Date: 31/01/2024 **Security in Computing**

Practical 4:

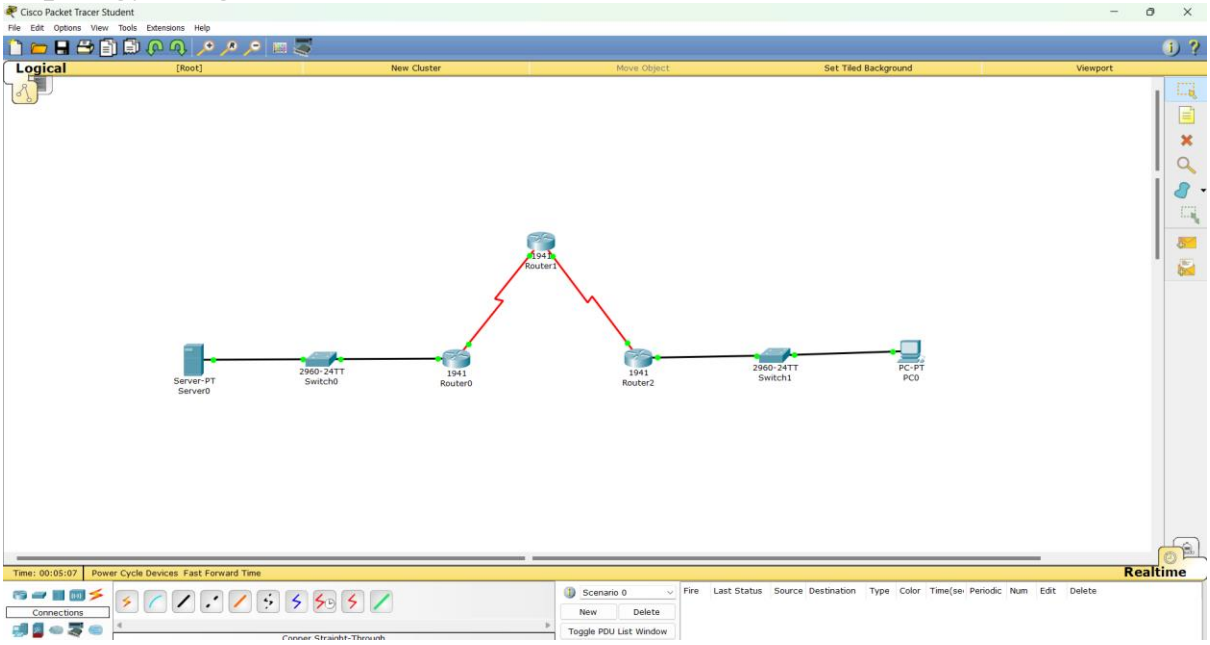
Aim: Configure IP ACLs to Mitigate Attacks

a. Verify connectivity among devices before firewall configuration.

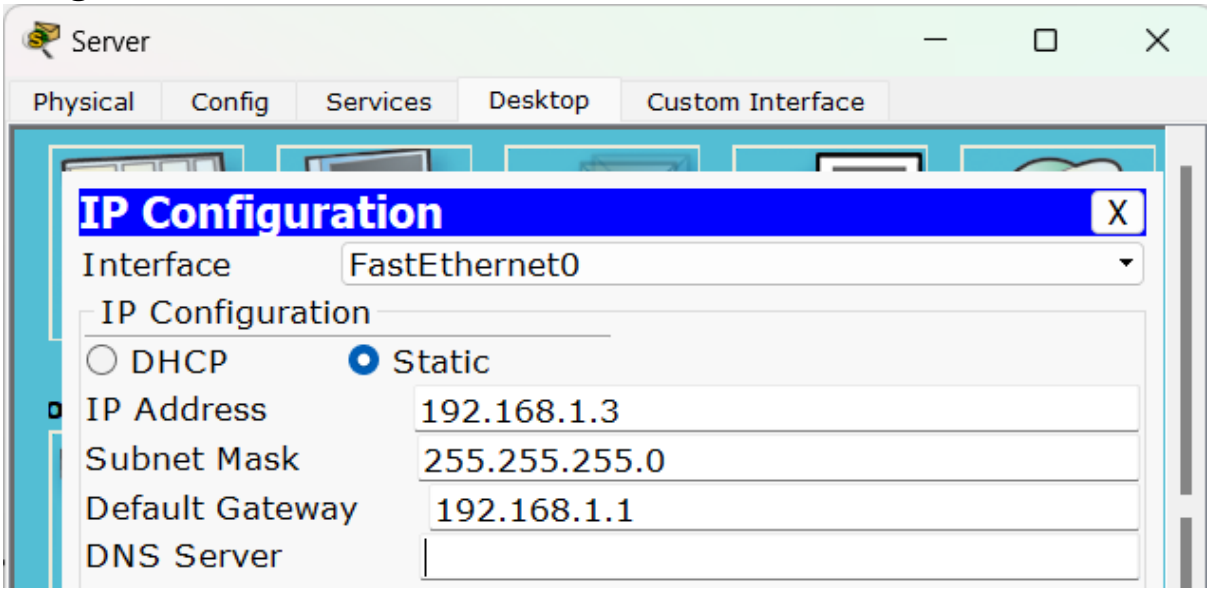
b. Use ACLs to ensure remote access to the routers Is available only from management station PC-c.

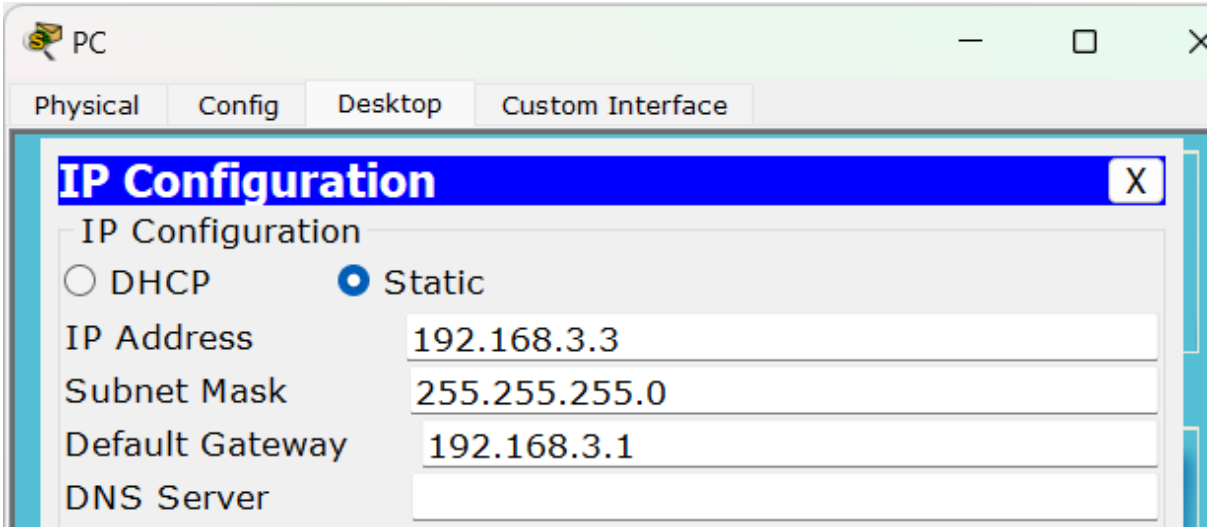
C Configure ACLs on to mitigate attacks.

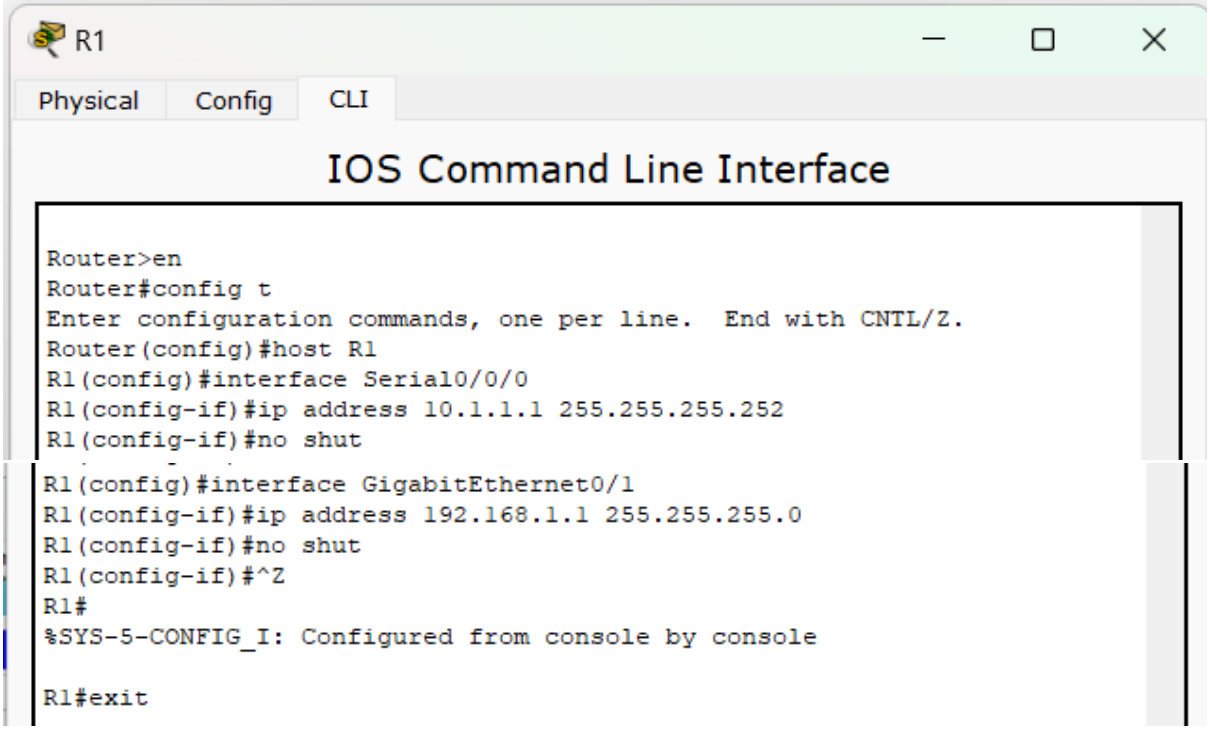
- **Topology Diagram**



- **Assign IP Addresses**




PC
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.3.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.1
DNS Server


R1
Physical
Config
CLI
IOS Command Line Interface
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R1
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#no shut
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit

R2

Physical Config CLI

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R2
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#interface Serial0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#int loopback1

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

R3

Physical Config CLI

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R3
R3(config)#interface Serial0/0/0
R3(config-if)#interface Serial0/0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shut
R3(config-if)#interface GigabitEthernet0/1
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

➢ Displaying IP Address Details of Routers

R1

Physical | Config | CLI

IOS Command Line Interface

```
R1>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES manual administratively down down

GigabitEthernet0/1     192.168.1.1     YES manual up                    up

Serial0/0/0            10.1.1.1        YES manual up                    up

Serial0/0/1            unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
```

R2

Physical | Config | CLI

IOS Command Line Interface

```
R2>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  administratively down down

GigabitEthernet0/1     unassigned      YES unset  administratively down down

Serial0/0/0            10.1.1.2        YES manual up                    up

Serial0/0/1            10.2.2.2        YES manual up                    up

Loopback1              192.168.2.1     YES manual up                    up

Vlan1                  unassigned      YES unset  administratively down down
```

R3

Physical | Config | CLI

IOS Command Line Interface

```
R3>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  administratively down down

GigabitEthernet0/1     192.168.3.1     YES manual up                    up

Serial0/0/0            unassigned      YES unset  administratively down down

Serial0/0/1            10.2.2.1        YES manual up                    up

Vlan1                  unassigned      YES unset  administratively down down
R3>
```

➢ Configure RIP on routers

R1

Physical | Config | CLI

IOS Command Line Interface

```
R1>en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.1.1.0
R1(config-router)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

R2

Physical | Config | CLI

IOS Command Line Interface

```
R2>en
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 10.1.1.0
R2(config-router)#network 10.2.2.0
R2(config-router)#network 192.168.2.0
R2(config-router)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

R3

Physical | Config | CLI

IOS Command Line Interface

```
R3>en
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 10.2.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

- **Displaying routing table of routers**

R1

Physical | Config | CLI

IOS Command Line Interface

```
R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:05, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R    192.168.2.0/24 [120/1] via 10.1.1.2, 00:00:05, Serial0/0/0
R    192.168.3.0/24 [120/2] via 10.1.1.2, 00:00:05, Serial0/0/0
R1>
```

R2

Physical | Config | CLI

IOS Command Line Interface

```
R2>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R    192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:17, Serial0/0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, Loopback1
L       192.168.2.1/32 is directly connected, Loopback1
R    192.168.3.0/24 [120/1] via 10.2.2.1, 00:00:19, Serial0/0/1
R2>
```

R3

Physical | Config | CLI

IOS Command Line Interface

```
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:18, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
R    192.168.1.0/24 [120/2] via 10.2.2.2, 00:00:18, Serial0/0/1
R    192.168.2.0/24 [120/1] via 10.2.2.2, 00:00:18, Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/1
L       192.168.3.1/32 is directly connected, GigabitEthernet0/1
R3>
```

- **Configure SSH on R2**

R2

Physical | Config | CLI

IOS Command Line Interface

```
R2>en
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip domain-name securityincomputing.com
R2(config)#username admin secret pwd
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#crypto key zeroize rsa
% No Signature RSA Keys found in configuration.

R2(config)#crypto key generate rsa
The name for the keys will be: R2.securityincomputing.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 0:37:42.439:  %SSH-5-ENABLED: SSH 2 has been enabled
R2(config)#ip ssh authentication-retries 2
R2(config)#ip ssh version 2
R2(config)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

- **Verify Basic Network Connectivity before ACL Configuration**

Server

Physical | Config | Services | Desktop | Custom Interface

Command Prompt

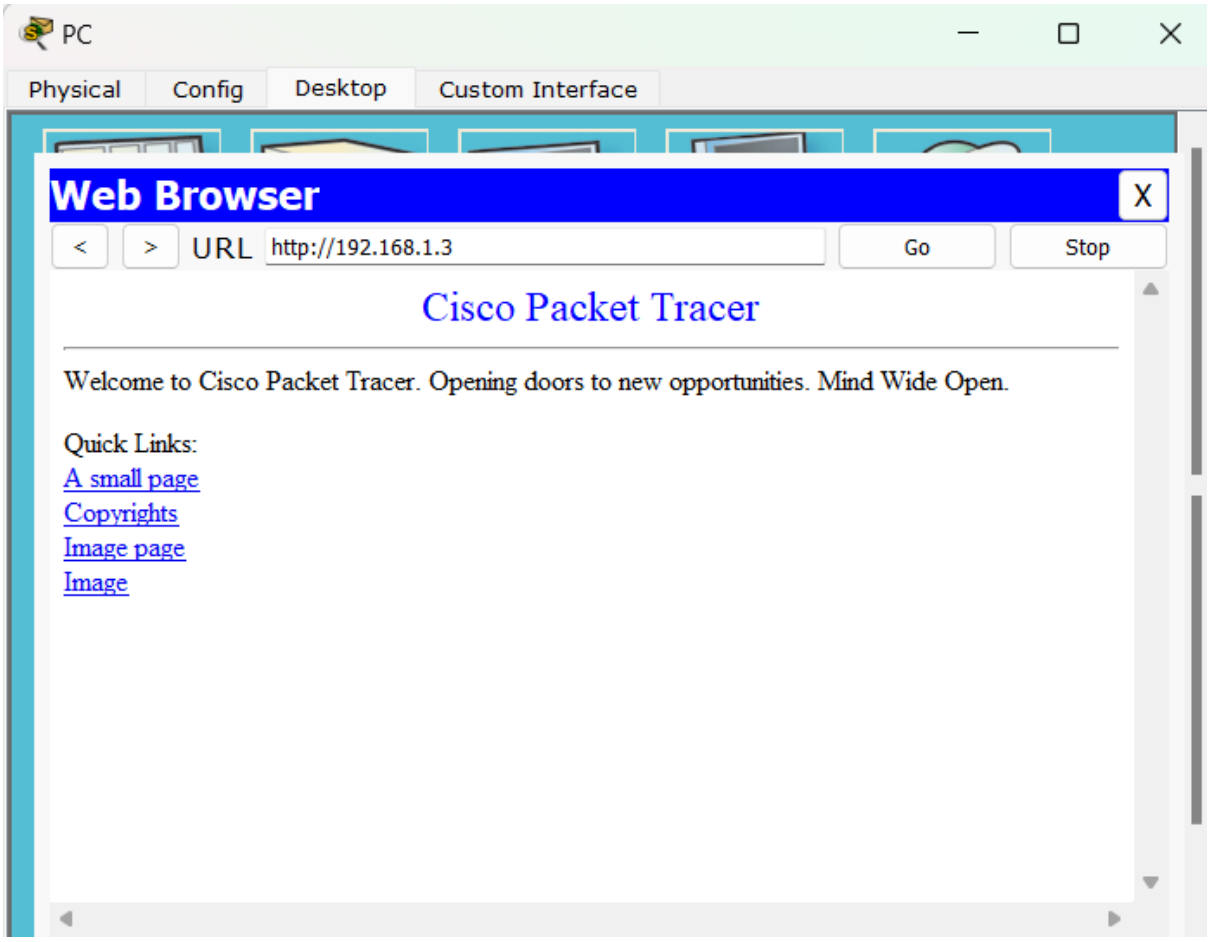
```
SERVER>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms 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 = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

SERVER>ssh -l admin 192.168.2.1
Open
Password:



R2>exit

[Connection to 192.168.2.1 closed by foreign host]
SERVER>
```

PC

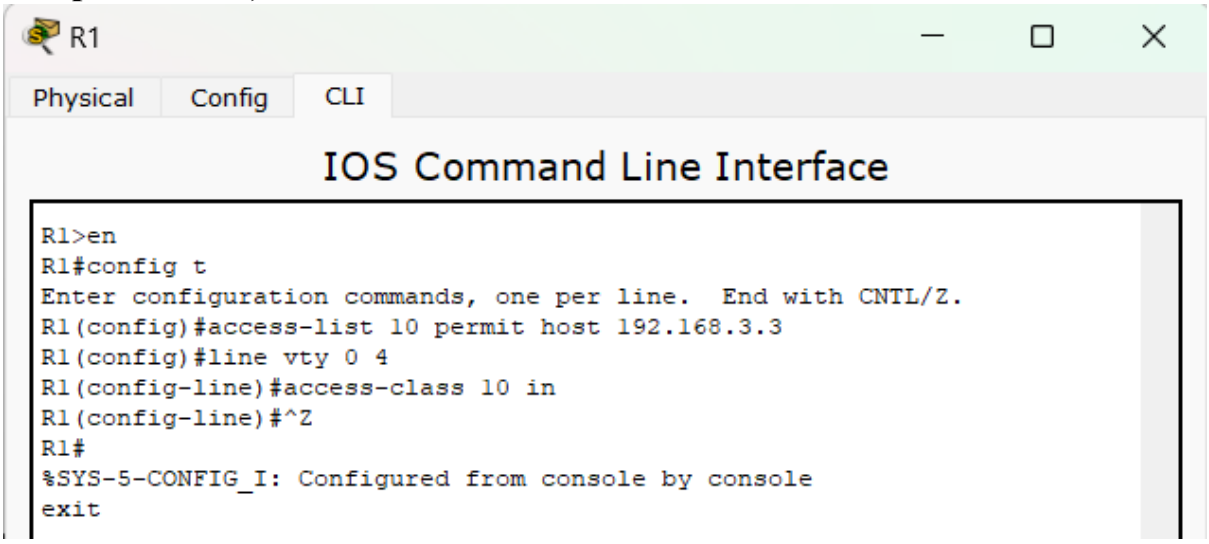
Physical | Config | Desktop | Custom Interface

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=13ms TTL=125
Reply from 192.168.1.3: bytes=32 time=3ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 13ms, Average = 5ms

PC>ssh -l admin 192.168.2.1
Open
Password:



R2>exit

[Connection to 192.168.2.1 closed by foreign host]
PC>
```



- **Configure ACL on routers (block all remote access to the routers except from PC)**



R2

Physical | Config | CLI

IOS Command Line Interface

```
R2>en
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 10 permit host 192.168.3.3
R2(config)#access-class 10 in
                         ^
% Invalid input detected at '^' marker.

R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

R3

Physical | Config | CLI

IOS Command Line Interface

```
R3>en
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 10 permit host 192.168.3.3
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

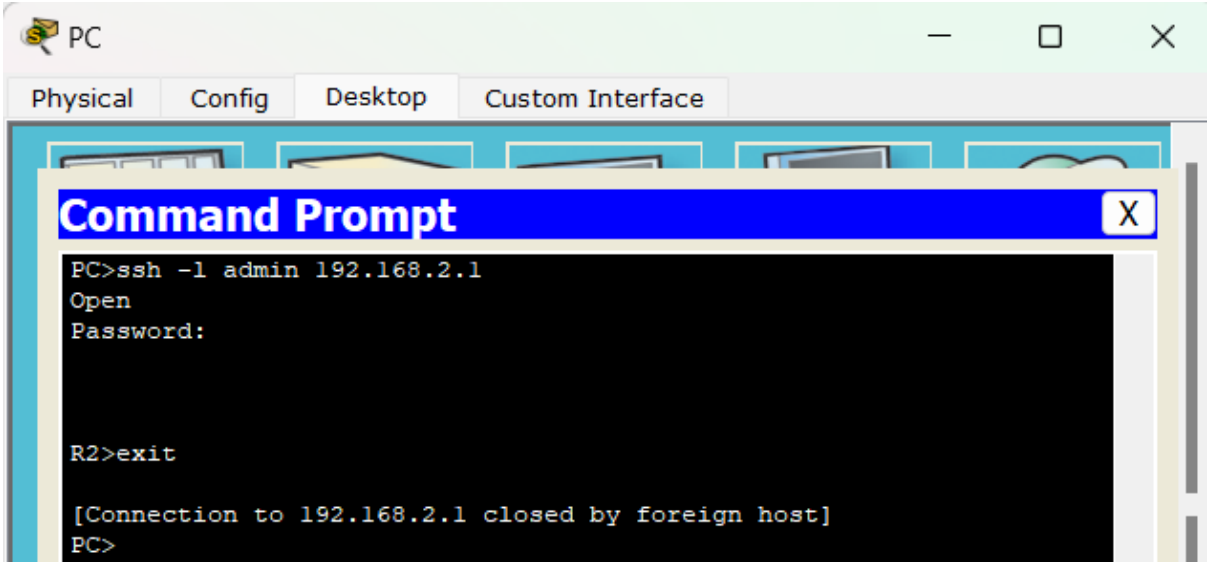
- **Verifying the working of ACL**

Server

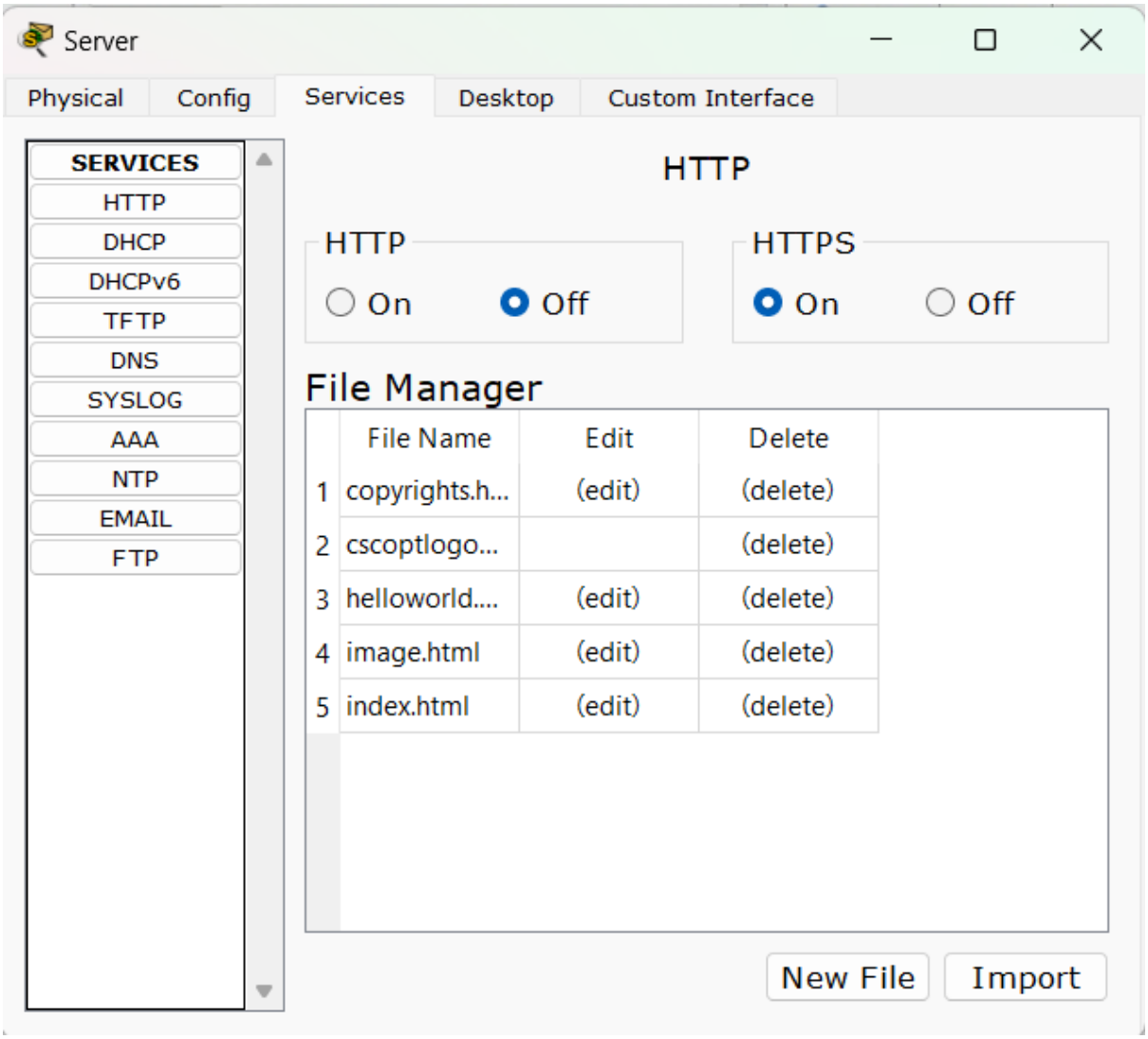
Physical | Config | Services | Desktop | Custom Interface

Command Prompt

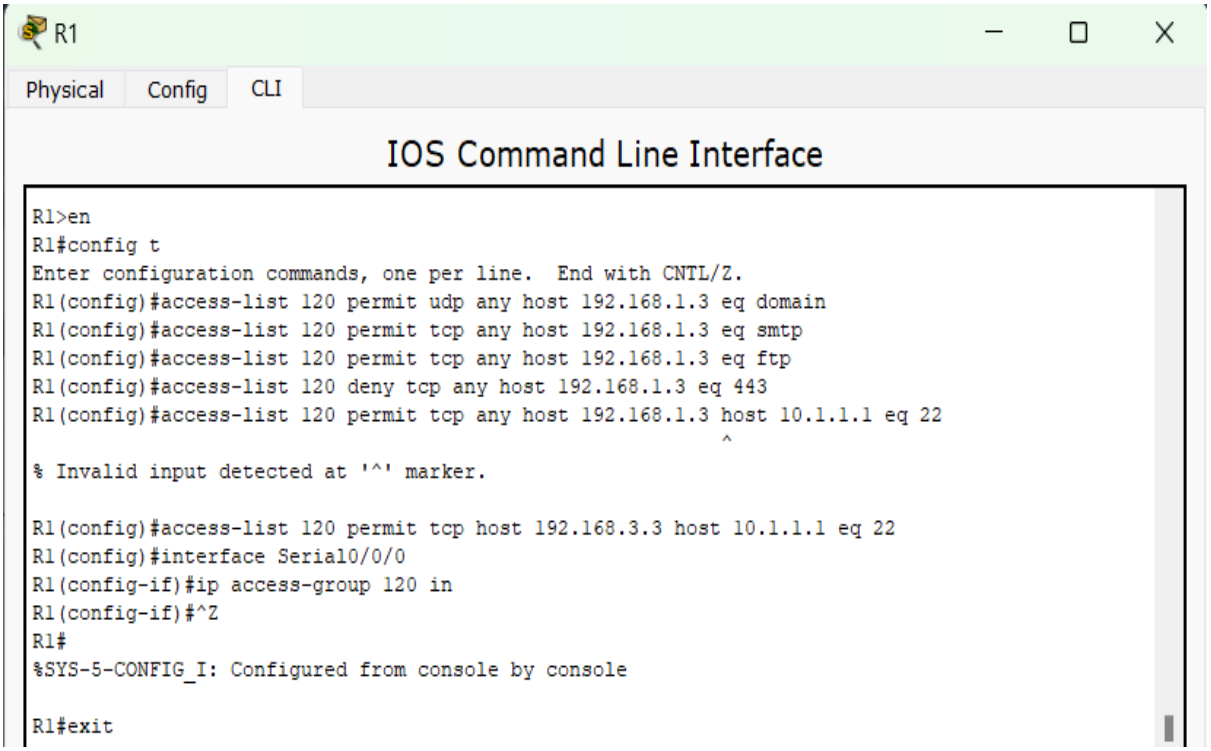
```
SERVER>ssh -l admin 192.168.2.1

% Connection refused by remote host
SERVER>
```



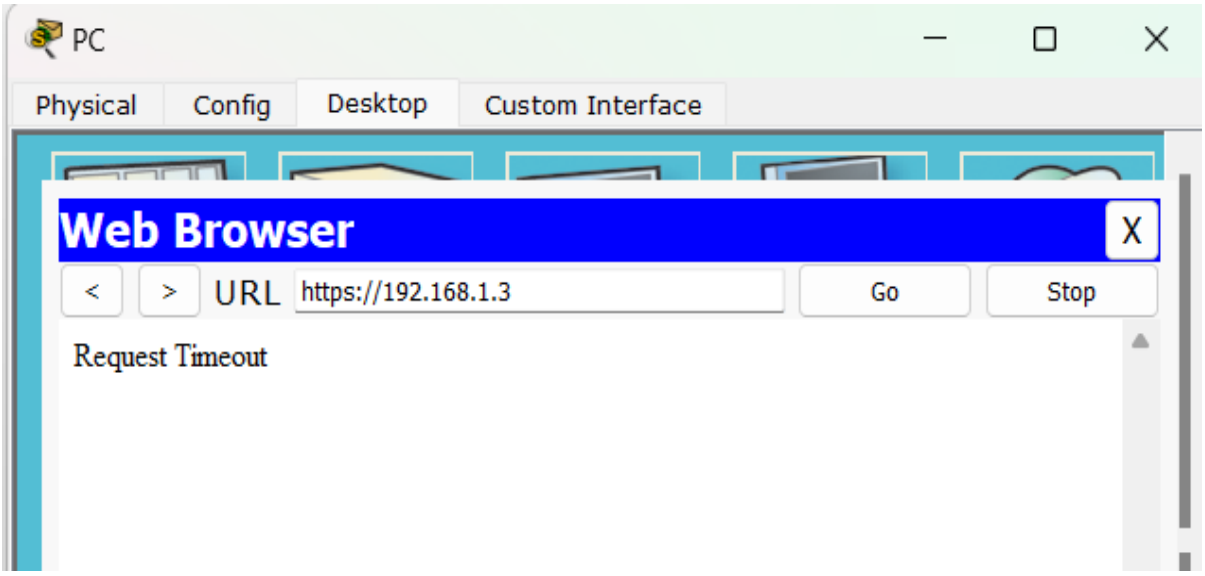
- **Disable HTTP and enable HTTPS on server**



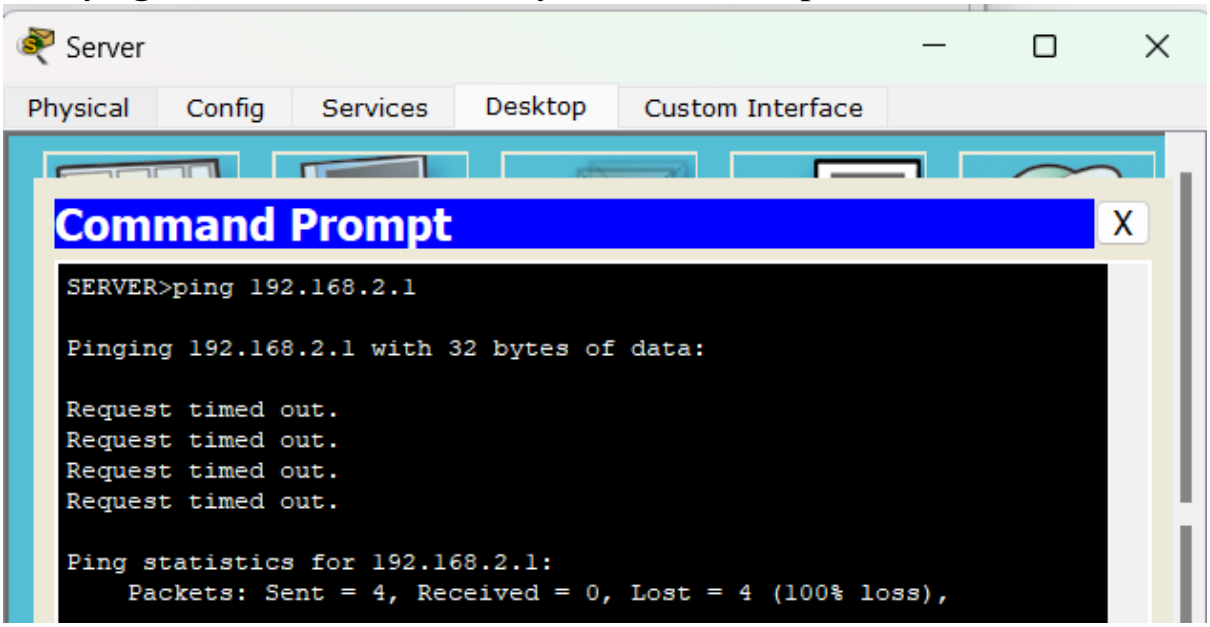
- **Configure ACL on routers**
  - Permit any outside host to access DNS, SMTP, and FTP services on Server
  - Deny any outside host access to HTTPS services on Server.
  - Permit PC to access RI via SSH.



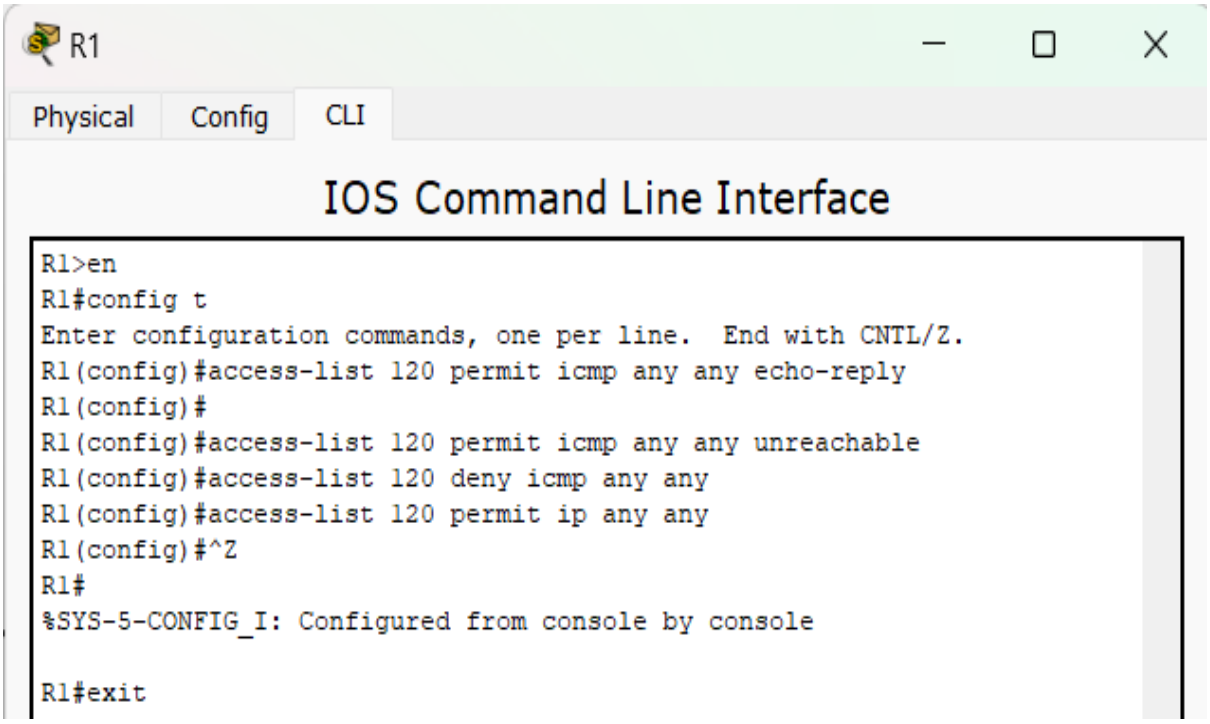
- **Verifying the working of ACL**



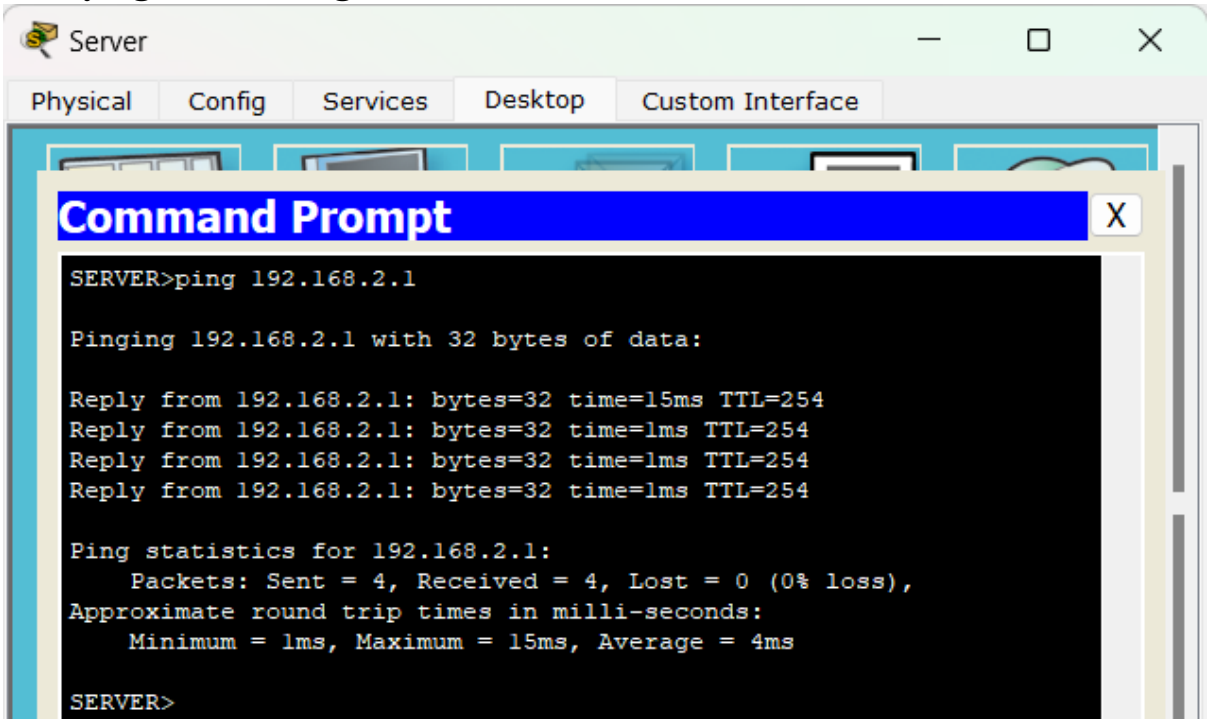
- **Verifying the network connectivity before ACL implementation**



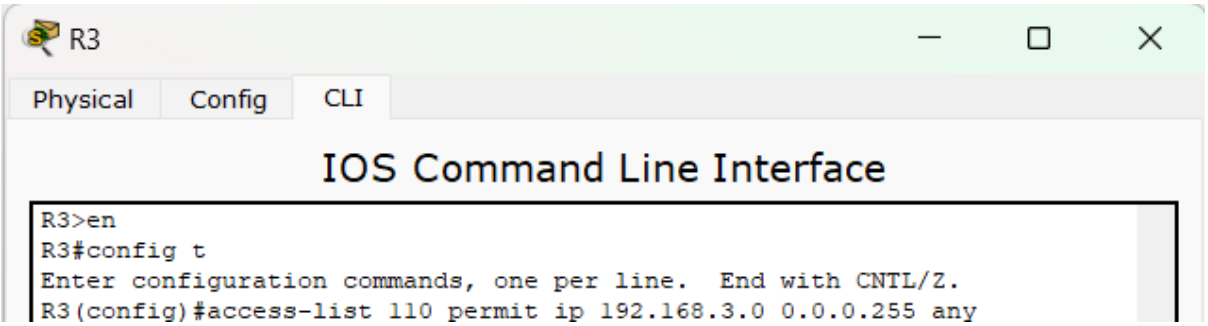
- **Modify an Existing ACL on R1**
  - (Permit ICMP echo replies and destination unreachable messages from the outside network. Deny all the other incoming ICMP packets.

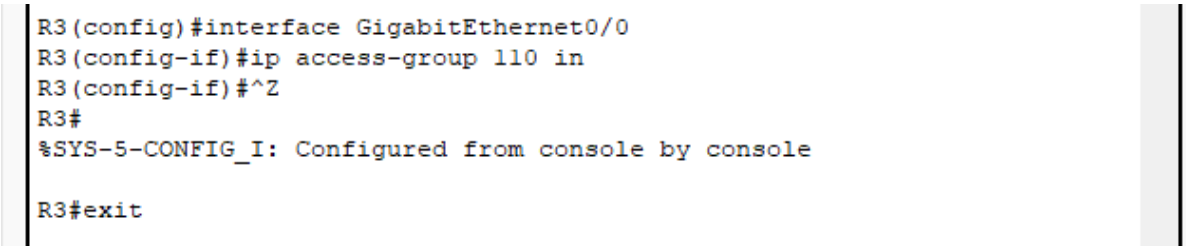


- **Verifying the working of ACL**



- **Configure ACL on routers**
  - (Deny all outbound packets with source address outside the range of internal IP addresses on R3)





- **Configure ACL on routers**
  - (On Rs, block all packets containing the source IP address from the following pool of addresses: private addresses, 127.0.0.0/8, and any IP multicast address. Permit SSH traffic from the 10.0.0.0/8 network to return to the host PC)

R3

Physical | Config | CLI

IOS Command Line Interface

```
R3>en
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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 permit3344 tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3
                                         ^
% Invalid input detected at '^' marker.

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 permit ip any any
R3(config)#interface Serial0/0/0
R3(config-if)#ip access-group 100 in
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

PC

Physical | Config | Desktop | Custom Interface

Command Prompt

```
PC>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),

PC>ssh -l admin 192.168.2.1

% Connection timed out; remote host not responding
PC>
```