

SECURITY IN COMPUTING

Practical-1

AIM- Configure Router

A: OSPF MD5 AUTHENTICATION

B: NTP SERVER

C: LOG MESSAGE TO THE SYSLOG SERVER

D: TO SUPPORT SSH CONNECTION

REQUIREMENT- REQUIRE 3 ROUTER , 2 SERVER, 1 PC

ROUTER SETUP:

THIS CONFIGURE SAME FOR ALL 3 ROUTER

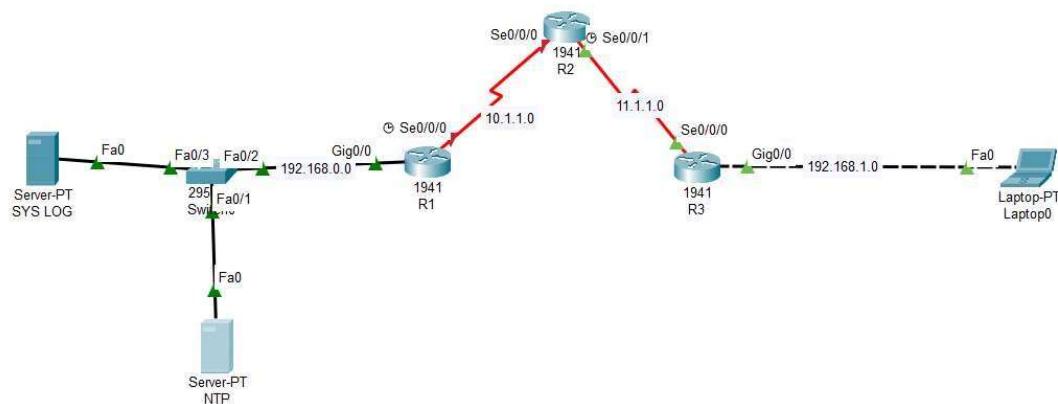
STEP1: TURN OFF ROUTER

STEP2: ADD MODULE 'HWIC-2T'

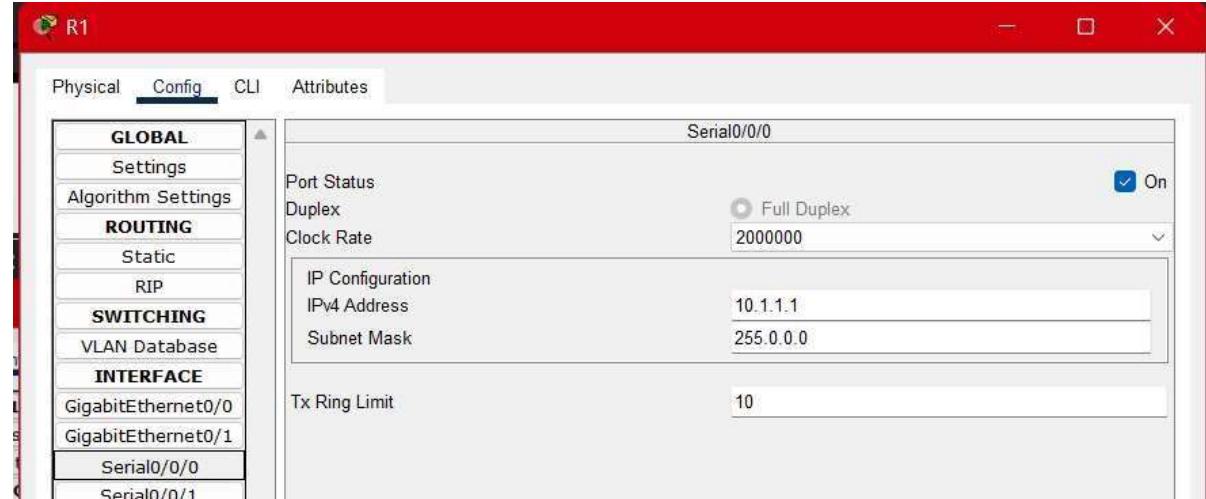
STEP3: TURN ON ALL THE ROUTER.

RENAME ROUTER NAME AND HOSTNAME FOR ALL 3 ROUTER MANUALLY IN MY CASE I GIVE R1, R2 AND R3 FOR HOSTNAME AND ROUTER NAME.

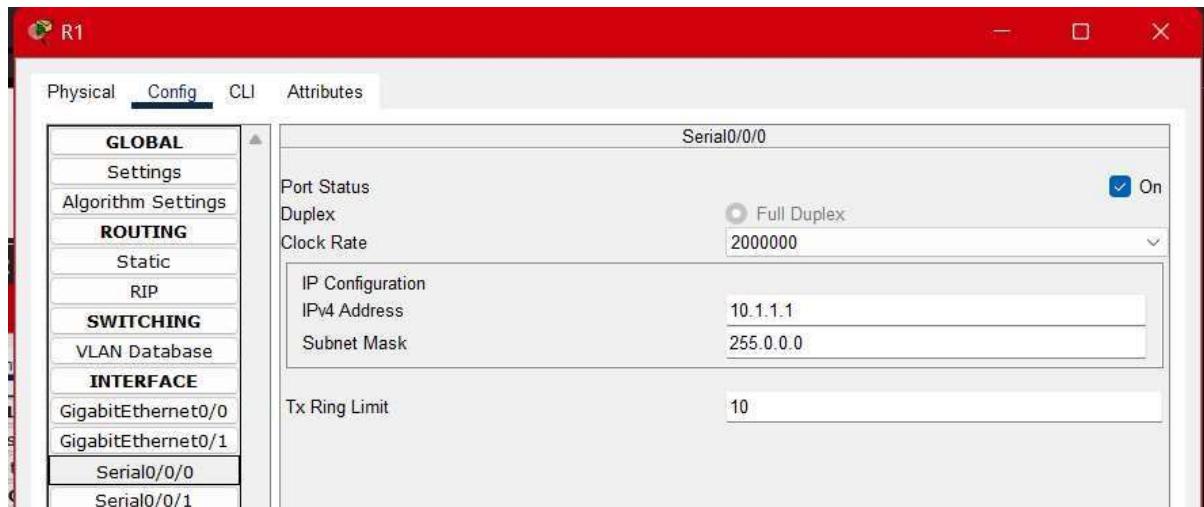
TOPOLOGY:



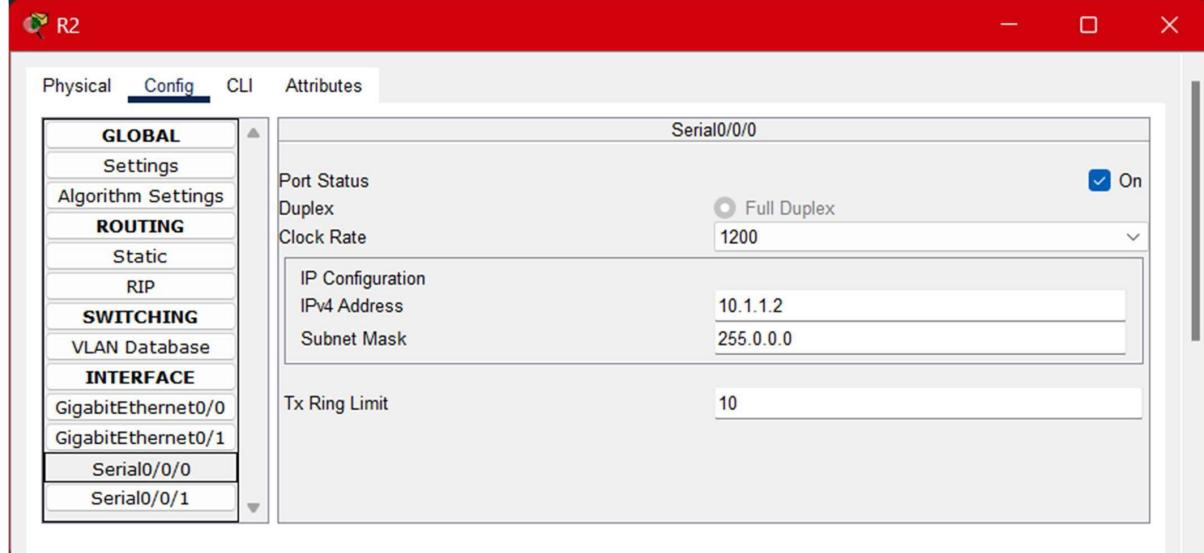
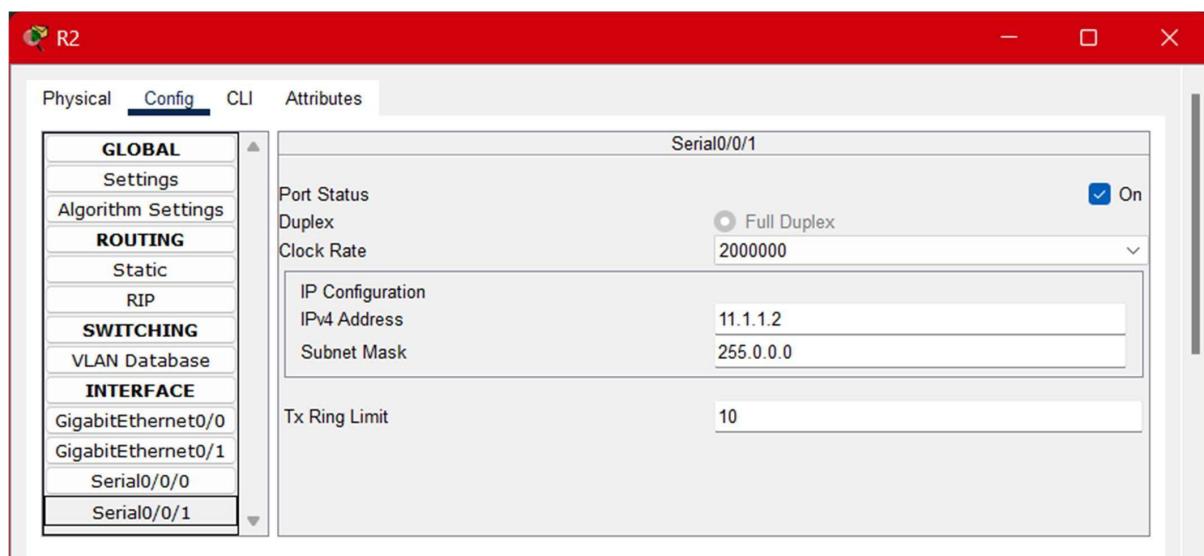
ROUTER R1: IP CONFIGURE



SECURITY IN COMPUTING

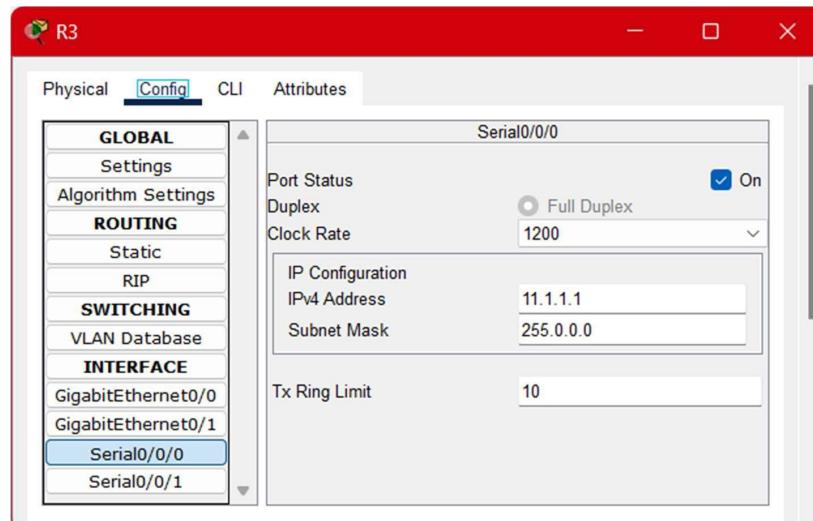
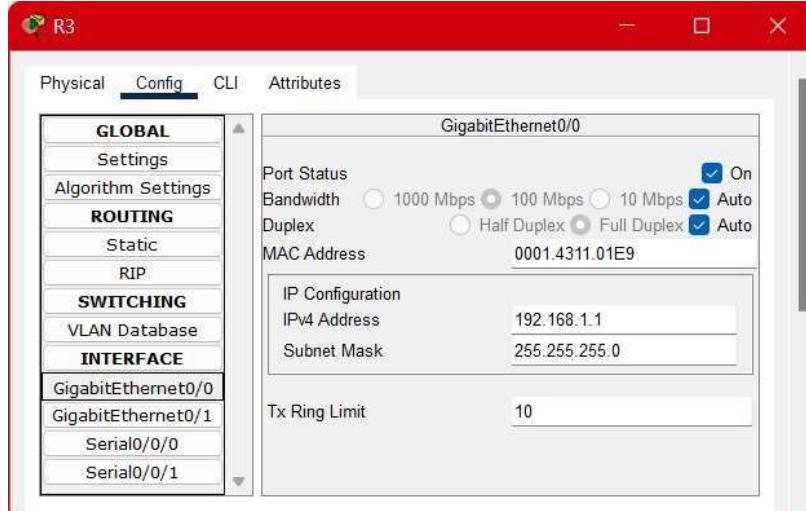


ROUTER R2: IP CONFIGURE



SECURITY IN COMPUTING

ROUTER R3 IP CONFIGURE



OSPF CONFIGURE OF R1

The screenshot shows the configuration interface for Router R1 in CLI mode. The command entered is:

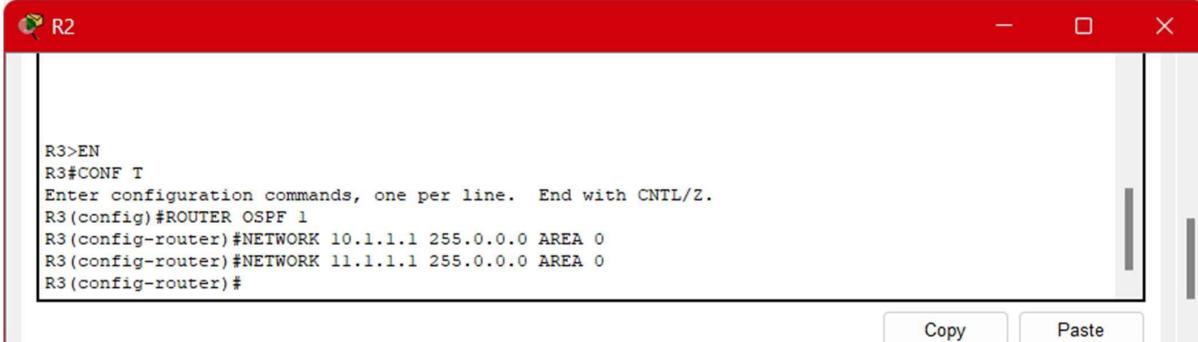
```
Router>en
Router#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ROUTER OSPF 1
Router(config-router)#NETWORK 192.168.0.1 255.255.255.255 AREA 0
Router(config-router)#NETWORK 10.1.1.1 255.0.0.0 AREA 0
Router(config-router)#

```

Buttons at the bottom include Copy and Paste.

OSPF CONFIGURE R2

SECURITY IN COMPUTING



R2

```
R3>EN
R3#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ROUTER OSPF 1
R3(config-router)#NETWORK 10.1.1.1 255.0.0.0 AREA 0
R3(config-router)#NETWORK 11.1.1.1 255.0.0.0 AREA 0
R3(config-router)#

```

Copy Paste

OSPF CONFIGURE R3



R3

```
R3>EN
R3#ROUTER OSPF 1
^
% Invalid input detected at '^' marker.

R3#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ROUTER OSPF 1
R3(config-router)#NETWORK 192.168.1.1 255.255.255.255 AREA 0
R3(config-router)#NETWORK
00:30:20: %OSPF-5-ADJCHG: Process 1, Nbr 11.1.1.2 on Serial0/0/0
from LOADING to FULL, Loading Done
11.1.1.1 255.0.0.0 AREA 0
R3(config-router)#

```

Copy Paste

Top

MD5 CONF FOR ALL 3 ROUTER (This step is same for all router)



R1

```
Router>EN
Router#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ROUTER OSPF 1
Router(config-router)#AREA 0 AUTHENTICATION MESSAGE-DIGEST
Router(config-router)#

```

Copy Paste

Top

MDF CONFI ON ALL THE SERIAL INTERFACE OF THE ROUTER

R1: HAVE ONE SERIAL INTERFACE IN USE

SECURITY IN COMPUTING



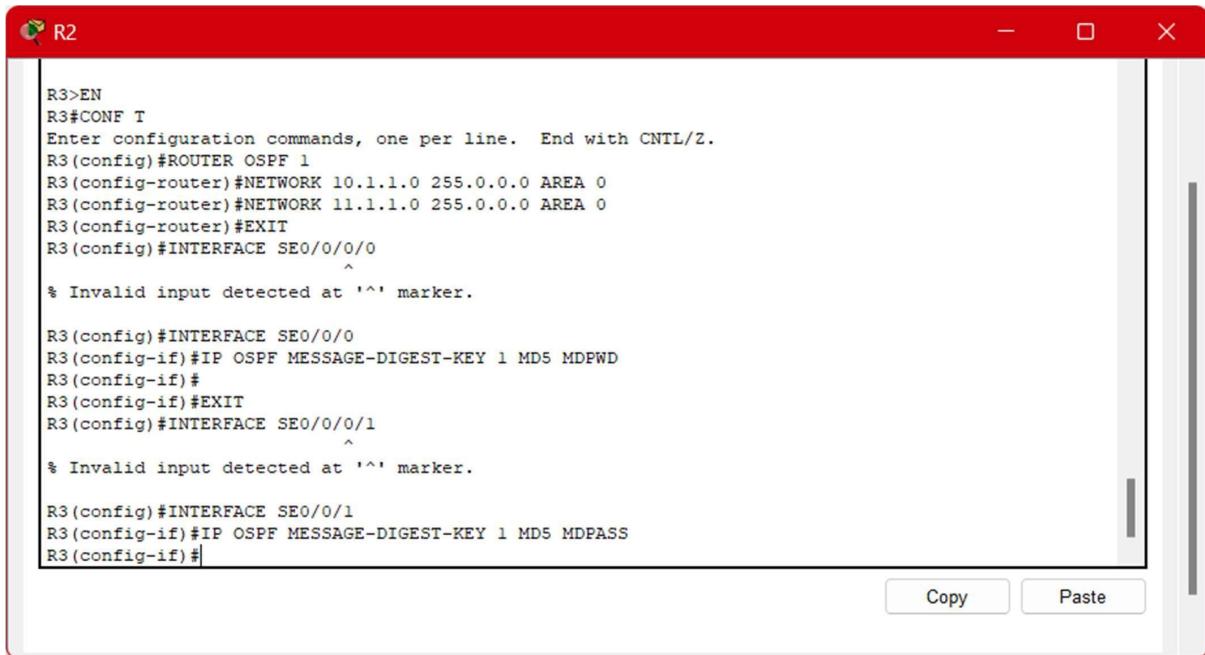
```
R1
Router(config-router)#NETWORK 192.168.0.0 255.255.255.255 AREA 0
Router(config-router)#NETWORK 10.1.1.0 255.0.0.0 AREA 0
Router(config-router)#AREA 0 AUTHENTICATION MESSAGE-DIGEST
Router(config-router)#EXIT
Router(config)#INTERFACE SE0/0/0\
^
% Invalid input detected at '^' marker.

Router(config)#INTERFACE SE0/0/0
Router(config-if)#IP OSPF MESSAGE-DIGEST-KEY 1 MD5 MDPWD
Router(config-if)#

```

Copy Paste

R2: HAVE 2 SERIAL INTRFACE IN USE



```
R2
R3>EN
R3#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ROUTER OSPF 1
R3(config-router)#NETWORK 10.1.1.0 255.0.0.0 AREA 0
R3(config-router)#NETWORK 11.1.1.0 255.0.0.0 AREA 0
R3(config-router)#EXIT
R3(config)#INTERFACE SE0/0/0\
^
% Invalid input detected at '^' marker.

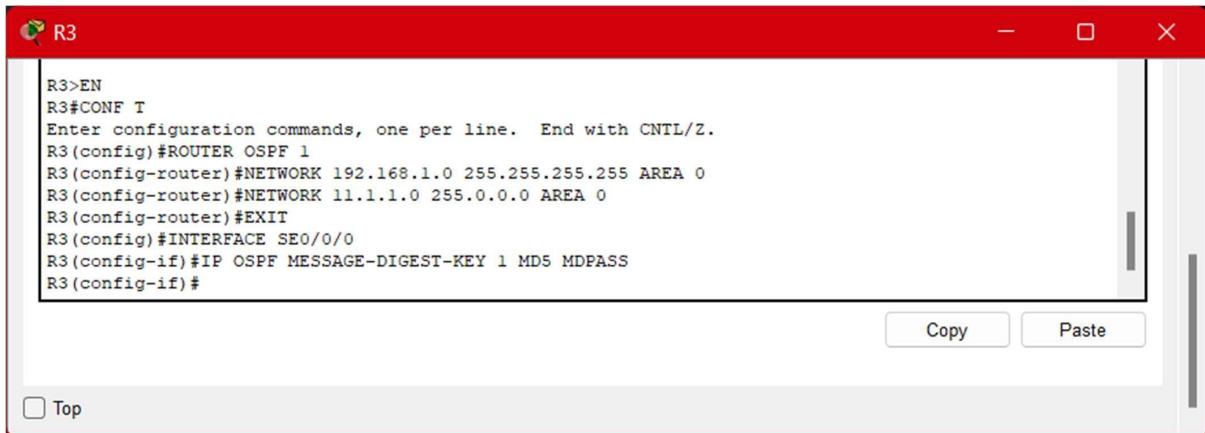
R3(config)#INTERFACE SE0/0/0
R3(config-if)#IP OSPF MESSAGE-DIGEST-KEY 1 MD5 MDPWD
R3(config-if)#
R3(config-if)#EXIT
R3(config)#INTERFACE SE0/0/0/1
^
% Invalid input detected at '^' marker.

R3(config)#INTERFACE SE0/0/1
R3(config-if)#IP OSPF MESSAGE-DIGEST-KEY 1 MD5 MDPASS
R3(config-if)#

```

Copy Paste

R3: HAVE 1 SERIAL PORT IN USE



```
R3
R3>EN
R3#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ROUTER OSPF 1
R3(config-router)#NETWORK 192.168.1.0 255.255.255.255 AREA 0
R3(config-router)#NETWORK 11.1.1.0 255.0.0.0 AREA 0
R3(config-router)#EXIT
R3(config)#INTERFACE SE0/0/0
R3(config-if)#IP OSPF MESSAGE-DIGEST-KEY 1 MD5 MDPASS
R3(config-if)#

```

Top Copy Paste

PART B: NTP

BEFORE NTP TIME SET THE OP OF ROUTER (THIS IS SAME IN ALL ROUTER)

SECURITY IN COMPUTING

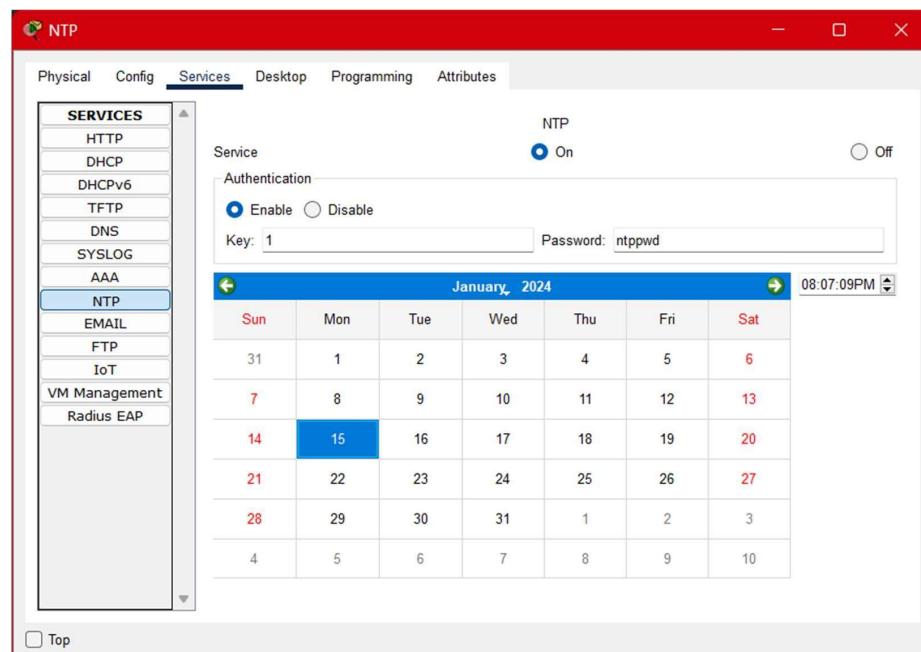
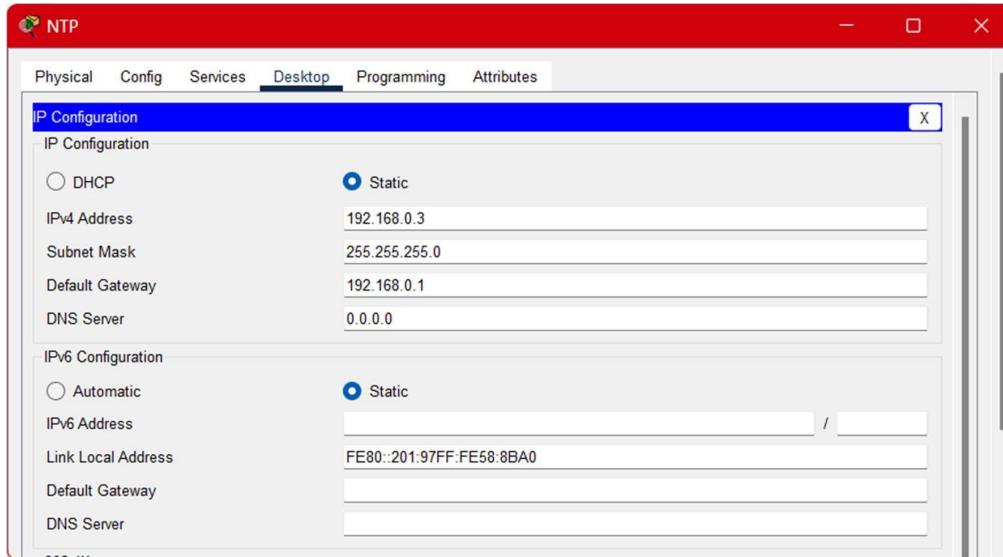


```
R3>SHOW CLOCK
*0:54:56.572 UTC Mon Mar 1 1993
R3>
```

Top

Copy Paste

NTP IP CONFIG



NTP SERVICE TURN ON

ADD NTP TO ALL THE ROUTER (THIS IS SAME FOR ALL ROUTER)

SECURITY IN COMPUTING

```
R3>SHOW CLOCK
*0:54:56.572 UTC Mon Mar 1 1993
R3>EN
R3#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#NTP SERVER 192.168.0.3
R3(config)#NTP UPDATE-CALENDAR
R3(config)#

 Top
```

Copy Paste

AFTER NTP SETUP IN ALL ROUTER

```
R1>SHOW CLOK
^
% Invalid input detected at '^' marker.

Router>SHOW CLCOK
^
% Invalid input detected at '^' marker.

Router>SHOW CLOCK
21:5:41.735 UTC Mon Jan 15 2024
Router>

 Top
```

Copy Paste

PART 3: SYS LOGGING

SETUP SYSLOG

SYS LOG

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG**
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

Syslog

Service On Off

Time	HostName	Message
1 03.01.1993 01:36:45.876 AM	11.1.1.1	%SYS-5-CONFIG_I: Configured from console by console
2 03.01.1993 01:36:45.876 AM	11.1.1.1	: %SYS-6-LOGGINGHOST_STARTSTO...
3 03.01.1993 01:38:15.161 AM	11.1.1.1	%SYS-5-CONFIG_I: Configured from console by console

ASUSUAL SAME FOR ALL ROUTER

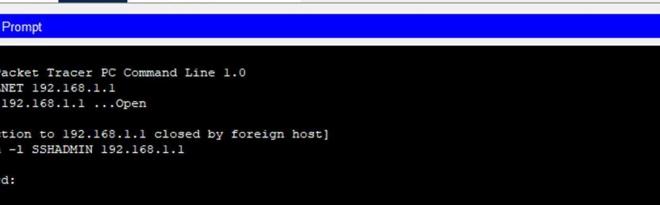
SECURITY IN COMPUTING

 R3 — □ ×

```
R3>EN
R3#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#LOGGIN HOST 192.168.0.2
R3(config)#
Copy Paste
```

PART 4: SSH

TELNET CONNECTION



Laptop0

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>TELNET 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l SSHADMIN 192.168.1.1

Password:

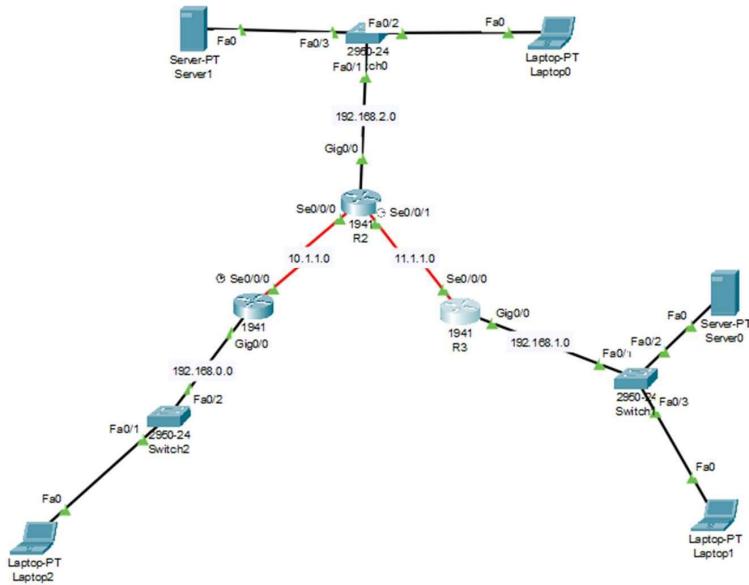
R3#
```

SECURITY IN COMPUTING

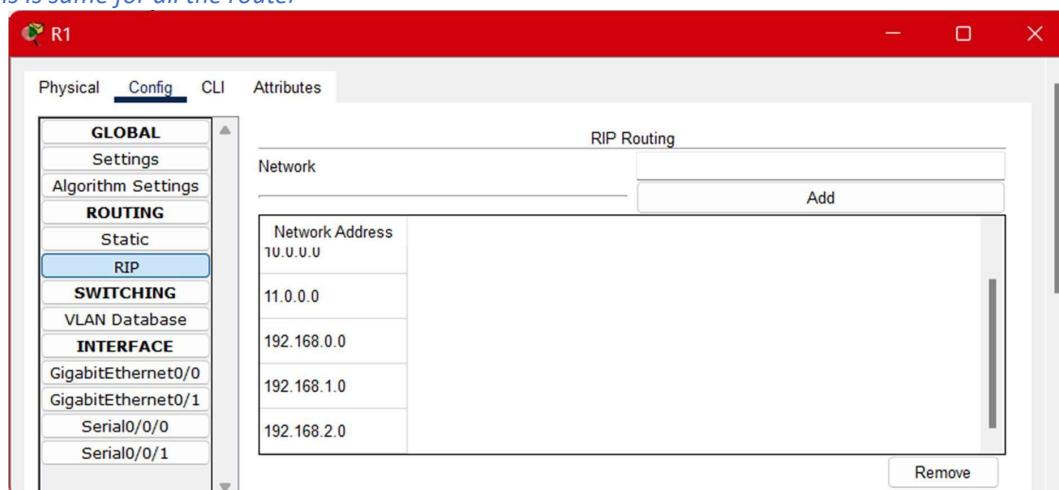
PRACTICAL 2

AIM - Configure AAA authenticate

Topology



Assign IP To All The Required devices
Perform a Routing Information Protocol (RIP)
This is same for all the router



SECURITY IN COMPUTING

CONFIGURE AUTHENTICATION, AUTHORIZATION AND ACCOUNTING (AAA)

CONFIGURE ROUTER 1 WITH AAA

```
R1
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/0/0, changed state to up

R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#username admin secret admin
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
R1(config)#line console 0
R1(config-line)#login authentication default
R1(config-line)#
R1#
```

AFTER CONFIGURE REQUIRED A LOCAL LOGIN.

A screenshot of a terminal window titled "R1". The window has a red header bar with the title "R1" and standard window control buttons (minimize, maximize, close). The main area shows the following text:

```
Username: admin
Password:
R1>
```

The text is displayed in a monospaced font, with "Username:" and "Password:" followed by a blank line, and "R1>" indicating the prompt.

CONFIGURE AUTHENTICATION, AUTHORIZATION AND ACCOUNTING (AAA) FOR VTY LINE 4

R1#

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ip domain-name sdk.com

R1(config)#crypto key generate rsa

% You already have RSA keys defined named R1.sdk.com .

% Do you really want to replace them? [yes/no]: y

The name for the keys will be: R1.sdk.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]

R1(config)#aaa authentication login ssh-login local

*Mar 1 0:14:8.241: %SSH-5-ENABLED: SSH 1.99 has been enabled

R1(config)#line vty 0 4

R1(config-line)#login authentication ssh login

% Invalid input detected at '^' marker.

R1(config-line)#login authentication ssh-login

R1(config-line)#transport input ssh

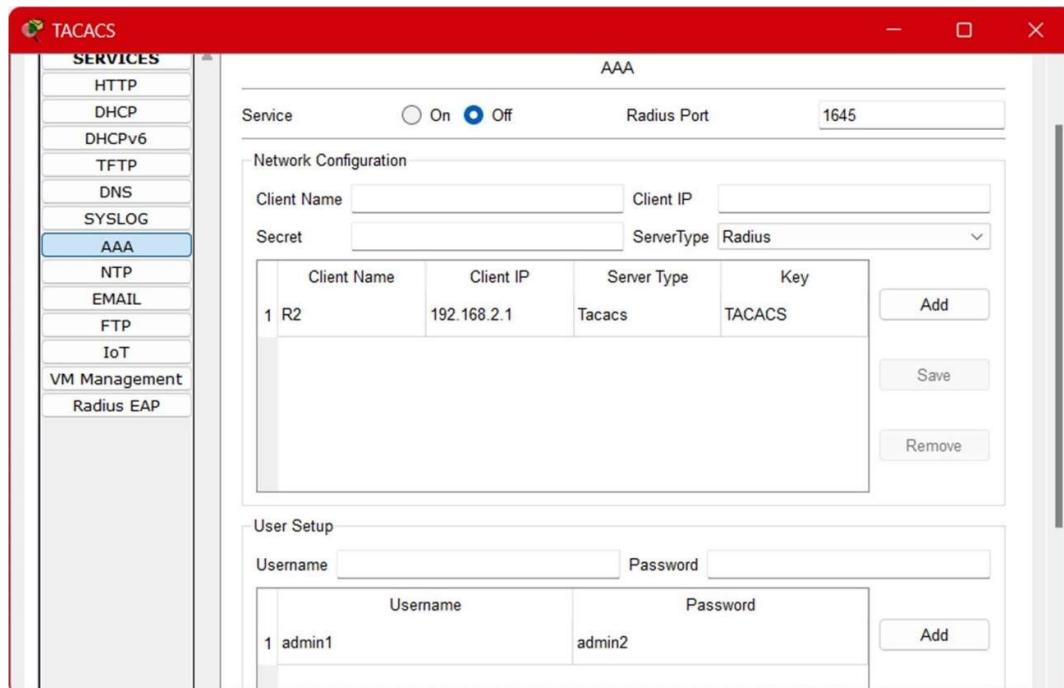
R1(config-line)#[

 Laptop2
C:\>
C:\>
C:\>ssh -l admin 192.168.0.1

Password:
R1>

SECURITY IN COMPUTING

CONFIGURE SERVER-BASED AAA AUTHENTICATION USING TACACS+ ON R2 SERVER



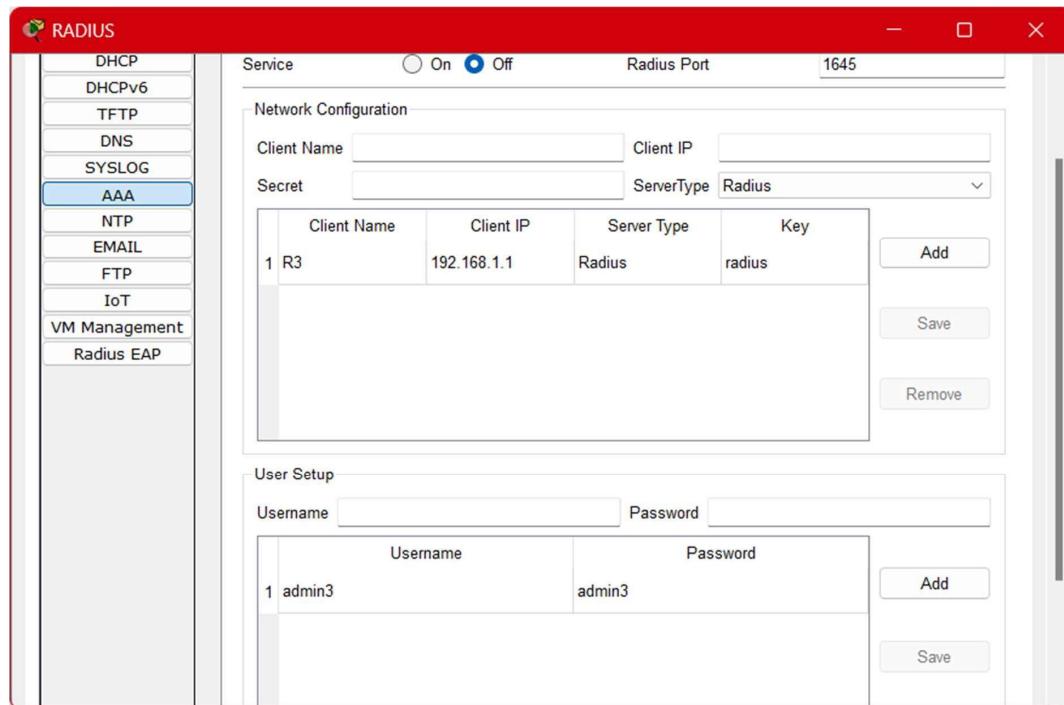
Router (R2)

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username admin2 secret admin2
R2(config)#tacacs-server host 192.168.2.3
R2(config)#tacacs-server key
R2(config)#tacacs-server key TACACS
R2(config)#aaa new-model
R2(config)#aaa authentication login defalut group tacacs+ local
R2(config)#line console 0
R2(config-line)#login authentication default
R2(config-line)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Buttons for 'Copy' and 'Paste' are visible at the bottom right. A 'Top' button is visible at the bottom left.

SECURITY IN COMPUTING

CONFIGURE SERVER-BASED AAA AUTHENTICATION USING RADIUS ON R3 SERVER



Router (R3)

The screenshot shows the R3 server's command-line interface. The configuration mode is active, displaying the following commands:

```
R3>
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#username admin3 secret admin3
R3(config)#radius-server host 192.168.1.2
R3(config)#radius-server key radius
R3(config)#aaa new-model
R3(config)#aaa authentication login default group radius local
R3(config)#line console 0
R3(config-line)#login authentication default
R3(config-line)#

```

At the bottom right of the CLI window are 'Copy' and 'Paste' buttons.

The screenshot shows the R3 server's command-line interface again, this time in User Access Verification mode. It prompts for a 'Username' (admin3) and a 'Password'.

IOS Command Line Interface

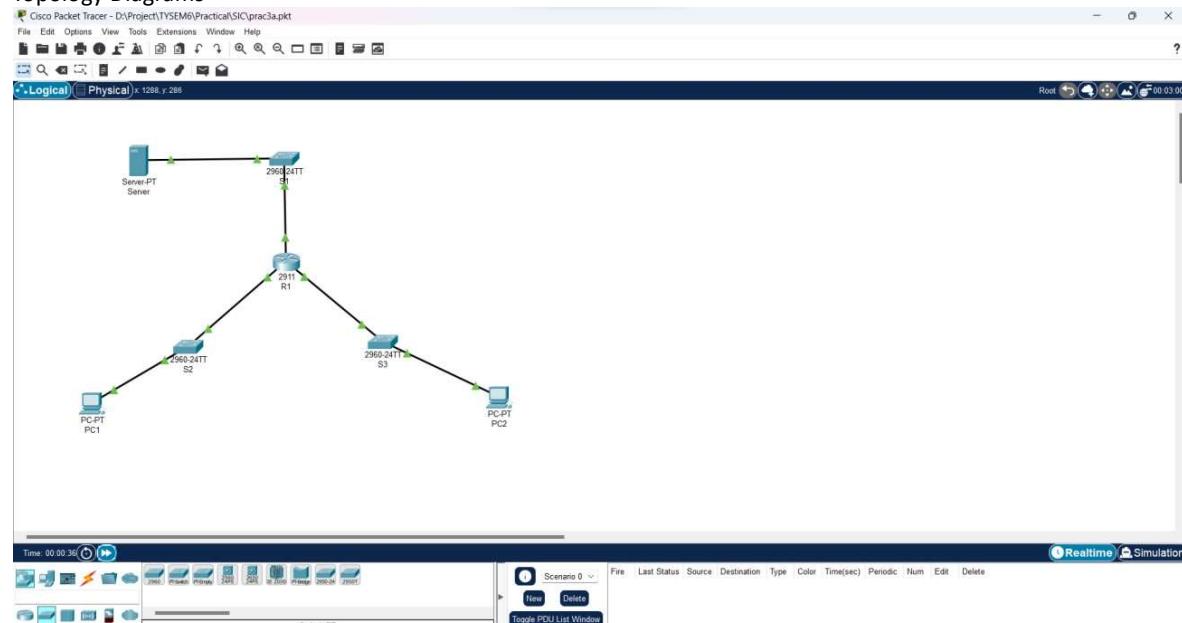
```
User Access Verification
Username: admin3
Password:
```

SECURITY IN COMPUTING

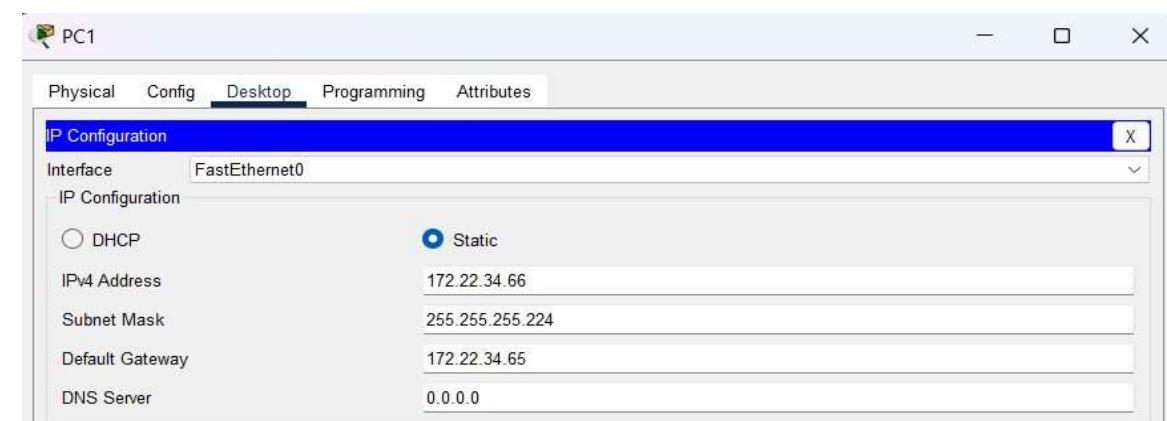
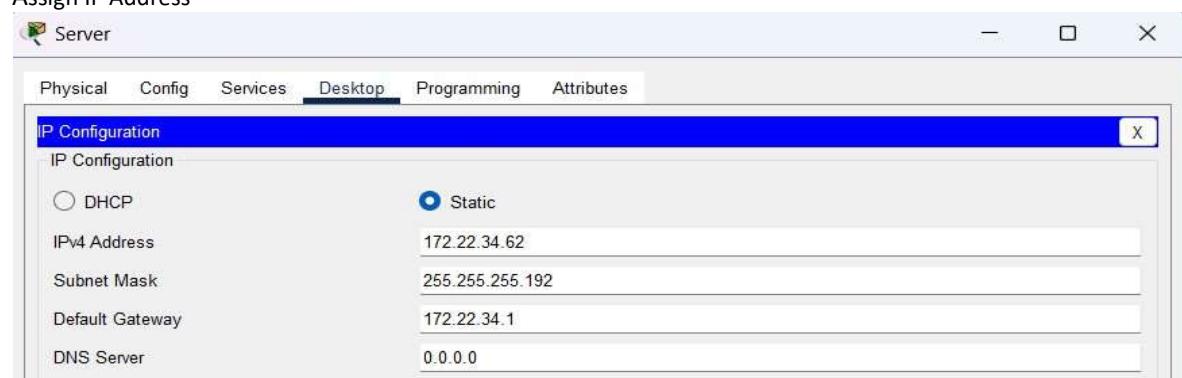
Practical 3a

Aim: Configuring Extended ACLs.

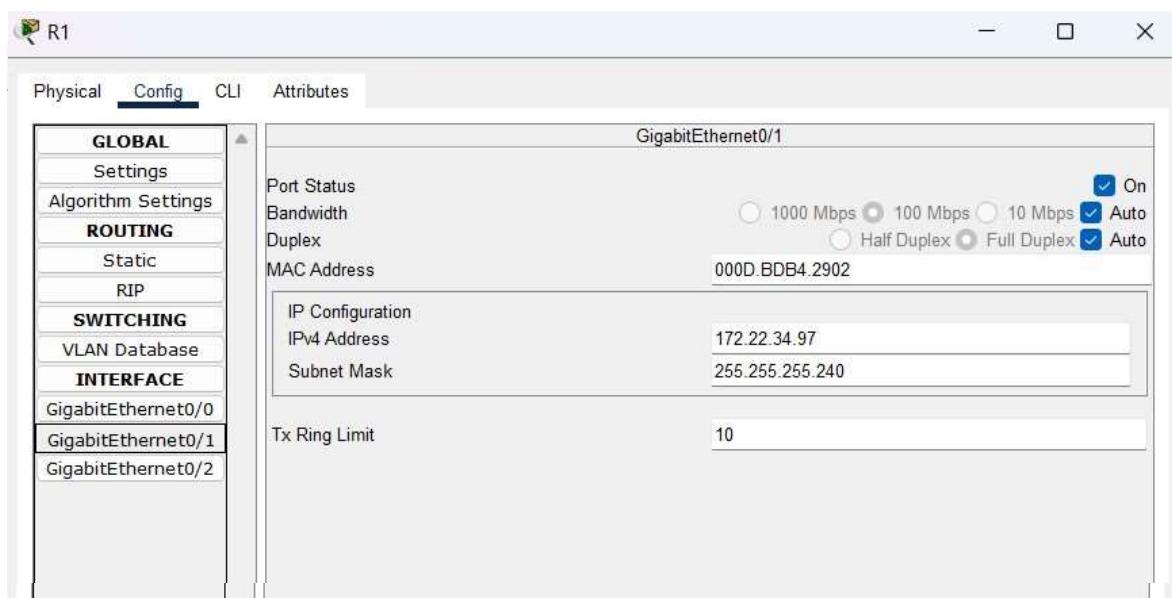
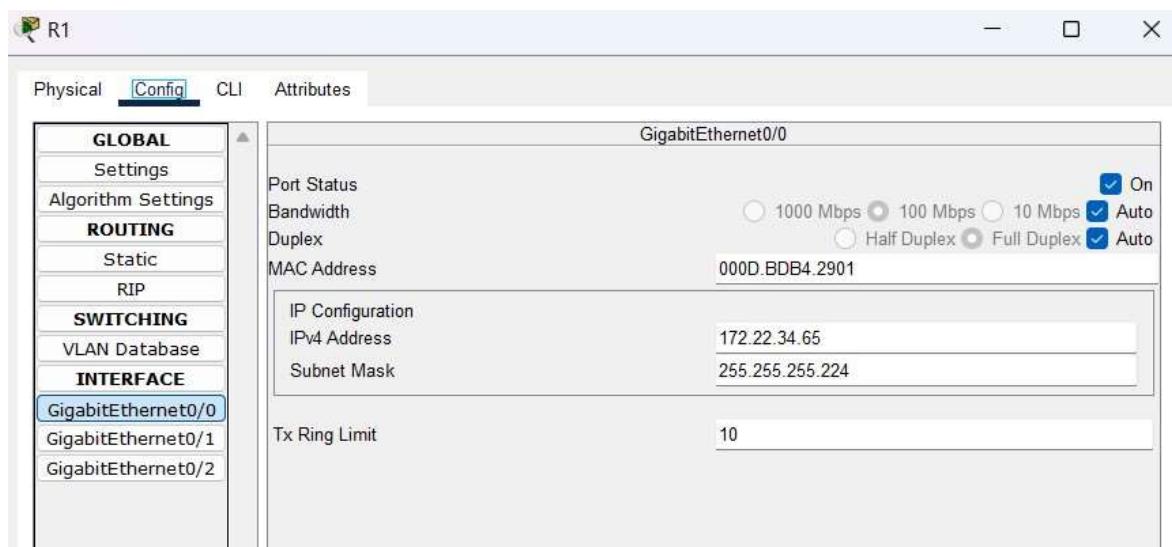
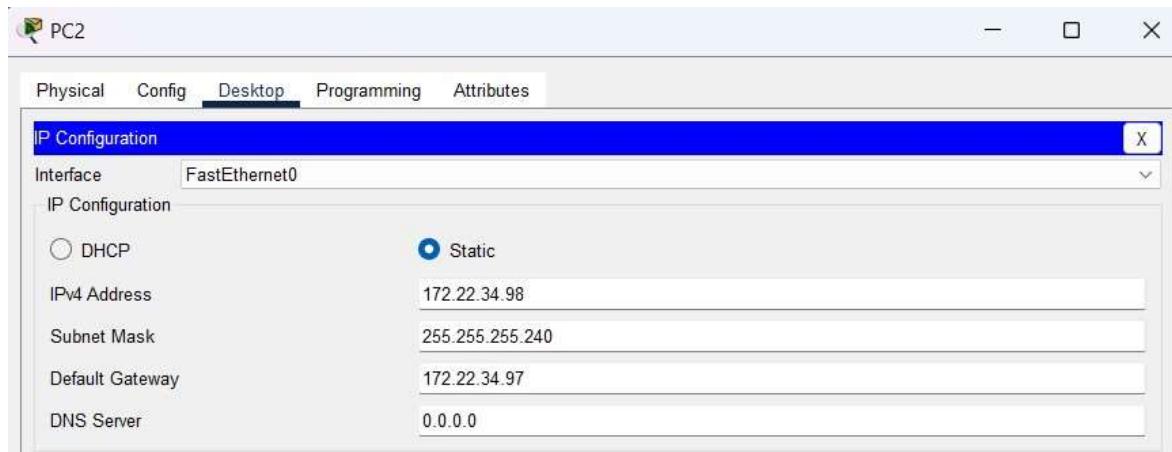
Topology Diagrams



Assign IP Address



SECURITY IN COMPUTING



Displaying IP Address Details of R1

SECURITY IN COMPUTING

R1>show ip interface brief

Interface	IP-Address	OK? Method Status	Protocol
GigabitEthernet0/0	172.22.34.65	YES manual up	up
GigabitEthernet0/1	172.22.34.97	YES manual up	up
GigabitEthernet0/2	172.22.34.1	YES manual up	up

Performing Ping from PC1 to Server and PC2

The screenshot shows a Cisco Packet Tracer window titled "PC1". The "Desktop" tab is selected. A "Command Prompt" window is open, showing the following command and its output:

```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 172.22.34.98

Pinging 172.22.34.98 with 32 bytes of data:

Request timed out.
Reply from 172.22.34.98: bytes=32 time<1ms TTL=127
Reply from 172.22.34.98: bytes=32 time<1ms TTL=127
Reply from 172.22.34.98: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Request timed out.
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Performing Ping from PC2 to server and PC1

The screenshot shows a Cisco Packet Tracer window titled "PC2". The "Desktop" tab is selected. A "Command Prompt" window is open, showing the following command and its output:

```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 172.22.34.66

Pinging 172.22.34.66 with 32 bytes of data:

Reply from 172.22.34.66: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:>ping 172.22.34.66

Pinging 172.22.34.66 with 32 bytes of data:

Reply from 172.22.34.66: bytes=32 time<1ms TTL=127
Reply from 172.22.34.66: bytes=32 time=20ms TTL=127
Reply from 172.22.34.66: bytes=32 time<1ms TTL=127
Reply from 172.22.34.66: bytes=32 time<1ms TTL=127

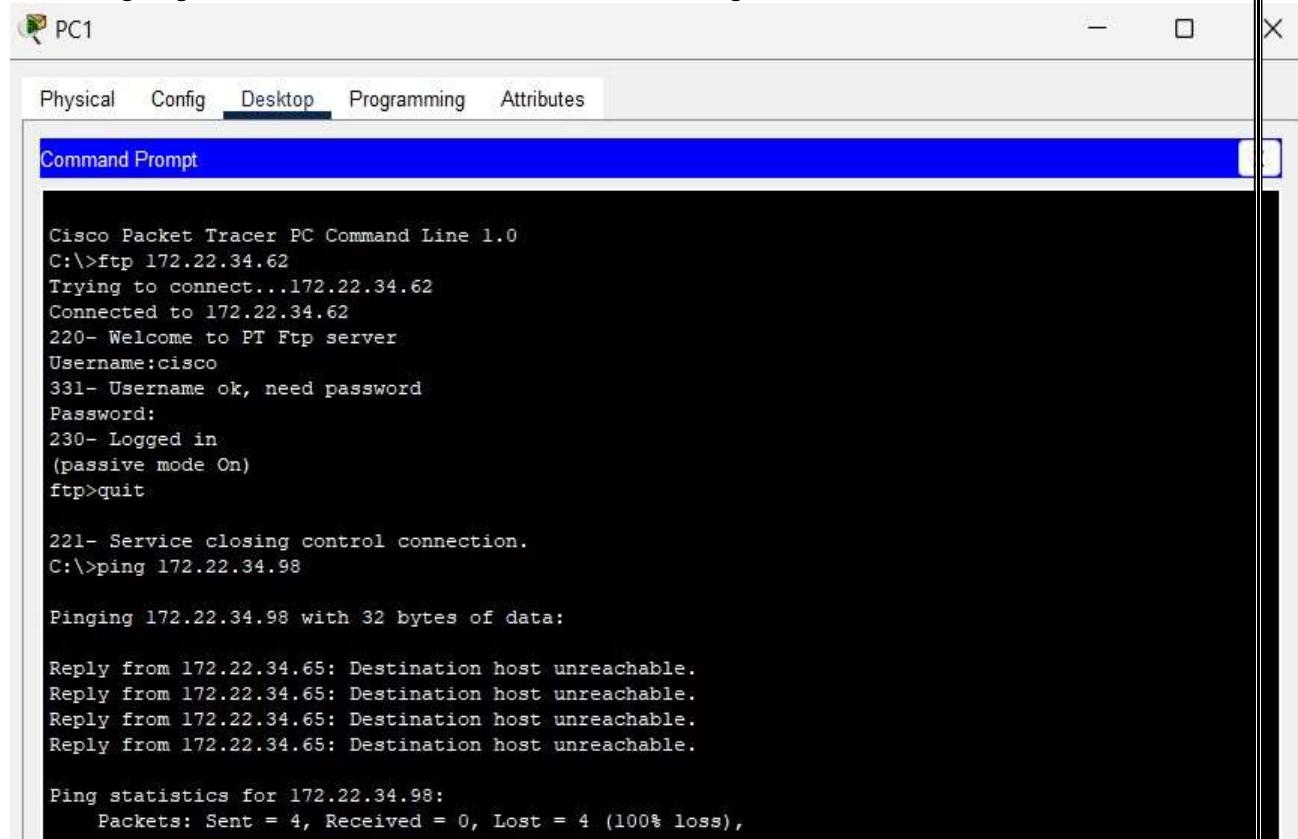
Ping statistics for 172.22.34.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 20ms, Average = 5ms
```

SECURITY IN COMPUTING

Configure, Apply and Verify an Extended Numbered ACL (PC1 needs only FTP access and should be able to ping the server, but not PC2)

```
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?
  dscp      Match packets with given dscp value
  eq       Match only packets on a given port number
  established  established
  gt       Match only packets with a greater port number
  lt       Match only packets with a lower port number
  neq      Match only packets not on a given port number
  precedence  Match packets with given precedence value
  range     Match packets in the range of port numbers
<cr>
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?
<0-65535>  Port number
  ftp      File Transfer Protocol (21)
  pop3    Post Office Protocol v3 (110)
  smtp    Simple Mail Transport Protocol (25)
  telnet   Telnet (23)
  www     World Wide Web (HTTP, 80)
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#{^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

Performing Ping from PC1 to Server and PC2 to check the working of ACL



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:>ping 172.22.34.98

Pinging 172.22.34.98 with 32 bytes of data:

Reply from 172.22.34.65: Destination host unreachable.

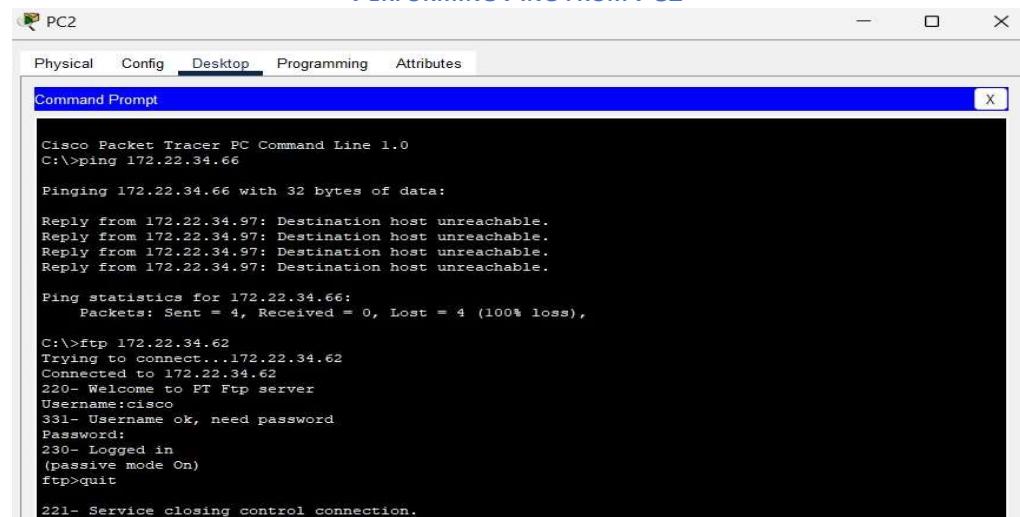
Ping statistics for 172.22.34.98:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

SECURITY IN COMPUTING

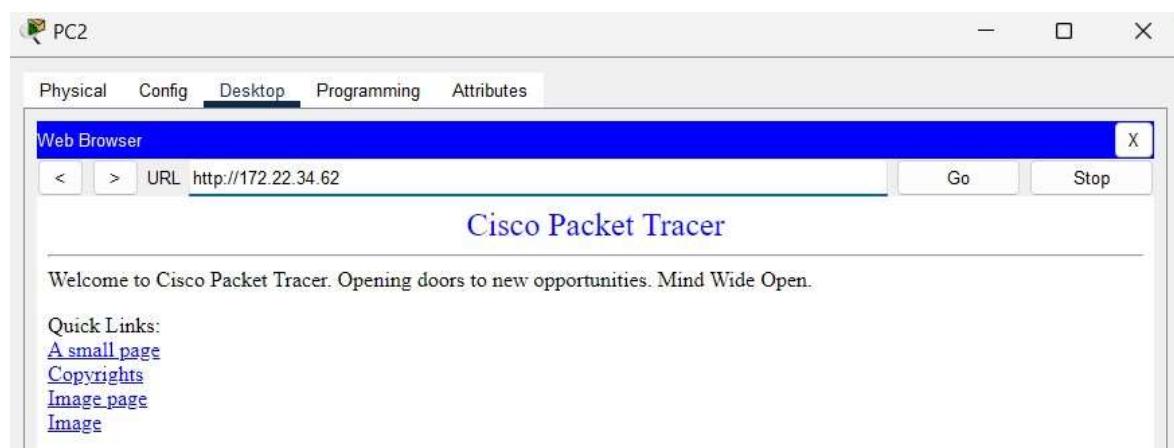
CONFIGURE, APPLY AND VERIFY AND EXTENDED NAMED ACL (PC2 NEEDS ONLY WEB ACCESS AND SHOULD BE ABLE TO PING THE SERVER, BUT NOT PC2)

```
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62
R1(config-ext-nacl)#interface GigabitEthernet0/1
R1(config-if)#ip access-group HTTP_ACL in
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
exit
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list ?
  extended  Extended Access List
  standard  Standard Access List
R1(config)#ip access-list extended ?
  <100-199>  Extended IP access-list number
    WORD        name
R1(config)#ip access-list extended HTTP_ACL
```

PERFORMING PING FROM PC2



TO SERVER AND PC1 TO CHECK THE WORKING OF ACL CHECKING HTTP CONNECTION FROM PC2

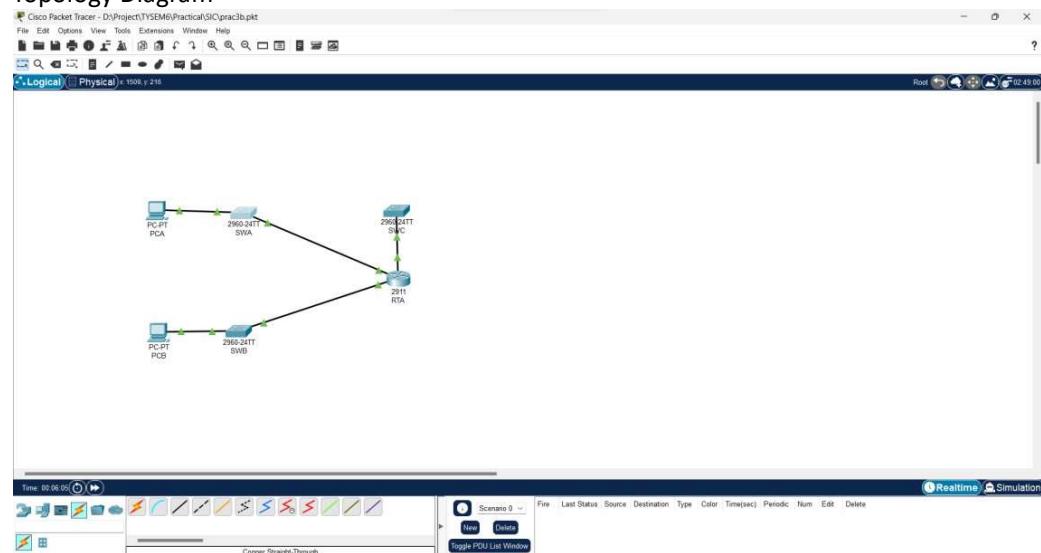


SECURITY IN COMPUTING

Practical 3B

Aim: Configure, Apply and Verify an Extended Numbered ACL

Topology Diagram



Assign IP Addresses

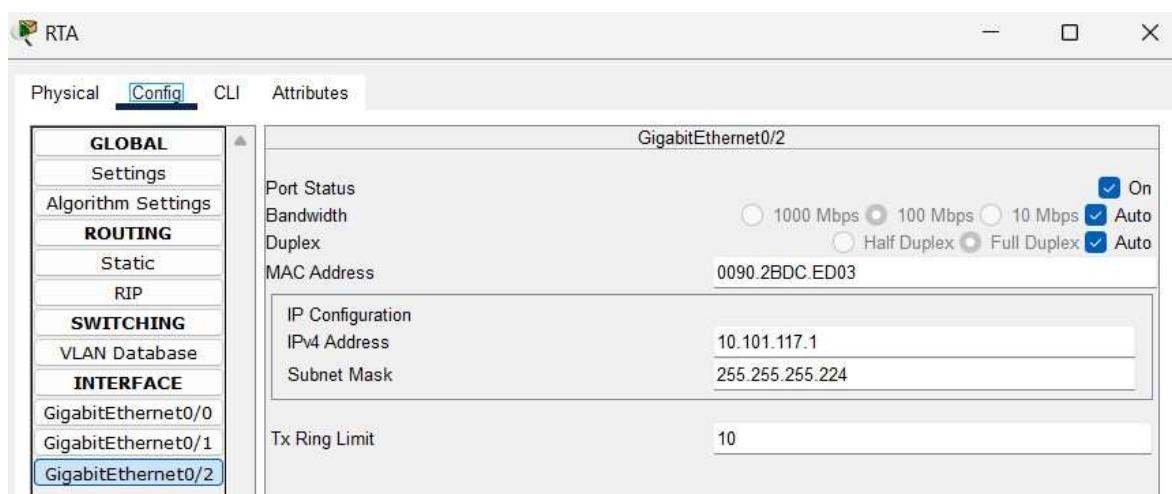
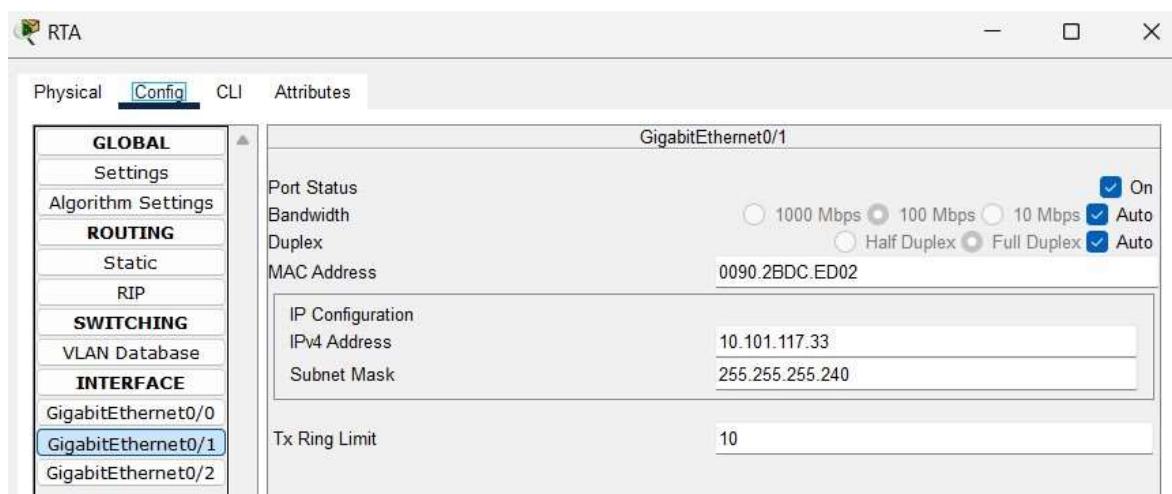
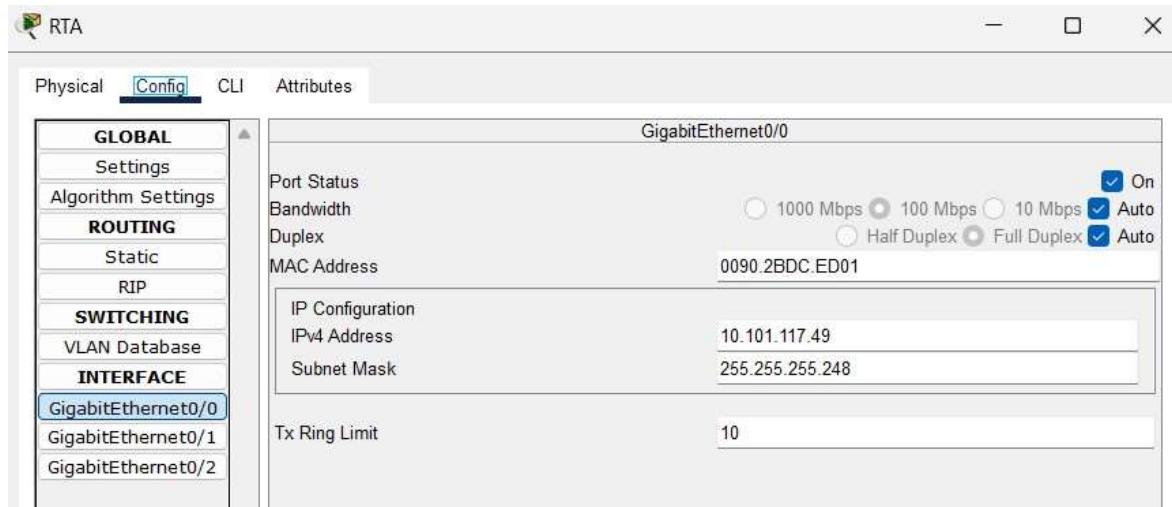
PCA

Physical		Config	Desktop	Programming	Attributes
IP Configuration					
Interface	FastEthernet0				
IP Configuration					
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static				
IPv4 Address	10.101.117.51				
Subnet Mask	255.255.255.248				
Default Gateway	10.101.117.49				
DNS Server	0.0.0.0				

PCB

Physical		Config	Desktop	Programming	Attributes
IP Configuration					
Interface	FastEthernet0				
IP Configuration					
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static				
IPv4 Address	10.101.117.35				
Subnet Mask	255.255.255.240				
Default Gateway	10.101.117.33				
DNS Server	0.0.0.0				

SECURITY IN COMPUTING



SECURITY IN COMPUTING

The image displays three separate windows, each titled "IOS Command Line Interface", showing the configuration of a Cisco switch. The windows are labeled SWA, SWB, and SWC from top to bottom.

SWA Configuration:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host s1
s1(config)#interface vlan 1
s1(config-if)#ip address 10.101.117.50 255.255.255.248
s1(config-if)#no shut

s1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
exit
s1(config)#ip default-gateway 10.101.117.49
s1(config)#+Z
s1#
%SYS-5-CONFIG_I: Configured from console by console

s1#exit
```

SWB Configuration:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host s2
s2(config)#interface vlan 1
s2(config-if)#ip address 10.101.117.34 255.255.255.240
s2(config-if)#no shut

s2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
exit
s2(config)#ip default-gateway 10.101.117.33
s2(config)#+Z
s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#exit
```

SWC Configuration:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host s3
s3(config)#interface vlan 1
s3(config-if)#ip address 10.101.117.2 255.255.255.224
s3(config-if)#no shut

s3(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
exit
s3(config)#ip default-gateway 10.101.117.1
s3(config)#+Z
s3#
%SYS-5-CONFIG_I: Configured from console by console

s3#exit
```

SECURITY IN COMPUTING

Displaying IP Address Details

Router:

```
| RTA>show ip interface brief
| Interface          IP-Address      OK? Method Status      Protocol
| GigabitEthernet0/0  10.101.117.49  YES manual up        up
| GigabitEthernet0/1  10.101.117.33  YES manual up        up
| GigabitEthernet0/2  10.101.117.1   YES manual up        up
| Vlan1              unassigned     YES unset administratively down down
```

S1:

```
| s1>show ip interface brief
| Interface          IP-Address      OK? Method Status      Protocol
| Vlan1              10.101.117.50  YES manual up        up
```

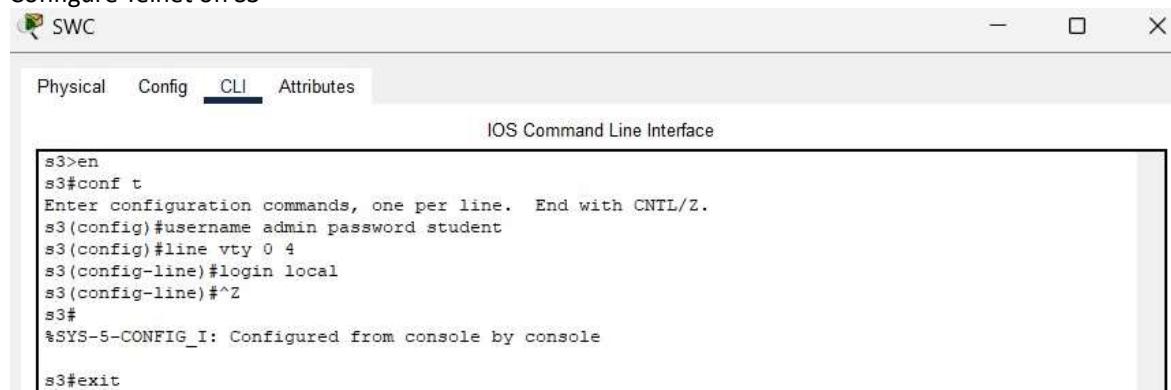
S2:

```
| s2>show ip interface brief
| Interface          IP-Address      OK? Method Status      Protocol
| Vlan1              10.101.117.34  YES manual up        up
```

S3:

```
| s3>show ip interface brief
| Interface          IP-Address      OK? Method Status      Protocol
| Vlan1              10.101.117.2   YES manual up        up
```

Configure Telnet on S3



The screenshot shows a Cisco IOS CLI window titled "SWC". The window has tabs for "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is the text "IOS Command Line Interface". The CLI output is as follows:

```
s3>en
s3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
s3(config)#username admin password student
s3(config)#line vty 0 4
s3(config-line)#login local
s3(config-line)#^Z
s3#
%SYS-5-CONFIG_I: Configured from console by console
s3#exit
```

SECURITY IN COMPUTING

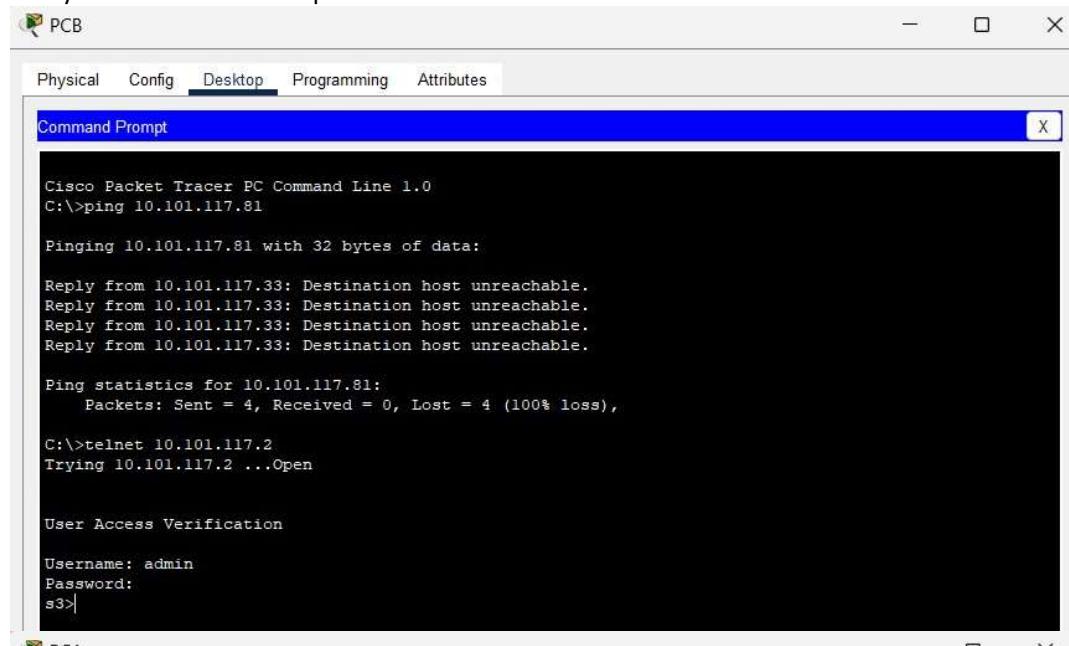
Configure, Apply and verify an extended numbered ACL

(Devices on LAN 10.101.117.32 are allowed to remotely access devices in LAN 10.101.117.0 using the TELNET protocol. Besides ICMP, all traffic from other networks is denied.)

```
RTA(config)#access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq ?
<0-65535> Port number
ftp      File Transfer Protocol (21)
pop3    Post Office Protocol v3 (110)
smtp    Simple Mail Transport Protocol (25)
telnet   Telnet (23)
www     World Wide Web (HTTP, 80)
RTA(config)#access-list 199 permit icmp any any
RTA(config)#interface GigabitEthernet0/2
RTA(config-if)#ip access-group 199 out
RTA(config-if)#^Z
RTA#
%SYS-5-CONFIG_I: Configured from console by console

RTA#exit
```

Verify the extended ACL Implementation



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.101.117.81

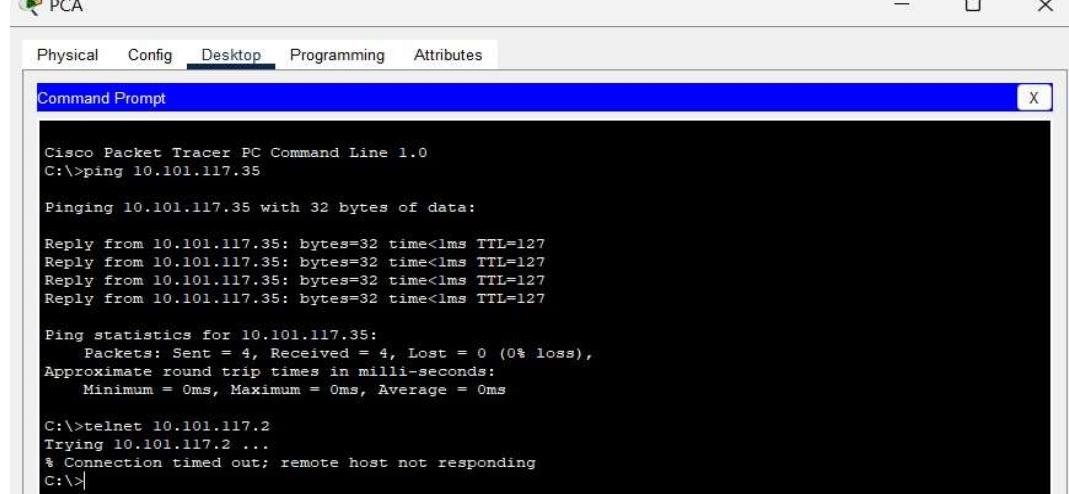
Pinging 10.101.117.81 with 32 bytes of data:

Reply from 10.101.117.33: Destination host unreachable.

Ping statistics for 10.101.117.81:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>telnet 10.101.117.2
Trying 10.101.117.2 ...Open

User Access Verification

Username: admin
Password:
s3>
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.101.117.35

Pinging 10.101.117.35 with 32 bytes of data:

Reply from 10.101.117.35: bytes=32 time<1ms TTL=127

Ping statistics for 10.101.117.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>telnet 10.101.117.2
Trying 10.101.117.2 ...
% Connection timed out; remote host not responding
C:\>
```

Practical 4

Aim:- Configure IP ACLs to Mitigate Attacks

Objectives

- Verify connectivity among devices before firewall configuration.
- Use ACLs to ensure remote access to the routers is available only from management station PC-C.
- Configure ACLs on R1 and R3 to mitigate attacks.
- Verify ACL functionality

Addressing Table

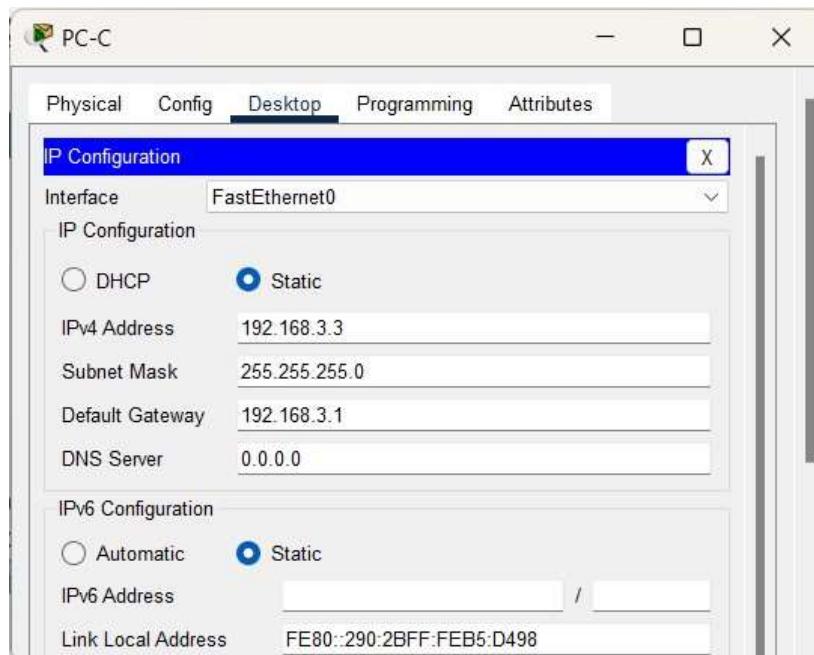
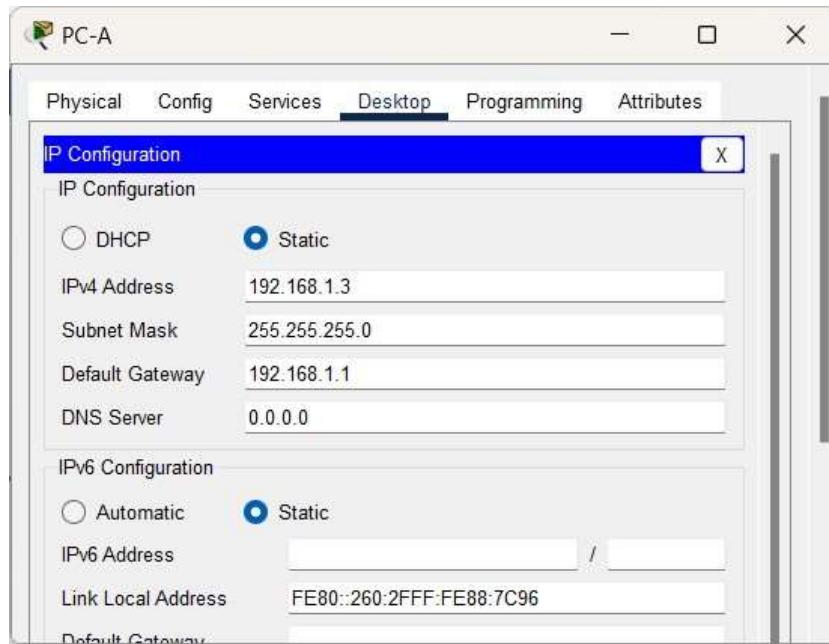
Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A	N/A
R3	G0/1	192.168.3.1	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

Topology



SECURITY IN COMPUTING

Assigning ip



Enable SSH on Router 2

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip domain-name securityincomputing.com

Router(config)#username admin secret pwd

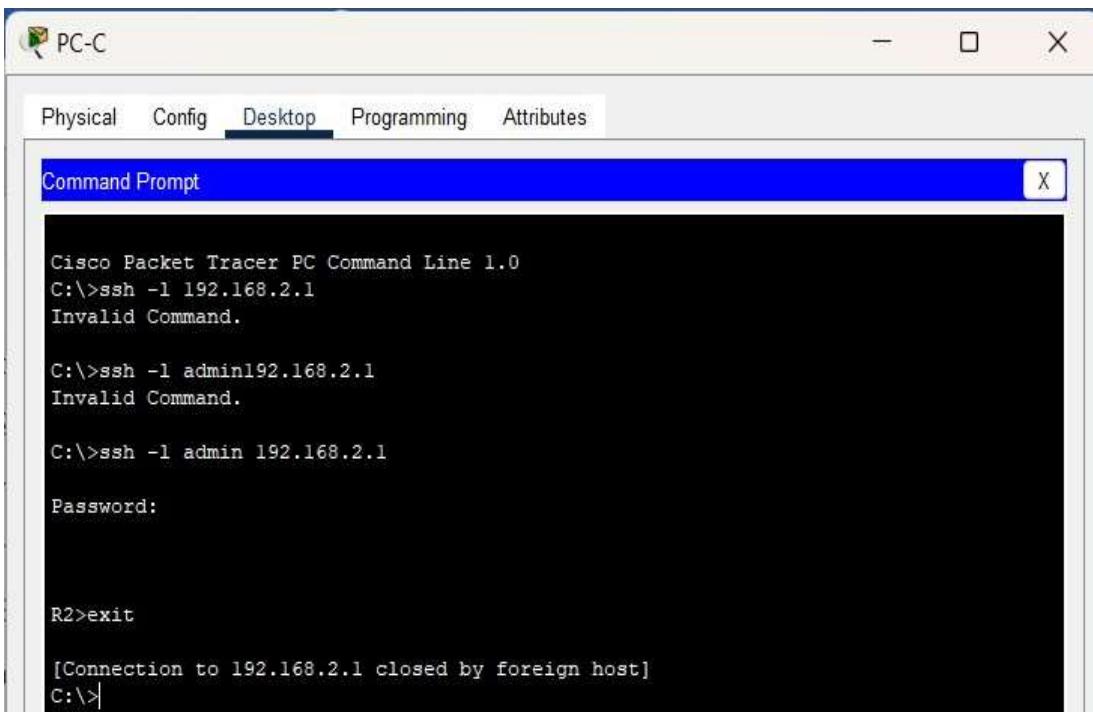
SECURITY IN COMPUTING

```
Router(config)#line vty 0 4
Router(config-line)#login local
Router(config-line)#transport input ssh
Router(config-line)#crypto key zeroize rsa
% No Signature RSA Keys found in configuration.
```

```
Router(config)#crypto key generate rsa
% Please define a hostname other than Router.
Router(config)#hostname R2
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 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#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip ssh authentication-retries 2
R2(config)#ip ssh version 2
```



The screenshot shows a Windows-style window titled "PC-C" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is selected. Inside, a "Command Prompt" window is open with a blue title bar. The command line shows several attempts to connect via SSH to host 192.168.2.1:

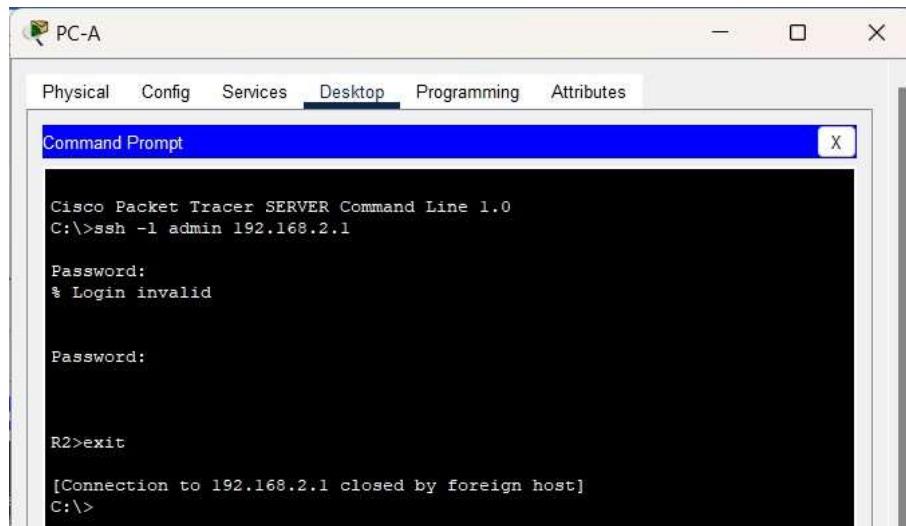
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l 192.168.2.1
Invalid Command.

C:\>ssh -l admin192.168.2.1
Invalid Command.

C:\>ssh -l admin 192.168.2.1
Password:

R2>exit
[Connection to 192.168.2.1 closed by foreign host]
C:\>
```

SECURITY IN COMPUTING



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

Router 1

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#access-list 10 permit host 192.168.3.3

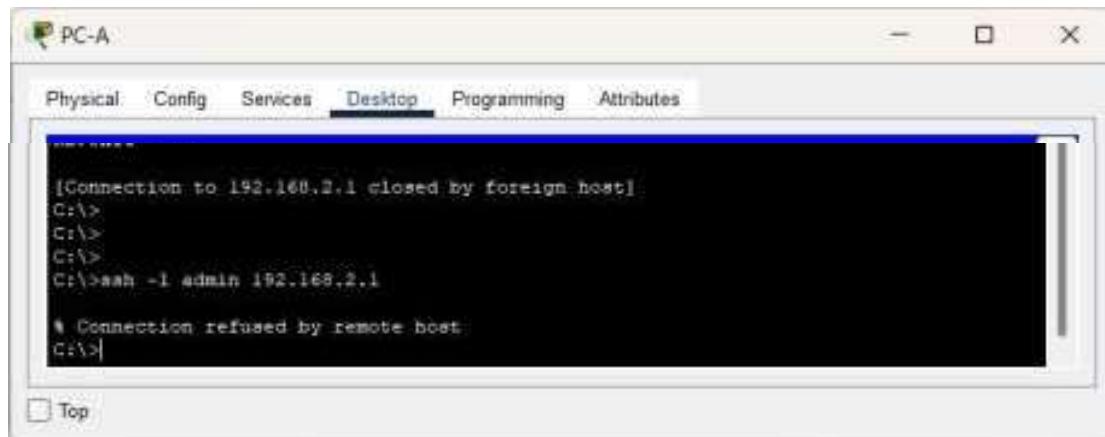
Router(config)#line vty 0 4

Router(config-line)#access-class 10 in

Router(config-line)#^Z

SECURITY IN COMPUTING

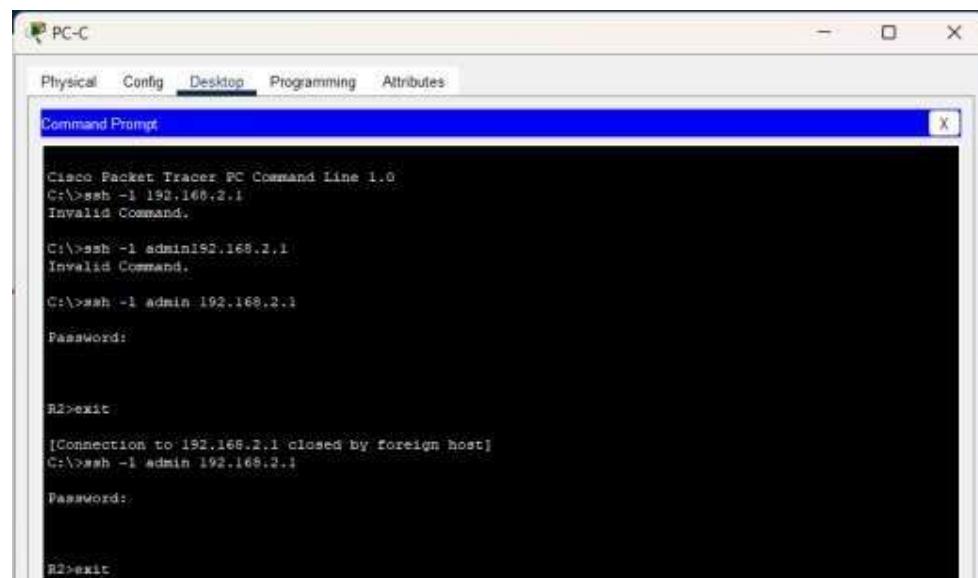
Verify the user with pcA



The screenshot shows a window titled "PC-A" with a tab bar containing "Physical", "Config", "Services", "Desktop", "Programming", and "Attributes". The "Desktop" tab is selected, revealing a terminal window titled "Command Prompt". The terminal output is as follows:

```
[Connection to 192.168.2.1 closed by foreign host]
C:\>
C:\>
C:\>
C:\>ssh -l admin 192.168.2.1
* Connection refused by remote host.
C:\>
```

Below the terminal window, there is a checkbox labeled "Top".



The screenshot shows a window titled "PC-C" with a tab bar containing "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is selected, revealing a terminal window titled "Cisco Packet Tracer PC Command Line 1.0". The terminal output is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l 192.168.2.1
Invalid Command.

C:\>ssh -l admin 192.168.2.1
Invalid Command.

C:\>ssh -l admin 192.168.2.1
Password:

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

R2>exit
```

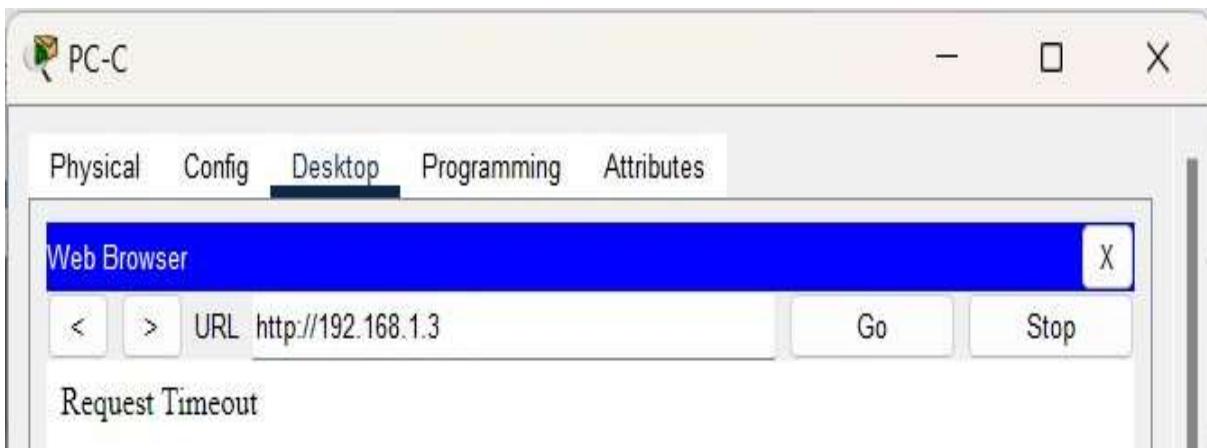
Configure ACL on routers Permit any outside host to access DNS, SMTP, and FTP services on Server o Deny any outside host access to HTTPS services on Server. Permit PCto access RI via SSH.

```
R1>en
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 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)#
```

SECURITY IN COMPUTING



The screenshot shows a window titled "PC-A" with a toolbar containing "Physical", "Config", "Services", "Desktop", "Programming", and "Attributes". The "Desktop" tab is selected. A sub-window titled "Command Prompt" is open, displaying the following terminal session:

```
Invalid Command.
C:\>ls
Invalid Command.

C:\>ssh -l admin 192.168.2.1
Password:

R2>en
* No password set.
R2>en
* No password set.
R2>conf t
^
* Invalid input detected at '^' marker.

R2>en
* No password set.
R2>exit

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

* Connection refused by remote host
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.

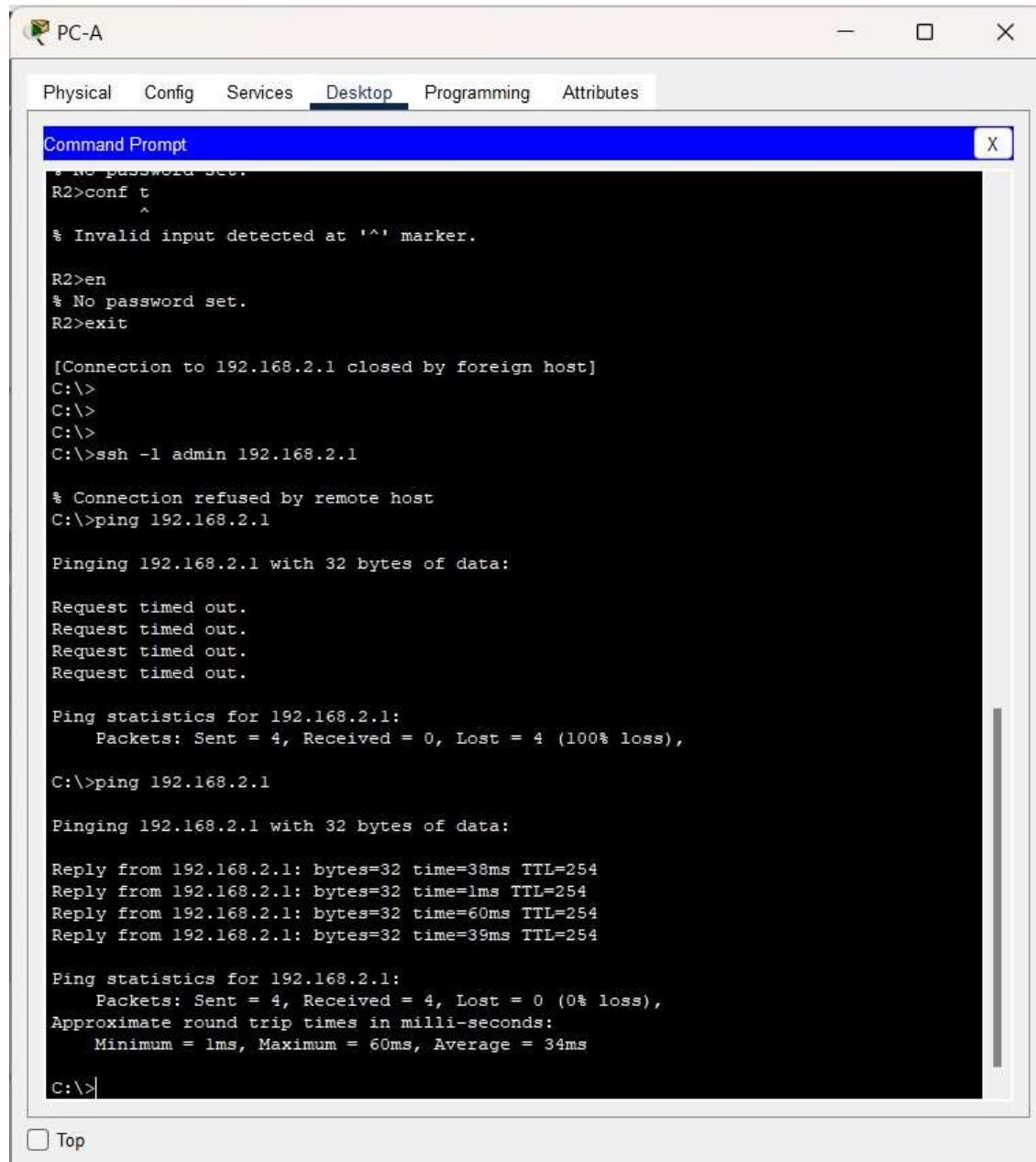
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

At the bottom left of the command prompt window, there is a checkbox labeled "Top".

SECURITY IN COMPUTING

Modify an Existing ACL on R1

```
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
```



The screenshot shows a Windows Command Prompt window titled "PC-A". The window has tabs at the top: Physical, Config, Services, Desktop (which is selected), Programming, and Attributes. The main area of the window displays the following command-line session:

```
* No password set.
R2>conf t
^
% Invalid input detected at '^' marker.

R2>en
% No password set.
R2>exit

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

% Connection refused by remote host
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),
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=38ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=60ms TTL=254
Reply from 192.168.2.1: bytes=32 time=39ms 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 = 60ms, Average = 34ms
C:\>
```

SECURITY IN COMPUTING

CONFIGURE ACL ON ROUTERS

```
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
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)#

```

The screenshot shows a Windows desktop environment with a 'PC-C' icon in the taskbar. A 'Command Prompt' window is open, displaying the following terminal session:

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

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 10.1.1.1: Destination host unreachable.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ssh -l admin 192.168.2.1

Password:

R2>exit

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

Password:
% Password: timeout expired!
% Login invalid

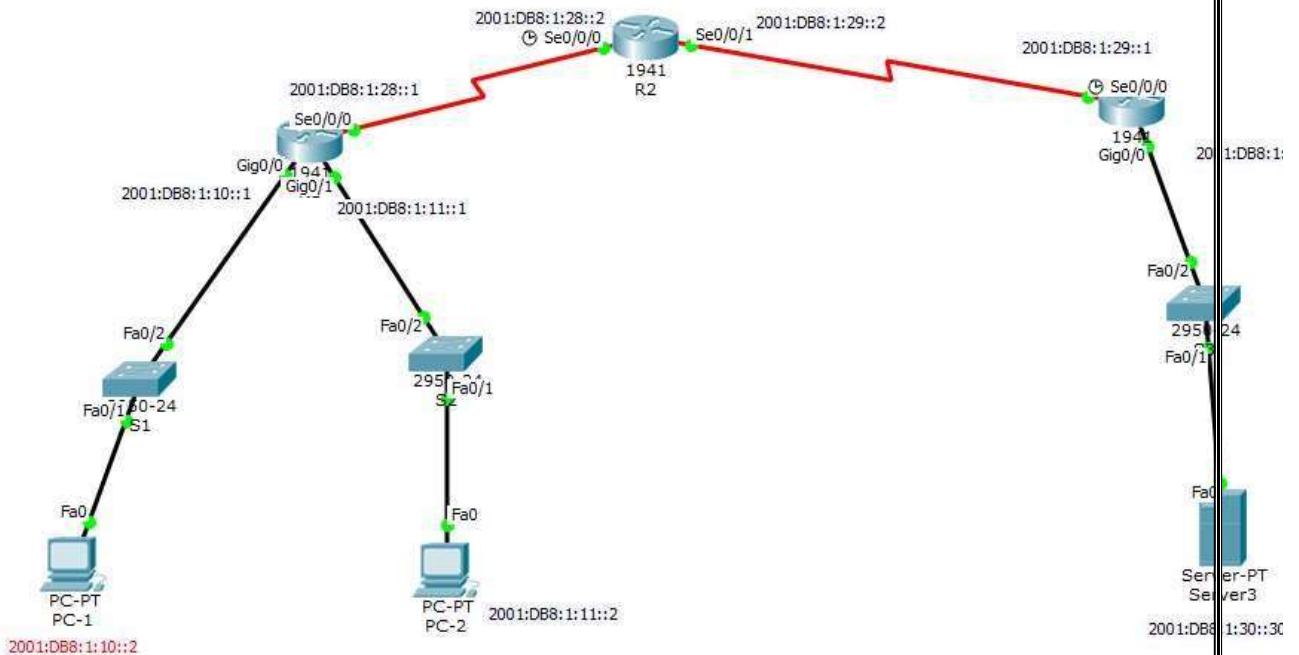
[Connection to 192.168.2.1 closed by foreign host]
C:\>
```

At the bottom left of the Command Prompt window, there is a checkbox labeled 'Top'.

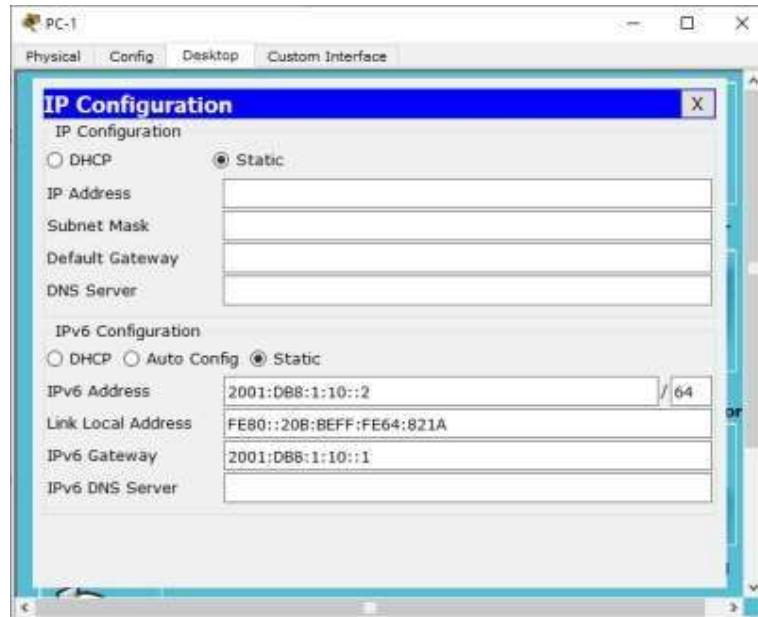
Practical 5

Configuring IPv6 ACLs

Topology

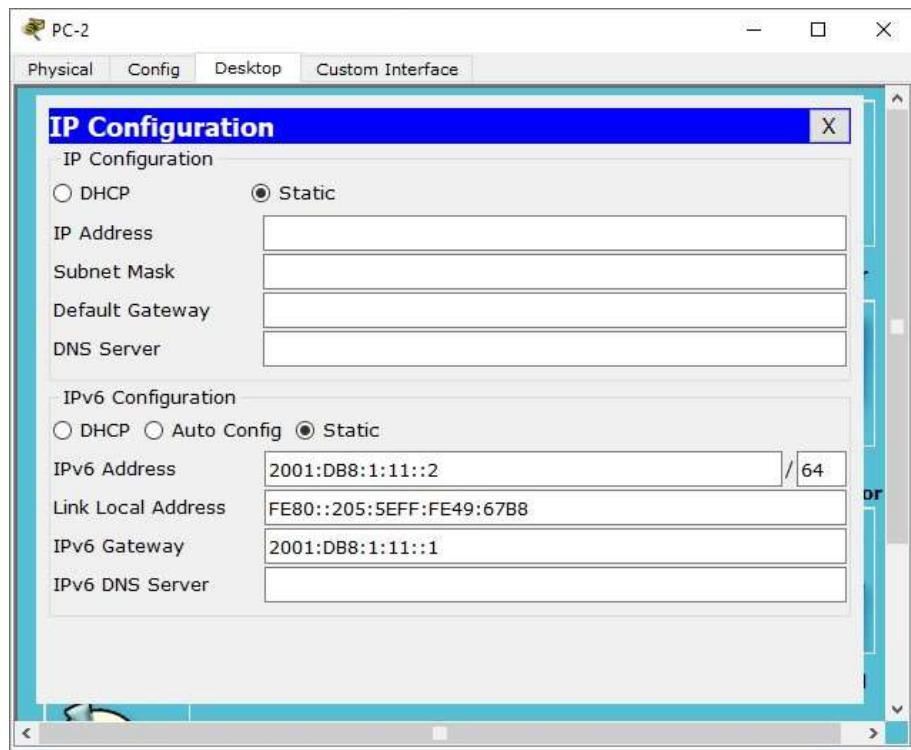


Assign IP Addresses on Pc 1

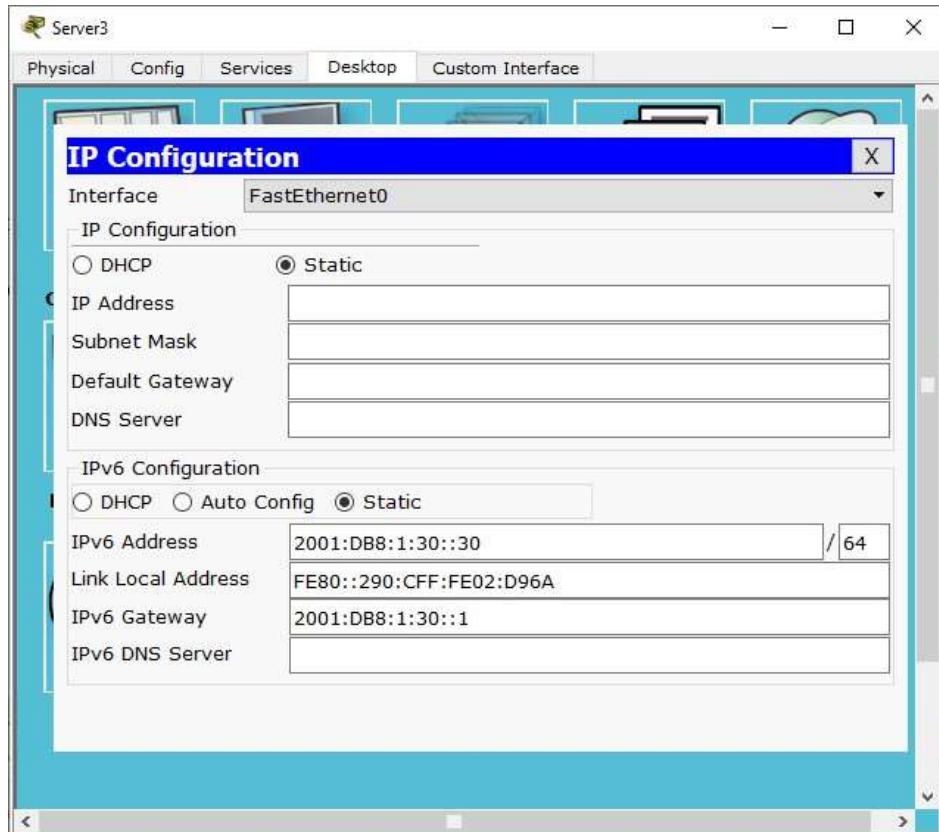


SECURITY IN COMPUTING

ASSIGN IP ADDRESSES ON PC 2



ASSIGN IP ADDRESSES ON SERVER3

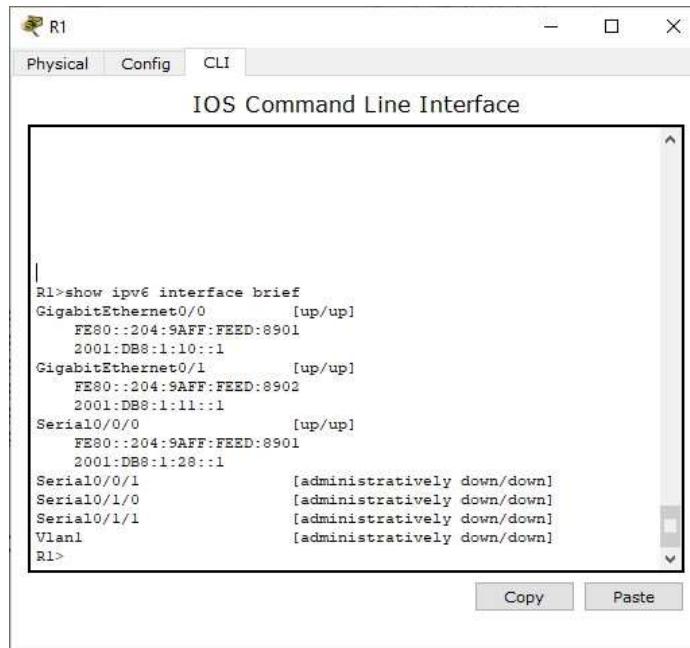


ASSIGN IPV6 ON ROUTER

SECURITY IN COMPUTING

ROUTER 1 CONFIGURATION

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
Router(config)#ipv6 unicast-routing
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:DB8:1:10::1/64
Router(config-if)#no shut
Router(config-if)#interface GigabitEthernet0/1
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:DB8:1:11::1/64
Router(config-if)#no shut
Router(config-if)#interface serial0/0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:DB8:1:28::1/64
Router(config-if)#no shut
```

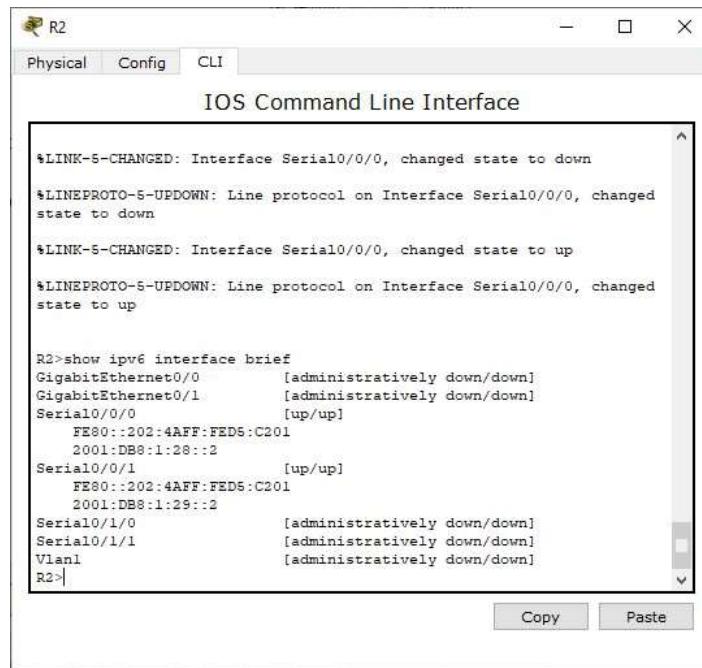


ROUTER 2 CONFIGURATION

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
Router(config)#ipv6 unicast-routing
Router(config)#interface serial0/0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:DB8:1:28::2/64
Router(config-if)#no shut
Router(config-if)#interface serial0/0/1
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:DB8:1:29::2/64
```

SECURITY IN COMPUTING

Router(config-if)#no shut



```
*LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to down

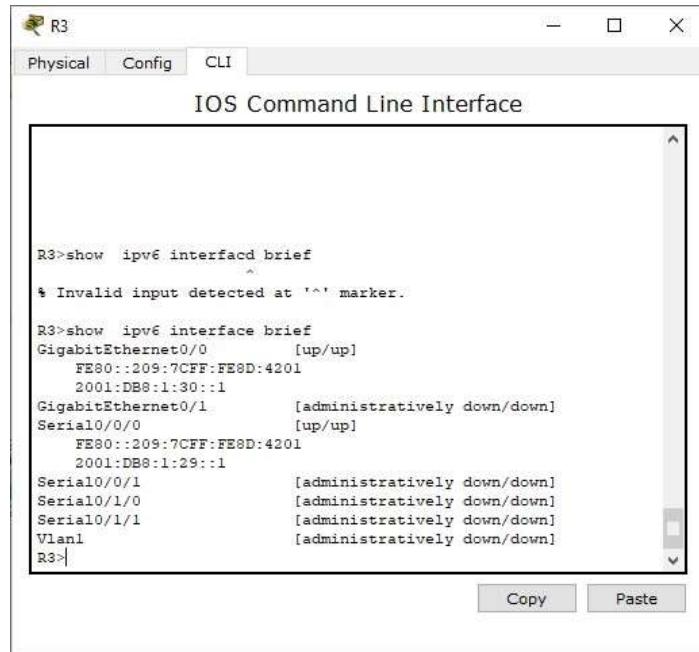
*LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up

R2>show ipv6 interface brief
GigabitEthernet0/0      [administratively down/down]
GigabitEthernet0/1      [administratively down/down]
Serial10/0/0            [up/up]
  FE80::202:4AFF:FE01:201
  2001:DB8:1:28::2
Serial10/0/1            [up/up]
  FE80::202:4AFF:FE01:201
  2001:DB8:1:29::2
Serial10/1/0            [administratively down/down]
Serial10/1/1            [administratively down/down]
Vlan1                  [administratively down/down]
R2>
```

Router 3 Configuration

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
Router(config)#ipv6 unicast-routing
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:DB8:1:30::1/64
Router(config-if)#no shut
Router(config-if)#interface serial0/0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:DB8:1:29::1/64
Router(config-if)#no shut
```

SECURITY IN COMPUTING



The image shows a screenshot of the Cisco IOS Command Line Interface (CLI) running on a router named R3. The window title is "R3". The tabs at the top are "Physical", "Config", and "CLI", with "CLI" being the active tab. The main area displays the command output for "show ipv6 interface brief". The output lists various interfaces with their status: GigabitEthernet0/0 is up/up; GigabitEthernet0/1, Serial0/0/0, Serial0/0/1, and Serial0/1/0 are administratively down/down; and Serial0/1/1 and Vlan1 are also administratively down/down. There is an error message at the top: "% Invalid input detected at '^' marker." at the start of the second command line.

```
R3>show ipv6 interface brief
%
% Invalid input detected at '^' marker.

R3>show ipv6 interface brief
GigabitEthernet0/0          [up/up]
  FE80::209:7CFF:FE8D:4201
  2001:DB8:1:30::1
GigabitEthernet0/1          [administratively down/down]
Serial0/0/0                 [up/up]
  FE80::209:7CFF:FE8D:4201
  2001:DB8:1:29::1
Serial0/0/1                 [administratively down/down]
Serial0/1/0                 [administratively down/down]
Serial0/1/1                 [administratively down/down]
Vlan1                       [administratively down/down]
R3>
```

RIP CONFIGURATION

Rip on router 1

```
ipv6 router rip Ripng interface GigabitEthernet0/0 ipv6 rip ripng enable interface GigabitEthernet0/1
ipv6 rip Ripng enable interface serial0/0/0 ipv6 rip Ripng enable
```

Rip on router 2

```
interface serial0/0/0 ipv6 rip Ripng enable interface serial0/0/1
ipv6 rip Ripng enable
```

Rip on router 3

```
interface GigabitEthernet0/0 ipv6 rip Ripng enable interface serial0/0/0
ipv6 rip Ripng enable
```

Checking network connectivity

SECURITY IN COMPUTING

PC-1

Physical Config Desktop Custom Interface

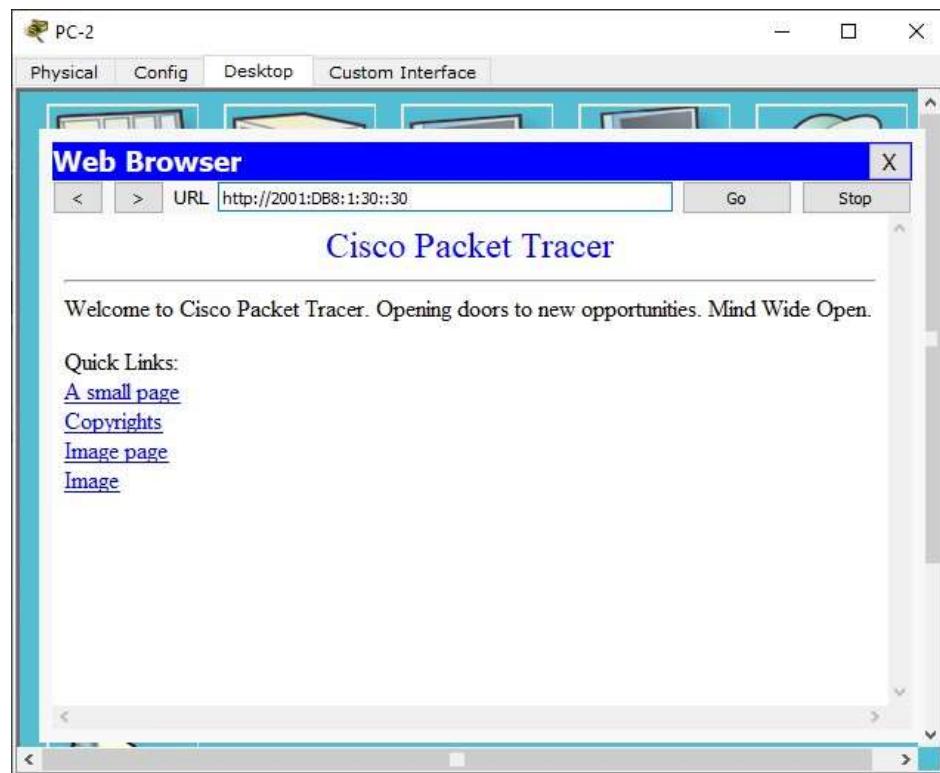
Command Prompt

```
PC>ping 2001:DB8:1:11::2
Pinging 2001:DB8:1:11::2 with 32 bytes of data:
Reply from 2001:DB8:1:11::2: bytes=32 time=11ms TTL=127
Reply from 2001:DB8:1:11::2: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:1:11::2: bytes=32 time=0ms TTL=127
Reply from 2001:DB8:1:11::2: bytes=32 time=0ms TTL=127

Ping statistics for 2001:DB8:1:11::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

PC>ping 2001:DB8:1:30::30
Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=3ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 13ms, Average = 5ms
```



SECURITY IN COMPUTING

Configuring ACL

(Block HTTP and HTTPS access and Allow all other IPv6 traffic to pass)

Router 1

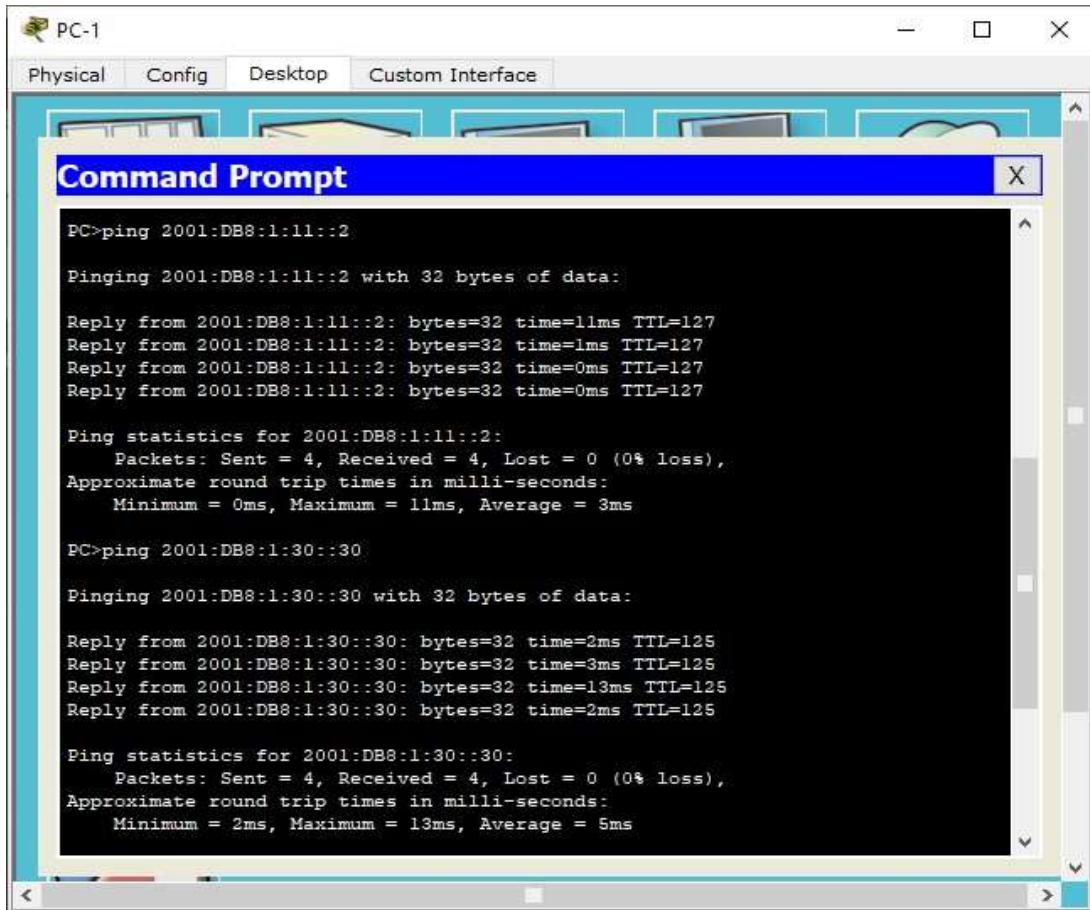
```
Router(config)#  
Router(config)#ipv6 access-list Block_https_acl  
Router(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www  
Router(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443  
Router(config-ipv6-acl)#permit ipv6 any any  
Router(config-ipv6-acl)#interface gigabitethernet0/0  
Router(config-if)#ipv6 traffic-filter Block_https_acl in  
Router(config-if)#^Z  
Router#
```

The screenshot shows a Cisco IOS Command Line Interface window titled 'IOS Command Line Interface'. The window has tabs for 'Physical', 'Config', and 'CLI', with 'CLI' being active. The title bar includes a logo and the identifier 'R1'. The main area displays the configuration commands entered by the user:

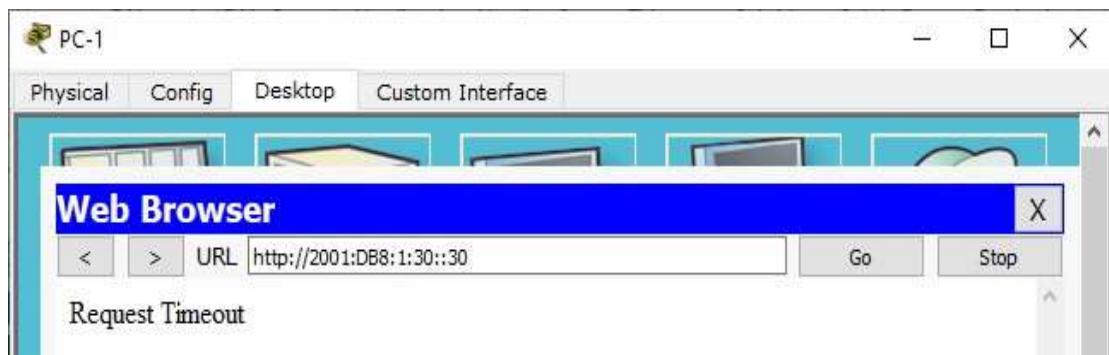
```
Router(config-if)#ex  
Router(config)#  
Router(config)#ipv6 access-list Block_https_acl  
Router(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www  
Router(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443  
Router(config-ipv6-acl)#permit ipv6 any any  
Router(config-ipv6-acl)#interface gigabitethernet0/0  
Router(config-if)#ipv6 traffic-filter Block_https_acl in  
Router(config-if)#^Z  
Router#  
%SYS-5-CONFIG_I: Configured from console by console
```

At the bottom of the terminal window, a message indicates that 'Router con0 is now available'. Below the terminal window are two buttons: 'Copy' and 'Paste'.

Verifying the working of ACL



PC>ping 2001:DB8:1:11::2
Pinging 2001:DB8:1:11::2 with 32 bytes of data:
Reply from 2001:DB8:1:11::2: bytes=32 time=11ms TTL=127
Reply from 2001:DB8:1:11::2: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:1:11::2: bytes=32 time=0ms TTL=127
Reply from 2001:DB8:1:11::2: bytes=32 time=0ms TTL=127
Ping statistics for 2001:DB8:1:11::2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 11ms, Average = 3ms
PC>ping 2001:DB8:1:30::30
Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=3ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Ping statistics for 2001:DB8:1:30::30:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 13ms, Average = 5ms



SECURITY IN COMPUTING



Configuring ACL (Block ICMP access and Allow all other IPv6 traffic to pass).

Router 3

```
R3>
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 access-list Block_icmp_acl
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#int gigabitethernet0/0
R3(config-if)#ipv6 traffic-filter Block_icmp_acl in
R3(config-if)#^Z
```

A screenshot of a terminal window titled 'R3'. The window displays the configuration commands entered on Router 3. The commands are identical to those shown in the previous text block, starting with 'R3>en' and ending with 'R3(config-if)#^Z'. The configuration includes creating an IPv6 access list named 'Block_icmp_acl', defining rules to deny ICMP and permit all other IPv6 traffic, and applying it to the 'gigabitethernet0/0' interface. A message at the bottom of the terminal window reads '%SYS-5-CONFIG_I: Configured from console by console'.

SECURITY IN COMPUTING

VERIFYING THE WORKING OF ACL

The image shows two NetworkMiner interface windows, labeled PC-1 and PC-2, each containing a Command Prompt window.

PC-1 Command Prompt Output:

```
PC>ping 2001:DB8:1:30::30
Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=3ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=13ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 13ms, Average = 5ms

PC>ping 2001:DB8:1:30::30
Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>
```

PC-2 Command Prompt Output:

```
PC>ping 2001:CB8:1:10::2
Pinging 2001:CB8:1:10::2 with 32 bytes of data:
Reply from 2001:DB8:1:11::1: Destination host unreachable.

Ping statistics for 2001:CB8:1:10::2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 2001:CB8:1:30::30
Pinging 2001:CB8:1:30::30 with 32 bytes of data:
Reply from 2001:DB8:1:11::1: Destination host unreachable.

Ping statistics for 2001:CB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>
```

Practical 6

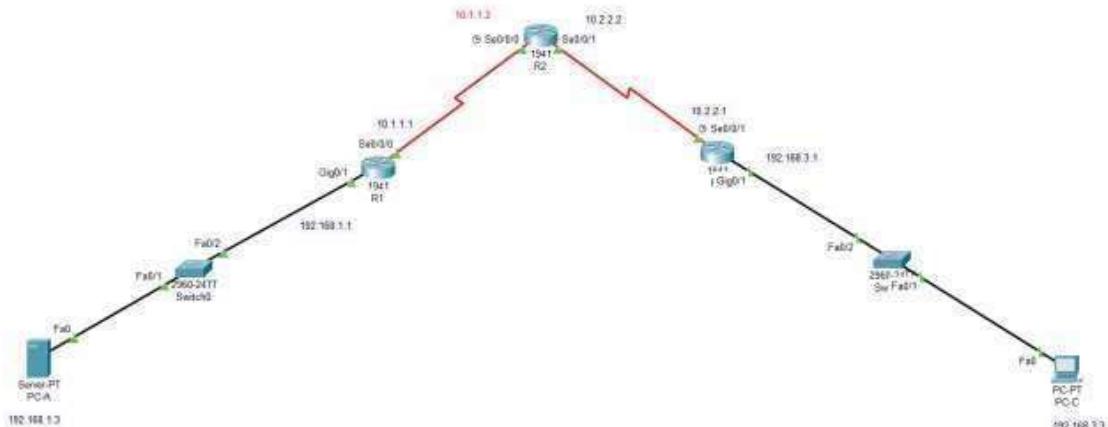
Configuring a Zone-Based Policy Firewall (ZPF)

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
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

Objectives

- Verify connectivity among devices before firewall configuration.
- Configure a zone-based policy (ZPF) firewall on R3.
- Verify ZPF firewall functionality using ping, SSH, and a web browser.

Topology

SECURITY IN COMPUTING

The image displays two windows from a network configuration application. Both windows have tabs for Physical, Config, Services, Desktop, Programming, and Attributes. The Desktop tab is selected.

PC-A Configuration:

IP Configuration	
IP Configuration	X
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

PC-C Configuration:

IP Configuration	
Interface	FastEthernet0
IP Configuration	X
<input type="radio"/> DHCP	<input checked="" type="radio"/> 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

Router 1 Configure

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
R1(config)#interface GigabitEthernet0/1
R1(config-if)#no ip address
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Serial0/0/0
```

SECURITY IN COMPUTING

```
R1(config-if)#ip address 10.1.1.1 255.0.0.0
R1(config-if)#ip address 10.1.1.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#ex
```

Configure Rip on Router 1

```
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.1.1.0
R1(config-router)#ex
R1(config)#
```

Router 2 configure on

```
Router>enable
Router(config)#interface Serial0/0/0 Router(config-if)#no ip address Router(config-if)#ip address
10.1.1.2 255.0.0.0
Router(config-if)#ip address 10.1.1.2 255.0.0.0
Router(config-if)#ip address 10.1.1.2 255.255.255.252
Router(config-if)#ip address 10.1.1.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#end
Router#configure terminal
Router(config)#hostname R2
R2(config)#interface Serial0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shutdown
```

Configure Rip on Router 2

```
R2(config-if)#ex
R2(config)#router rip
R2(config-router)#network 10.1.1.0
R2(config-router)#network 10.2.2.0
R2(config-router)#ex
R2(config)#
```

Router 3 configura on

```
Router>enable
Router#configure terminal
Enter configura on commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#
R3(config)#
R3(config)#
R3(config)#interface GigabitEthernet0/1
R3(config-if)#no ip address
```

SECURITY IN COMPUTING

```
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface Serial0/0/0
R3(config-if)#
R3(config-if)#exit
R3(config)#interface Serial0/0/1
R3(config-if)#ip address 10.2.2.1 255.0.0.0
R3(config-if)#ip address 10.2.2.1 255.0.0.0
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shutdown
Rip configuration on Router 3
R3(config-if)#ex
R3(config)#router rip
R3(config-router)#network 192.168.3.0
R3(config-router)#network 10.2.2.0
R3(config-router)#ex
R3(config)#

```

Configure SSH On Router 2

```
R2(config)#ip domain-name securityincompu ng.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 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 authen ca on-retries 2
```

*Mar 1 0:20:53.121: %SSH-5-ENABLED: SSH 1.99 has been enabled

R2(config)#in ssh version 2

R2(config)#^Z

R2#

Verify Basic Network Connectivity

Step 1: Check connectivity from PCA to PCC

SECURITY IN COMPUTING

Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time=3ms TTL=255
Reply from 192.168.3.1: bytes=32 time=2ms TTL=255
Reply from 192.168.3.1: bytes=32 time=2ms TTL=255
Reply from 192.168.3.1: bytes=32 time=2ms TTL=255
Ping statistics for 192.168.3.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 10ms
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=23ms TTL=125
Reply from 192.168.3.3: bytes=32 time=34ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=48ms 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 = 48ms, Average = 26ms
C:\>

Step 2: Access R2 using SSH.

PCC>ssh -l admin 10.2.2.2

Password:pwd

R2>exit

PC-C
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1
Ping request could not find host 192.168.1... Please check the name and try again.
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=3ms TTL=125
Reply from 192.168.1.3: bytes=32 time=18ms 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 = 36ms, Average = 18ms
C:\>ssh -l admin 10.2.2.2
Password:
R2>ex
[Connection to 10.2.2.2 closed by foreign host]
C:\>

Step 3: From PC-C, open a web browser to the PC-A server. Desktop -> Web Browser

URL: http://192.168.1.3

(Successful)

SECURITY IN COMPUTING



CREATE THE FIREWALL ZONES ON R3

Enable the Security Technology package on R3

R2>

R2>en

R2#show version

Technology Package License Informa on for Module:'c1900'

Technology	Technology-package	Technology-package
Current	Type	Next reboot

ipbase	ipbasek9	Permanent	ipbasek9	security	None
None	None	data	None	None	None

Configura on register is 0x2102

R2#

R3>en

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#license boot module c1900 technology-package securityk9

ACCEPT? [yes/no]: yes

% use 'write' command to make license boot config take effect on next boot

R3(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next reboot level = securityk9 and License = securityk9

R3(config)#ex

R3#

%SYS-5-CONFIG_I: Configured from console by console

R3#reload

System configuration has been modified. Save? [yes/no]:yes Building configuration...

[OK]

Proceed with reload? [confirm]

Device# PID SN

*0 CISCO1941/K9 FTX1524KW47-

SECURITY IN COMPUTING

Technology Package License Information for Module:'c1900'

Technology Technology-package Technology-package
Current Type Next reboot

----- ipbase ipbasek9 Permanent ipbasek9 security
securityk9 Evaluation securityk9 data disable None None
Configuration register is 0x2102

Create a Firewall zones,class Map and ACL on Router 3

```
R3>
R3>enable
R3#
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#zone security IN-ZONE
R3(config-sec-zone)#exit
R3(config)#zone security OUT-ZONE
R3(config-sec-zone)#exit
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)#match access-group 101
R3(config-cmap)#exit
R3(config)#policy-map type inspect IN-2-OUT-PMAP
R3(config-pmap)#class type inspect IN-NET-CLASS-MAP
R3(config-pmap-c)#inspect
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols will be
inspected R3(config-pmap-c)#exit
R3(config-pmap)#exit
R3(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)#exit
R3(config)#interface GigabitEthernet0/0
R3(config)#interface GigabitEthernet0/0
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#ex
R3(config)#interface serial0/0/0
R3(config-if)#zone-member security OUT-ZONE
R3(config-if)#exit
R3(config)#
R3(config)#
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console R3#copy running-config startup-config Des na
on filename [startup-config]?
Building configura on...
[OK]
```

SECURITY IN COMPUTING

```
R3#  
R3>enable  
R3#  
R3#configure terminal  
Enter configuration commands, one per line. End with CONTROL/Z.  
R3(config)#  
R3(config)#zone security IN-OUTZONE  
R3(config)#zone security OUT-ZONE  
R3(config)#zone security OUT-INZONE  
R3(config)#access-list 10 permit ip 192.168.1.0 0.0.0.255 any  
R3(config)#map type inspect match-all IN-NET-CLASS-MAP  
R3(config)#map type inspect access-group 101  
R3(config-map)#exit  
R3(config)#map type inspect IN-I-OUT-MAP  
R3(config-map)#class type inspect IN-NET-CLASS-MAP  
R3(config-map-c)#inspect  
No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols will be  
inspected  
R3(config-map-c)#exit  
R3(config-map)#exit  
R3(config)#zone-pair security IN-I-OUT-PAIR source IN-ZONE destination OUT-ZONE  
R3(config)#zone-pair#service-policy type inspect IN-I-OUT-MAP  
R3(config)#zone-pair#exit  
R3(config)#interface GigabitEthernet2/0  
R3(config)#interface Serial0/0/1  
R3(config)#zone-member security IN-OUTZONE  
R3(config)#interface Serial0/0/0  
R3(config)#zone-member security OUT-ZONE  
R3(config-if)#exit  
R3(config)#exit  
R3(config)#  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up  
  
R3(config)#exit  
R3#  
R3#SYS-5-CONFIG_I: Configured from console by console  
  
R3#copy running-config startup-config  
Destination filename [startup-config]?  
Overwriting configuration...  
(OK)  
R3#
```

Test FireWall Functionality From IN-ZONE to OUT-ZONE

Physical Config Desktop Programming Attributes

Command Prompt X

Password:

R2>ex

[Connection to 10.2.2.2 closed by foreign host]

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=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 = 3, Lost = 1 (25% loss),

 Approximate round trip times in milli-seconds:

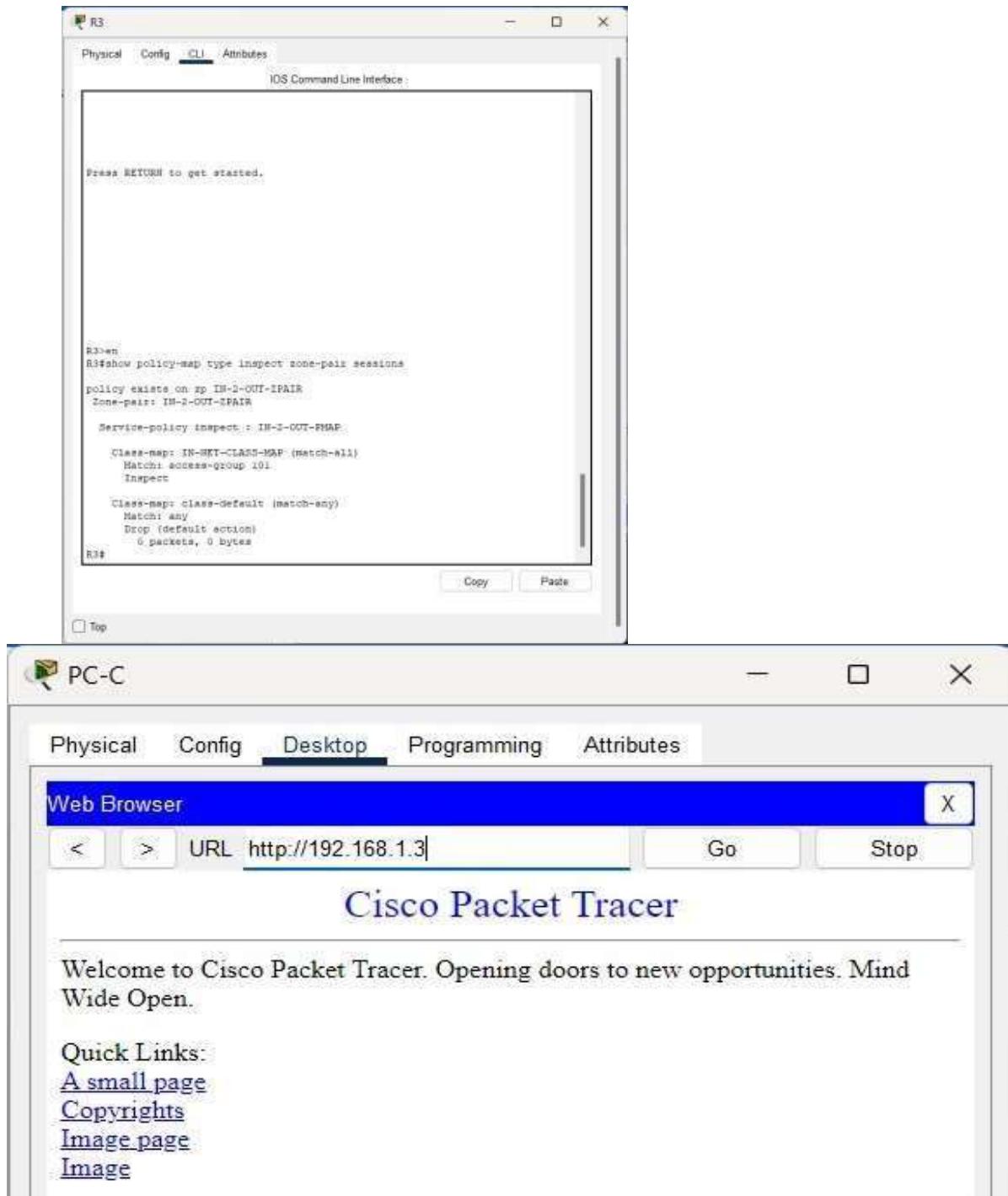
 Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>ssh -l admin 10.2.2.2

Password:

R2>

SECURITY IN COMPUTING



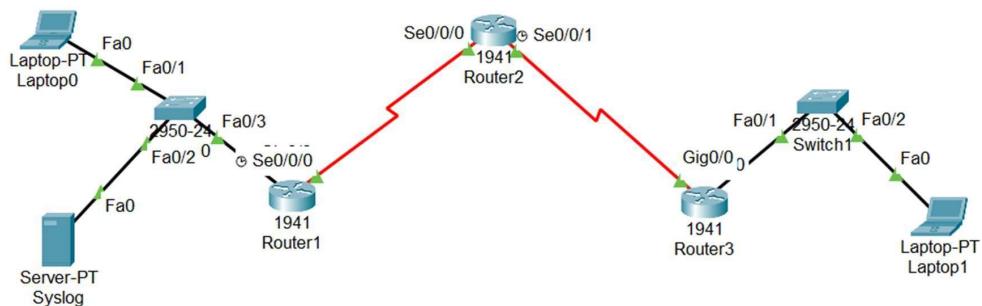
SECURITY IN COMPUTING

PRACTICAL 7

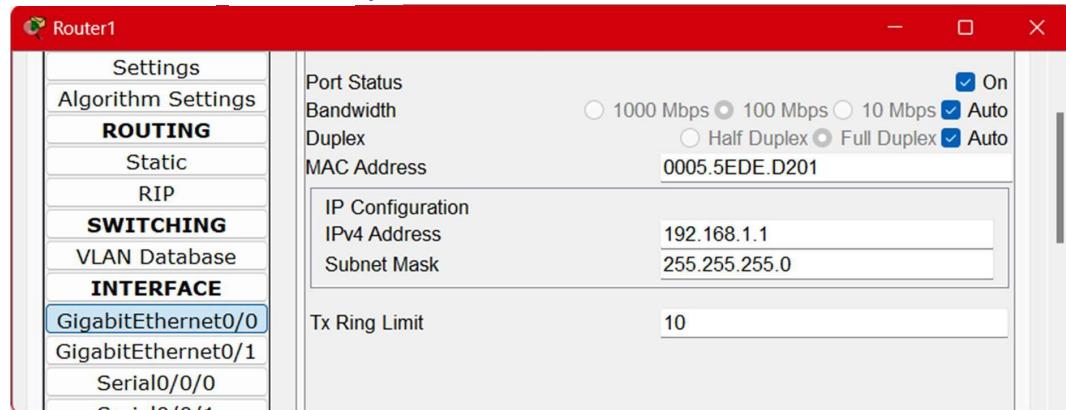
Aim Configure ISO intrusion prevent on system(IPS) using CLI

- Enable IOS IPS
- Modify an IPS signature

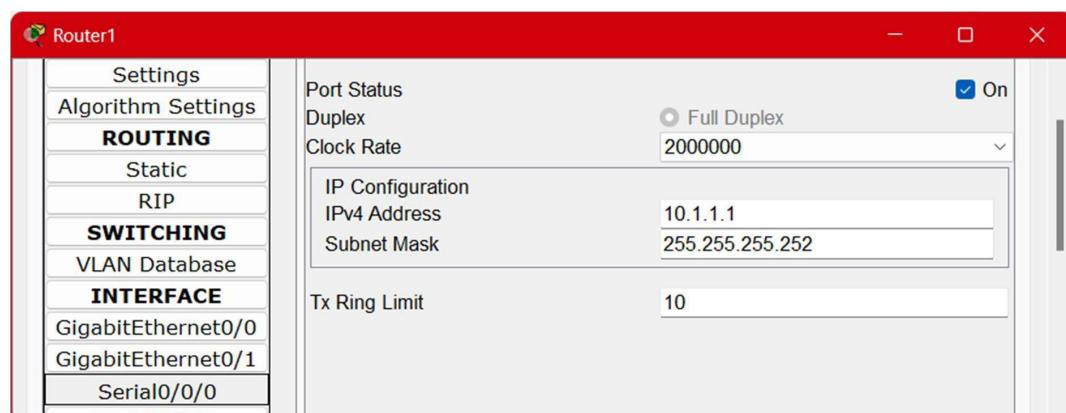
TOPOLOGY



ASSIGN IP TO ROUTER 1 INTERFACE G 0/0

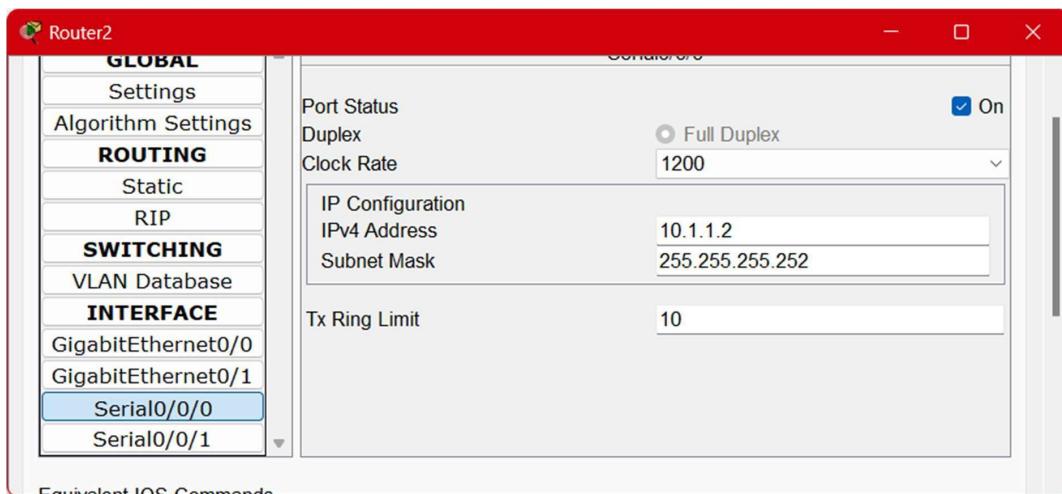


ASSIGN IP TO ROUTER₁ INTERFACE S_{E0/0/0}

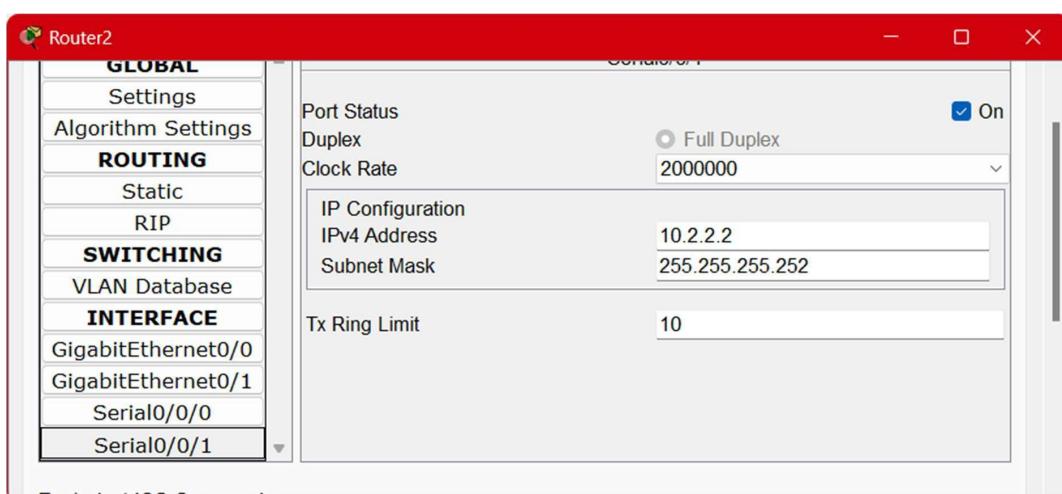


SECURITY IN COMPUTING

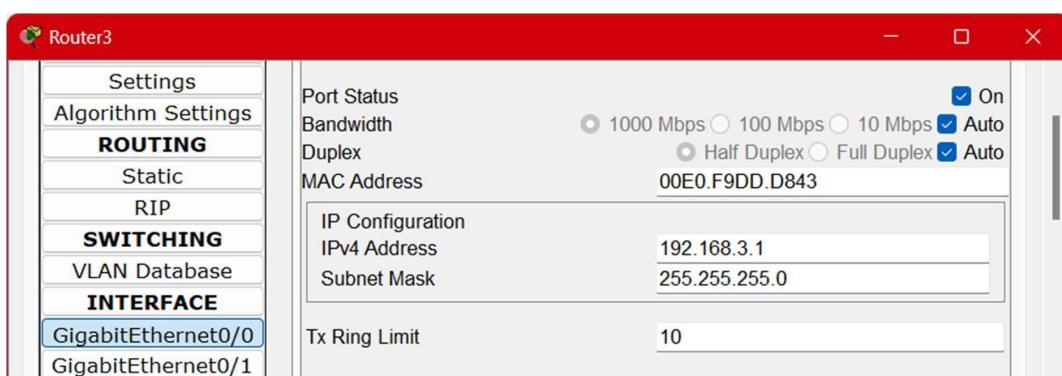
ASSIGN IP TO ROUTER2 INTERFACE S_{E0/0/0}



ASSIGN IP TO ROUTER₃ INTERFACE S_{E0/0/1}

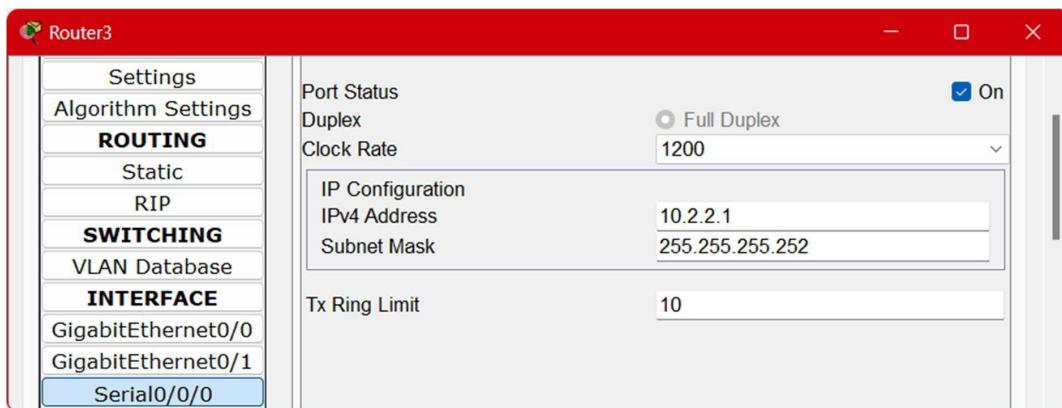


ASSIGN IP TO ROUTER₃ INTERFACE G_{0/0}

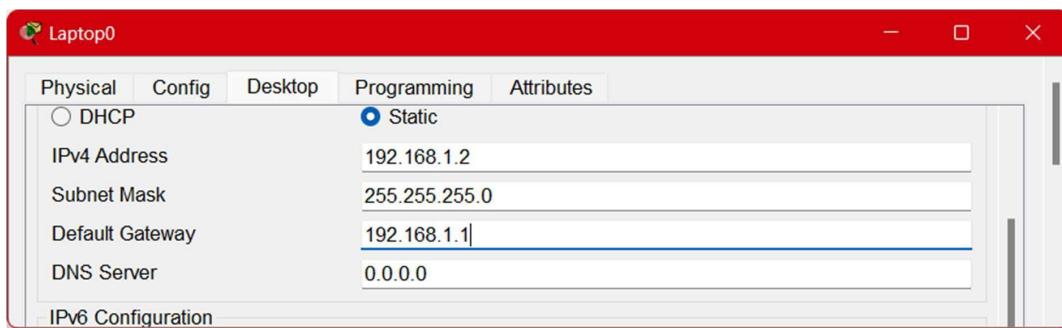


SECURITY IN COMPUTING

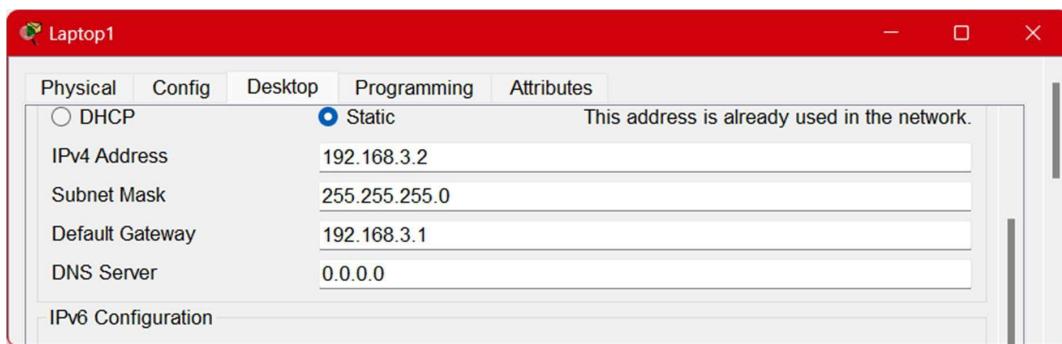
ASSIGN IP TO ROUTER₃ INTERFACE S_{E0/0/0}



IP TO LAPTOP A AND B

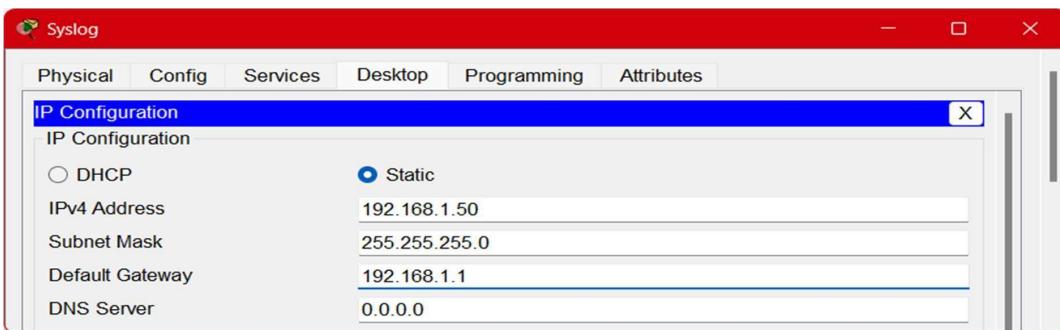


LAPTOP B



SECURITY IN COMPUTING

SYSLOG SERVER IP



CONFIGURE RIP ON ROUTERS



ENABLE THE SECURE TECHNOLOGY PACKAGE OF ROUTER1

```
Router1(config)#lisence boot module c1900 technology-package securityk9  
ACCEPT? [yes/no]: yes  
% use 'write' command to make license boot config take effect on next boot  
Router1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:  
Module name = C1900 Next reboot level = securityk9 and License = securityk9  
Router1(config)#exit  
Router1#  
%SYS-5-CONFIG_I: Configured from console by console reload
```

SECURITY IN COMPUTING

AFTER THIS YOU CAN CHECK USING COMMAND SHOW VERSION

```
Technology Package License Information for Module:'c1900'
-----
Technology Technology-package Technology-package
      Current        Type     Next reboot
-----
ipbase ipbasek9 Permanent ipbasek9 security securityk9 Evaluation securityk9
data       disable           None            None
```

ENABLE IOS IPS ON ROUTER1

```
Router1#mkdir ipsdir
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#ip ips config location flash:ipsdir
Router1(config)#ip ips name iosips
Router1(config)#ip ips notify log
Router1(config)#exit
Router1#
Router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#service timestamps log datetime msec
Router1(config)#ip ips signature-category
Router1(config-ips-category)#category all
Router1(config-ips-category-action)#retired true

Router1(config-ips-category-action)#category ios_ips basic
Router1(config-ips-category-action)#retired false
Router1(config-ips-category-action)#exit
Router1(config-ips-category)#
Router1(config-ips-category)#interface gig0/0
Router1(config-if)#ip ips iosips out Router1(config-if)#
-----
```

MODIFY THE SIGNATURE OF THE IPS

```
Router1#show ip ips all
IPS Signature File Configuration Status Configured Config
Locations: flash:ipsdir Last signature default load time:
Last signature delta load time:
Last event action (SEAP) load time: -none-
General SEAP Config:
```

SECURITY IN COMPUTING

Global Deny Timeout: 3600 seconds

Global Overrides Status: Enabled

Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status

Event notification through syslog is enabled

Event notification through SDEE is enabled

IPS Signature Status

Total Active Signatures: 1

Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status

IPS Rule Configuration

IPS name iosips

IPS fail closed is disabled

IPS deny-action ips-interface is false

Fastpath ips is enabled

Quick run mode is enabled

Interface Configuration

Interface GigabitEthernet0/0

Inbound IPS rule is not set

Outgoing IPS rule is iosips

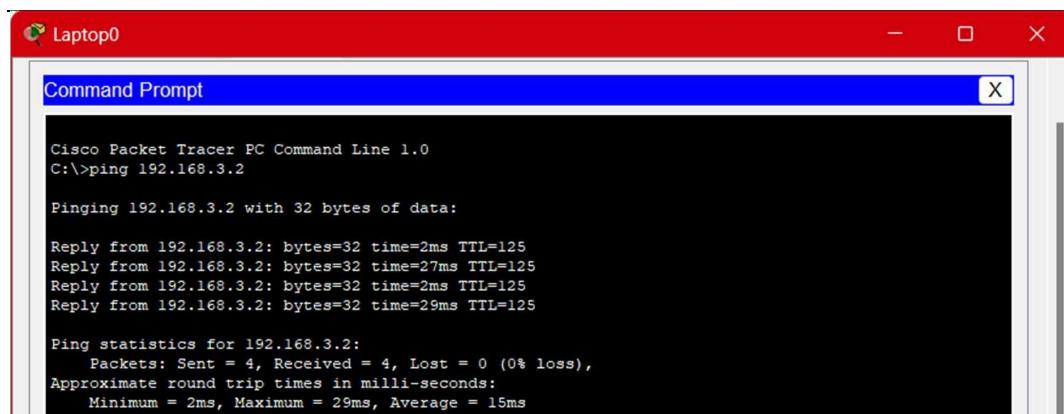
IPS Category CLI Configuration:

Category all

Retire: True

Category ios_ips basic

Retire: False



Laptop0

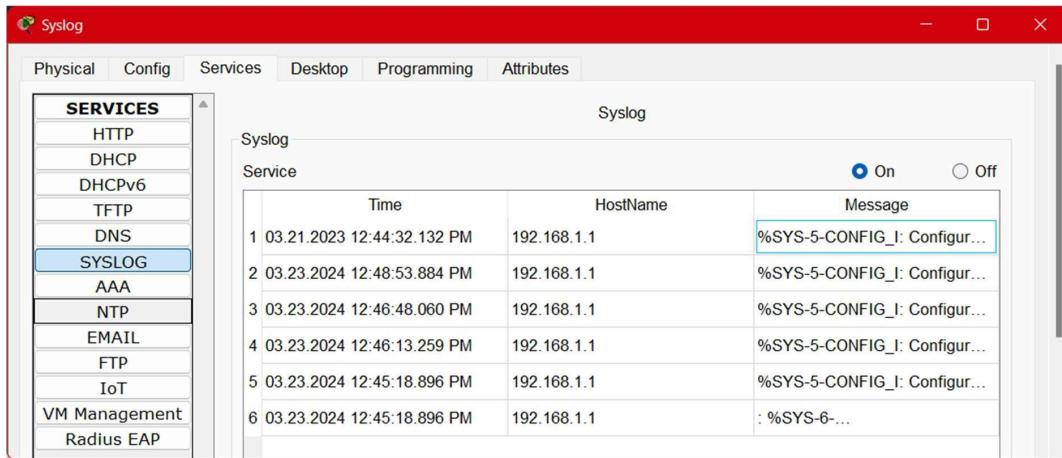
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

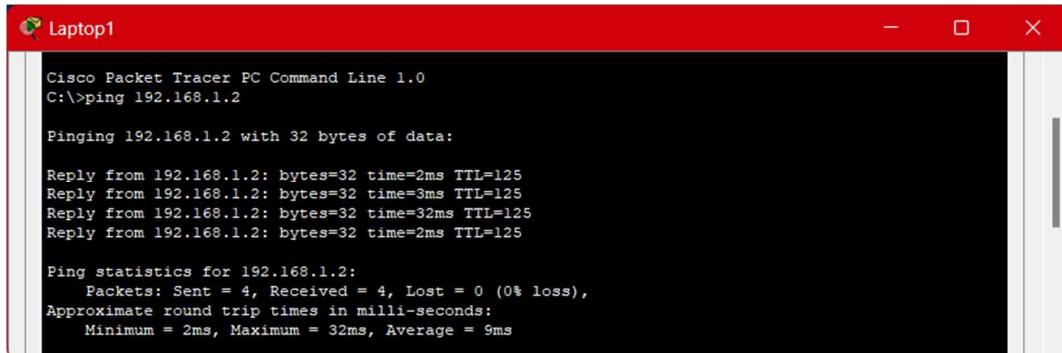
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=27ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=29ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 29ms, Average = 15ms
```

SECURITY IN COMPUTING



before modify the ips



NOW MODIFY THE IPS

```
Router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#ip ips signature-definition
Router1(config-sigdef)#signature 2004 0
Router1(config-sigdef-sig)#status
Router1(config-sigdef-sig-status)#retired false
Router1(config-sigdef-sig-status)#enable true
Router1(config-sigdef-sig-status)#exit
Router1(config-sigdef-sig)#engine
Router1(config-sigdef-sig-engine)#event-action produce-alert
Router1(config-sigdef-sig-engine)#event-action deny-packet-inline
Router1(config-sigdef-sig-engine)#exit
Router1(config-sigdef-sig)#exit
Router1(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILD_STARTED:
```

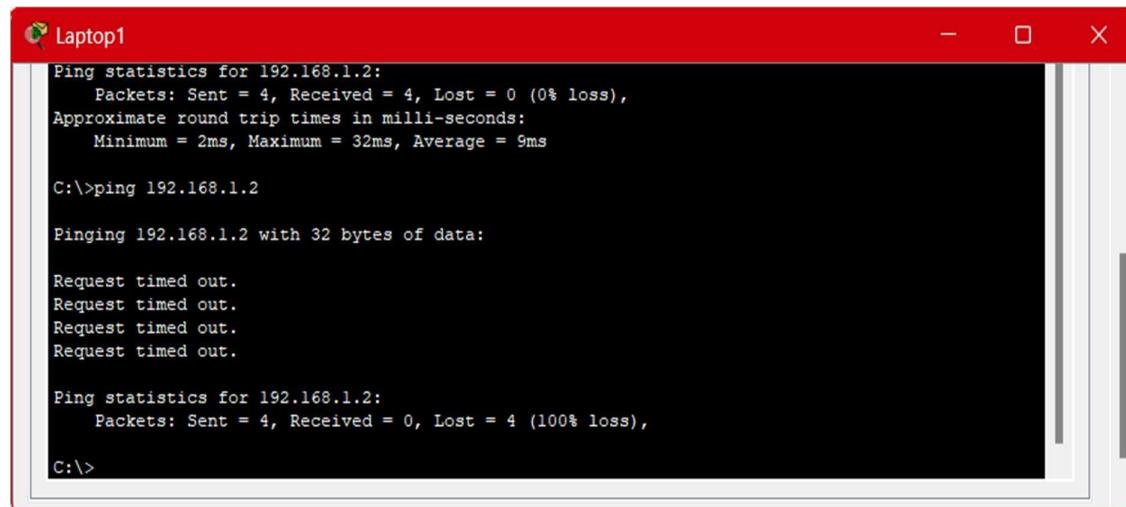
SECURITY IN COMPUTING

%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines

%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine will be scanned

%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms after modifying

modifying the ips



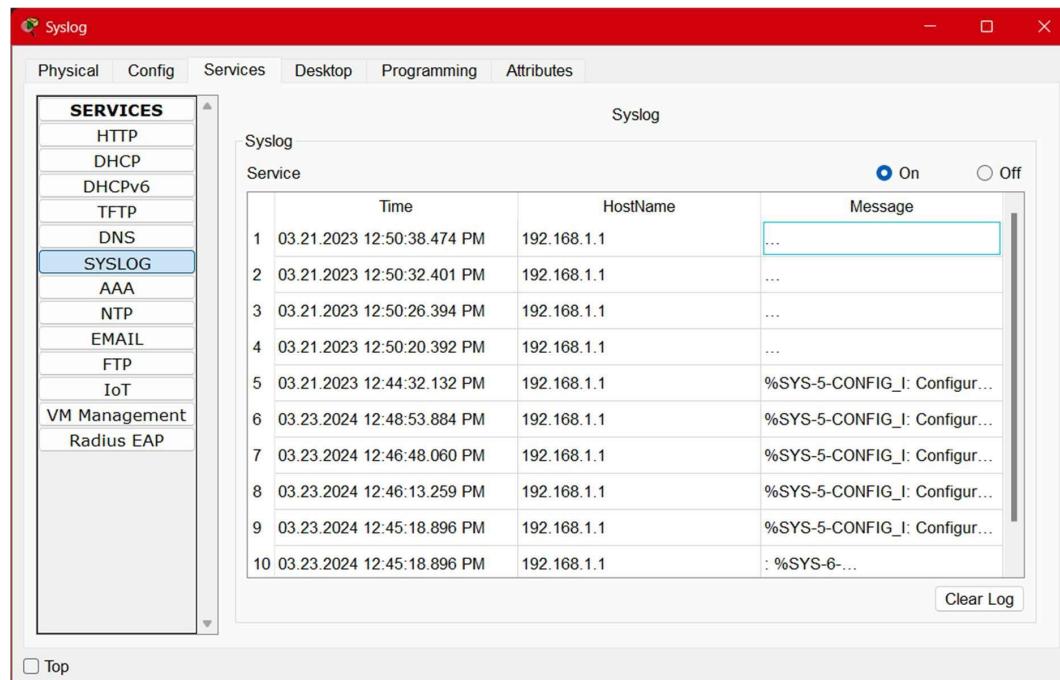
```
Laptop1
Ping statistics for 192.168.1.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 32ms, Average = 9ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

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

Ping statistics for 192.168.1.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  C:\>
```

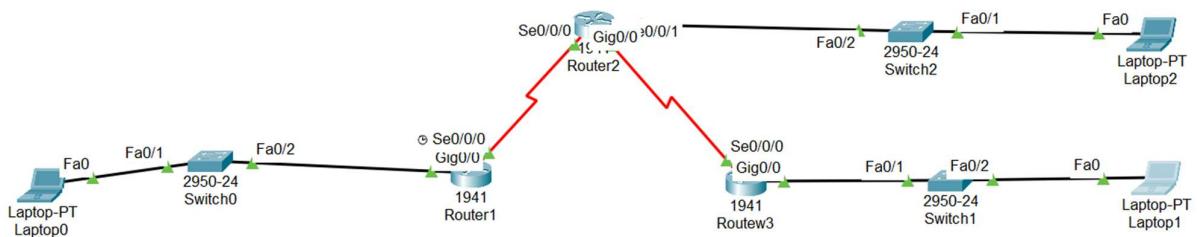


Time	HostName	Message
1 03.21.2023 12:50:38.474 PM	192.168.1.1	...
2 03.21.2023 12:50:32.401 PM	192.168.1.1	...
3 03.21.2023 12:50:26.394 PM	192.168.1.1	...
4 03.21.2023 12:50:20.392 PM	192.168.1.1	...
5 03.21.2023 12:44:32.132 PM	192.168.1.1	%SYS-5-CONFIG_I: Configur...
6 03.23.2024 12:48:53.884 PM	192.168.1.1	%SYS-5-CONFIG_I: Configur...
7 03.23.2024 12:46:48.060 PM	192.168.1.1	%SYS-5-CONFIG_I: Configur...
8 03.23.2024 12:46:13.259 PM	192.168.1.1	%SYS-5-CONFIG_I: Configur...
9 03.23.2024 12:45:18.896 PM	192.168.1.1	%SYS-5-CONFIG_I: Configur...
10 03.23.2024 12:45:18.896 PM	192.168.1.1	: %SYS-6-...

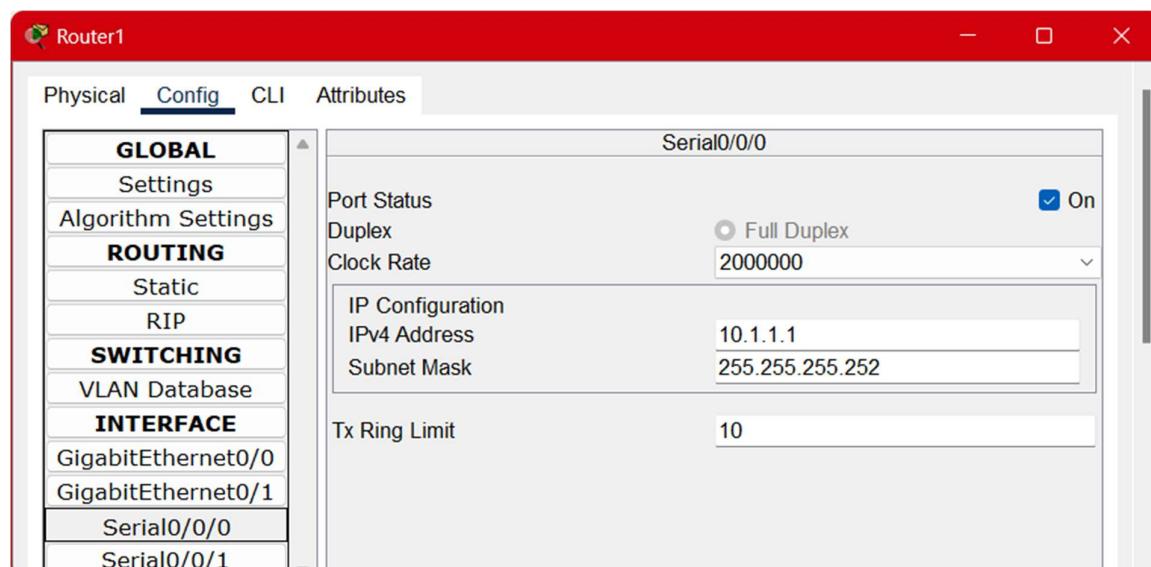
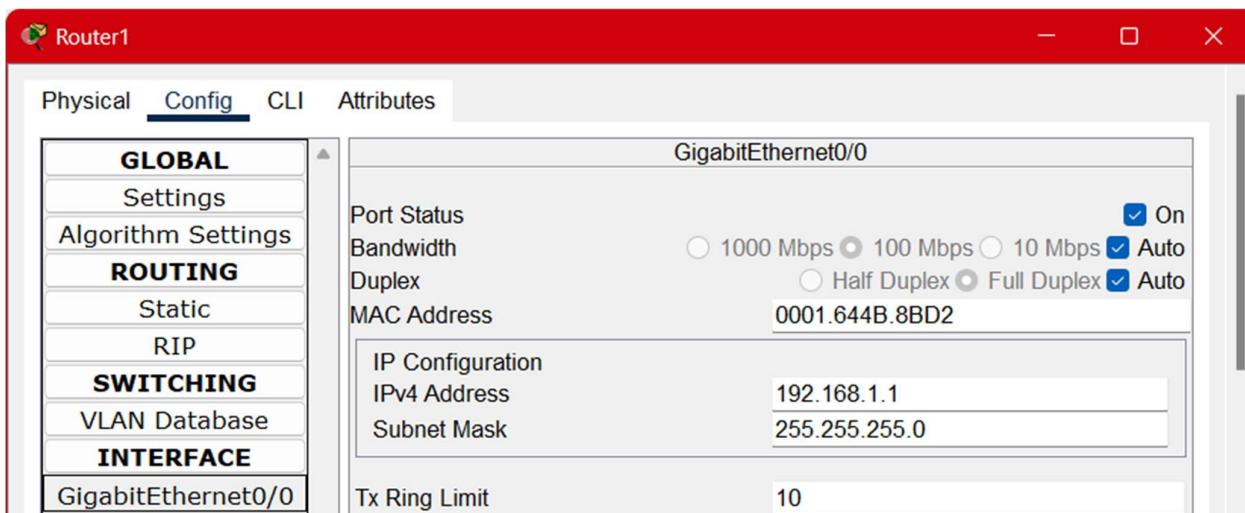
SECURITY IN COMPUTING

Practical 8

Aim : configure and verify a Site-to-Site Ipsec VPN using CLI
Topology

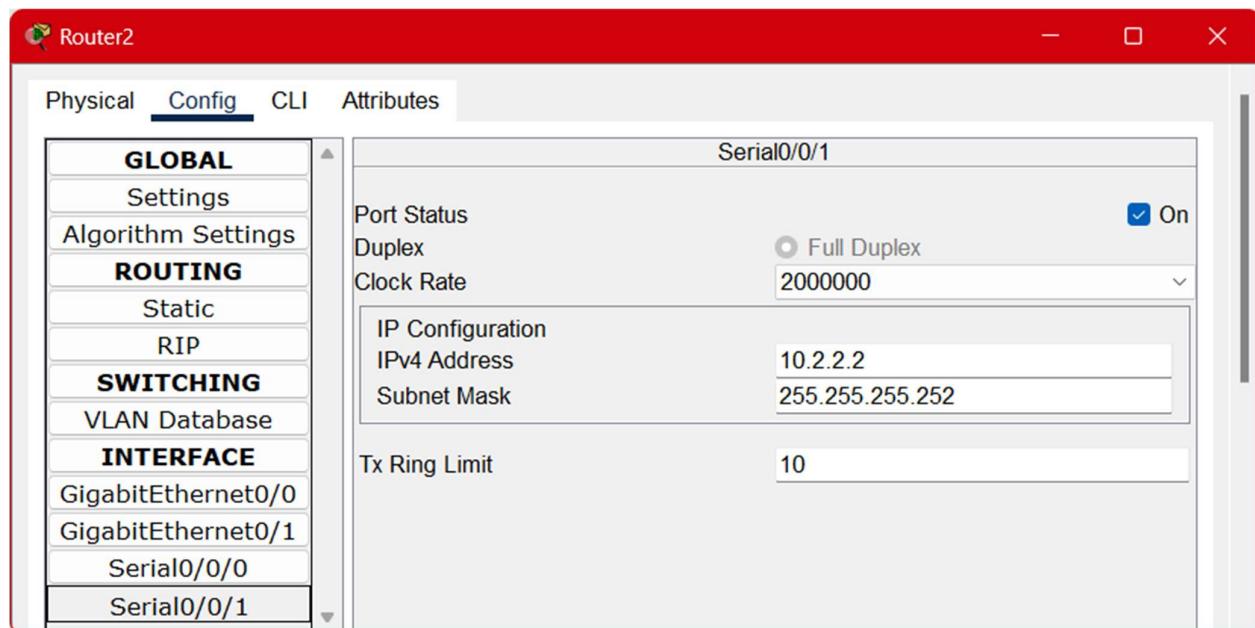
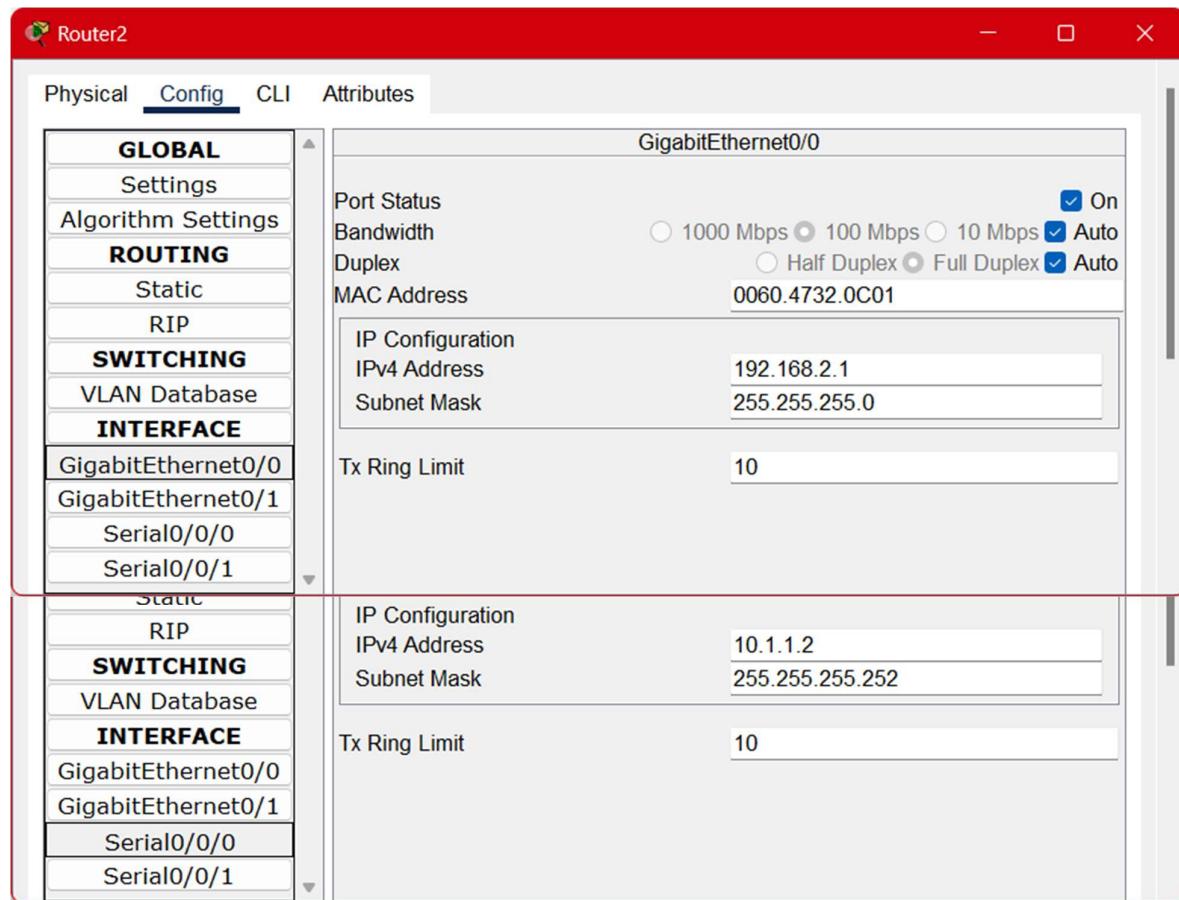


Assign Ip Address Router1



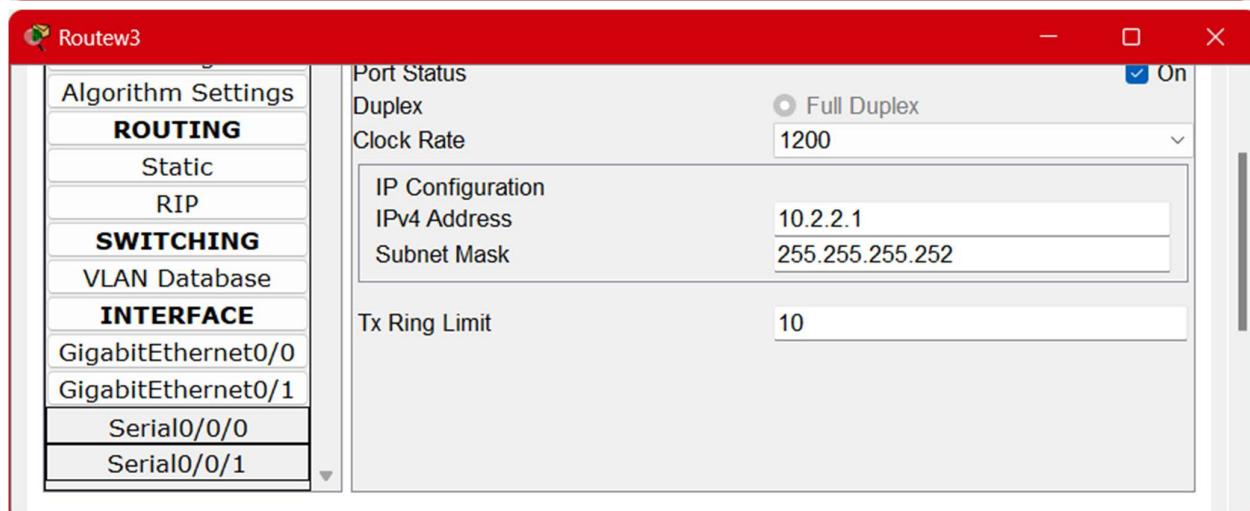
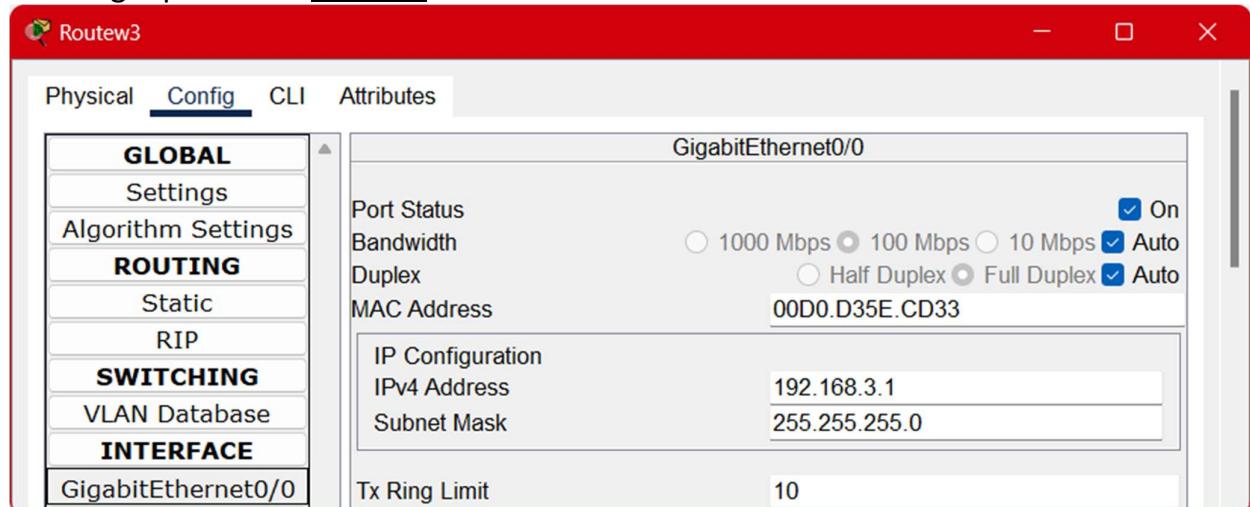
SECURITY IN COMPUTING

Assign Ip Address Router2

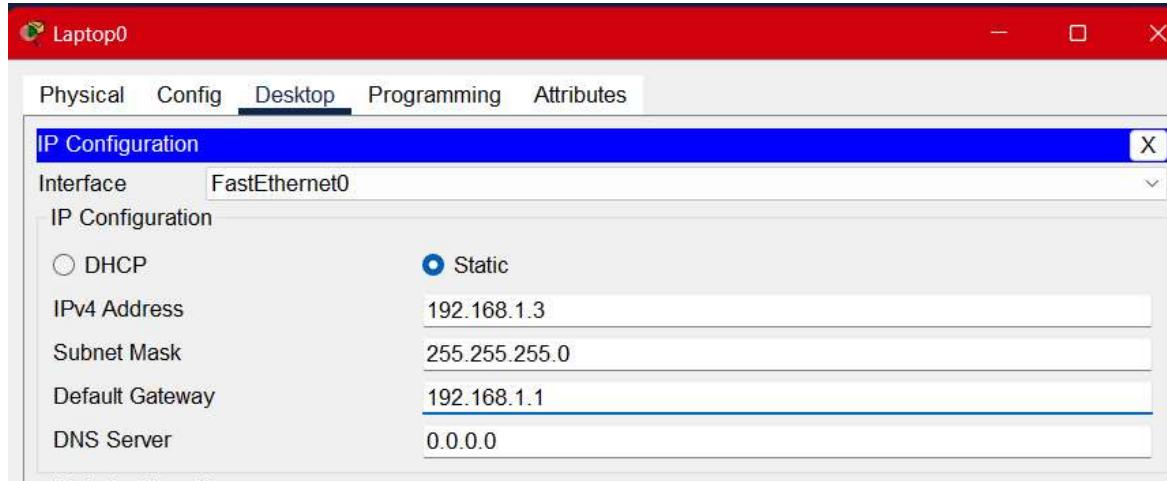


SECURITY IN COMPUTING

Assign Ip Address Router3

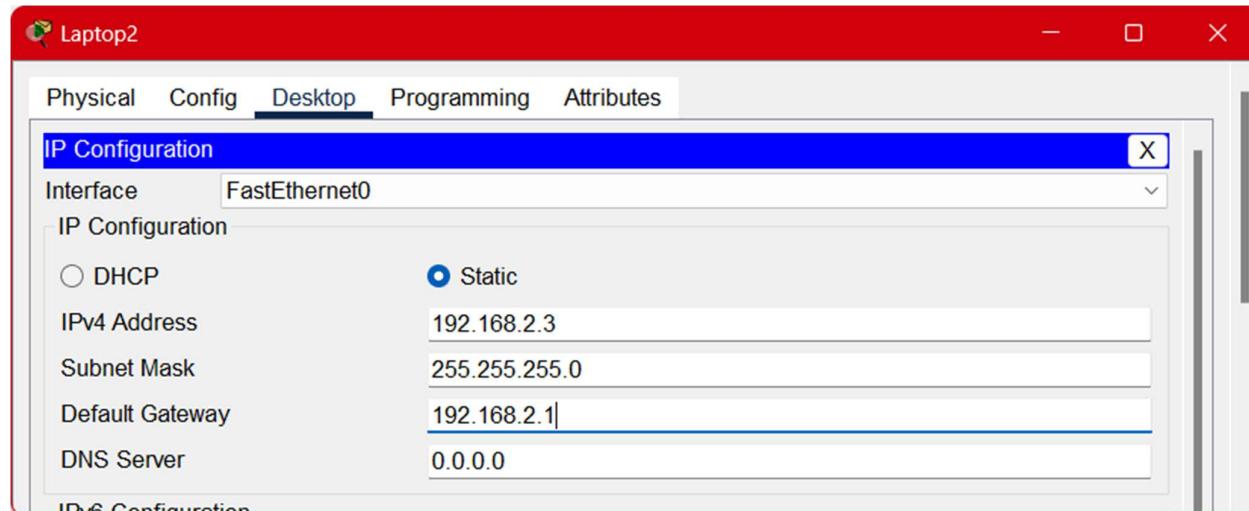


Ip to the Laptop 1

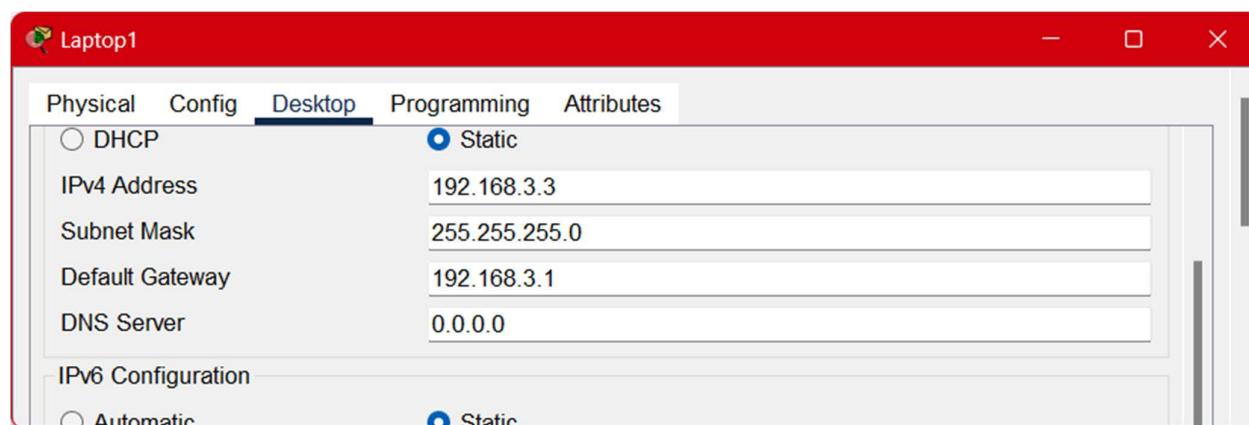


SECURITY IN COMPUTING

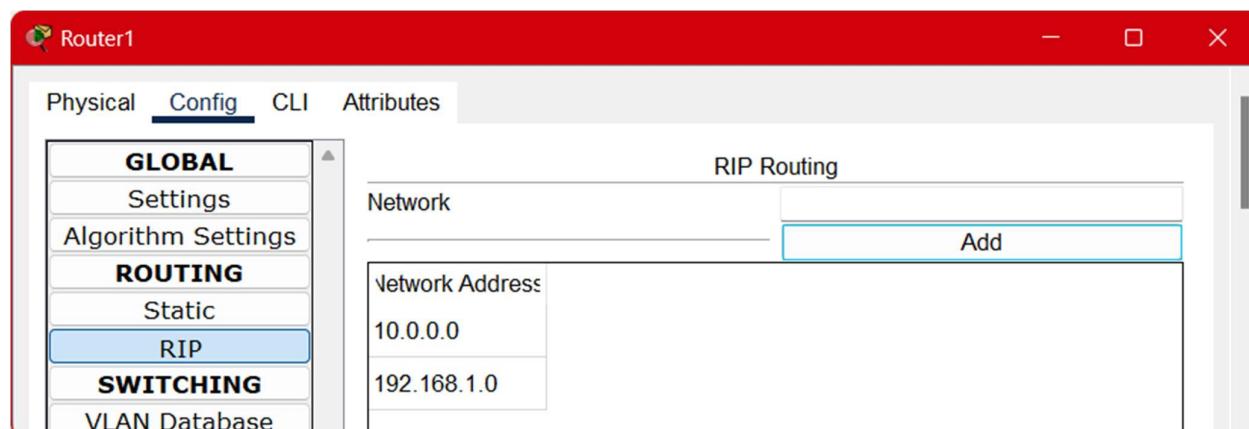
ip to laptop 2



ip to laptop3

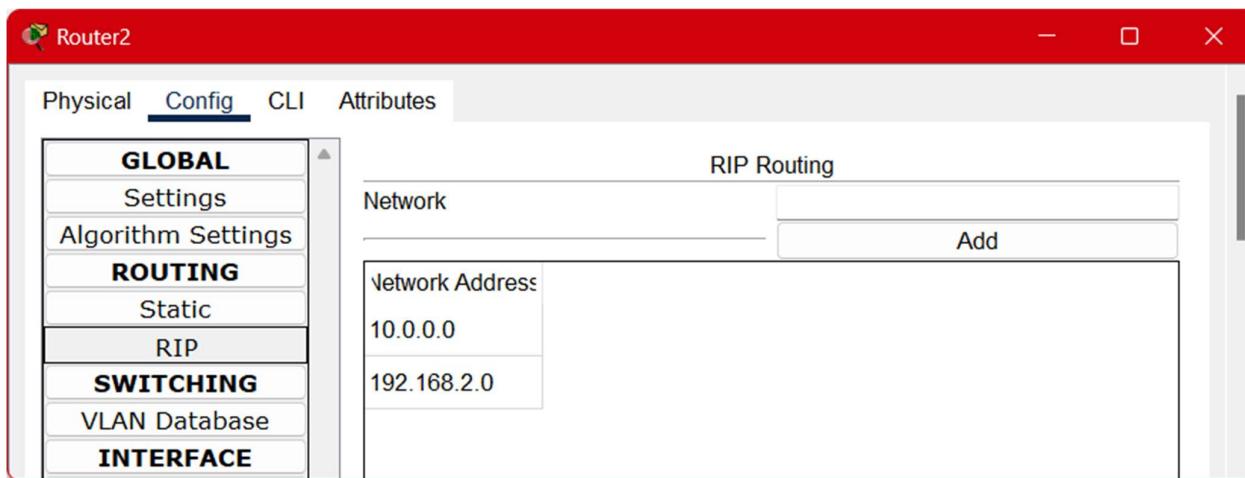


Performing RIP on router1

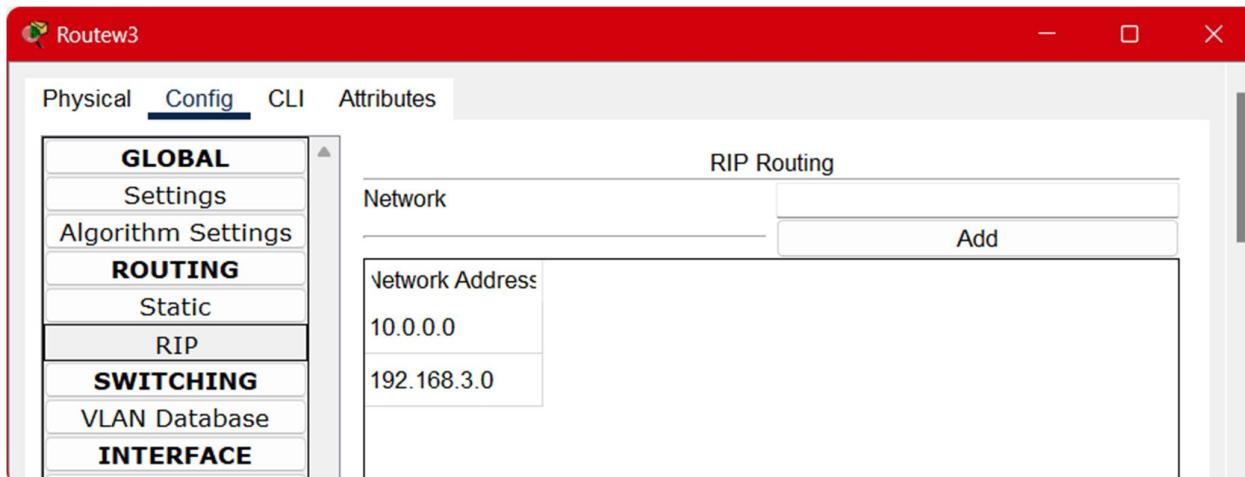


SECURITY IN COMPUTING

Performing RIP on router2



Performing RIP on router3



Enable Security Technology package on router 1 and router 3

Router1>show version

In the end of the this command this is same in both the router

Technology Package License Information for Module:'c1900'

Technology Technology-package Technology-package
Current Type Next reboot

ipbase ipbasek9 Permanent ipbasek9
security disable None None
data disable None None

Configuration register is 0x2102

SECURITY IN COMPUTING

ENABLE SECURITY TECHNOLOGY PACKAGE ON ROUTER 1 AND ROUTER 3

Router1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#license boot module c1900 technology-package securityk9

ACCEPT? [yes/no]: yes

% use 'write' command to make license boot config take effect on next boot

Router1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:
Module name = C1900 Next reboot level = securityk9 and License = securityk9

Router1(config)#exit

Router1#

%SYS-5-CONFIG_I: Configured from console by console

reload

System configuration has been modified. Save? [yes/no]:yes

AFTER RELOAD RE RUN THE COMMAND

License UDI:

Device# PID SN

*0 CISCO1941/K9 FTX1524CHY3-

Technology Package License Information for Module:'c1900'

Technology Technology-package Technology-package

Current Type Next reboot

ipbase ipbasek9 Permanent ipbasek9

security securityk9 Evaluation securityk9

data disable None None

SAME PROCESS FOR THE ROUTER 3

CONFIGURE ACL< IKE PHASE 1 ISAKMP POLICY AND IKE PHASE2 IPSEC POLICY ON ROUTER 1

Router1>en

Router1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Router1(config)#crypto isakmp policy 10

Router1(config-isakmp)#encryption aes 256

Router1(config-isakmp)#authentication pre-share

Router1(config-isakmp)#group 5

Router1(config-isakmp)#crypto isakmp key vnpwd address 10.2.2.1

Router1(config)#crypto ipsec transform-set vpn-set esp-aes esp-sha-hmac

Router1(config)#crypto map vpn-map 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

SECURITY IN COMPUTING

and a valid access list have been configured.

```
Router1(config-if)#description vpn connection to routwe3
Router1(config-if)#crypto isakmp key vpnpwd address 10.2.2.1
A pre-shared key for address mask 10.2.2.1 255.255.255.255 already exists!
Router1(config)#crypto map vpn-map 10 ipsec-isakmp
Router1(config-crypto-map)#description vpn connection to routew3
Router1(config-crypto-map)#set peer 10.2.2.1
Router1(config-crypto-map)#set transform-set vpn-set
Router1(config-crypto-map)#match address 110
Router1(config-crypto-map)#exit
Router1(config)#interface se0/0/0
Router1(config-if)#crytpo map vpn-map
^
% Invalid input detected at '^' marker.
Router1(config-if)#crypto map vpn-map
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router1(config-if)#

```

CONFIGURE ACL< IKE PHASE 1 ISAKMP POLICY AND IKE PHASE2 IPSEC POLICY ON ROUTER 3

```
Router3>en
Router3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
Router3(config)#crypto isakmp policy 10
Router3(config-isakmp)#encryption aes 256
Router3(config-isakmp)#authentication pre-share
Router3(config-isakmp)#group 5
Router3(config-isakmp)#exit
Router3(config)#crypto isakmp key vpnpwd address 10.1.1.1
Router3(config)#crypto ipsec transform-set vpn-set esp-aes esp-sha-hmac
Router3(config)#crypto map vpn-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router3(config-crypto-map)#description vpn connection to router1
Router3(config-crypto-map)#set peer 10.1.1.1
Router3(config-crypto-map)#set transform-set vpn-set
Router3(config-crypto-map)#match address 110
Router3(config-crypto-map)#exit
Router3(config)#interface se0/0/0
Router3(config-if)#crypto map vpn-map
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

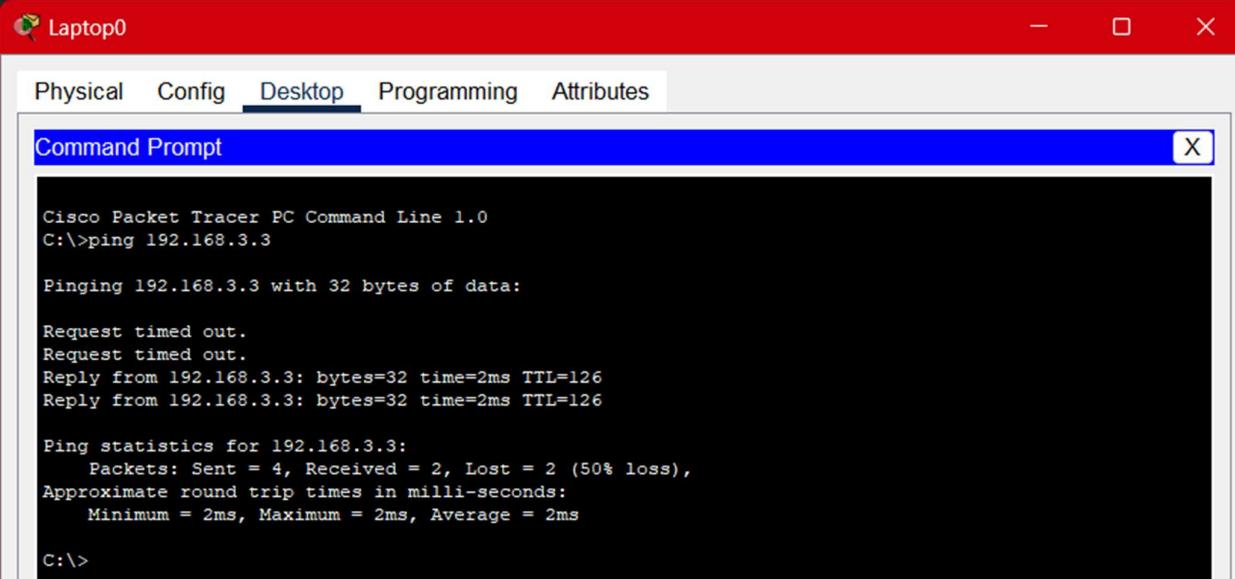
VERITY THE WORKING OF IPSEC VPN FOR INTERESTING TRAFFIC ON ROUTER 1 BEFORE PINGING FROM LAPTOP 1 TO IP 192.168.3.3

```
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
```

SECURITY IN COMPUTING

```
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0  
#pkts not decompressed: 0, #pkts decompress failed: 0  
#send errors 0, #recv errors 0
```

AFTER PINGING



The screenshot shows a Cisco Packet Tracer interface titled "Laptop0". The top menu bar includes "Physical", "Config", "Desktop" (which is selected), "Programming", and "Attributes". A "Command Prompt" window is open, displaying the output of a ping command. The output is as follows:

```
Cisco Packet Tracer PC Command Line 1.0  
C:>ping 192.168.3.3  
  
Pinging 192.168.3.3 with 32 bytes of data:  
  
Request timed out.  
Request timed out.  
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126  
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126  
  
Ping statistics for 192.168.3.3:  
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 2ms, Maximum = 2ms, Average = 2ms  
  
C:>
```

ROUTER1

```
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)  
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)  
current_peer 10.2.2.1 port 500  
PERMIT, flags={origin_is_acl,}  
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0  
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0  
#pkts not decompressed: 0, #pkts decompress failed: 0  
#send errors 1, #recv errors 0
```