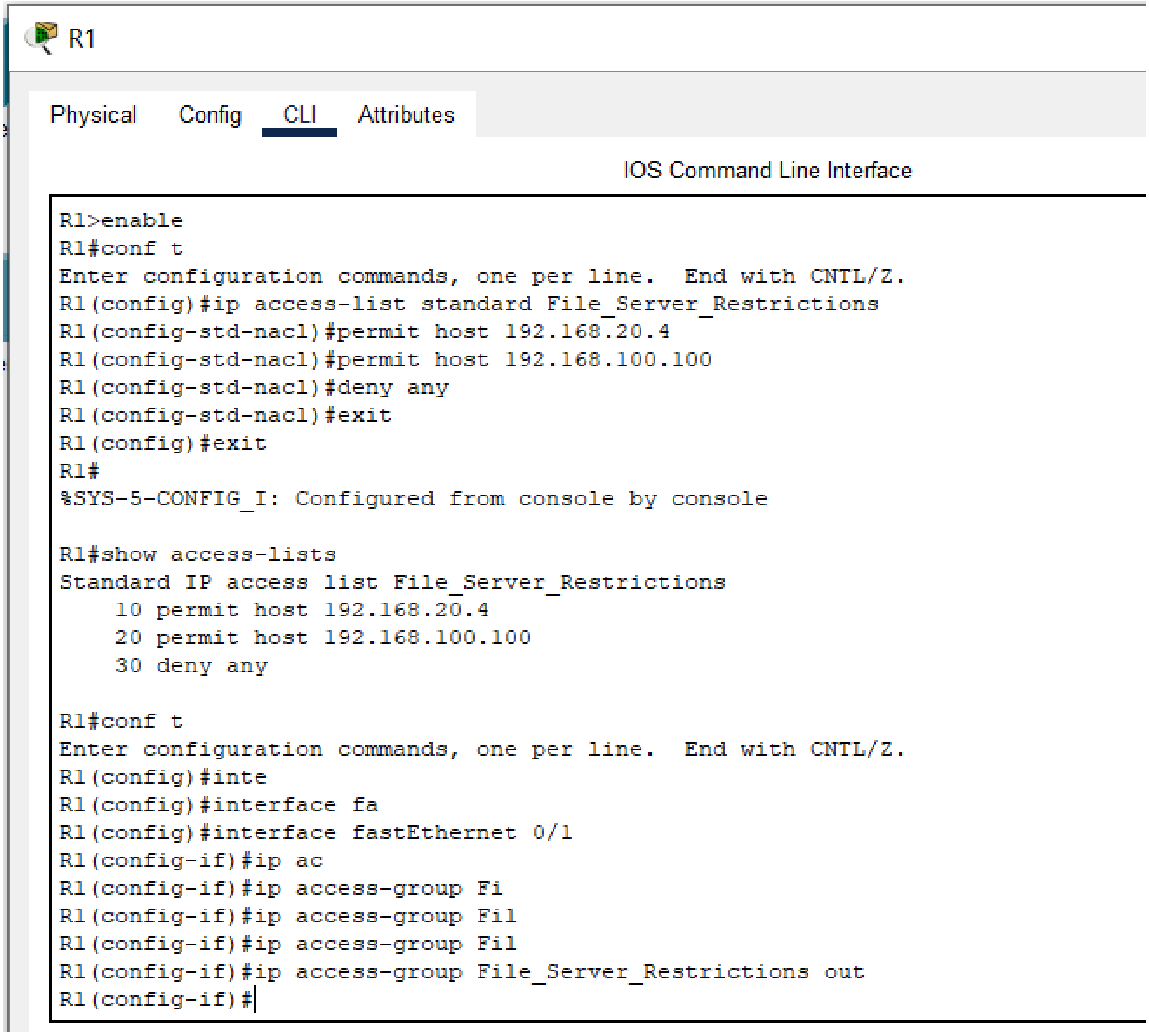
Step 3: Apply the named ACL.

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.

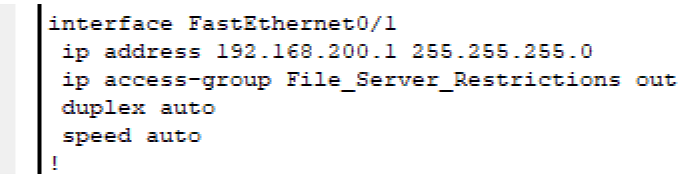


```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard File_Server_Restrictions
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#permit host 192.168.100.100
R1(config-std-nacl)#deny any
R1(config-std-nacl)#exit
R1(config)#exit
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

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#inte
R1(config)#interface fa
R1(config)#interface fastEthernet 0/1
R1(config-if)#ip ac
R1(config-if)#ip access-group Fi
R1(config-if)#ip access-group Fil
R1(config-if)#ip access-group Fil
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#
```

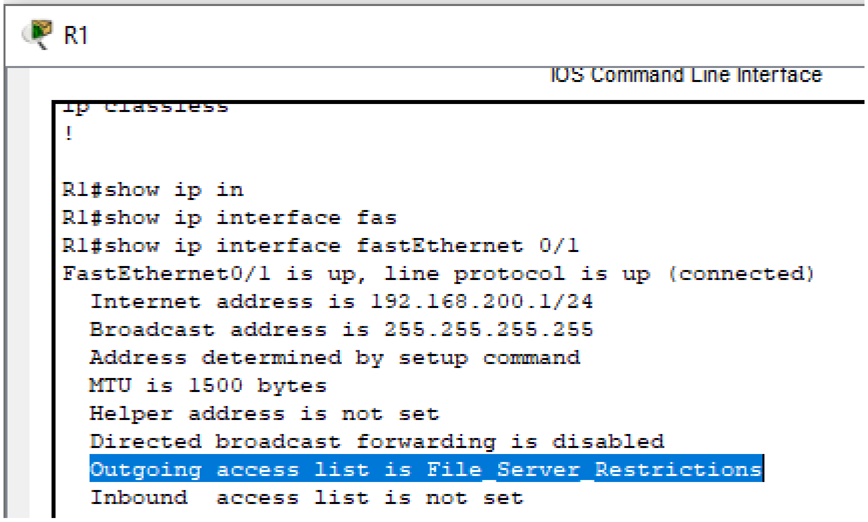
Part 2: Verify the ACL Implementation

Step 1: 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.



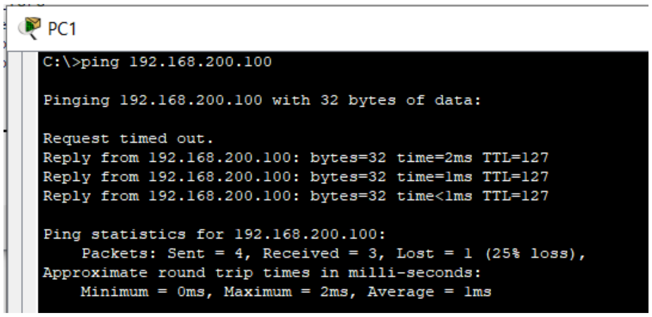
```
interface FastEthernet0/1
 ip address 192.168.200.1 255.255.255.0
 ip access-group File_Server_Restrictions out
 duplex auto
 speed auto
!
```



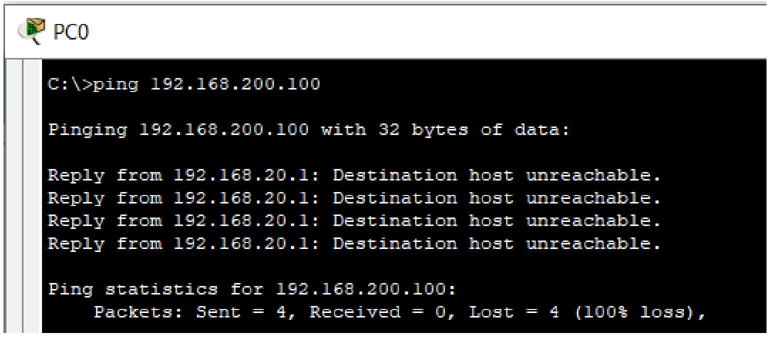
```
ip classless
!

R1#show ip in
R1#show ip interface fas
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
```

Step 2: Verify that the ACL is working properly.

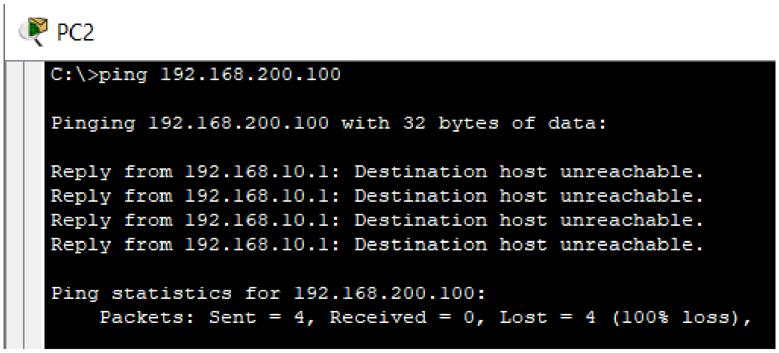
All three workstations should be able to ping the **Web Server**, but only **PC1** and the **Web Server** should be able to ping the **File Server**. Repeat the **show access-lists** command to see the number of packets that matched each statement.



```
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.200.100: bytes=32 time=2ms 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 = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

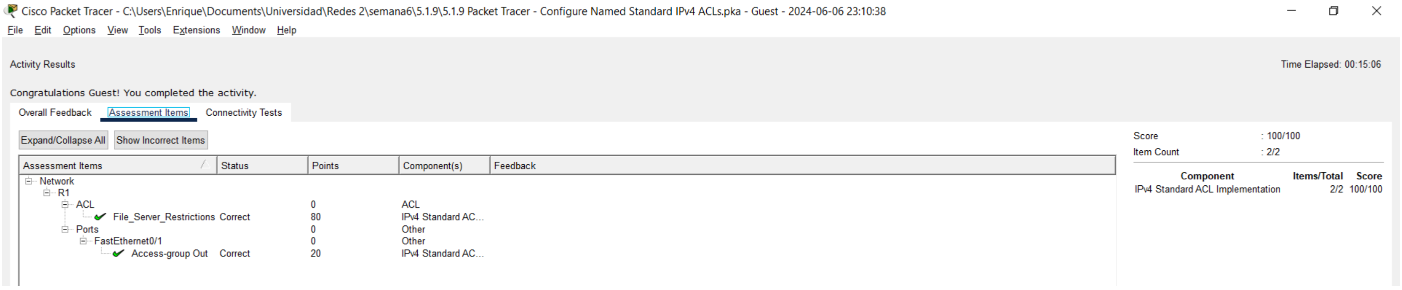


```
C:\>ping 192.168.200.100

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 192.168.200.100

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),
```

Captura de pantalla:



Cisco Packet Tracer - C:\Users\Enrique\Documents\Universidad\Redes 2\semana6\5.1.9\5.1.9 Packet Tracer - Configure Named Standard IPv4 ACLs.pka - Guest - 2024-06-06 23:10:38

Activity Results

Time Elapsed: 00:15:06

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

Observación:

El archivo .pka no pidió el ingreso del nombre como normalmente lo hace.