Configure IP ACLs to Mitigate Attacks

Introduction

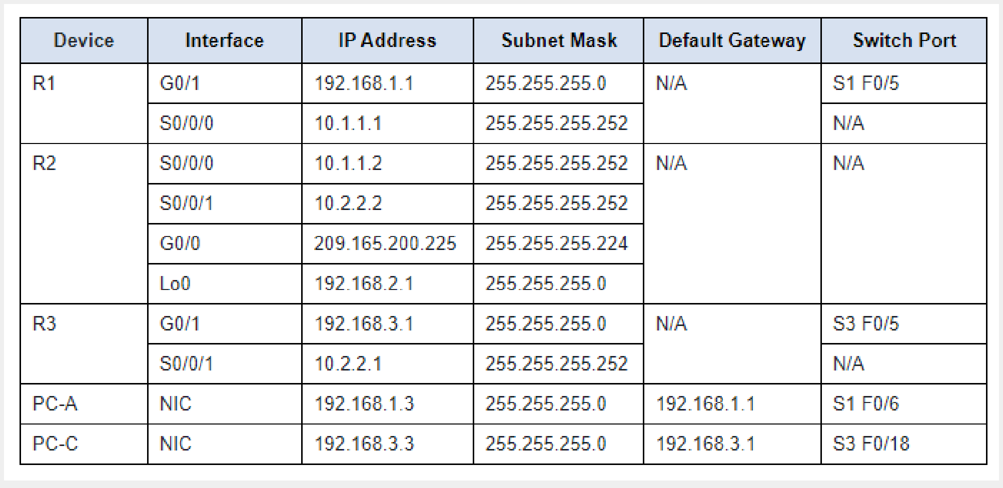
In this activity, you will configure access control lists (ACLs) to meet network communication security goals.

Background / Scenario

A company is implementing ACLs to help prevent malicious traffic from entering the network. Your task is to configure ACLs to meet the goals that have been provided by security personnel. Standard operating procedure is to apply ACLs on edge routers to mitigate common threats.

The routers have been pre-configured with the following:

Enable password: `ciscoenpa55`
Password for console: `ciscoconpa55`
SSH login username and password: `SSHadmin/ciscosshpa55`



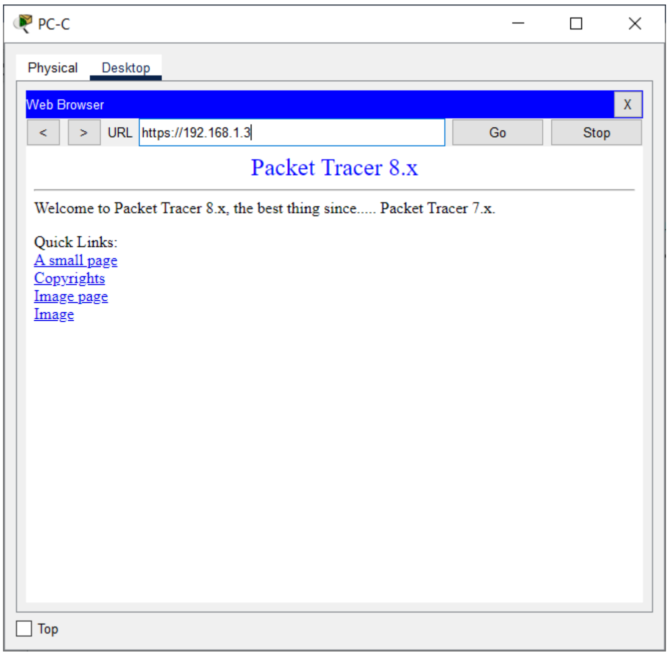
Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0	10.1.1.1	255.255.255.252		N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1	10.2.2.2	255.255.255.252		
	G0/0	209.165.200.225	255.255.255.224		
	Lo0	192.168.2.1	255.255.255.0		
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252		N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Part 1: Verify end-to-end connectivity.

The following connections should be tested before applying ACLs:

- Verify end-to-end connectivity.
- Use a web browser to access the web server at PC-A.
- From the hosts, establish SSH sessions to R2's Lo0 interface and the GigabitEthernet interfaces on each router.

Step 1: Verify network connectivity between PC-A and PC-C.



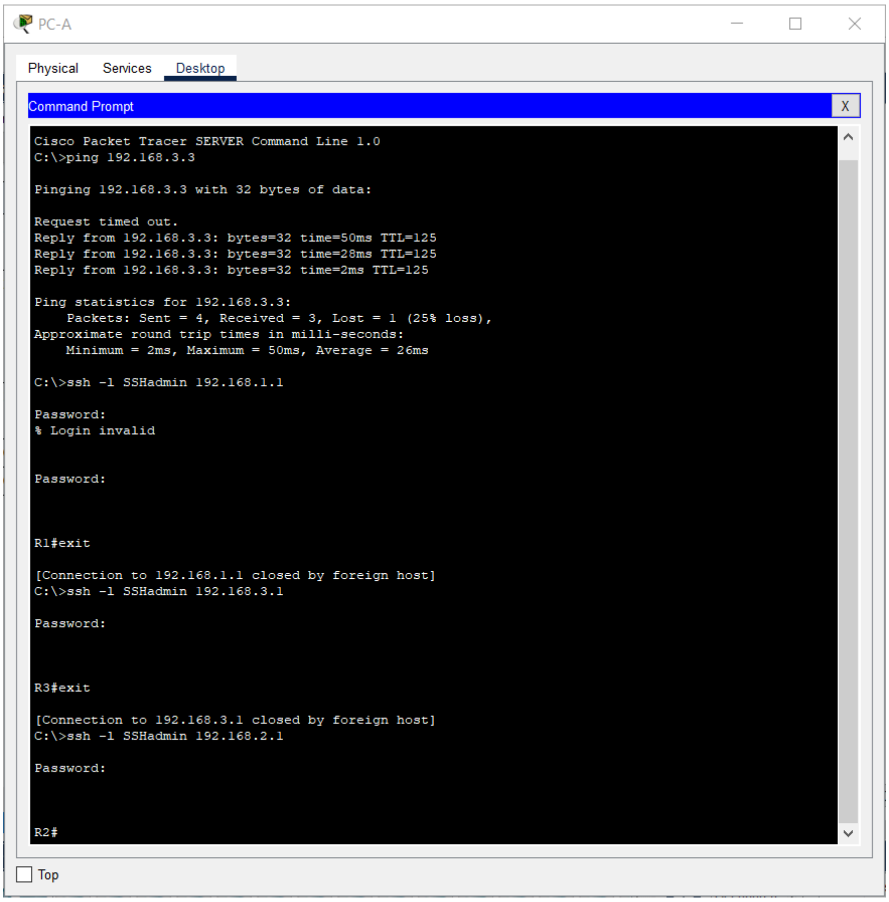
URL https://192.168.1.3

Packet Tracer 8.x

Welcome to Packet Tracer 8.x, the best thing since..... Packet Tracer 7.x.

Quick Links:
A small page
Copyrights
Image page
Image

a. From each PC, establish SSH sessions to the following to verify that SSH is working properly:
   - R1 G0/1
   - R2 G0/0 and Lo0
   - R3 G0/1



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=50ms TTL=125
Reply from 192.168.3.3: bytes=32 time=28ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 50ms, Average = 26ms

C:\>ssh -l SSHadmin 192.168.1.1

Password:
% Login invalid


Password:



R1#exit

[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.3.1

Password:



R3#exit

[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.2.1

Password:



R2#
```

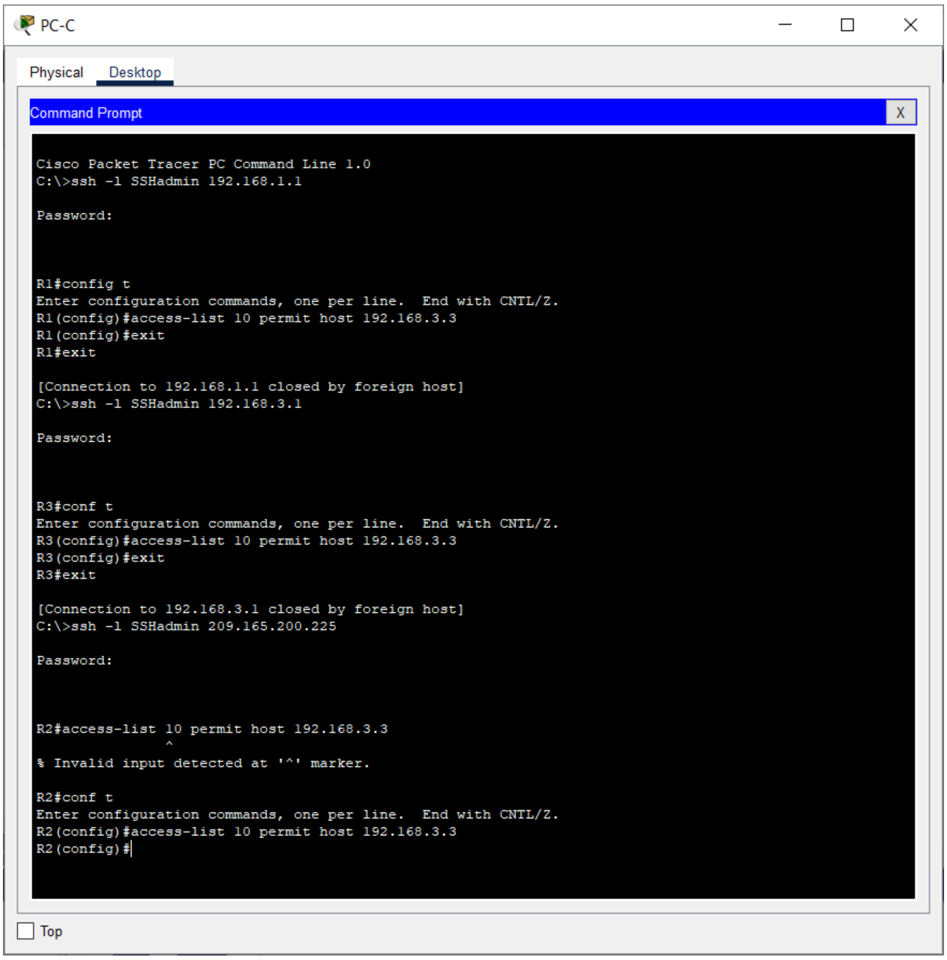
Part 2: Configure and apply ACLs

In this part of the activity, you will configure and apply ACLs that secure remote access (SSH) to the routers except from the administration host PC-C.

Configure ACLs on all three routers to meet the following criteria:

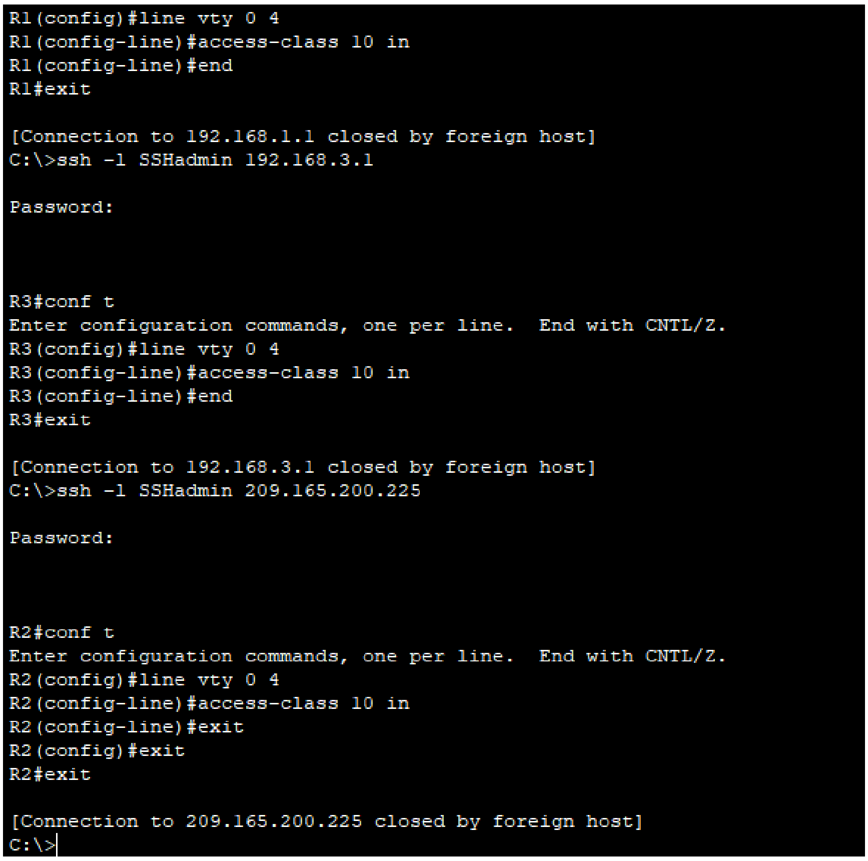
- PC-A cannot access the management interfaces of all three routers.
- PC-C can establish SSH sessions to all the routers.

Step 1: Create ACLs on the routers to allow PC-C to access the routers remotely.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l SSHadmin 192.168.1.1

Password:



R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 10 permit host 192.168.3.3
R1(config)#exit
R1#exit

[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.3.1

Password:



R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 10 permit host 192.168.3.3
R3(config)#exit
R3#exit

[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l SSHadmin 209.165.200.225

Password:



R2#access-list 10 permit host 192.168.3.3
               ^
% Invalid input detected at '^' marker.

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 10 permit host 192.168.3.3
R2(config)#
```

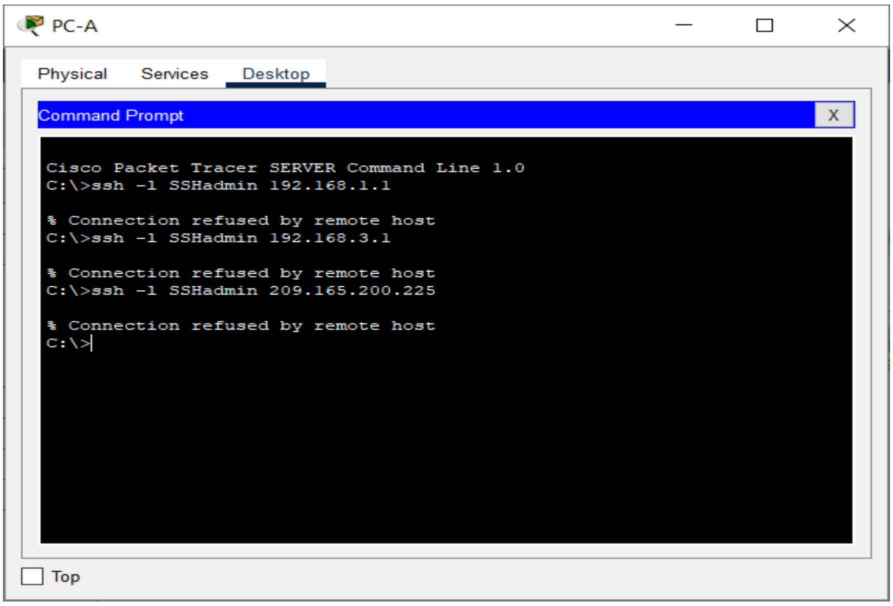
Step 2: Apply the ACL on all three routers to block all remote access to them except from PC-C.



```
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#end
R1#exit

[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.3.1

Password:



R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#end
R3#exit

[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l SSHadmin 209.165.200.225

Password:



R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#exit
R2(config)#exit
R2#exit

[Connection to 209.165.200.225 closed by foreign host]
C:\>
```

Step 3: Verify exclusive access from management station PC-C.

a. Can PC-A SSH into the routers? If the ACLs are configured and applied at the correct interface, PC-A should FAIL.



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ssh -l SSHadmin 192.168.1.1

% Connection refused by remote host
C:\>ssh -l SSHadmin 192.168.3.1

% Connection refused by remote host
C:\>ssh -l SSHadmin 209.165.200.225

% Connection refused by remote host
C:\>
```

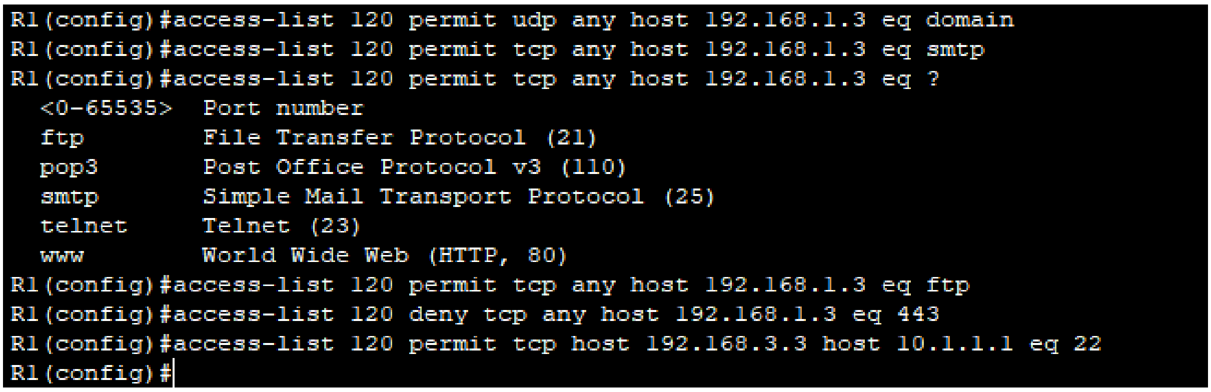
Part 3: Configure an ACL to filter specific incoming traffic.

Step 1: You will configure an ACL to filter specific incoming traffic on R1. You will also apply this ACL at the appropriate interface.

a. Permit any outside host to access DNS, SMTP, and FTP services on server PC-A.

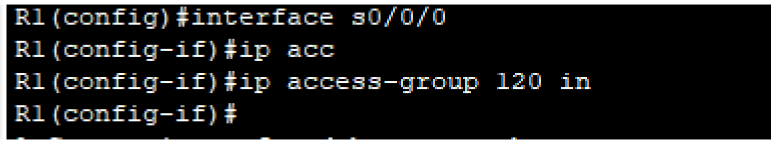
b. Deny any outside host access to HTTPS services on PC-A.

c. Permit PC-C to access the IP address of R1 S0/0/0 interface via SSH.



```
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ?
  <0-65535>  Port number
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R1(config)#
```

d. Apply the ACL to the proper router interface.

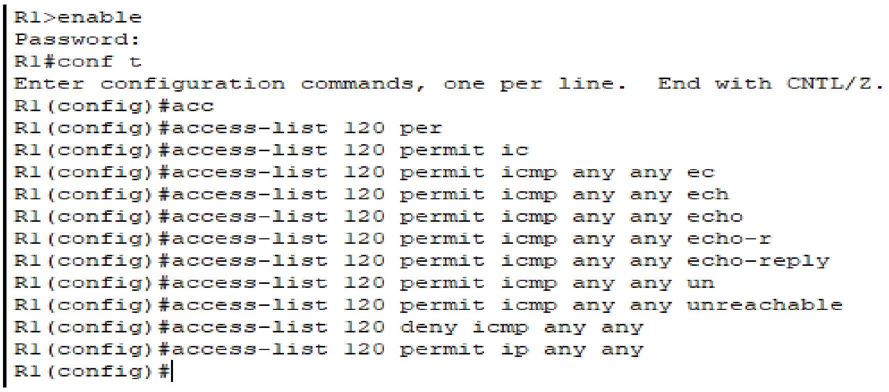


```
R1(config)#interface s0/0/0
R1(config-if)#ip acc
R1(config-if)#ip access-group 120 in
R1(config-if)#
```

Part 4: Verifying connectivity.

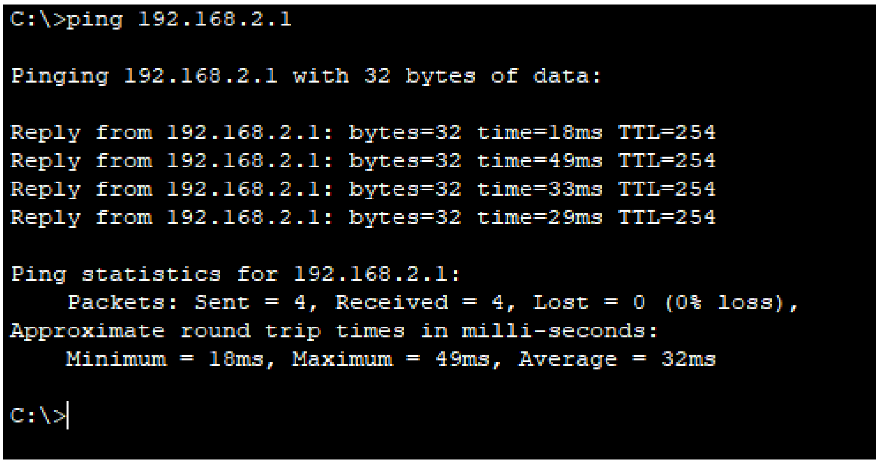
Step 1: Verify connectivity before modifying the ACL you just created in the previous screen to meet the following criteria:

a. Permit ICMP echo replies and destination unreachable messages from the outside network (relative to R1).
b. Deny all other incoming ICMP packets.
c. Permit all other traffic.



```
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#acc
R1(config)#access-list 120 per
R1(config)#access-list 120 permit ic
R1(config)#access-list 120 permit icmp any any ec
R1(config)#access-list 120 permit icmp any any ech
R1(config)#access-list 120 permit icmp any any echo
R1(config)#access-list 120 permit icmp any any echo-r
R1(config)#access-list 120 permit icmp any any echo-reply
R1(config)#access-list 120 permit icmp any any un
R1(config)#access-list 120 permit icmp any any unreachable
R1(config)#access-list 120 deny icmp any any
R1(config)#access-list 120 permit ip any any
R1(config)#
```

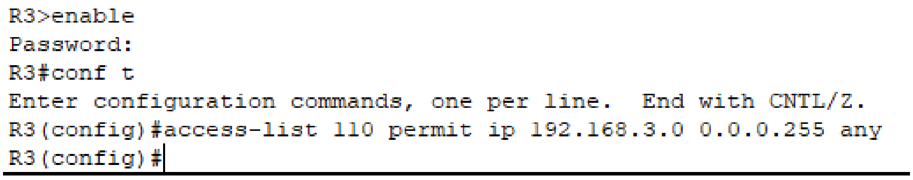
d. After modifying the ACL, verify that PC-A can successfully ping the loopback interface on R2.



```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=18ms TTL=254
Reply from 192.168.2.1: bytes=32 time=49ms TTL=254
Reply from 192.168.2.1: bytes=32 time=33ms TTL=254
Reply from 192.168.2.1: bytes=32 time=29ms TTL=254

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 49ms, Average = 32ms

C:\>
```

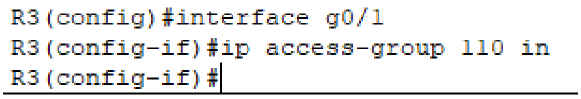
Part 5: Configuring an ACL to permit R3 traffic.

a. Create an ACL to permit only the IP addresses of the internal network on R3 to enter the router from the LAN.



```
R3>enable
Password:
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#
```

b. Apply the ACL to the appropriate interface.



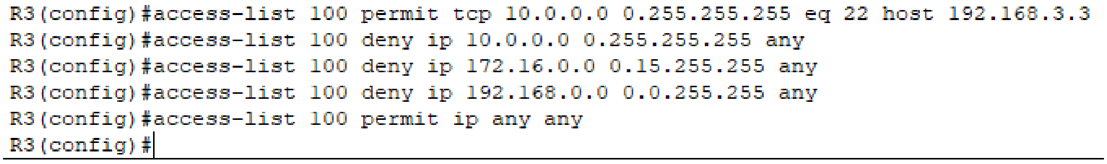
```
R3(config)#interface g0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#
```

Part 6: Applying an ACL to block all incoming packets.

Step 1: On R3, create and apply an ACL to block all incoming packets from a source IP address that is in any private network address range specified in RFC 1918. Be sure to allow all other traffic.

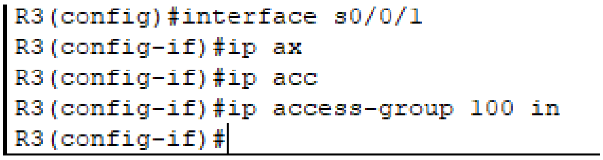
Because PC-C is being used for remote management, permit SSH traffic from the 10.0.0.0/8 network to return to the host PC-C.

a. Permit SSH traffic from `10.0.0.0/8` to PC-C.
b. Deny traffic from `10.0.0.0/8, 172.16.0.0/12`, and `192.168.0.0/16`.
c. Permit all other traffic.



```
R3(config)#access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#
```

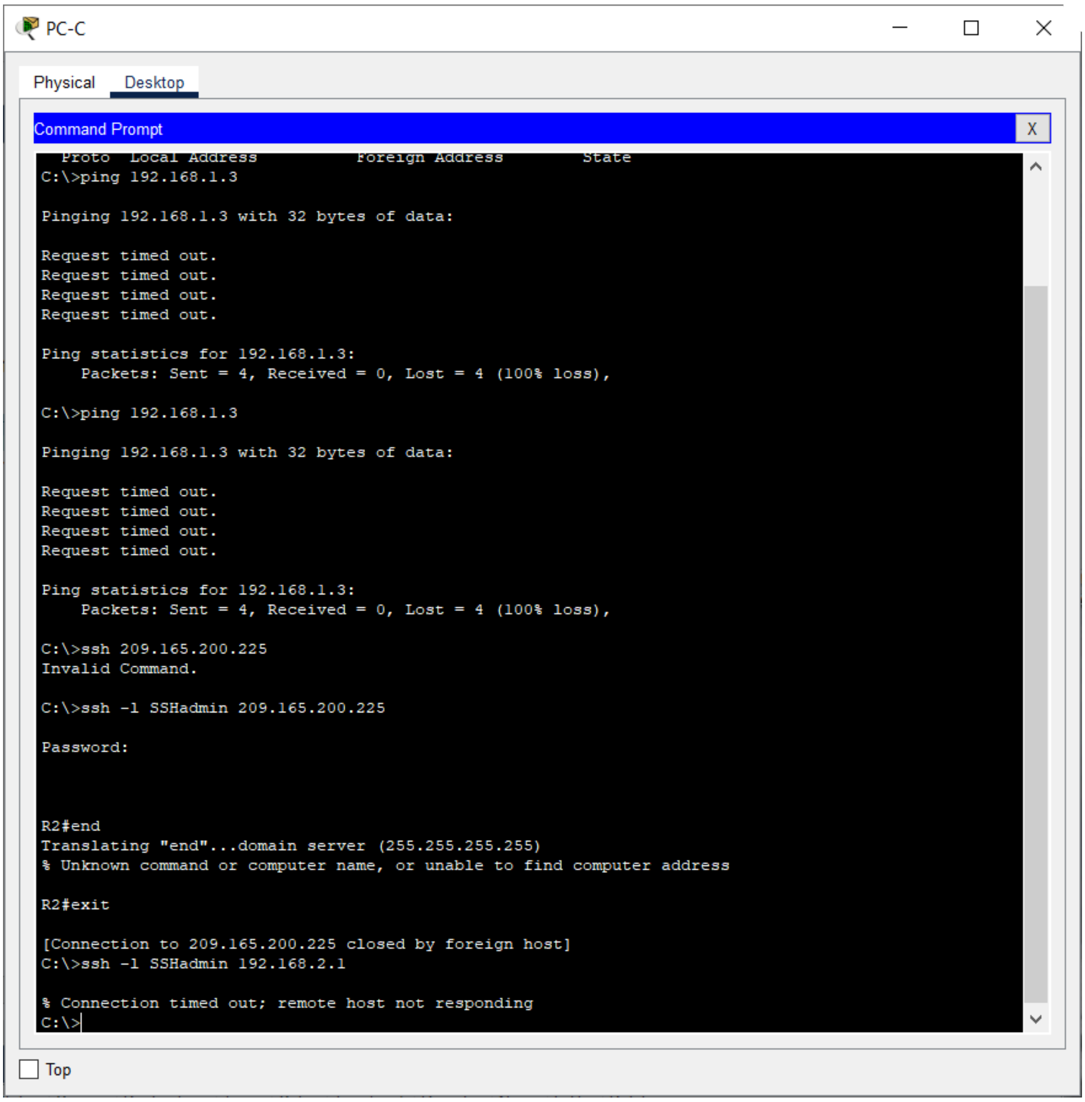
d. Apply the ACL to the S0/0/1 interface.



```
R3(config)#interface s0/0/1
R3(config-if)#ip ax
R3(config-if)#ip acc
R3(config-if)#ip access-group 100 in
R3(config-if)#
```

Step 2: Confirm that the specified traffic entering interface Serial 0/0/1 is handled correctly.

a. Verify that pings from PC-C to PC-A server fail.
b. From PC-C, establish an SSH session to `209.165.200.225`. It should work.
c. From PC-C establish an SSH session to `192.168.2.1`. It should not work.



```
   Proto  Local Address          Foreign Address        State
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ssh 209.165.200.225
Invalid Command.

C:\>ssh -l SSHadmin 209.165.200.225

Password:



R2#end
Translating "end"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

R2#exit

[Connection to 209.165.200.225 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.2.1

% Connection timed out; remote host not responding
C:\>
```

Reflections

- It is important to verify connectivity before configuring ACLs to ensure that any changes in connectivity are the result of the ACLs and not network faults.

- Remote management should be limited to only specific IP addresses so that unauthorized users cannot reach the management interface. This is one line of defense against malicious tampering with network devices by external threat actors.

- ICMP can be used as a reconnaissance tool by threat actors. Blocking specific types of ICMP messages from outside can prevent threat actors from learning about the internal network.