VSIT

Security in Computing
Practical #4

Name	Sanjeev Gupta	**Roll Number**	21302B0023
Class	TYBScIT	**Division**	C
Subject/Course	Security in Computing		
Topic	Configure IP ACLs to Mitigate Attacks		

1 Verify Basic Network Connectivity
2 Secure Access to Routers

Enable password: ciscoenpa55

- **Password for console: ciscoconpa55**
- **SSH logon username and password: SSHadmin/ciscosshpa55**

Verify Basic Network Connectivity

Step 1: From PC-A, verify connectivity to PC-C and R2.

a. From the command prompt, ping PC-C (192.168.3.3).

b. From the command prompt, establish an SSH session to R2 Lo0 interface (192.168.2.1) using username SSHadmin and password ciscosshpa55. When finished, exit the SSH session.

SERVER> ssh –l SSHadmin 192.168.2.1

Step 2: From PC-C, verify connectivity to PC-A and R2.

a. From the command prompt, ping PC-A (192.168.1.3).

b. From the command prompt, establish an SSH session to R2 Lo0 interface (192.168.2.1) using username SSHadmin and password ciscosshpa55. Close the SSH session when finished.

c. PC> ssh –l SSHadmin 192.168.2.1

d. Open a web browser to the PC-A server (192.168.1.3) to display the web page. Close the browser when done.

Secure Access to Routers

Step 1: Configure ACL 10 to block all remote access to the routers except from PC-C.

```
R1(config)# access-list 10 permit host 192.168.3.3
line vty 0 4
R2(config)# access-list 10 permit host 192.168.3.3
line vty 0 4
R3(config)# access-list 10 permit host 192.168.3.3
line vty 0 4
```

Step 2: Apply ACL 10 to ingress traffic on the VTY lines.

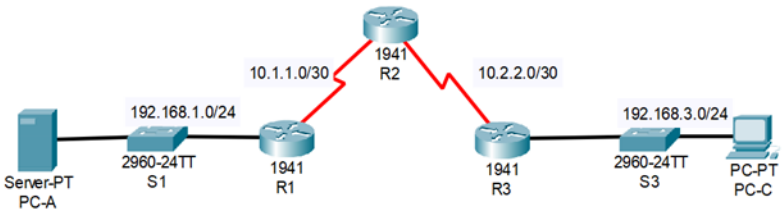
```
R1(config-line)# access-class 10 in
R2(config-line)# access-class 10 in
R3(config-line)# access-class 10 in
```

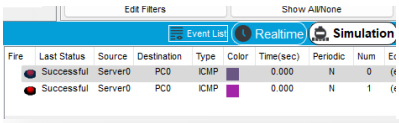
Verify exclusive access from management station PC-C

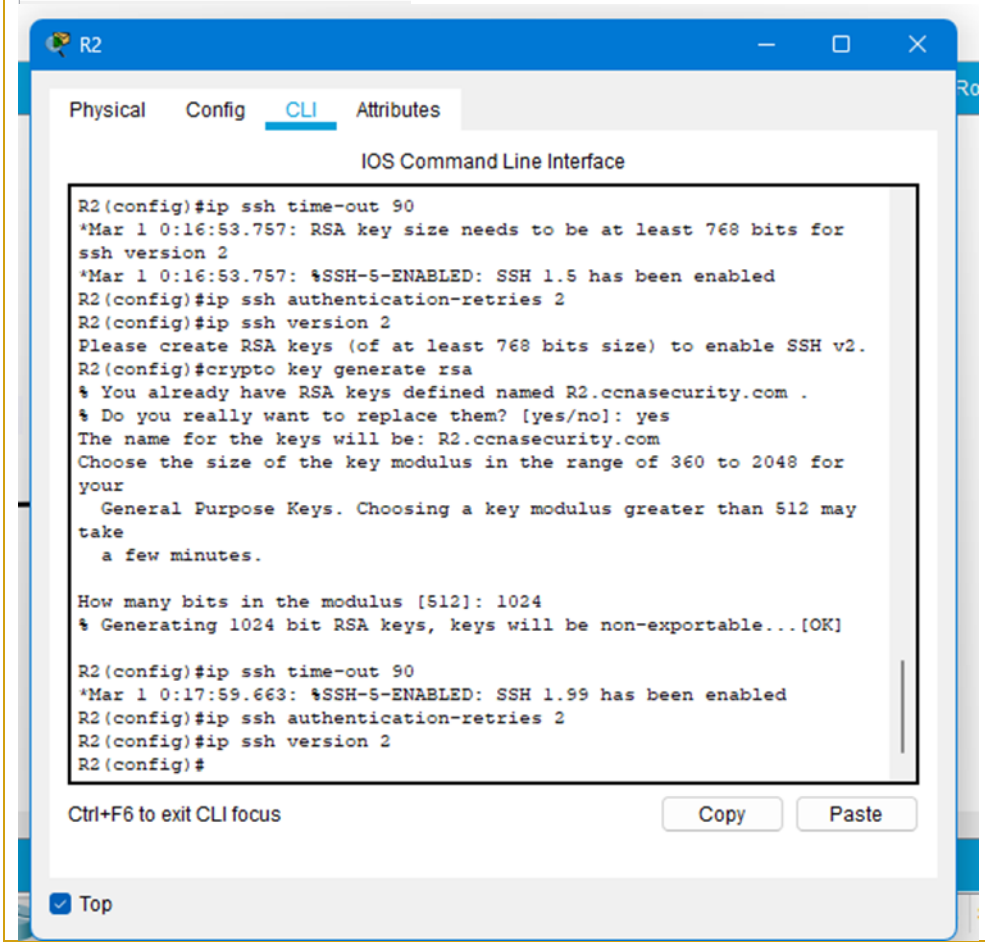
Establish an SSH session to 192.168.2.1 from PC-C (should be successful).

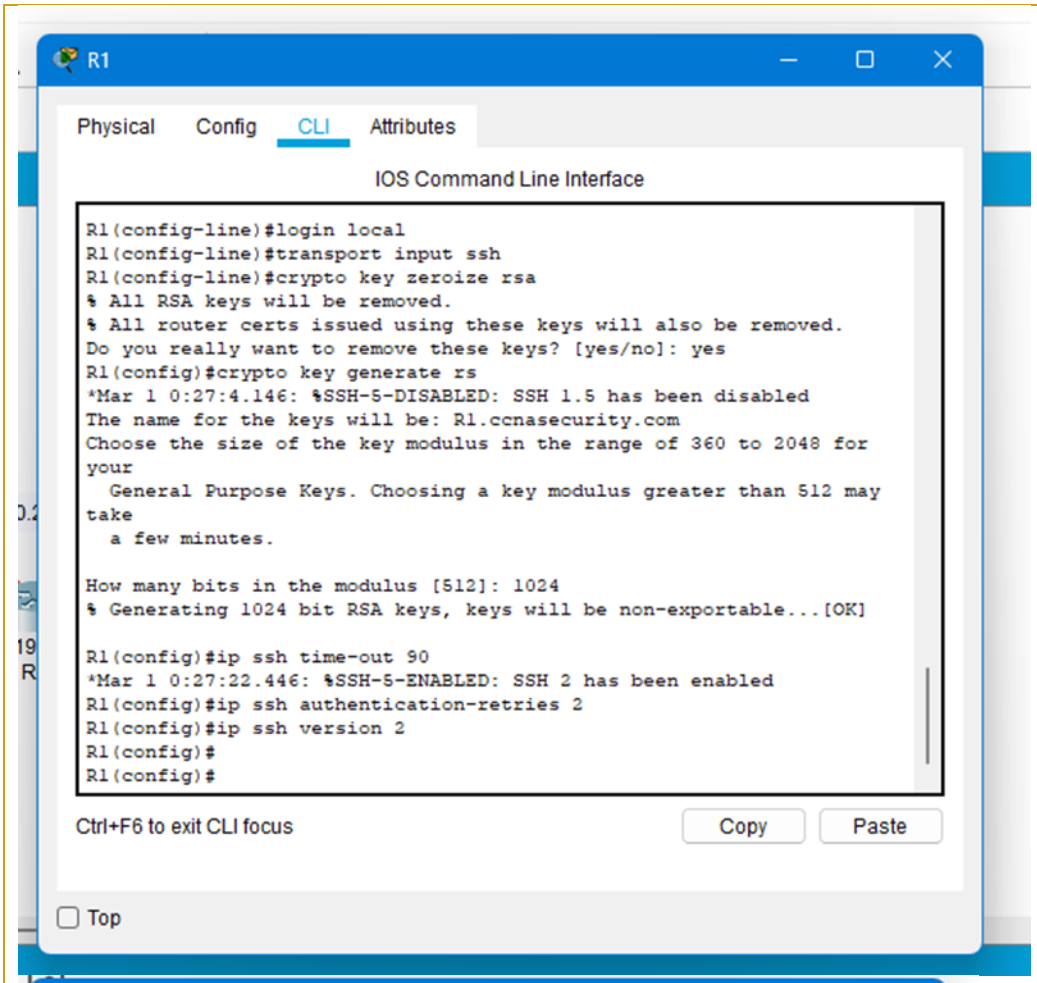
```
ssh –l SSHadmin 192.168.2.1
```

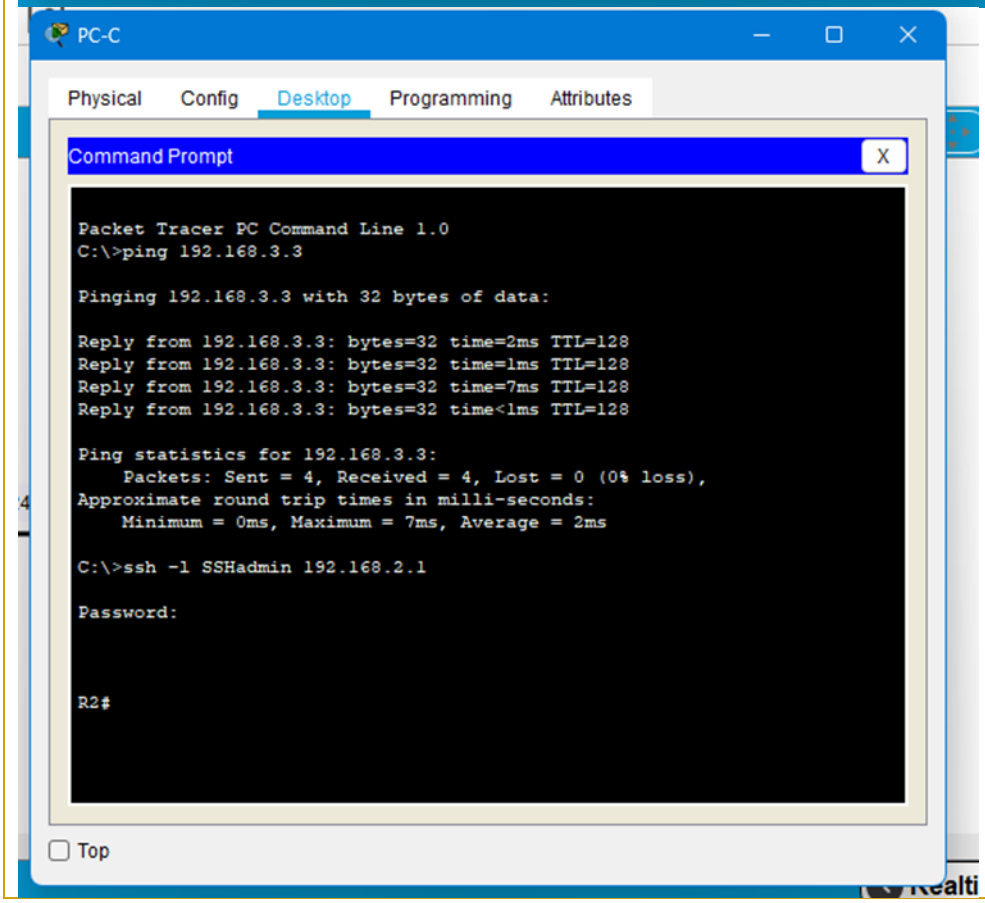
Establish an SSH session to 192.168.2.1 from PC-A (should fail).

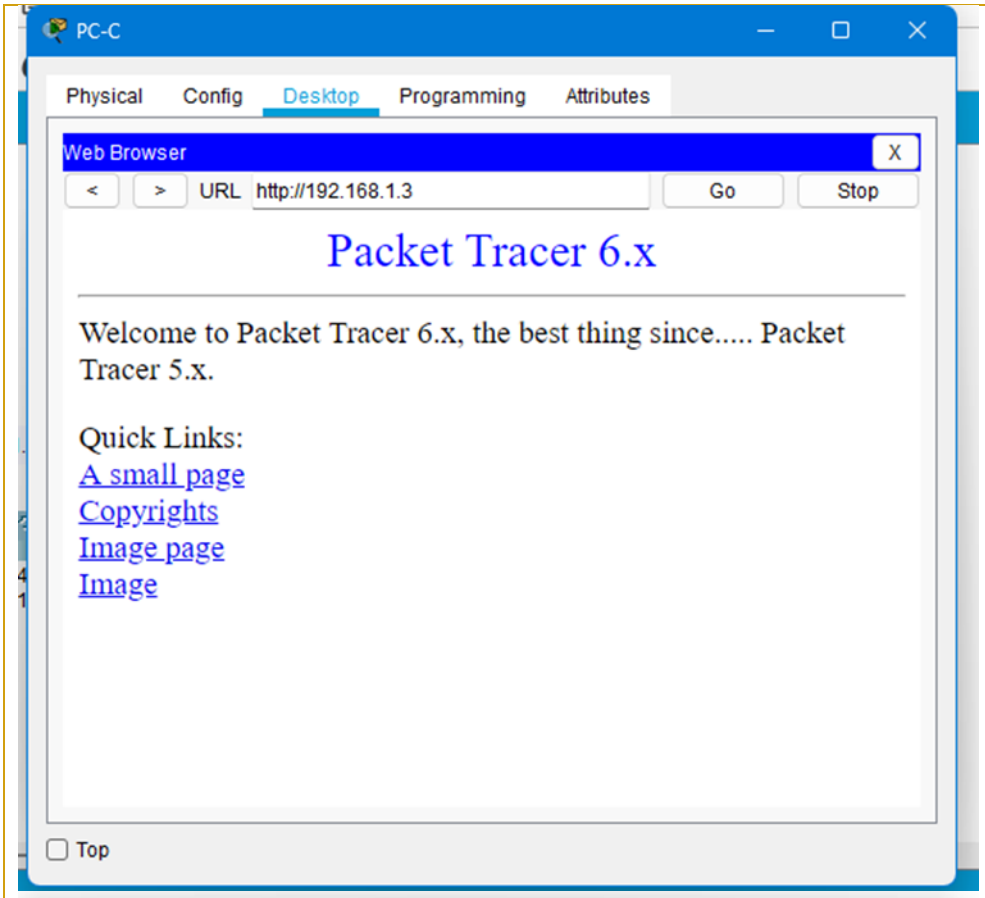

1941
R2
10.1.1.0/30
10.2.2.0/30
192.168.1.0/24
192.168.3.0/24
2960-24TT
S1
1941
R1
1941
R3
2960-24TT
S3
Server-PT
PC-A
PC-PT
PC-C

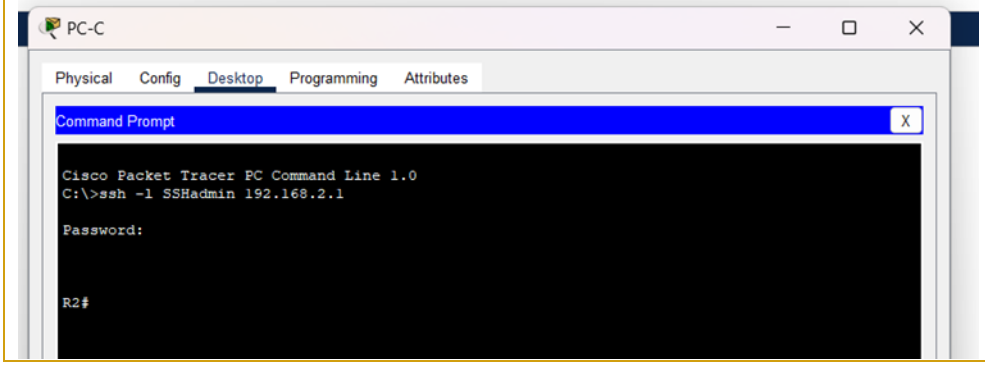

Edit Filters
Show All/None
Event List
Realtime
Simulation
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Successful
Server0
PC0
ICMP
0.000
N
0
Successful
Server0
PC0
ICMP
0.000
N
1


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
R2(config)#ip ssh time-out 90
*Mar 1 0:16:53.757: RSA key size needs to be at least 768 bits for
ssh version 2
*Mar 1 0:16:53.757: %SSH-5-ENABLED: SSH 1.5 has been enabled
R2(config)#ip ssh authentication-retries 2
R2(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R2(config)#crypto key generate rsa
% You already have RSA keys defined named R2.ccnasecurity.com .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: R2.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
General Purpose Keys. Choosing a key modulus greater than 512 may
take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R2(config)#ip ssh time-out 90
*Mar 1 0:17:59.663: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#ip ssh authentication-retries 2
R2(config)#ip ssh version 2
R2(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#crypto key zeroize rsa
% All RSA keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
R1(config)#crypto key generate rs
*Mar 1 0:27:4.146: %SSH-5-DISABLED: SSH 1.5 has been disabled
The name for the keys will be: R1.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
General Purpose Keys. Choosing a key modulus greater than 512 may
take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#ip ssh time-out 90
*Mar 1 0:27:22.446: %SSH-5-ENABLED: SSH 2 has been enabled
R1(config)#ip ssh authentication-retries 2
R1(config)#ip ssh version 2
R1(config)#
R1(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


PC-C
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=2ms TTL=128
Reply from 192.168.3.3: bytes=32 time=1ms TTL=128
Reply from 192.168.3.3: bytes=32 time=7ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.3.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 7ms, Average = 2ms
C:\>ssh -l SSHadmin 192.168.2.1
Password:
R2#
Top





3 Create a Numbered IP ACL 120 on R1
4 Modify an Existing ACL on R1

Create a Numbered IP ACL 120 on R1

Step 1: Verify that PC-C can access the PC-A via HTTPS using the web browser.

Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.

```
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 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
```

For PC A set HTTP services off and HTTPS on

Verify that PC-C can access the PC-A via HTTPS using the web browser.

Step 3: Apply the ACL to interface S0/0/0.

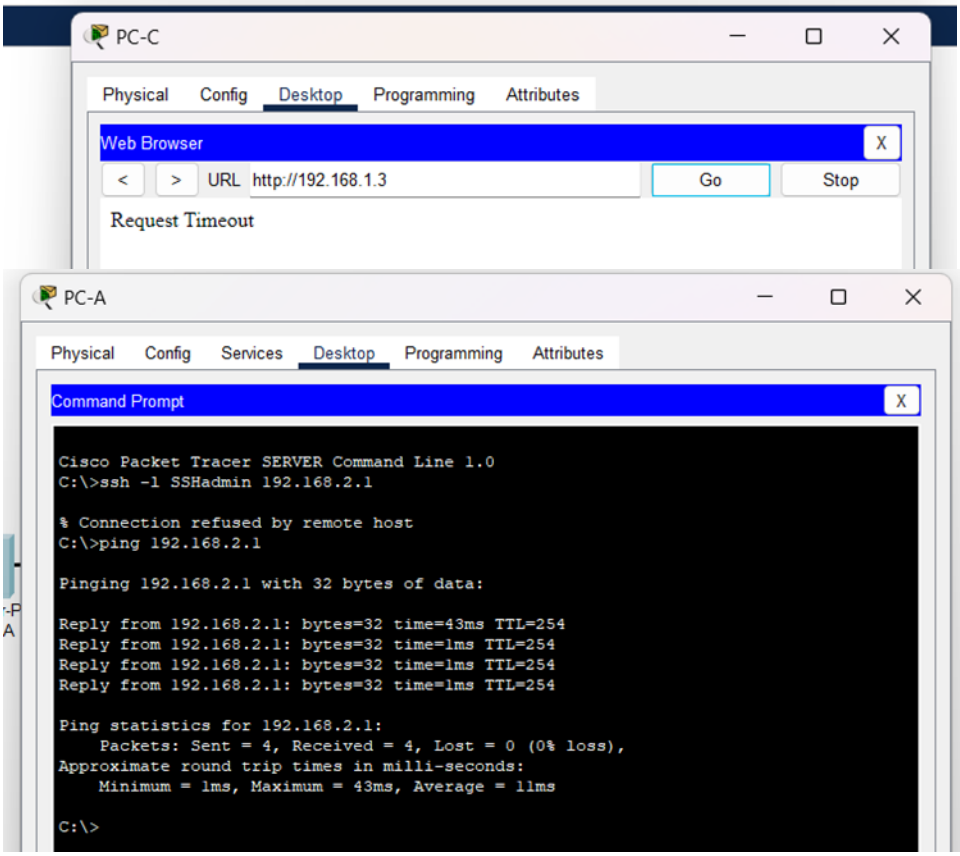
```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 120 in
```

Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser.

Modify an Existing ACL on R1

Step 1: Make any necessary changes to ACL 120 to permit and deny the specified traffic.

R1(config)# access-list 120 permit icmp any any echo-reply
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



5 Create a Numbered IP ACL 110 on R3
6 Create a Numbered IP ACL 100 on R3

Create a Numbered IP ACL 110 on R3

Step 1: Configure ACL 110 to permit only traffic from the inside network.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 any

Step 2: Apply the ACL to interface G0/1

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

Create a Numbered IP ACL 100 on R3

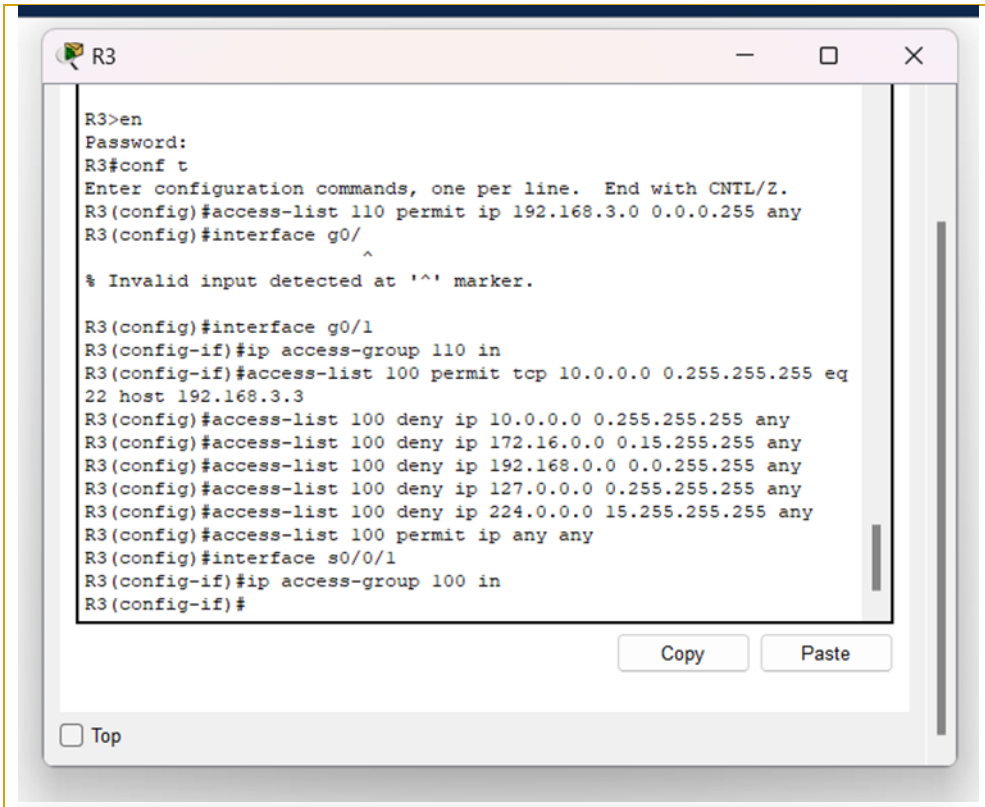
Step 1: Configure ACL 100 to block all specified traffic from the outside network.

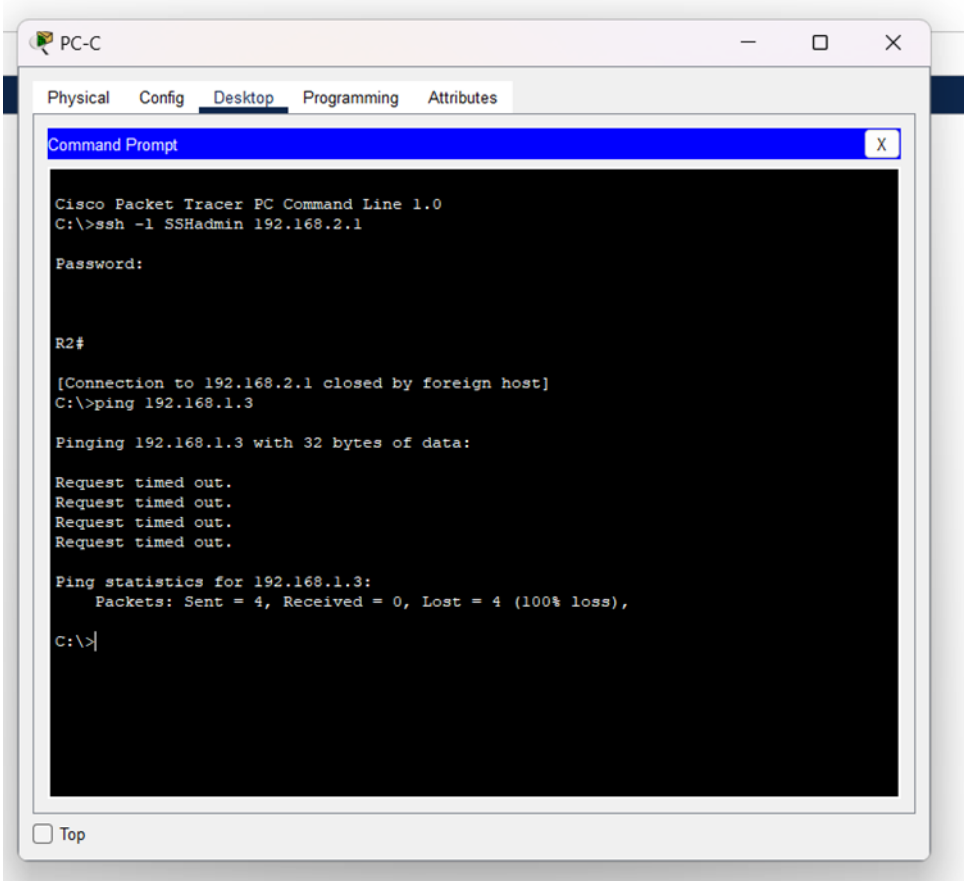
R3(config)# access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3
R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)# access-list 100 permit ip any any

Step 2: Apply the ACL to interface Serial 0/0/1.

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

Step 3: Check results.


R3
R3>en
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)#interface g0/
^
% Invalid input detected at '^' marker.
R3(config)#interface g0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#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 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#
Copy
Paste
Top


PC-C
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l SSHadmin 192.168.2.1
Password:
R2#
[Connection to 192.168.2.1 closed by foreign host]
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:\>
Top