**Date: 12/02/2024** **Security in Computing**

**Practical 4:**

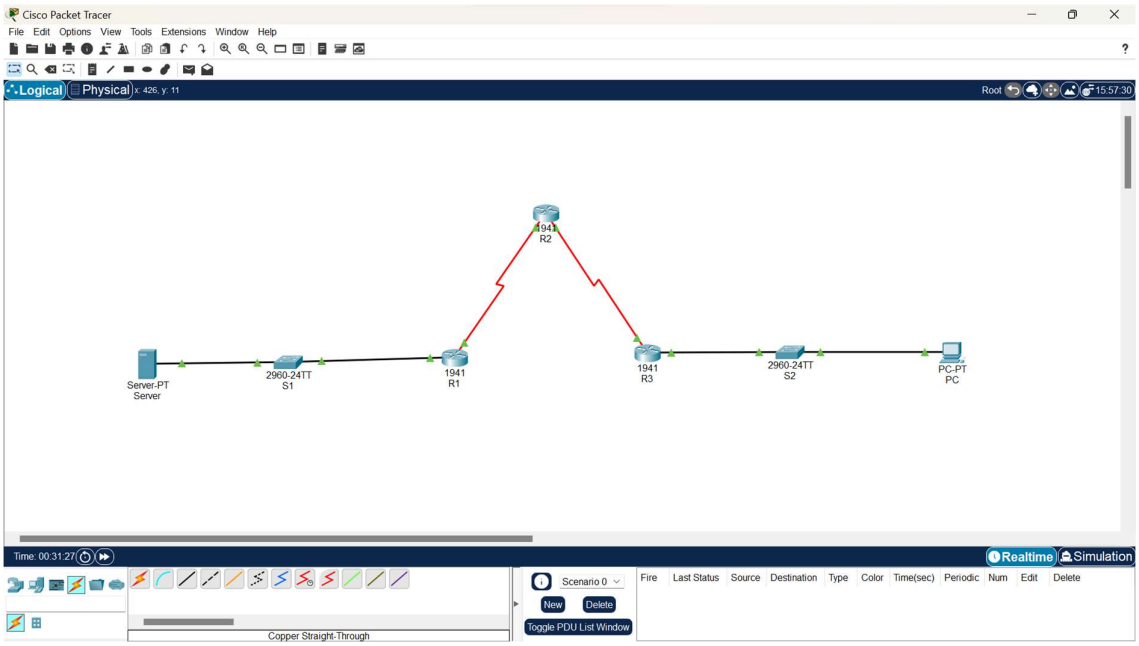
**Aim:** Configure IP ACLs to Mitigate Attacks

a. Verify connectivity among devices before firewall configuration.

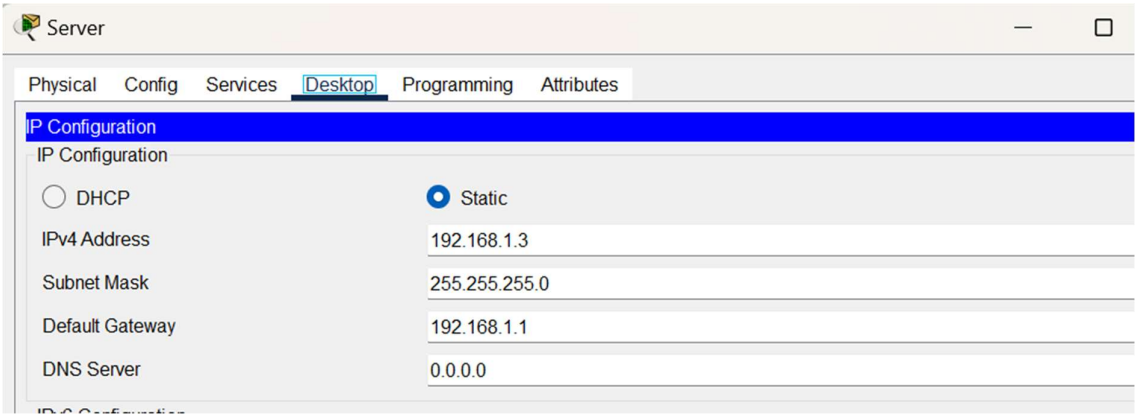
b. Use ACLs to ensure remote access to the routers Is available only from management station PC-c.

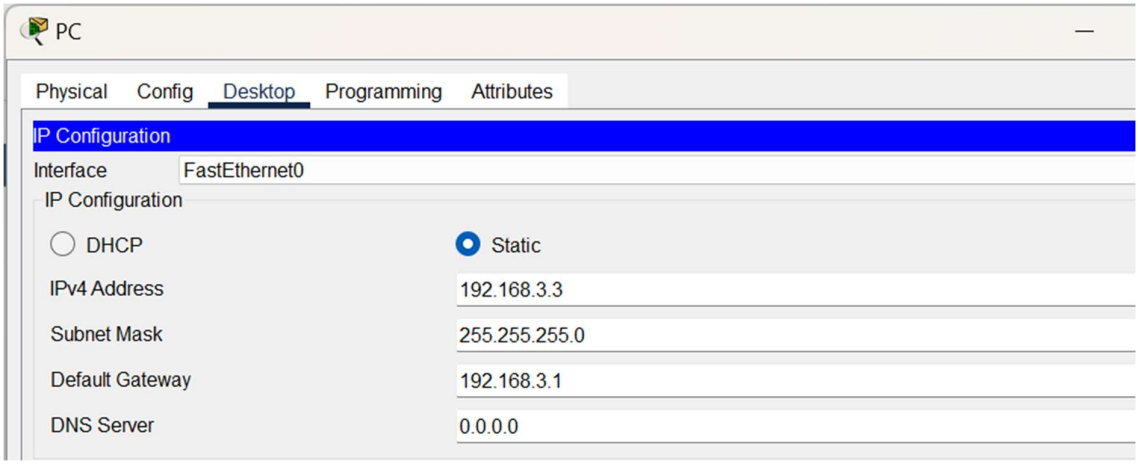
C Configure ACLs on to mitigate attacks.

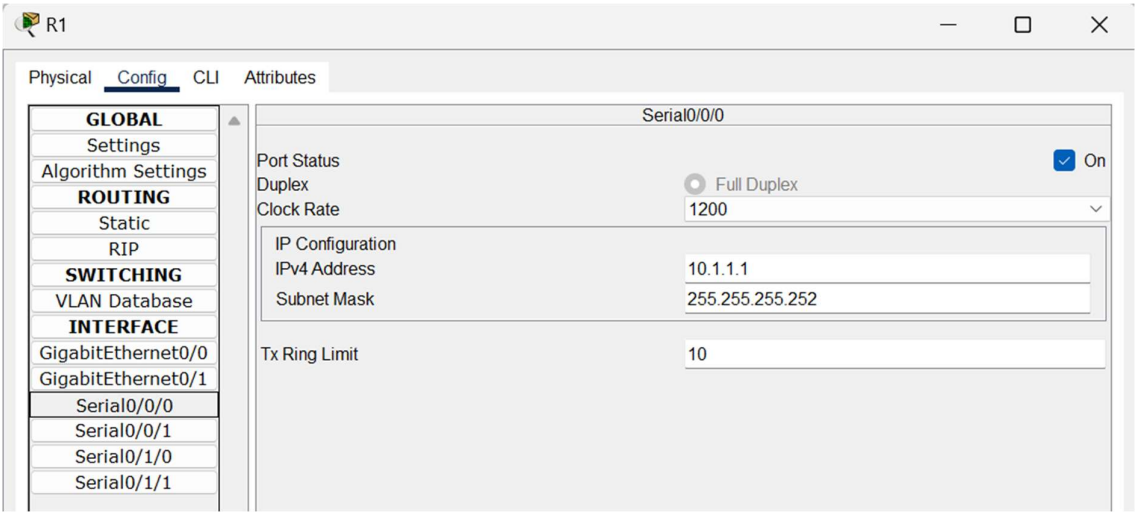
- **Topology Diagram**

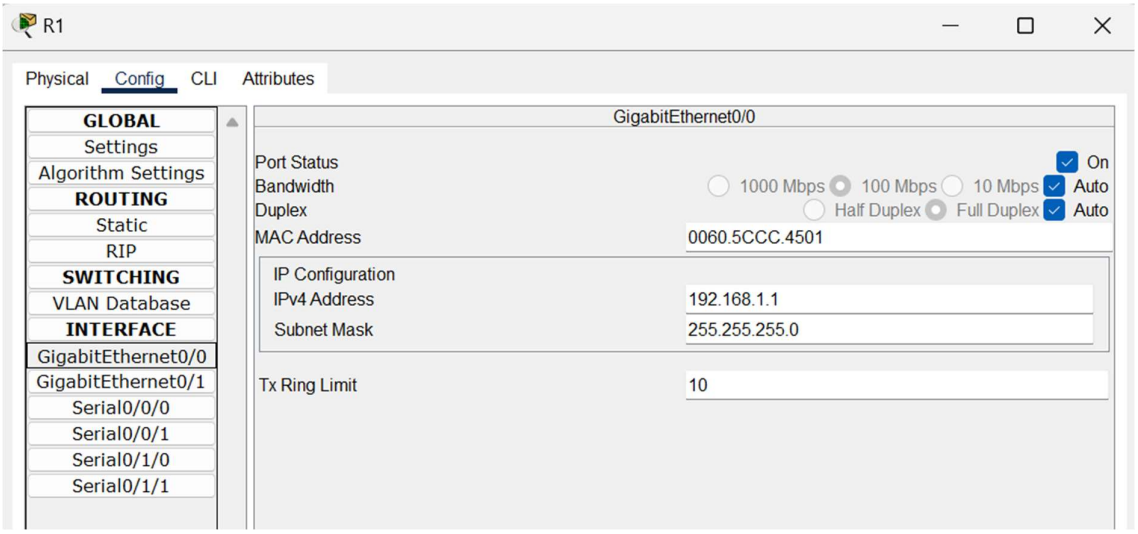


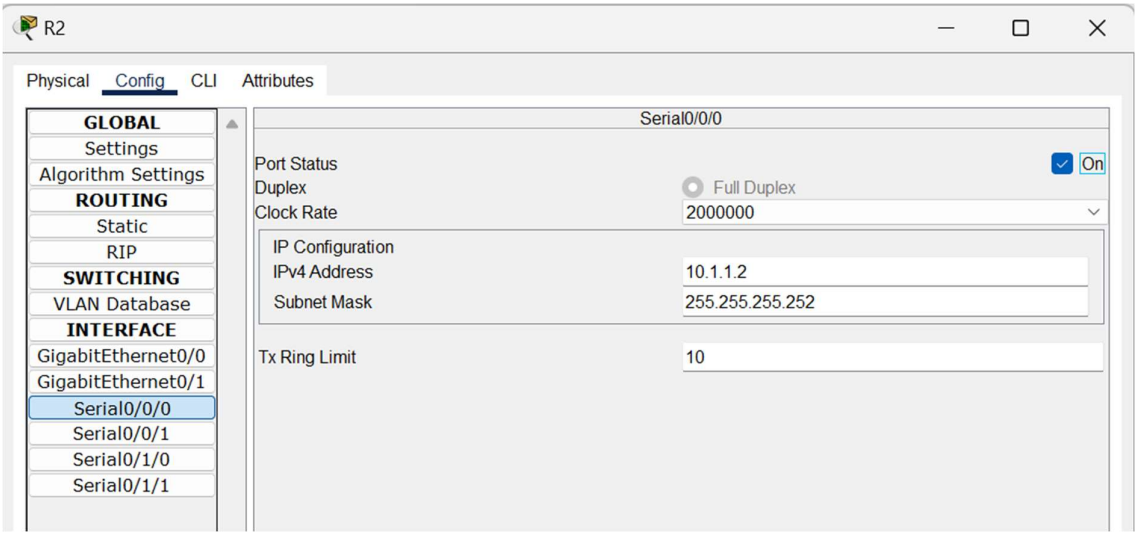

- **Assign IP Addresses**

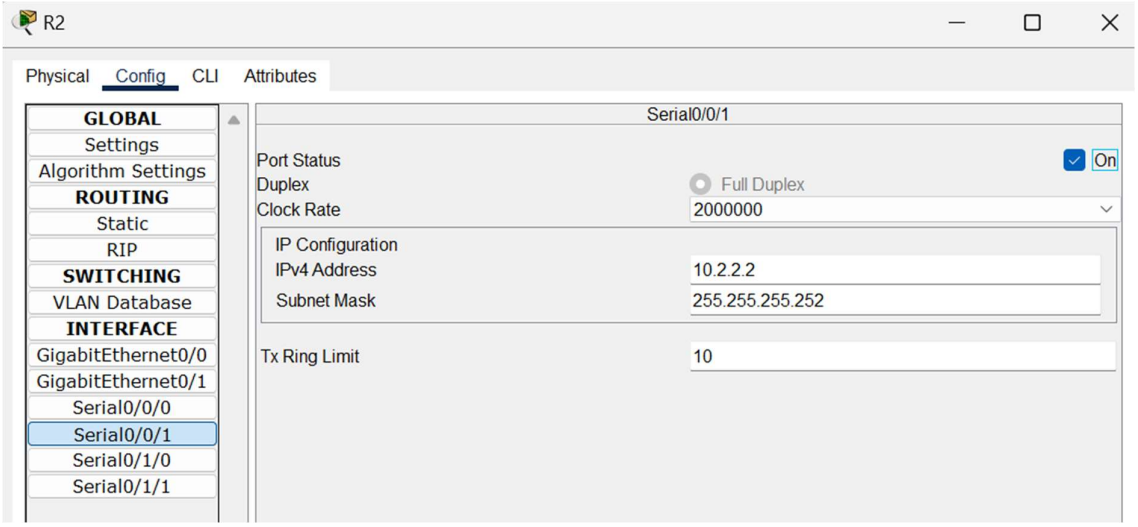


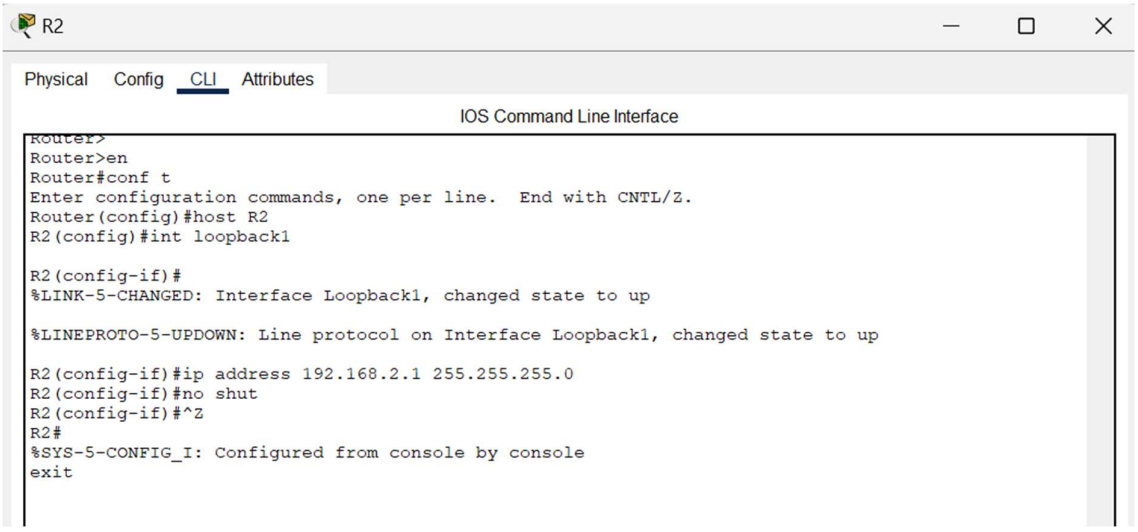

PC
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.3.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.1
DNS Server
0.0.0.0

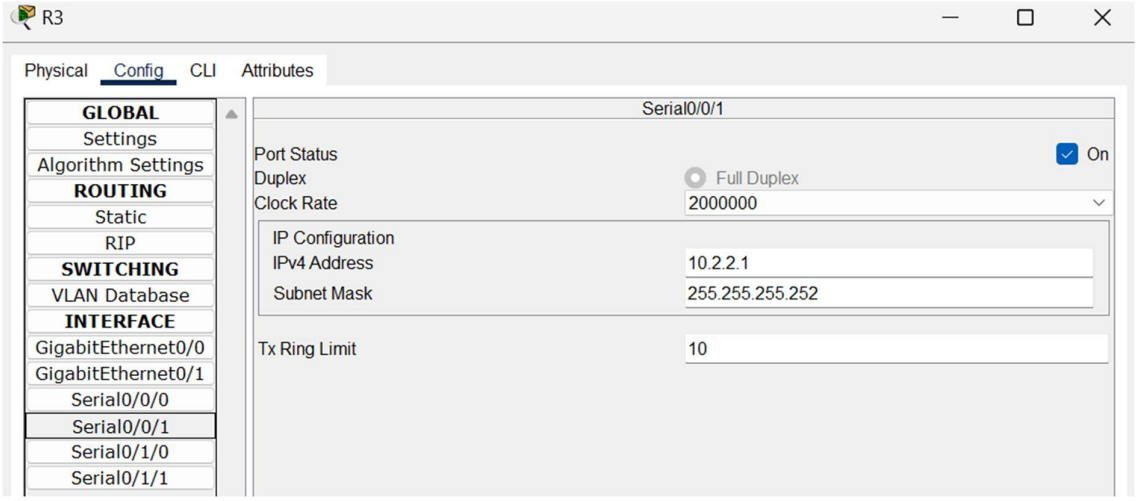

R1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IPv4 Address
10.1.1.1
Subnet Mask
255.255.255.252
Tx Ring Limit
10

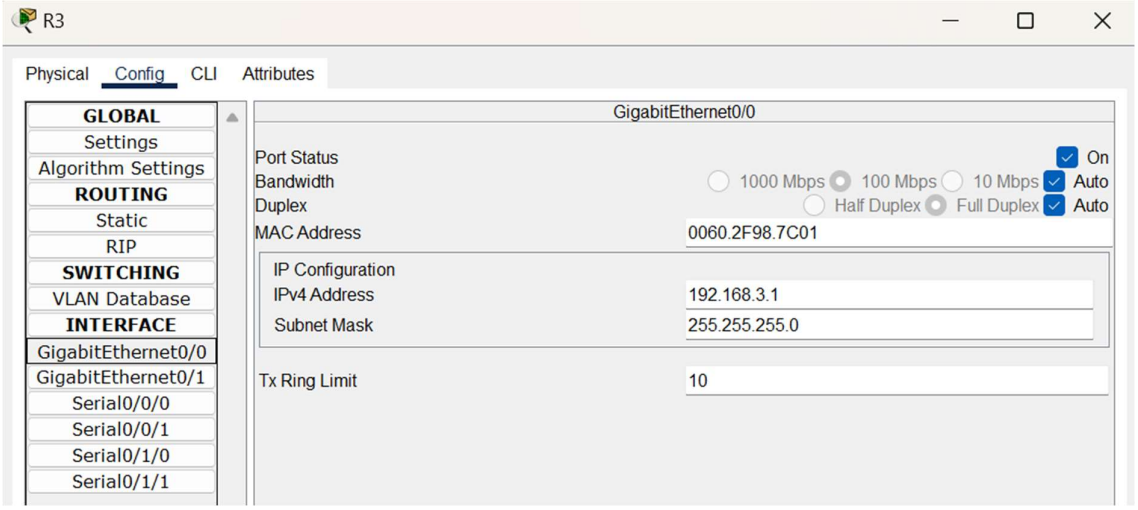

R1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.5CCC.4501
IP Configuration
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10


R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
10.1.1.2
Subnet Mask
255.255.255.252
Tx Ring Limit
10

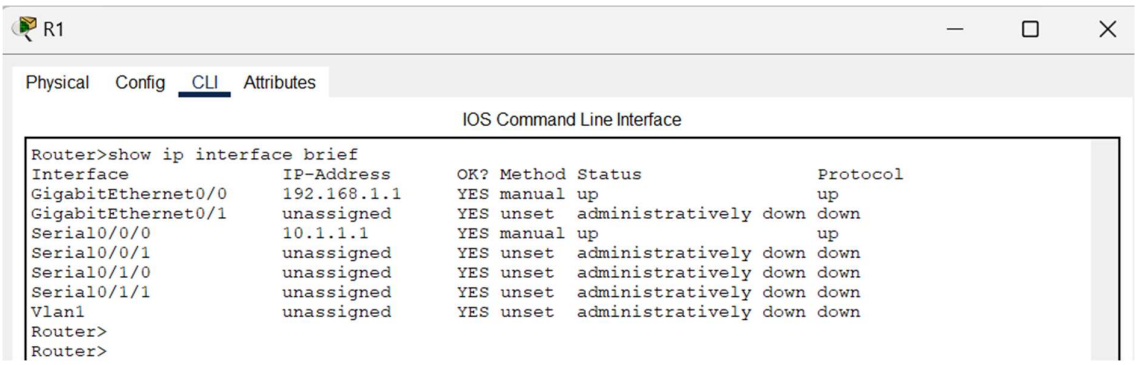

R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Serial0/0/1
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
10.2.2.2
Subnet Mask
255.255.255.252
Tx Ring Limit
10


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R2
R2(config)#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
R2(config-if)#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




## ➢ Displaying IP Address Details of Routers



R2

Physical Config CLI Attributes

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
Serial0/1/0            unassigned      YES unset  administratively down down
Serial0/1/1            unassigned      YES unset  administratively down down
Loopback1              192.168.2.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R2>
R2>
```

R3

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.3.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            unassigned      YES manual administratively down down
Serial0/0/1            10.2.2.1        YES manual up                    up
Serial0/1/0            unassigned      YES unset  administratively down down
Serial0/1/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router>
```

## ➢ Configure RIP on routers

R1

Physical Config CLI Attributes

IOS Command Line Interface

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

R2

Physical Config CLI Attributes

IOS Command Line Interface

```
R2>en
R2#conf 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
exit
```

R3

Physical Config CLI Attributes

IOS Command Line Interface

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

## ➢ Displaying routing table of routers

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>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, 00:00:27, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
R    192.168.2.0/24 [120/1] via 10.1.1.2, 00:00:27, Serial0/0/0
R    192.168.3.0/24 [120/2] via 10.1.1.2, 00:00:27, Serial0/0/0
```

R2

Physical Config CLI Attributes

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, 00:00:07, 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, 00:00:25, Serial0/0/1
```

R3

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>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, 00:00:14, 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, 00:00:14, Serial0/0/1
R    192.168.2.0/24 [120/1] via 10.2.2.2, 00:00:14, Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/30 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
```

## ➢ Configure SSH on R2

R2

Physical Config CLI Attributes

IOS Command Line Interface

```
R2>en
R2#conf 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
% 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
R2(config)#crypto key generate rsa
*Mar 1 0:4:8.504: %SSH-5-DISABLED: SSH 1.5 has been disabled
The name for the keys will be: R2.securityincomputing.com
Choose the size of the key modulus in the range of 360 to 4096 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 0:4:31.407: %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
exit
```

## ➢ Verify Basic Network Connectivity before ACL Configuration

PC-A

Physical Config Services Desktop Programming Attributes

Command Prompt

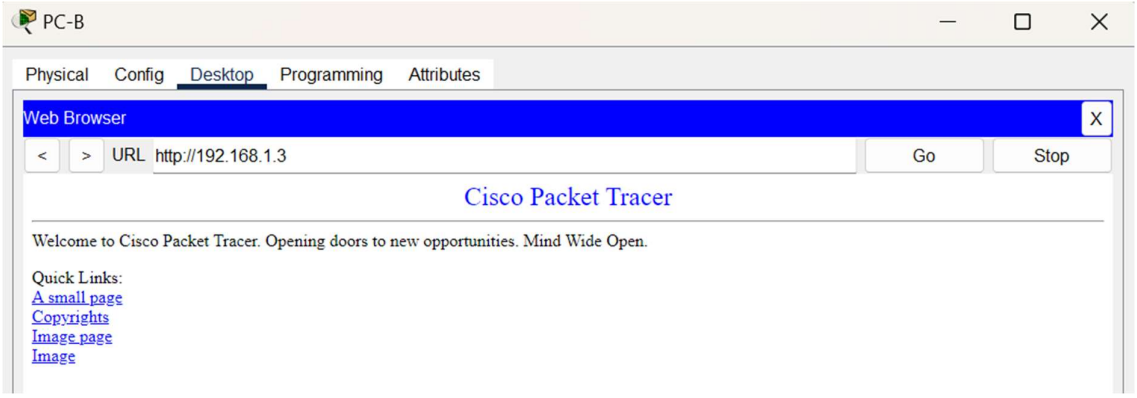
```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 10.2.2.1: bytes=32 time=3ms TTL=253
Reply from 10.2.2.1: bytes=32 time=2ms TTL=253
Reply from 10.2.2.1: bytes=32 time=34ms TTL=253
Reply from 10.2.2.1: bytes=32 time=26ms TTL=253

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 = 34ms, Average = 16ms

C:\>ssh -l admin 192.168.2.1

Password:



R2>exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>
```

PC-B

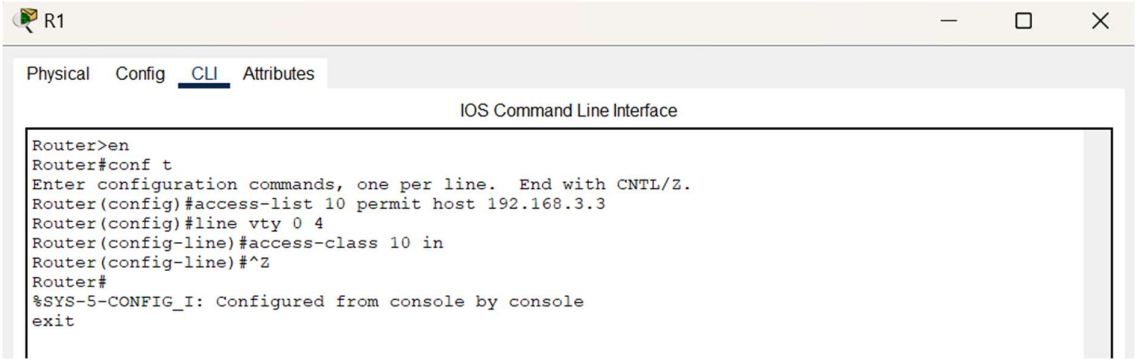
Physical Config Desktop Programming Attributes

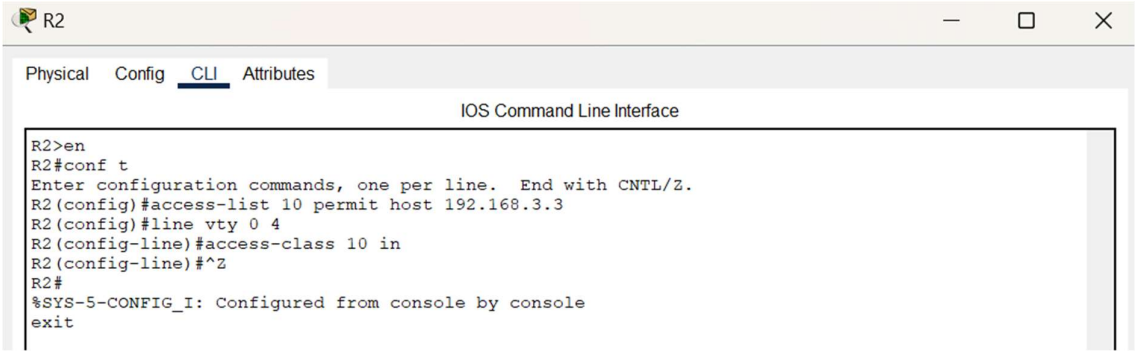
Command Prompt

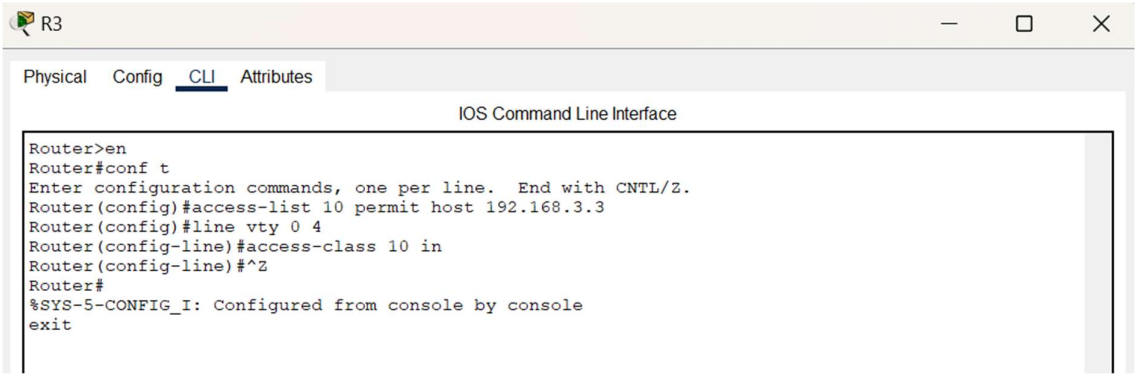
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=2ms 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

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>ssh -l admin 192.168.2.1

Password:



R2>exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>
```



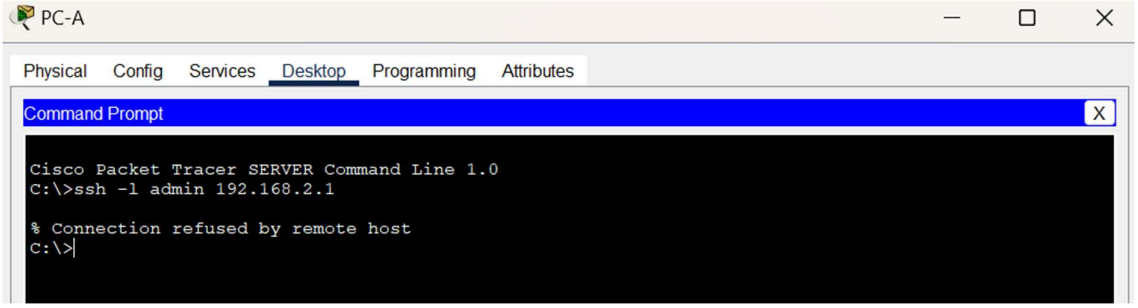

- **Configure ACL on routers (block all remote access to the routers except from PC)**

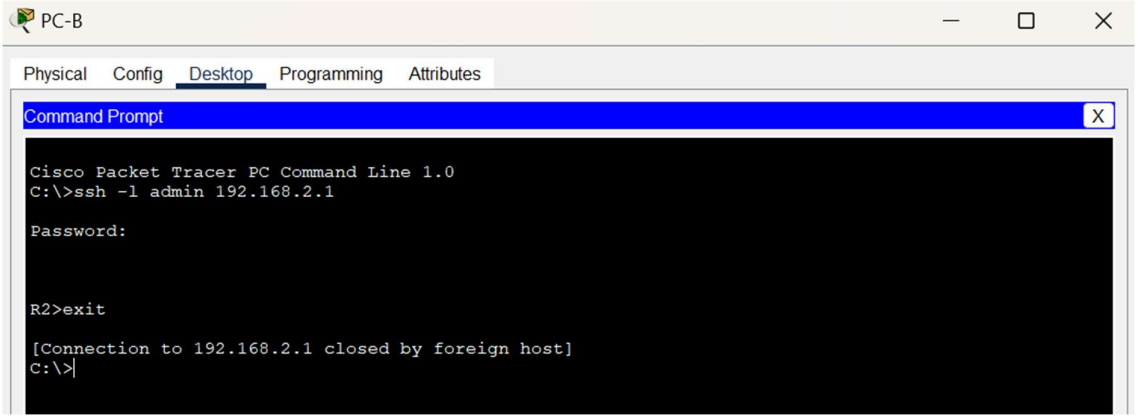


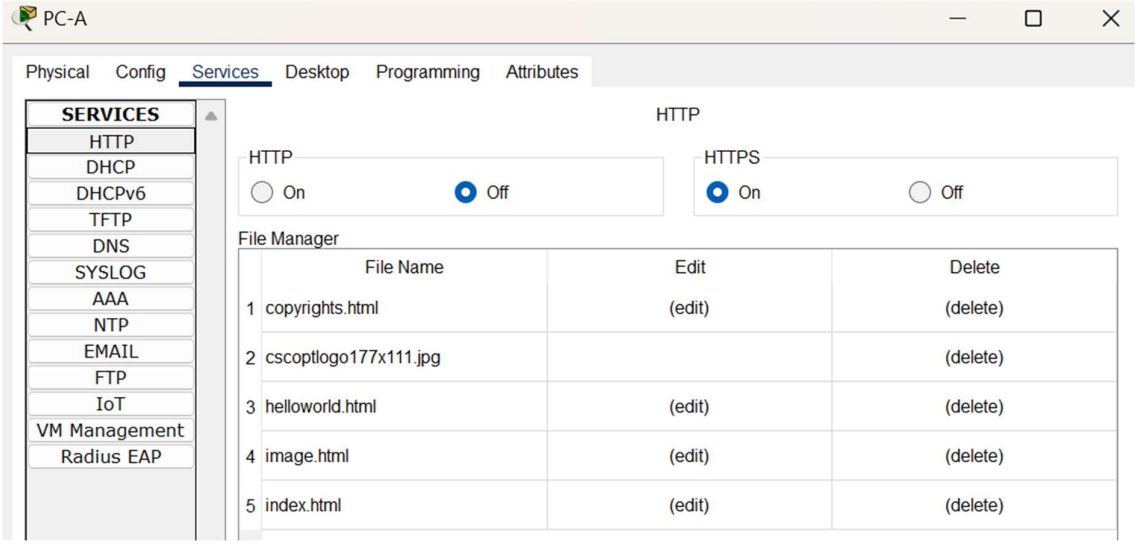



## ➢ Verifying the working of ACL




## ➢ 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.

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
Router(config)#access-list 120 permit tcp any host 192.168.1.3 eqsmtp
                                                                ^
% Invalid input detected at '^' marker.

Router(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
Router(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
Router(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
Router(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
Router(config)#interface Serial0/0/0
Router(config-if)#ip access-group 120 in
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#exit
```

## ➢ Verifying the working of ACL

PC-B

Physical Config Desktop Programming Attributes

Web Browser

< > URL https://192.168.1.3 Go Stop

Request Timeout

## ➢ Verifying the network connectivity before ACL implementation

PC-A

Physical Config Services Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

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

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- **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.

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 120 permit icmp any any echo-reply
Router(config)#access-list 120 permit icmp any any unreachable
Router(config)#access-list 120 permit ip any any
Router(config)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

- **Verifying the working of ACL**

PC-A

Physical Config Services Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer SERVER Command Line 1.0
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=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=11ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms 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 = 1ms, Maximum = 11ms, Average = 3ms

C:\>
```

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

R3

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip access-group 110 in
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

- **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 Attributes

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
Router(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
Router(config)#access-list 100 deny ip 172.168.0.0 0.0.255.255 any
Router(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
Router(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
Router(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
Router(config)#access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3
Router(config)#access-list 100 permit ip any any
Router(config)#interface Serial0/0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

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>
```