

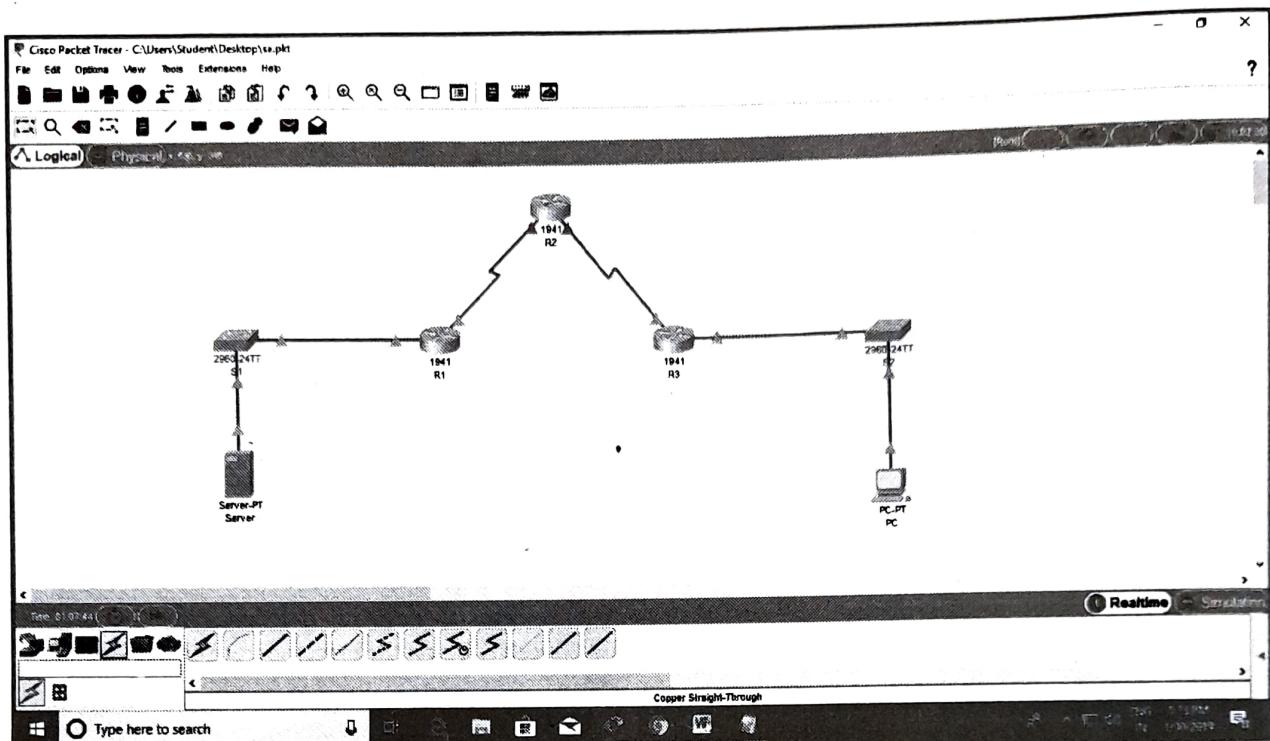
Practical 4

► 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

Server Configuration:

Setting	Value
IP Address	192.168.1.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

PC Configuration:

Setting	Value
IP Address	192.168.3.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.3.1
DNS Server	0.0.0.0

```
Router>en
Router#conf t
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 GigabitEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)# ^ Z
R1#exit
```

```
Router>en
Router#conf t
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)#interface Serial0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shut
R2(config)#int loopback1
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)# ^ Z
R2#exit
```

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#interface Serial0/0/0
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shut
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)# ^ Z
R3#exit
```



☞ Displaying IP Address Details of Routers

```
R1>show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 192.168.1.1 YES manual up up
GigabitEthernet0/1 unassigned YES unset administratively down down
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>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>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 10.2.2.1 YES manual up up
Serial0/0/1 unassigned YES unset administratively down down
Vlan1 unassigned YES unset administratively down down
```

☞ Configure RIP on routers

```
R1>en
R1#conf t
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#exit
```



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

```
R3>en
R3#conf t
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#exit
```

☞ Displaying routing table of routers

```
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, 00:00:01, 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, 00:00:01, Serial0/0/0

R 192.168.3.0/24 [120/2] via 10.1.1.2, 00:00:01, Serial0/0/0

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, 00:00:10, 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, 00:00:28, Serial0/0/1

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, 00:00:11, Serial0/0/0
C 10.2.2.0/30 is directly connected, Serial0/0/0
L 10.2.2.1/32 is directly connected, Serial0/0/0
R 192.168.1.0/24 [120/2] via 10.2.2.2, 00:00:11, Serial0/0/0
R 192.168.2.0/24 [120/1] via 10.2.2.2, 00:00:11, Serial0/0/0
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.3.0/24 is directly connected, GigabitEthernet0/0
L 192.168.3.1/32 is directly connected, GigabitEthernet0/0

☛ Configure SSH on R2

```
R2>en
R2#conf t
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 zeroizersa
% 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)#ipssh time-out 90
*Mar 1 0:21:14.577: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#ipssh authentication-retries 2
R2(config)#ipssh version 2
R2(config)# ^ Z
R2#exit
```



☛ Verify Basic Network Connectivity before ACL Configuration

Server

Physical Config Services Desktop **Programming** Attributes

Command Prompt

```
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=11ms TTL=125
Reply from 192.168.3.3: bytes=32 time=11ms TTL=125
Reply from 192.168.3.3: bytes=32 time=1ms 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 = 1ms, Maximum = 11ms, Average = 3ms

C:\>ssh -l admin 192.168.2.1
Password:

R2>exit

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

Command Prompt

```
C:\>ping 192.168.1.3
```

```
Pinging 192.168.1.3 with 32 bytes of data:
```

```
Reply from 192.168.1.3: bytes=32 time=2ms TTL=128
Reply from 192.168.1.3: bytes=32 time=11ms TTL=128
Reply from 192.168.1.3: bytes=32 time=11ms TTL=128
Reply from 192.168.1.3: bytes=32 time=13ms TTL=128
```

```
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 = 6ms
```

```
C:\>ssh -l admin 192.168.1.1
```

```
Password:
```

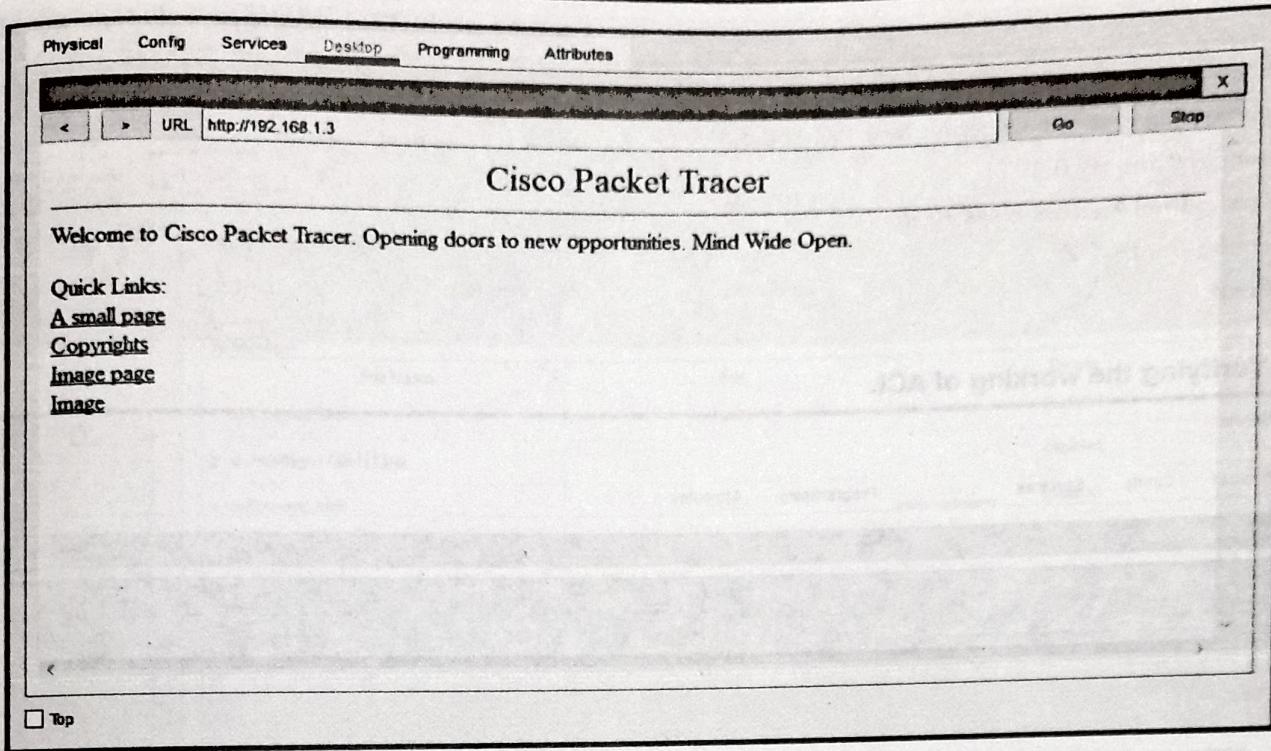
```
* Login invalid
```

```
Password:
```

```
R>exit
```

```
[Connection to 192.168.1.1 closed by foreign host]
```

Top



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

```
R1>en
R1#conf t
R1(config)# access-list 10 permit host 192.168.3.3
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)# ^ Z
R1#exit
```

```
R2>en
R2#conf t
R2(config)#access-list 10 permit host 192.168.3.3
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)# ^ Z
R2#exit
```



R3>en

R3#conf t

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#exit

☛ Verifying the working of ACL

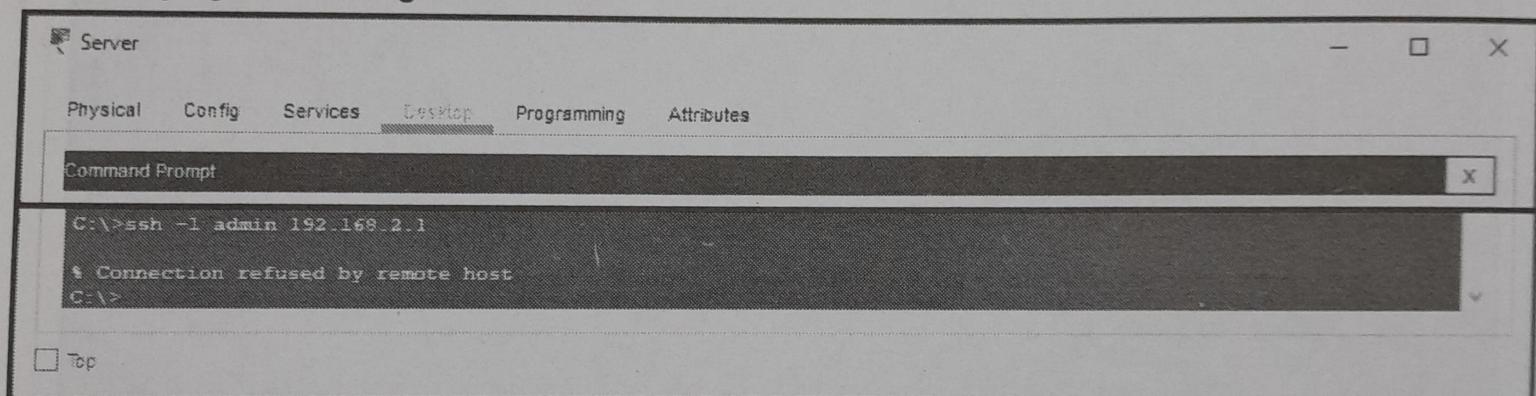
Server

Physical Config Services Desktop **Programming** Attributes

Command Prompt

```
C:\>ssh -l admin 192.168.2.1
* Connection refused by remote host
C:\>
```

Top



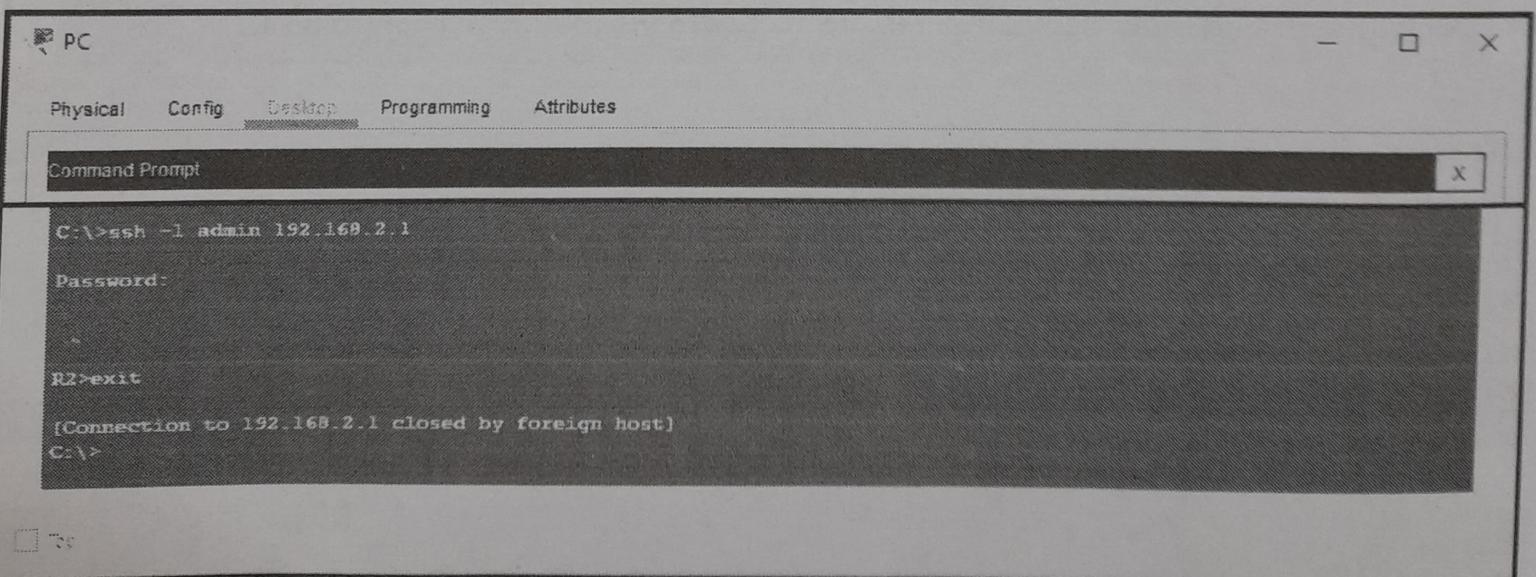
PC

Physical Config Desktop **Programming** Attributes

Command Prompt

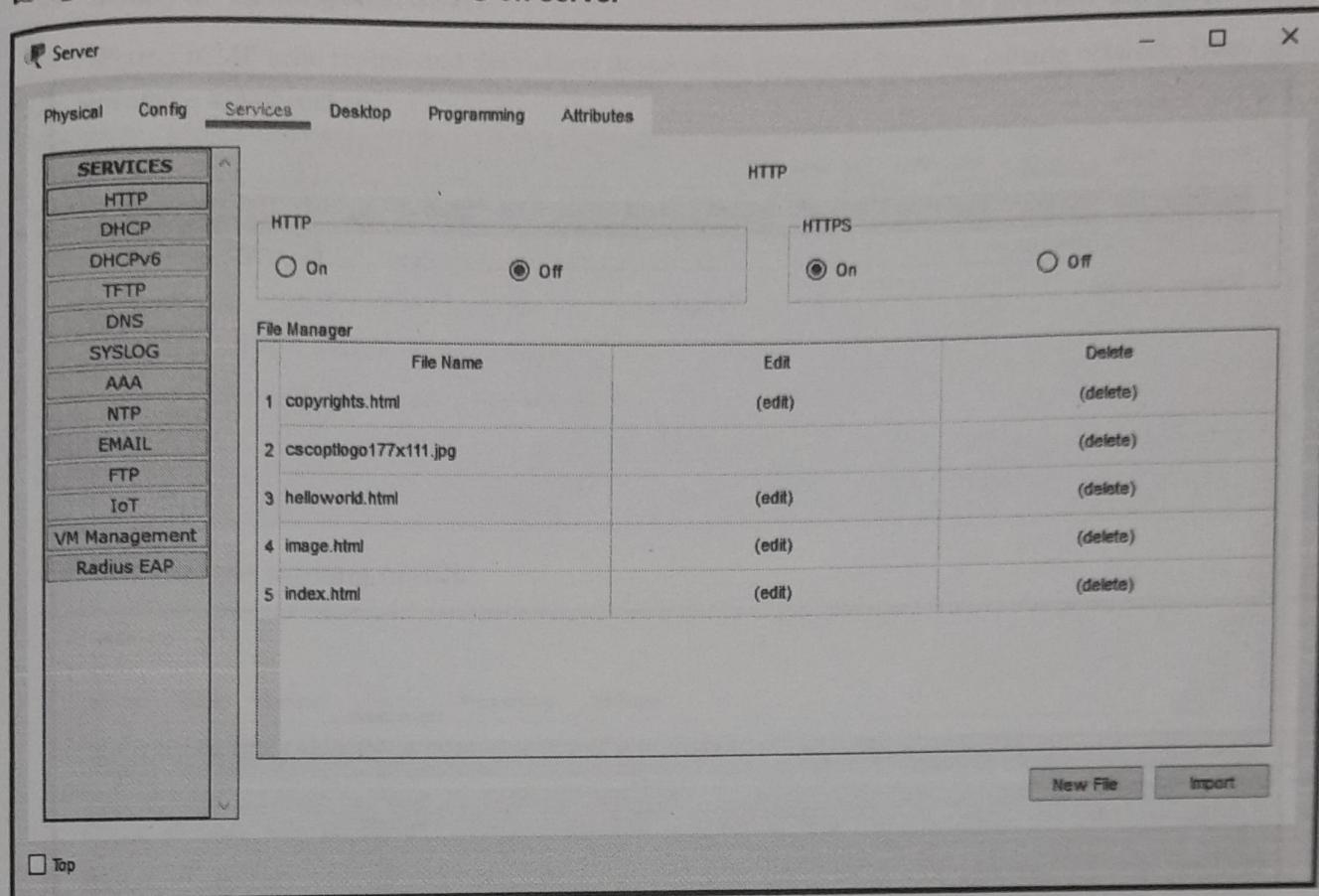
```
C:\>ssh -l admin 192.168.2.1
Password:
R2>exit
[Connection to 192.168.2.1 closed by foreign host]
C:\>
```

Top





Disable HTTP and enable HTTPS on server



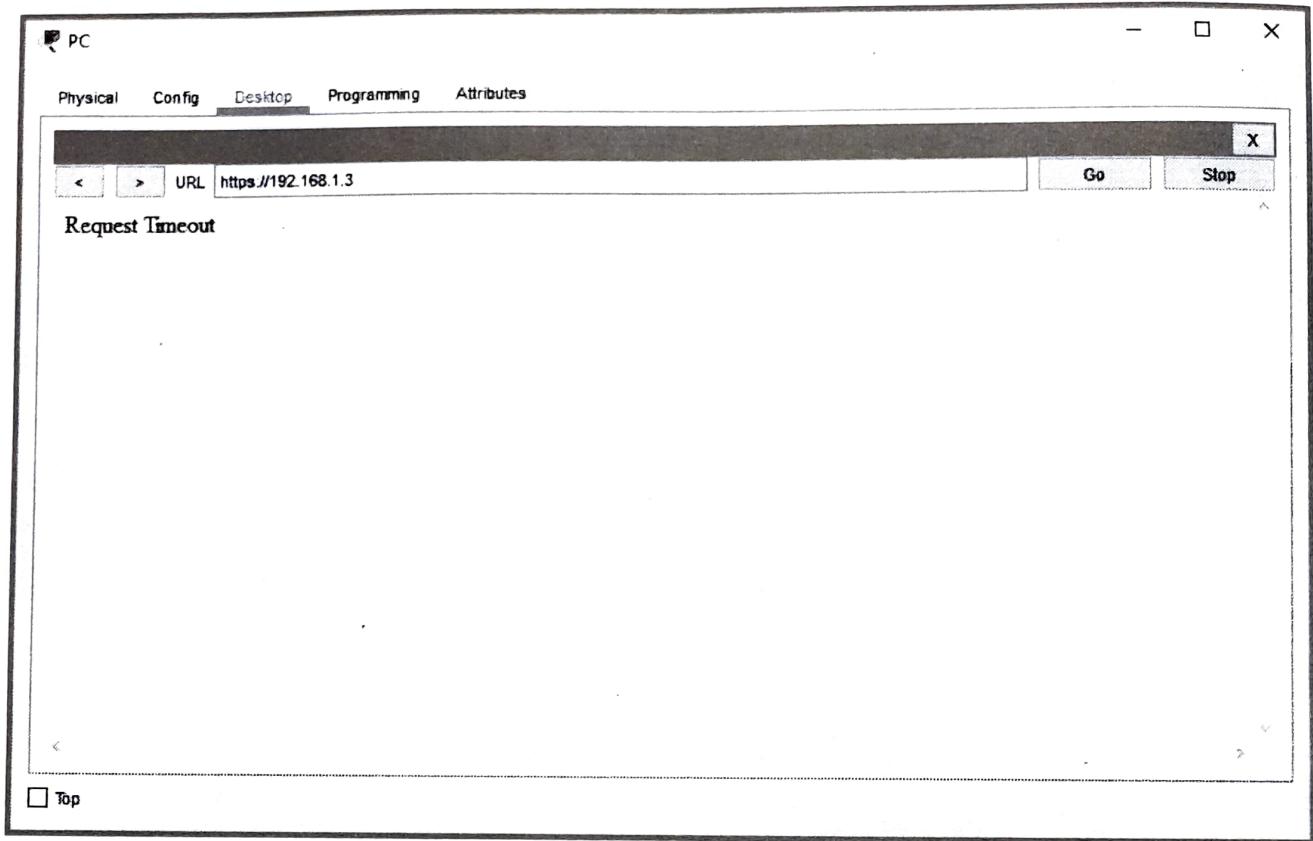
Configure ACL on routers

- o Permit any outside host to access DNS, SMTP, and FTP services on Server.
- o Deny any outside host access to HTTPS services on Server.
- o Permit PCto access R1 via SSH.

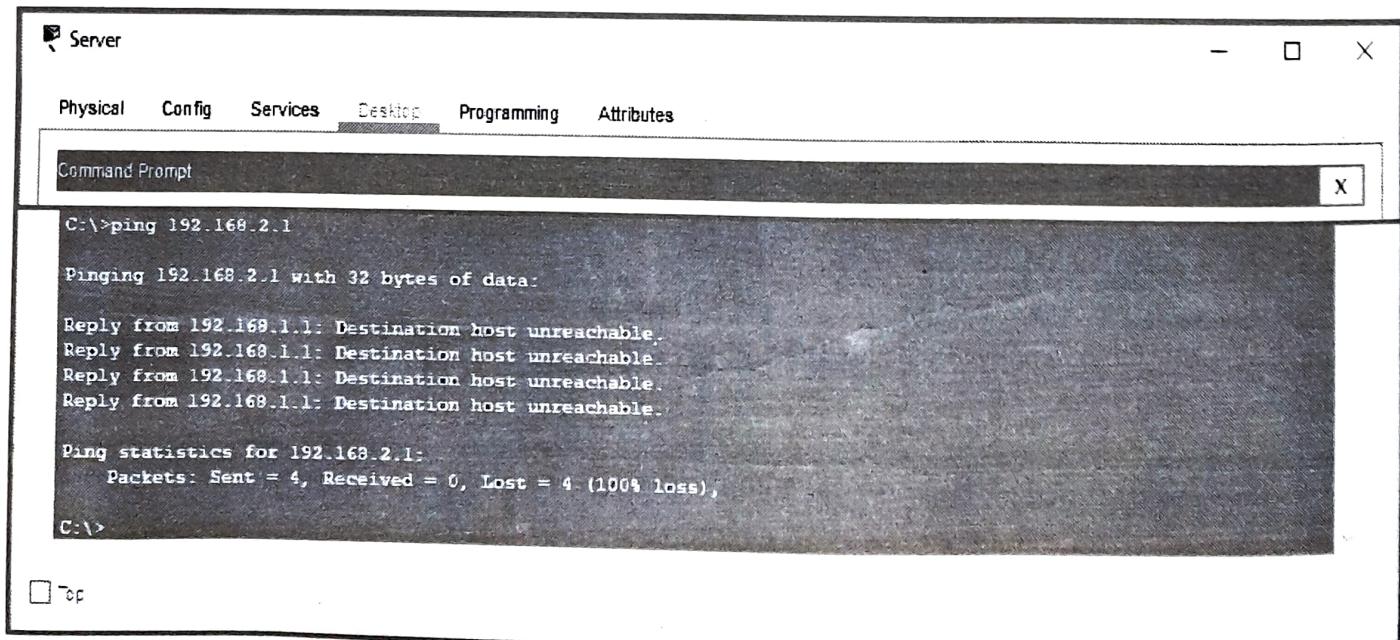
```
R1>en
R1#conf t
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R1(config)#interface Serial0/0/0
R1(config-if)#ip access-group 120 in
R1(config-if)#^Z
R1#exit
```



☒ 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 other incoming ICMP packets.)

```
R1>en
R1#conf t
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
R1(config)# ^Z
R1#exit
```

Verifying the working of ACL

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window is part of a "Server" application, indicated by the tab bar above it. The "Desktop" tab is selected. The Command Prompt window contains the following text:

```
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=14ms TTL=254
Reply from 192.168.2.1: bytes=32 time<1ms 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 = 0ms, Maximum = 14ms, Average = 4ms

C:\>
```

Configure ACL on routers

(Deny all outbound packets with source address outside the range of internal IP addresses on R3)

```
R3>en
R3#conf t
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface GigabitEthernet0/0
R3(config-if)# ip access-group 110 in
R3(config-if)# ^Z
R3#exit
```



☛ Configure ACL on routers

(On R3, 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>en
R3#conf t
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 tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3
R1(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#exit
```

The screenshot shows a Windows Command Prompt window titled "PC". The window has tabs at the top: Physical, Config, Desktop, Programming, and Attributes. The "Config" tab is selected. The command prompt itself is titled "Command Prompt". It contains the following text:

```
PC

Physical Config Desktop Programming Attributes

Command Prompt

Password:

R2>
[Connection to 192.168.2.1 closed by foreign host]
C:\>
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 -l admin 192.168.3.1

* Connection timed out: remote host not responding
C:\>ssh -l admin 192.168.2.1

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