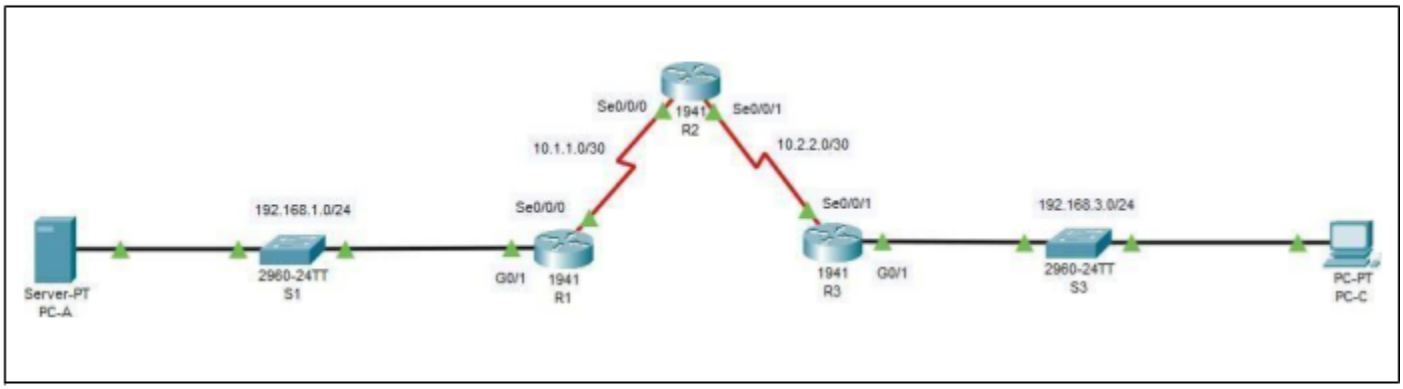
BSCITP602

Name :Harsh Kadu Roll No : 33

PRACTICAL NO 4

Aim: Configure IP ACLs to Mitigate Attacks.



Addressing Table:

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 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A	N/A
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	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

Name :Harsh Kadu Roll No : 33

Step 1 : Place the components as shown in the figure above and setup a network . It is necessary to configure each components placed in the network . Use proper connection wire to connect between the devices.

To Check if Routers R1, R2 and R3 are configured :

For Router R1:

Click on Router R1 → Go to CLI Tab → and type the following commands to check the configuration.

```
R1>show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     unassigned      YES unset  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
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
```

For Router R2:

Click on Router R2 → Go to CLI Tab → and type the following commands to check the configuration.

Name :Harsh Kadu Roll No : 33

```
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 manual administratively down
down
Loopback1              192.168.2.1     YES manual up
up
Vlan1                  unassigned      YES unset  administratively down
down
```

For Router R3:

Click on Router R3 → Go to CLI Tab → and type the following commands to check the configuration.

```
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
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
```

To set Loopback address on R2 :

Click on Router R2 → Go to CLI Tab → and type the following commands to set loopback address.

```
R2(config)#int loopback 1

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
```

Now Test the connectivity whether the devices are able to communicate.

- Ping From **PC-A** to **PC-C** .

Click on PC-A → Go to desktop option → Go to Command prompt → enter the command as shown below:

```
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 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Request timed out.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Ping From **PC-C** to **PC-A** .

Click on PC-C → Go to desktop option → Go to Command prompt → enter the command as shown below:

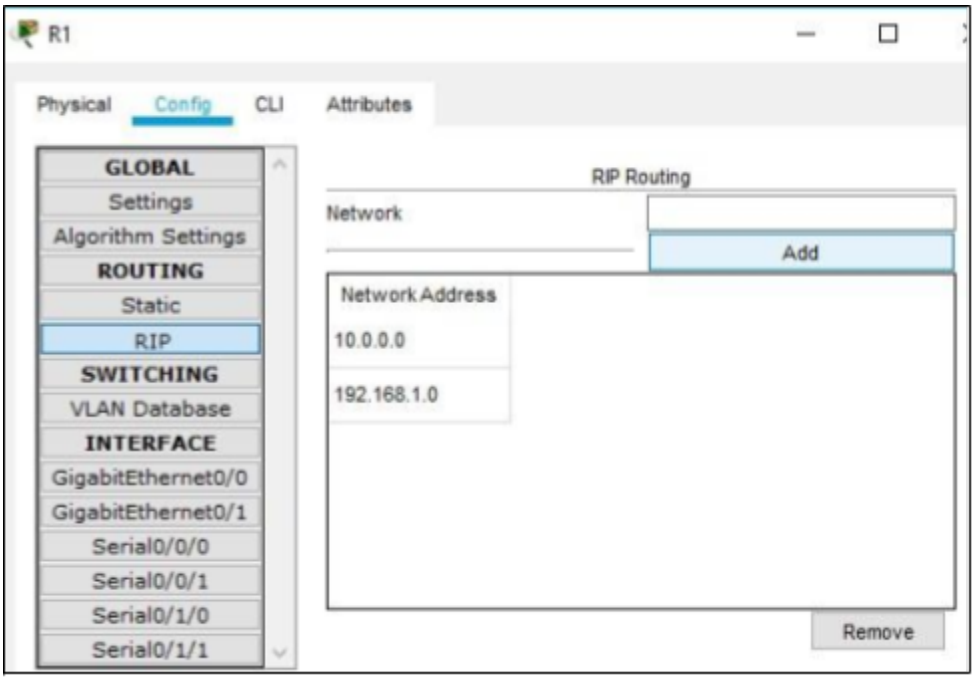
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

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

If this fails we have to do static RIP routing on R1, R2, R3 to connect from one network to another .

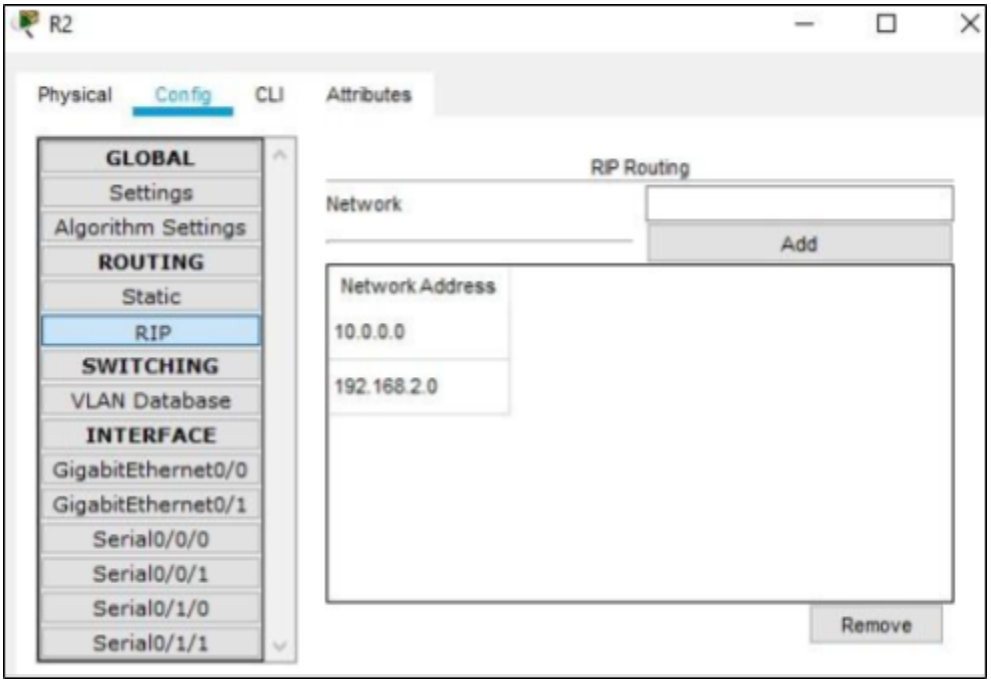
Click on Router R1 → Go to Config tab → Click on RIP → Give network address as per addressing table. → Add these two network addresses (192.168.1.0 , 10.0.0.0) in RIP routing .

BSCITP602

Name :Harsh Kadu Roll No : 33

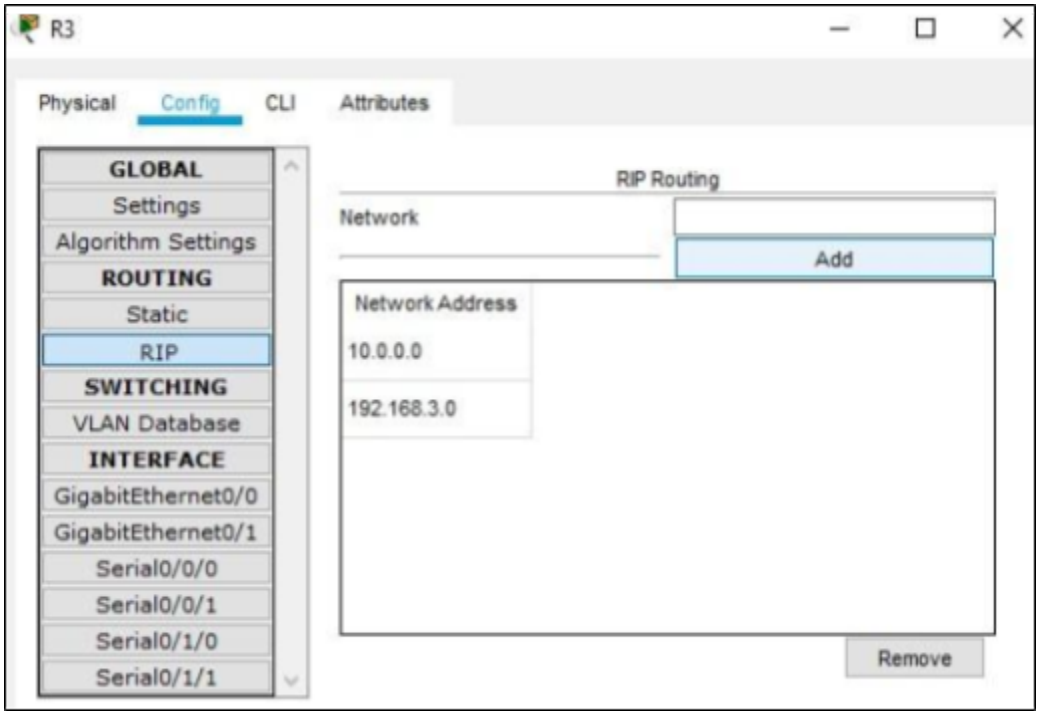


Click on Router R2 → Go to Config tab → Click on RIP → Give network address as per addressing table. → Add these two network addresses (10.0.0.0, 192.168.2.0) in RIP routing .



Name :Harsh Kadu Roll No : 33

Click on Router R3 → Go to Config tab → Click on RIP → Give network address as per addressing table. → Add these two network addresses (10.0.0.0, 192.168.3.0) in RIP routing .



Now check whether the devices are connected from one network to another once connection is done.

- Ping From **PC-A** to **PC-C** .

```
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=9ms TTL=125
Reply from 192.168.3.3: bytes=32 time=9ms 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 = 9ms, Average = 5ms
```

- Ping From **PC-C** to **PC-A** .

```
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=7ms 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
Reply from 192.168.1.3: bytes=32 time=6ms 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 = 7ms, Average = 4ms
```

Since its now get connected and we can share messages from one network to another and further Operation can be performed . Hence it is necessary to configure devices within network and outside the network to do further operations on it.

Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

Step 1 :

a. From PC-A, verify connectivity to PC-C and R2.

```
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=9ms TTL=125
Reply from 192.168.3.3: bytes=32 time=9ms 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 = 9ms, Average = 5ms
```

b. From the command prompt, establish an SSH session to R2 Lo0 interface Click on

Router R2 → Go to CLI tab → And the following commands :

```
R2#enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip domain-name securityincomputing.com
R2(config)#username SSHadmin secret ciscosshpa55
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 authentication-retries 2
*Mar 1 1:0:50.634: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#ip ssh time-out 90
R2(config)#ip ssh version 2
```

Verify the SSH configuration SSH to **R2** from the command prompt of **PC-A**.

Go to PC-A → Click on Desktop tab → Click on Command prompt → and type the following command :

```
C:\>ssh -l SSHadmin 192.168.2.1

Password:



R2>
```

Step 2:

a. From PC-C, verify connectivity to PC-A and R2.

```
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=9ms TTL=125
Reply from 192.168.3.3: bytes=32 time=9ms 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 = 9ms, Average = 5ms
```

b. From the command prompt, establish an SSH session to R2 Lo0 interface Establish SSH session once at the starting of Step 1.

Verify the SSH configuration SSH to **R2** from the command prompt of **PC-C**.

Go to PC-C → Click on Desktop tab → Click on Command prompt → and type the following command :

```
C:\>ssh -l SSHadmin 192.168.2.1

Password:


R2>
```

c. Open a web browser to the **PC-A** server (192.168.1.3) to display the web page.

Go to PC-A → Click on Desktop tab → Click on Web Browser → and enter the url:

Part 2 : Secure Access to Routers

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

Use the **access-list** command to create a numbered IP ACL on **R1**, **R2**, and **R3**.

On Router R1:

Click on Router R1 → Go to CLI tab → And the following commands :

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

On Router R2:

Click on Router R2 → Go to CLI tab → And the following commands :

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

On Router R3:

Click on Router R3 → Go to CLI tab → And the following commands :

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

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

Use the **access-class** command to apply the access list to incoming traffic on the VTY lines.

On Router R1:

Click on Router R1 → Go to CLI tab → And the following commands :

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

On Router R2:

Click on Router R2 → Go to CLI tab → And the following commands :

```
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
```

On Router R3:

Click on Router R3 → Go to CLI tab → And the following commands :

```
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
```

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

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

Go to PC-C → Click on Desktop tab → Click on Command prompt → and type the following command :

```
C:\>ssh -l SSHadmin 192.168.2.1

Password:



R2>
```

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

Go to PC-A → Click on Desktop tab → Click on Command prompt → and type the following command :

```
C:\>ssh -l SSHadmin 192.168.2.1

% Connection refused by remote host
```

Part 3: Create a Numbered IP ACL 120 on R1

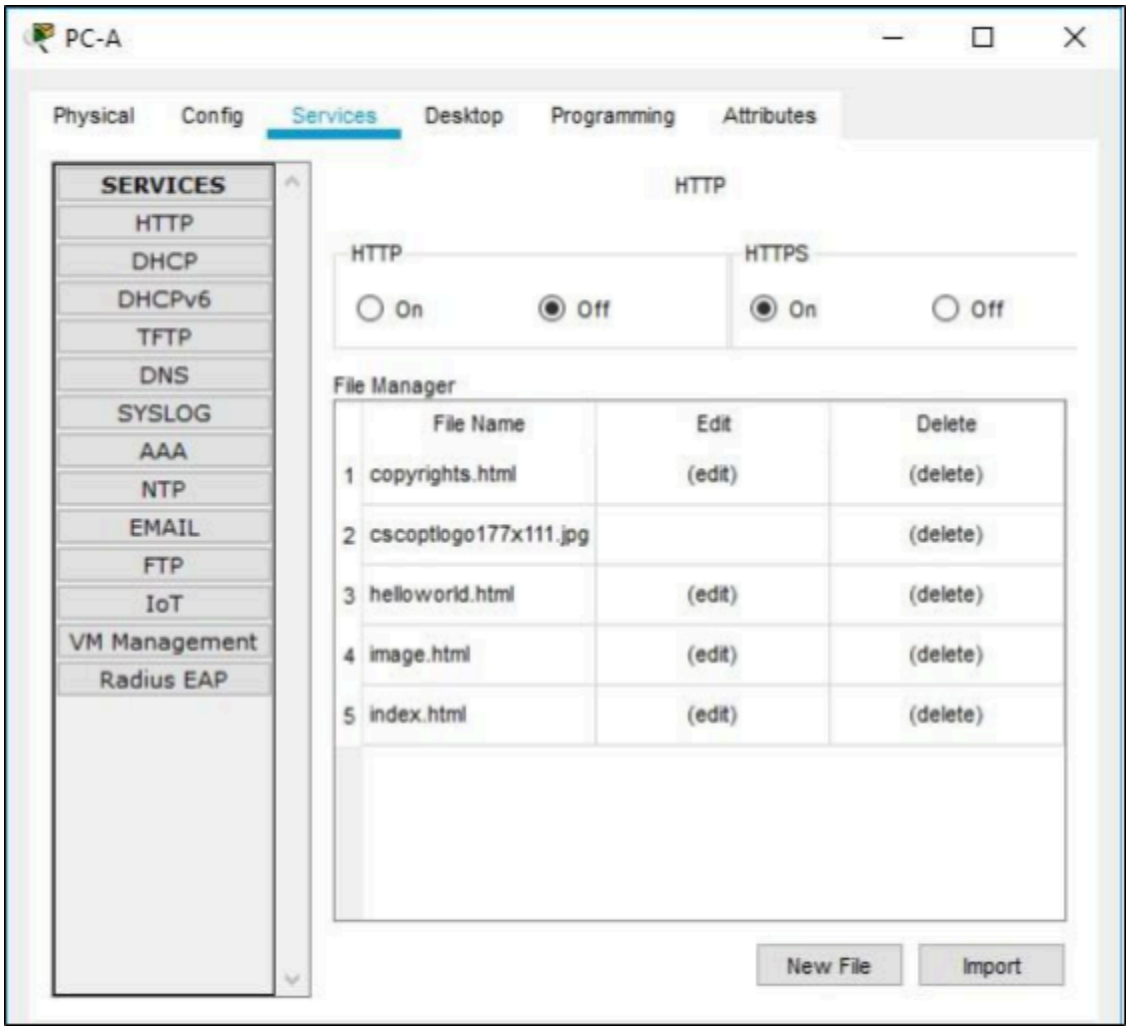
Create an IP ACL numbered 120 with the following rules:

- Permit any outside host to access DNS, SMTP, and FTP services on server **PC-A**.
- Deny any outside host access to HTTPS services on PC-A. • Permit PC-C to access R1 via SSH.

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

Be sure to disable HTTP and enable HTTPS on server PC-A.

Go to PC-A → Click on Services tab → Under Services option choose HTTP → enable **HTTPS** and disable **HTTP**



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

Use the **access-list** command to create a numbered IP ACL.

Click on Router R1 → Go to CLI tab → And the following commands :

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq ?
  <0-65535>      Port number
  bootpc         Bootstrap Protocol (BOOTP) client (68)
  bootps         Bootstrap Protocol (BOOTP) server (67)
  domain         Domain Name Service (DNS, 53)
  isakmp         Internet Security Association and Key Management Protocol
(500)
  non500-isakmp  Internet Security Association and Key Management Protocol
                 (4500)
  snmp           Simple Network Management Protocol (161)
  tftp           Trivial File Transfer Protocol (69)
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 any host 192.168.3.3 host 10.1.1.1
eq 22
                                                              ^
% Invalid input detected at '^' marker.

R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
```

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

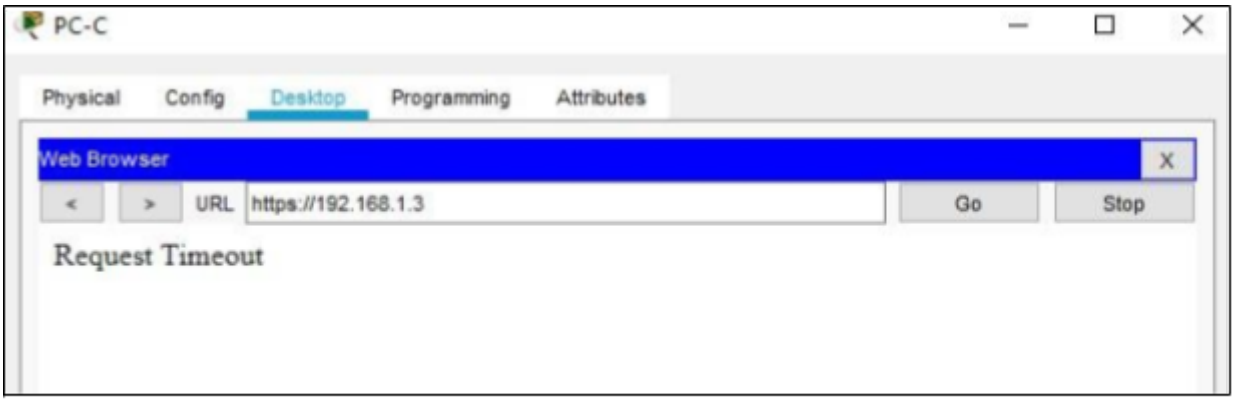
Use the **ip access-group** command to apply the access list to incoming traffic on interface **S0/0/0**.

Click on Router R1 → Go to CLI tab → And the following commands :

```
R1(config)#interface se0/0/0
R1(config-if)#ip access-group 120 in
R1(config-if)#
```

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

Go to PC-C → Click on Desktop tab → Click on Web Browser → and enter the url:



Part 4: Modify an Existing ACL on R1

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

Step 1: Verify that PC-A cannot successfully ping the loopback interface on R2.

Go to PC-A → Click on Desktop tab → Click on Command prompt → and type the command to check connectivity (it should fail):

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Request timed out.
Reply from 192.168.1.1: Destination host unreachable.

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

Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

Click on Router R1 → Go to CLI tab → And the following commands :

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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
```

Step 3: Verify that PC-A can successfully ping the loopback interface on R2.

Go to PC-A → Click on Desktop tab → Click on Command prompt → and type the command to check connectivity (it should now ping) :

```
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=2ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=3ms 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 = 3ms, Average = 1ms
```

Part 5: Create a Numbered IP ACL 110 on R3

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

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

Use the **access-list** command to create a numbered IP ACL.

Click on Router R3 → Go to CLI tab → And the following commands :

```
R3>enable
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
```

Step 2: Apply the ACL to interface G0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface G0/1.

Click on Router R3 → Go to CLI tab → And the following commands :

```
R3(config)#interface g0/1
R3(config-if)#ip access-group 110 in
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

Part 6: Create a Numbered IP ACL 100 on R3

On R3, block all packets containing the source IP address from the following pool of addresses:

- any RFC 1918 private addresses,
- 127.0.0.0/8,
- and any IP multicast address.

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

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

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address.

Use the **access-list** command to create a numbered IP ACL.

Click on Router R3 → Go to CLI tab → And the following commands :

```
R3#conf 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 permit ip any any
```

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

Use the ip access-group command to apply the access list to incoming traffic on interface Se0/0/1.

Click on Router R3 → Go to CLI tab → And the following commands :

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

Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is handled correctly.

a. From the PC-C command prompt, ping the PC-A server.

The ICMP echo replies are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.

Go to PC-C → Click on Desktop tab → Click on Command prompt → and type the command to check connectivity :

```
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),
```

b. Establish an SSH session to 192.168.2.1 from **PC-C** (should fail since we have blocked).

Go to PC-C → Click on Desktop tab → Click on Command prompt → and type the following command :

```
C:\>ssh -l SSHadmin 192.168.3.1


[Connection to 192.168.3.1 closed by foreign host]
```