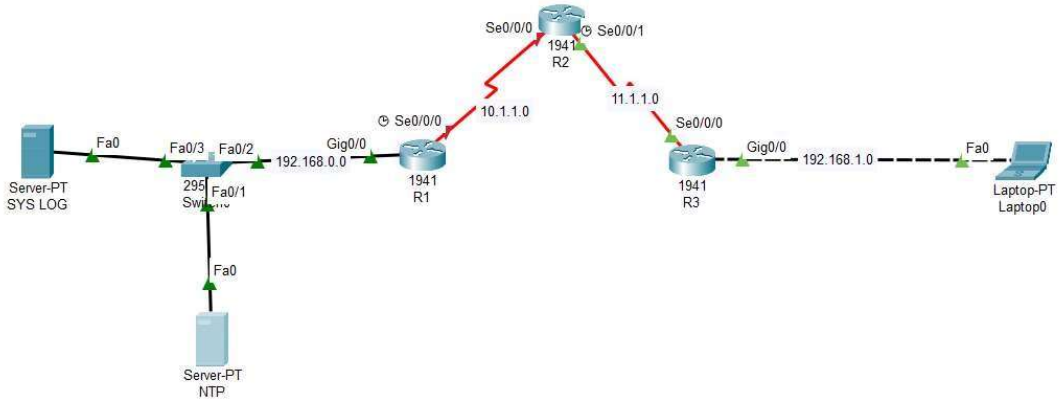
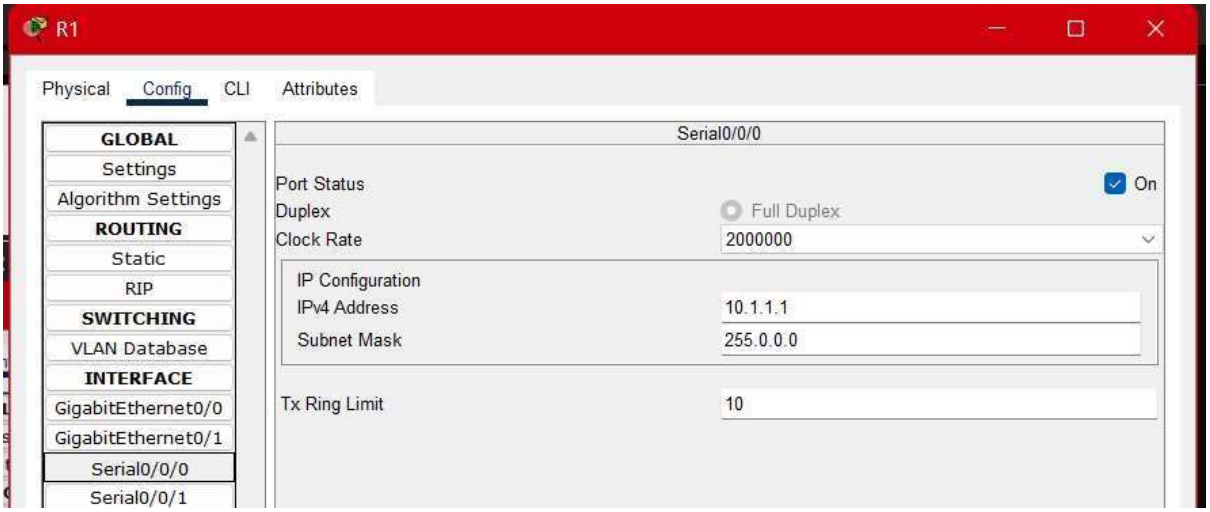
Practical-1

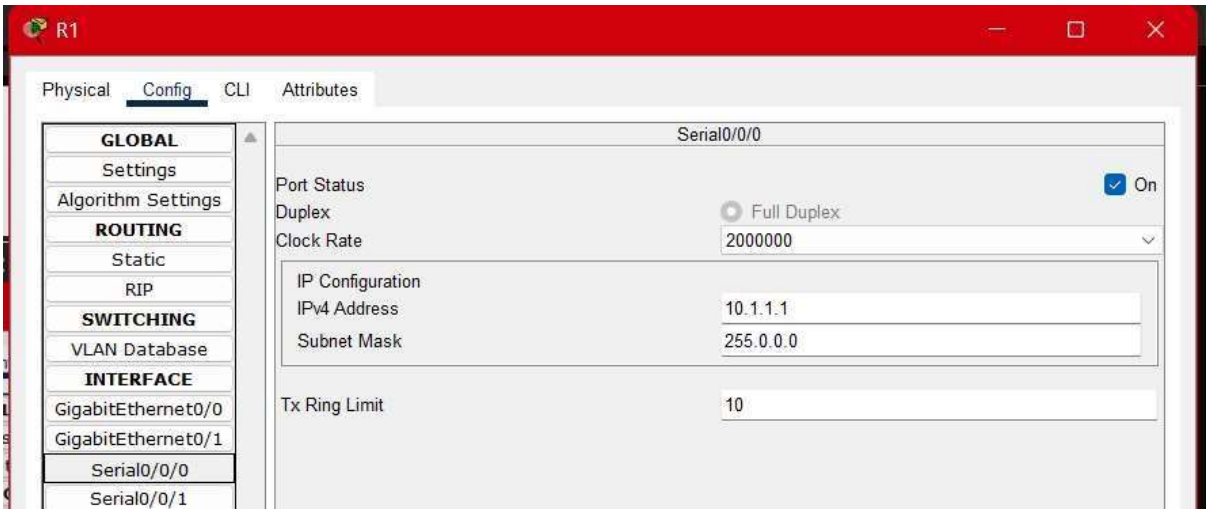
AIM- Configure Router

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:

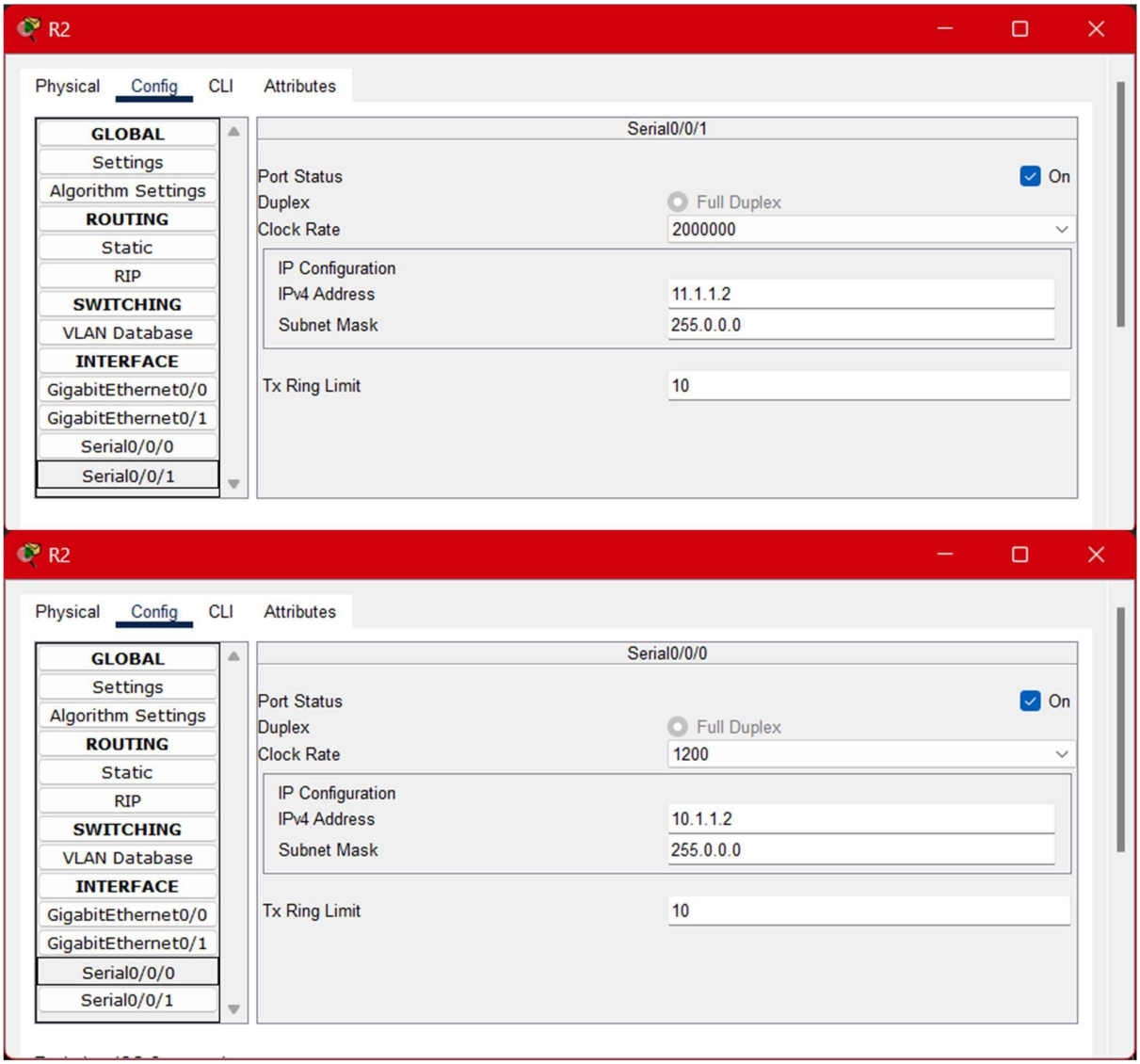


ROUTER R1: IP CONFIGURE

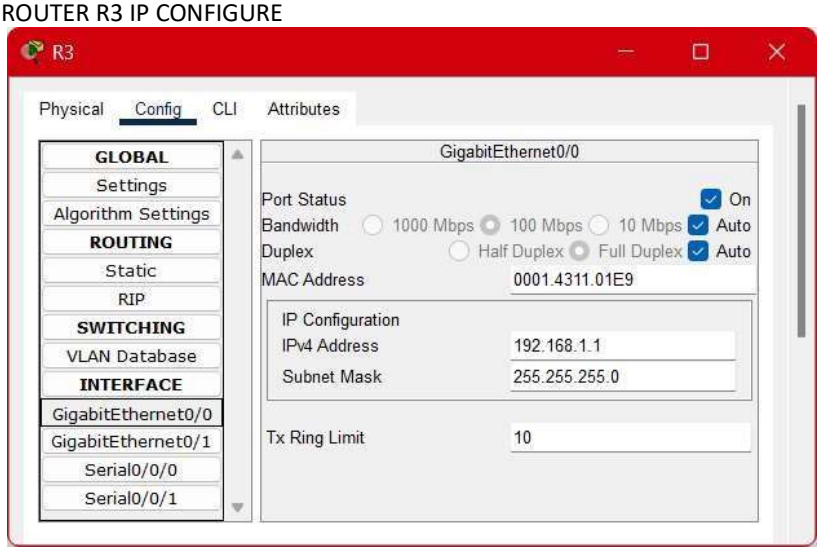


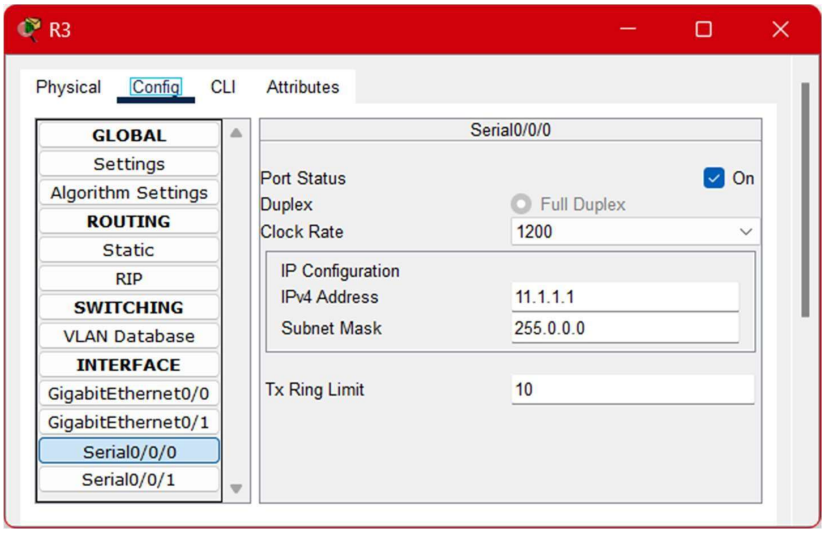


ROUTER R2: IP CONFIGURE

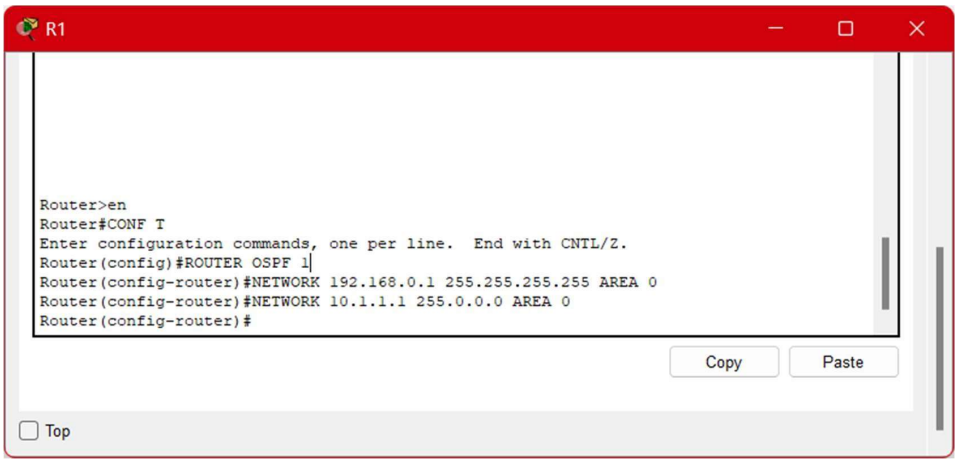


ROUTER R3 IP CONFIGURE

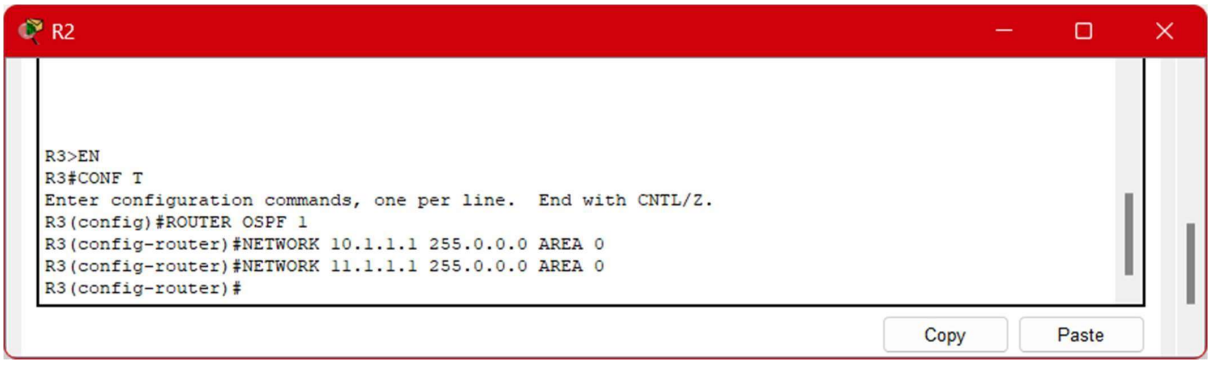




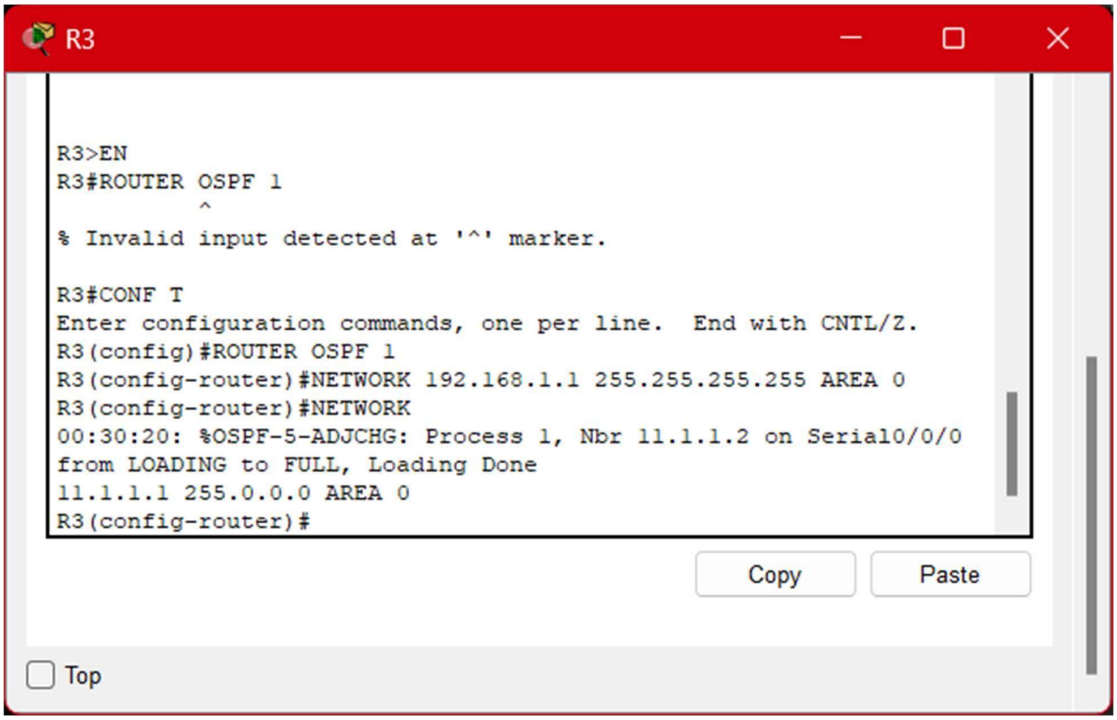
OSPF CONFIGURE OF R1



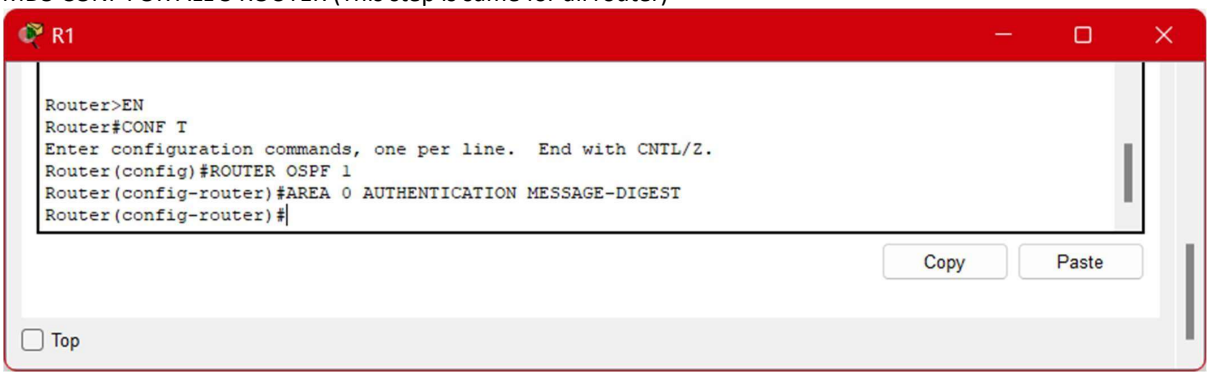
OSPF CONFIGURE R2



OSPF CONFIGURE R3



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



MDF CONFI ON ALL THE SERIAL INTERFACE OF THE ROUTER
R1: HAVE ONE SERIAL INTERFACE IN USE

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 SE0/0/0/0
                    ^
% 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

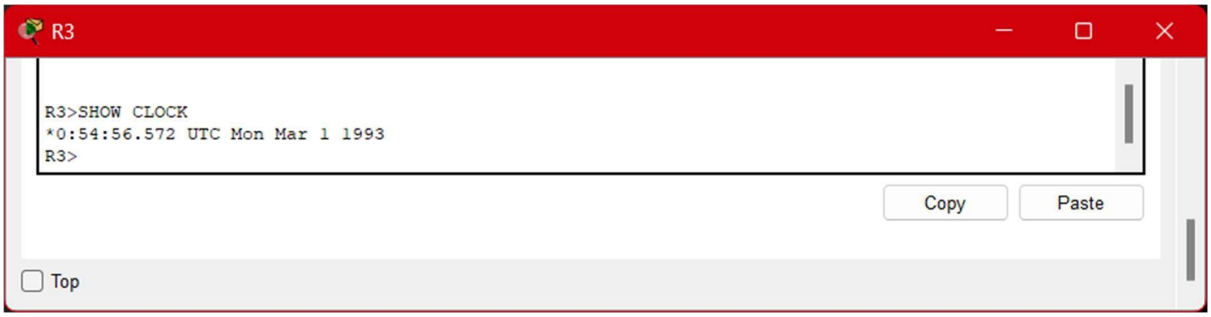
```
R3>EN
R3#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ROUTER OSPF 1
R3(config-router)#NETWORK 192.168.1.0 255.255.255.255 AREA 0
R3(config-router)#NETWORK 11.1.1.0 255.0.0.0 AREA 0
R3(config-router)#EXIT
R3(config)#INTERFACE SE0/0/0
R3(config-if)#IP OSPF MESSAGE-DIGEST-KEY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

Copy Paste

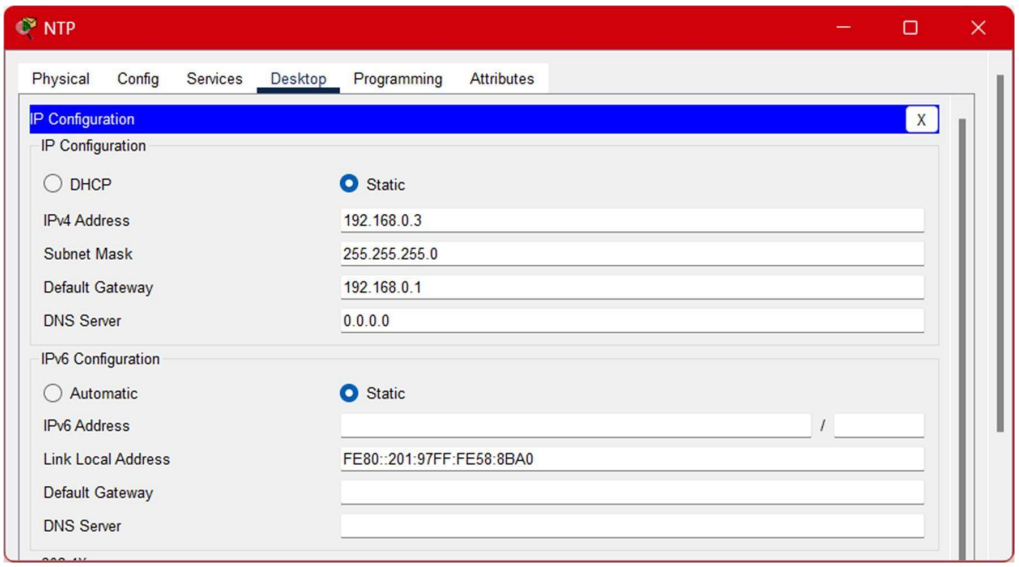
Top

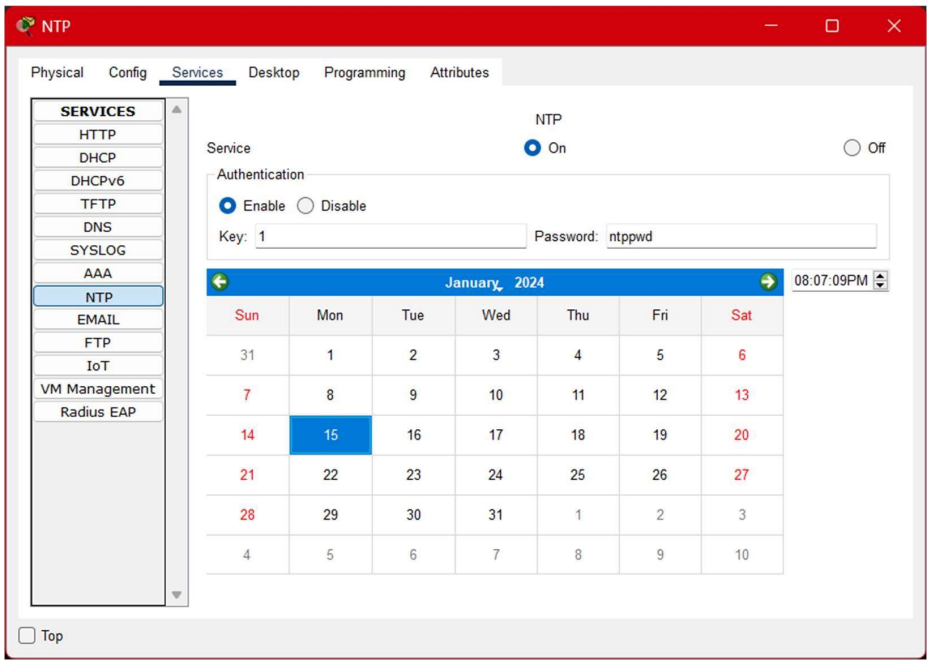
PART B: NTP

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



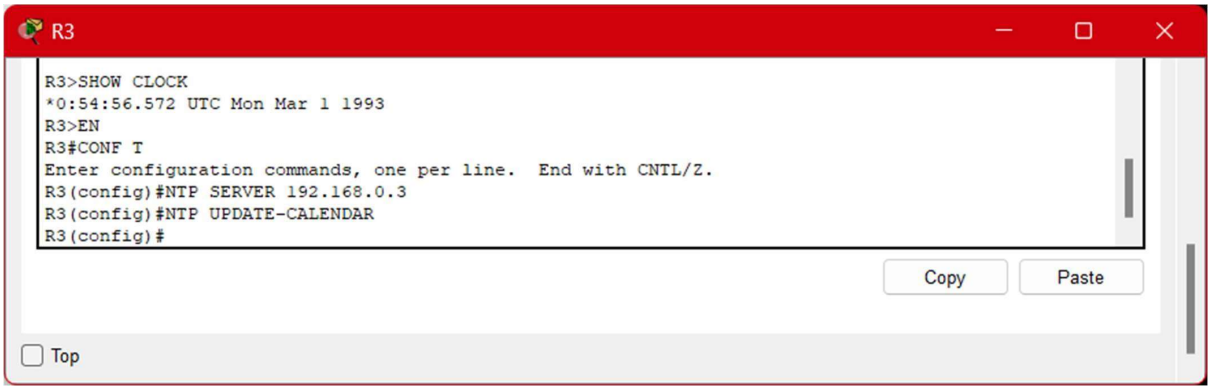
NTP IP CONFIG



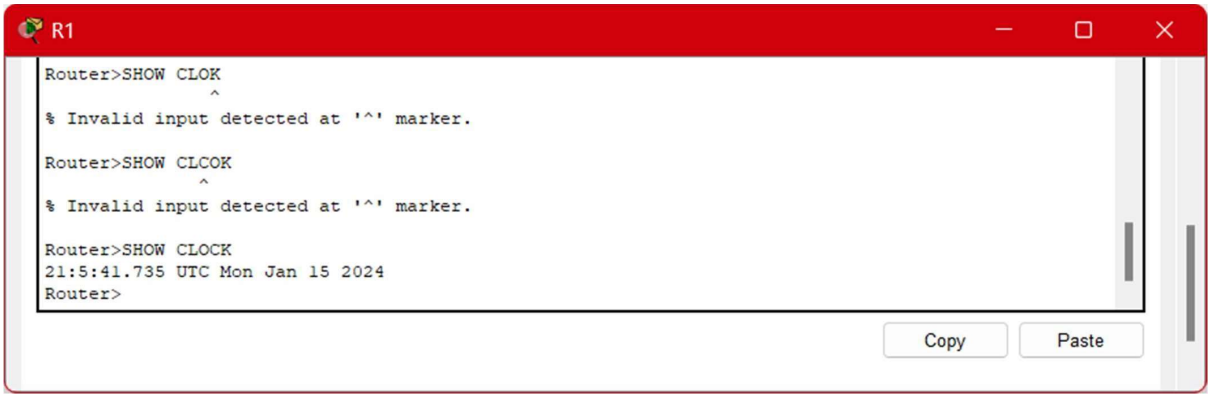


NTP SERVICE TURN ON

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

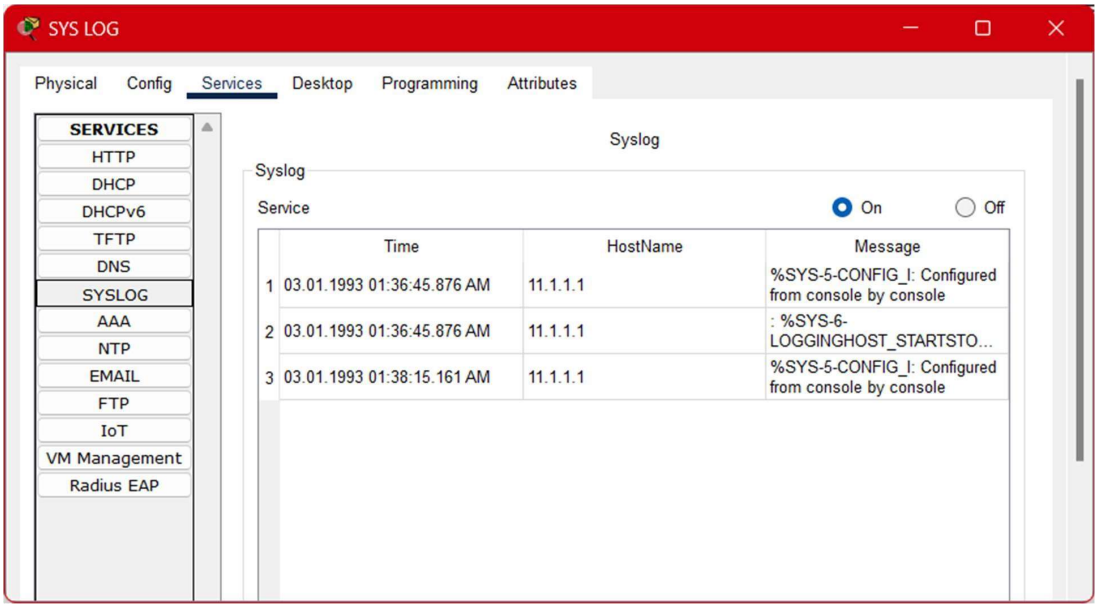


AFTER NTP SETUP IN ALL ROUTER

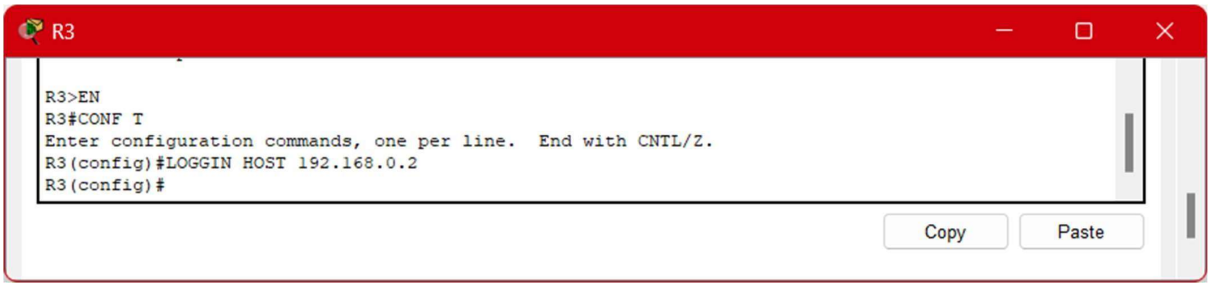


PART 3: SYS LOGGING

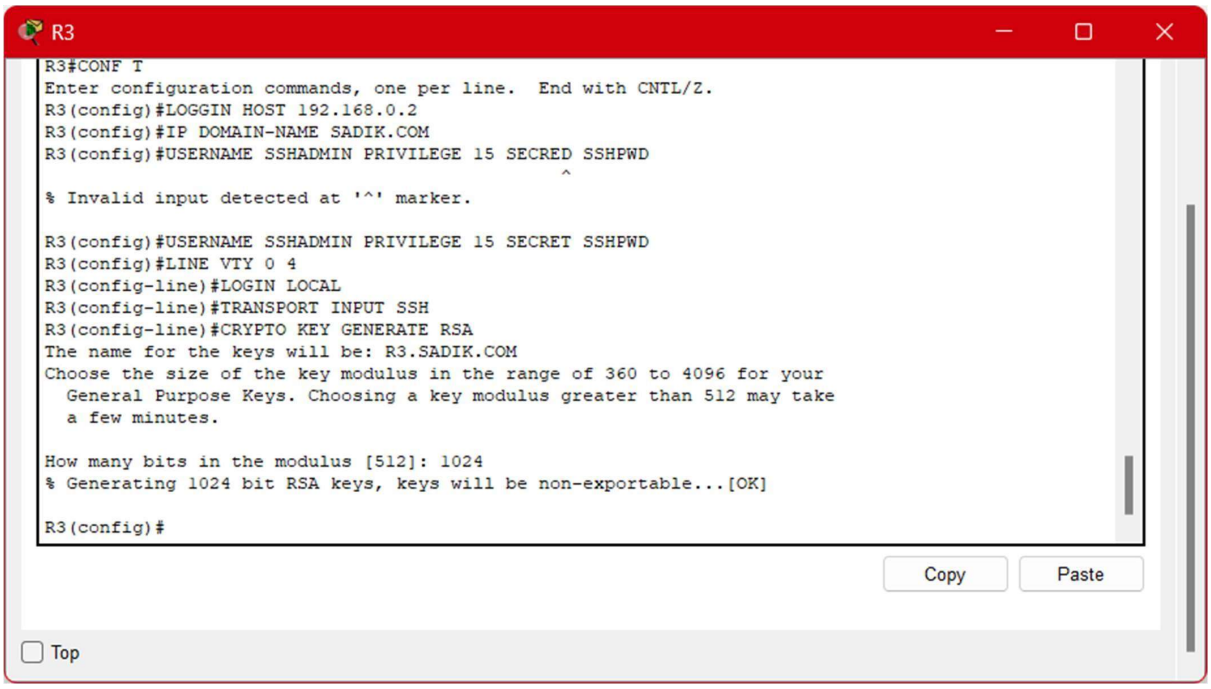
SETUP SYSLOG



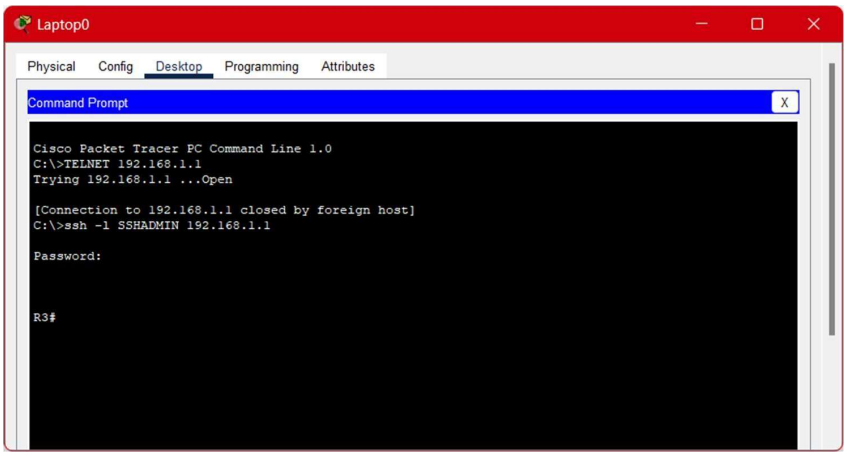
ASUSUAL SAME FOR ALL ROUTER



PART 4: SSH



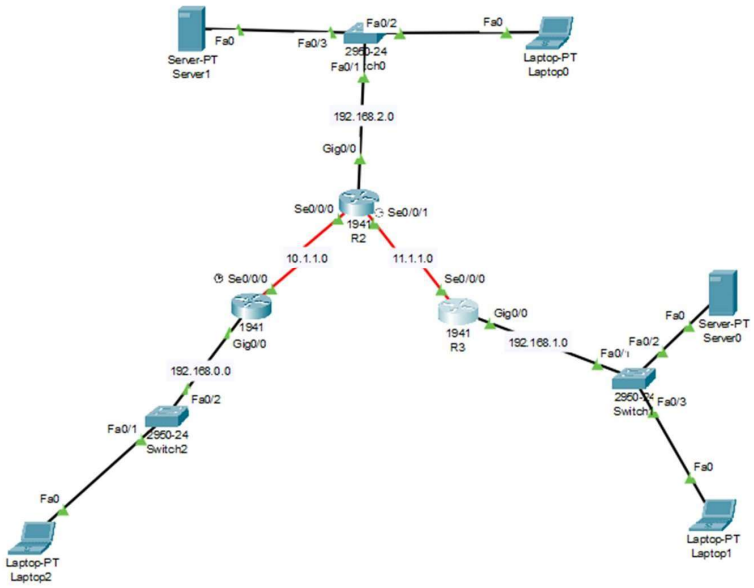
TELNET CONNECTION



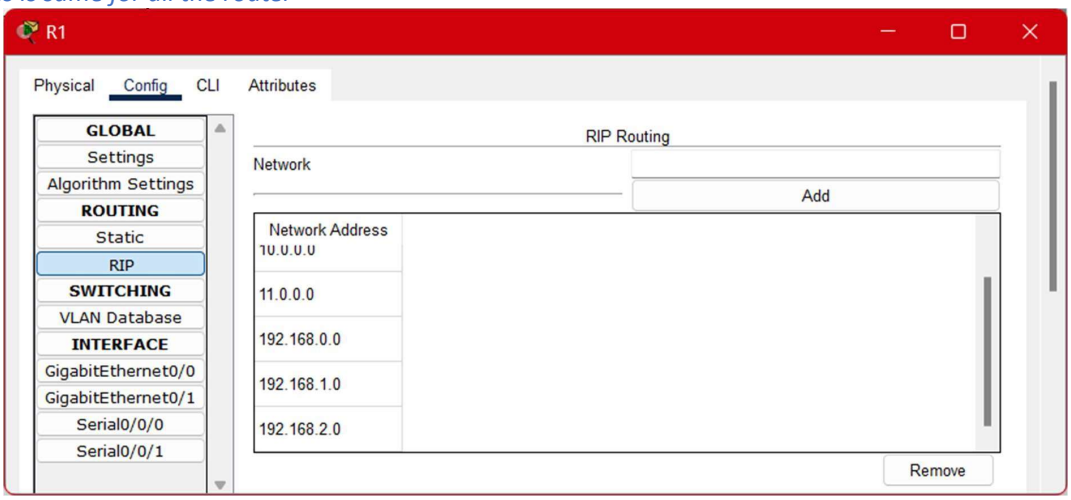
PRACTICAL 2

AIM - Configure AAA authenticate

Topology

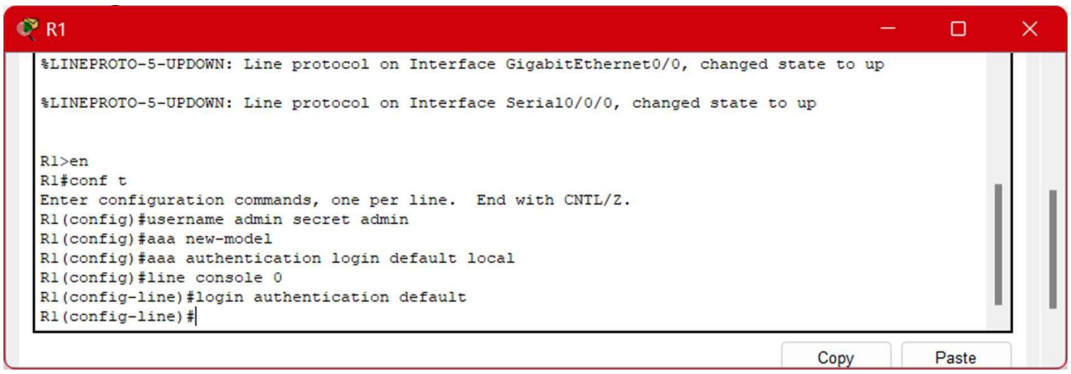


Assign IP To All The Required devices
Perform a Routing Information Protocol (RIP)
This is same for all the router

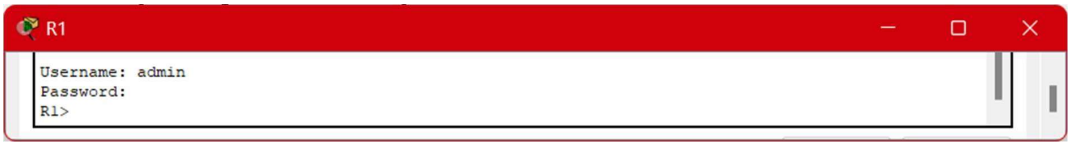


CONFIGURE AUTHENTICATION, AUTHORIZATION AND ACCOUNTING (AAA)

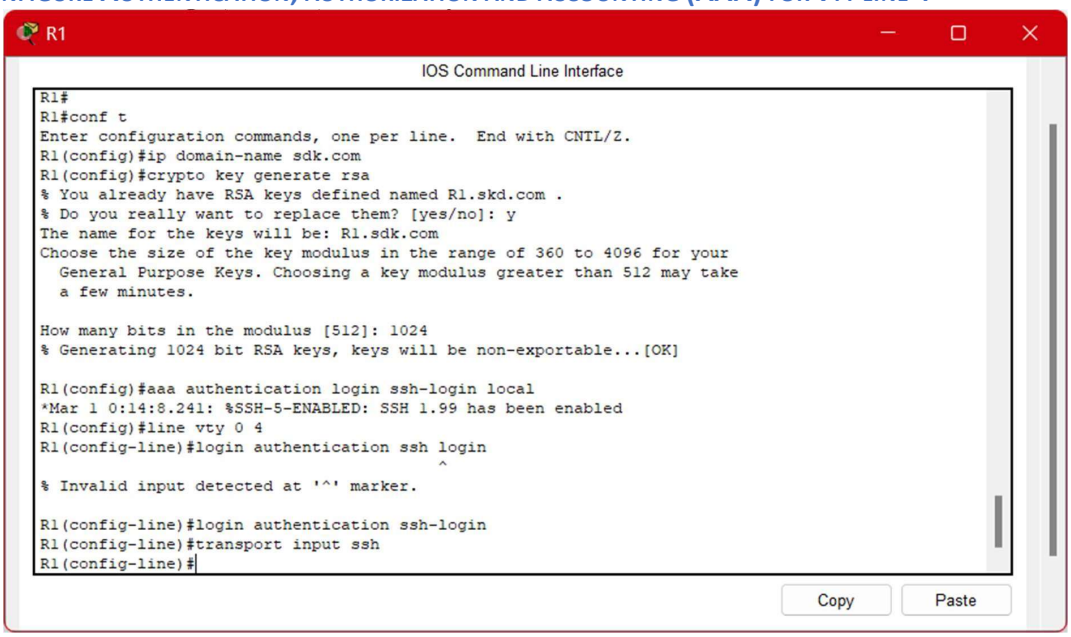
CONFIGURE ROUTER 1 WITH AAA



AFTER CONFIGURE REQUIRED A LOCAL LOGIN.

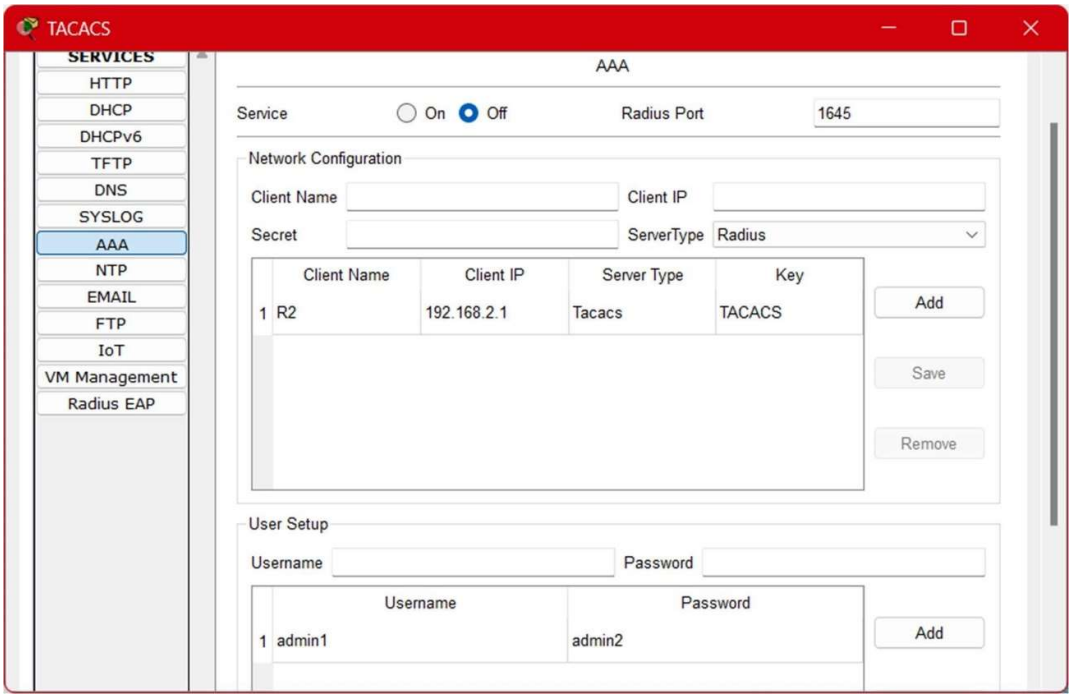


CONFIGURE AUTHENTICATION, AUTHORIZATION AND ACCOUNTING (AAA) FOR VTY LINE 4

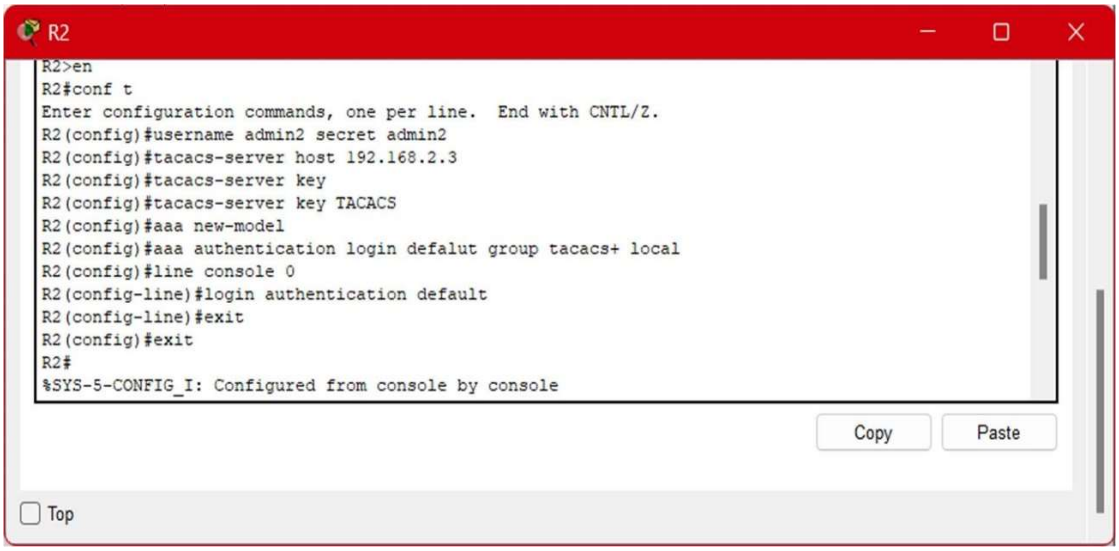


CONFIGURE SERVER-BASED AAA AUTHENTICATION USING TACACS+ ON R2

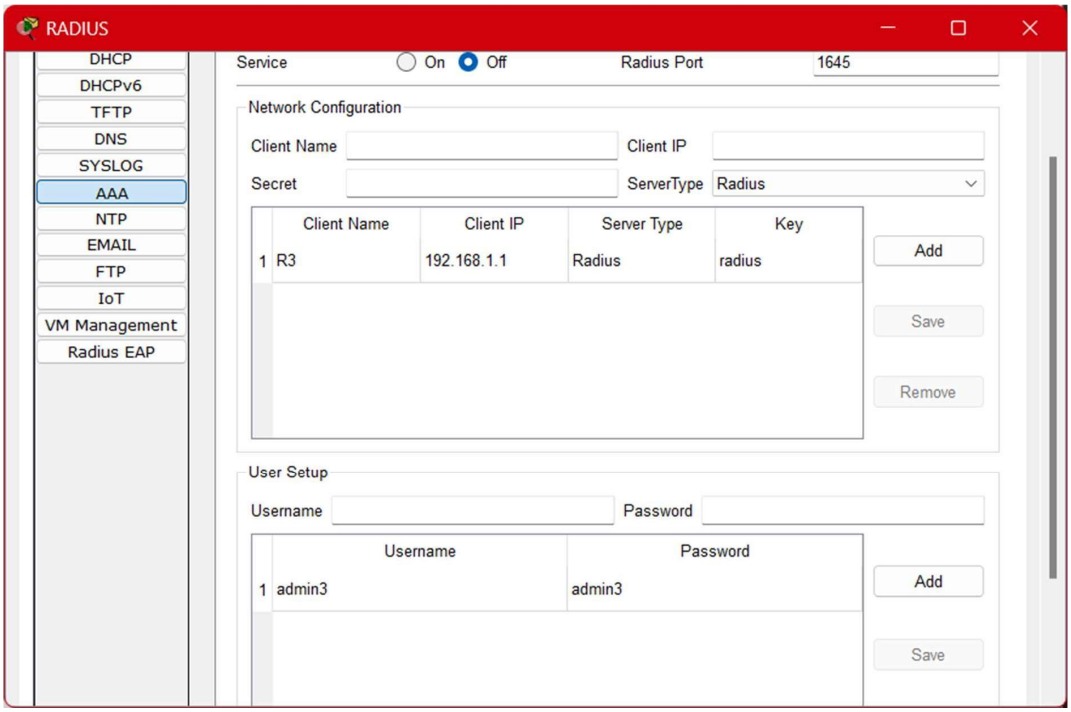
SERVER



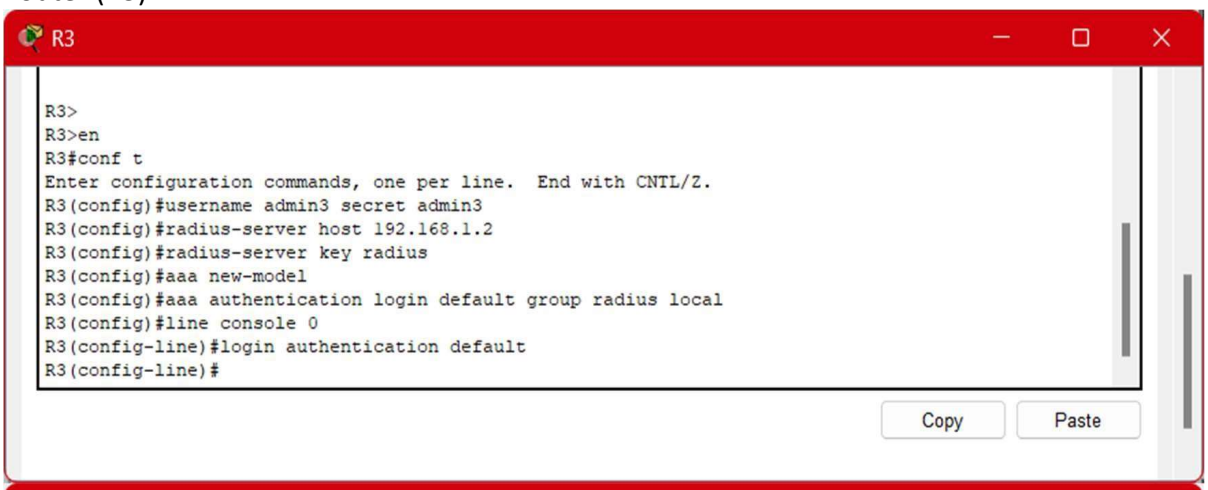
Router (R2)

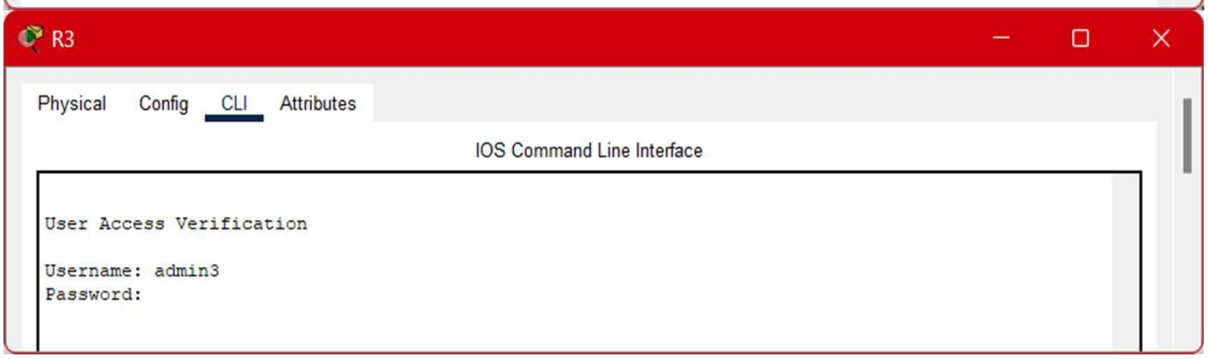


CONFIGURE SERVER-BASED AAA AUTHENTICATION USING RADIUS ON R3 SERVER



Router (R3)

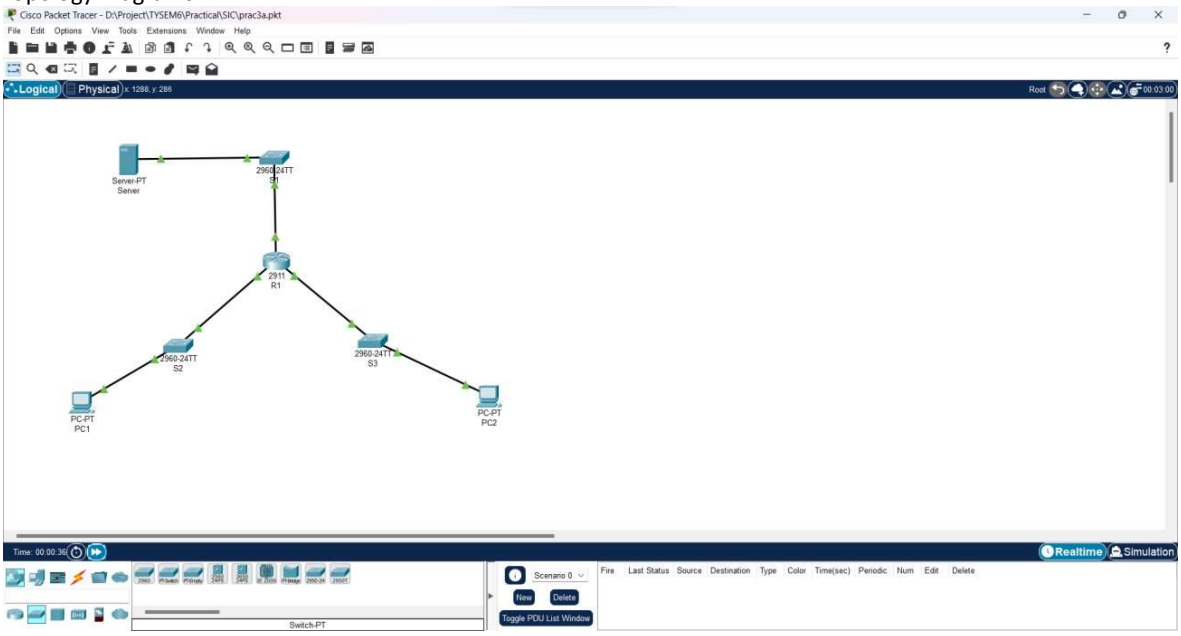




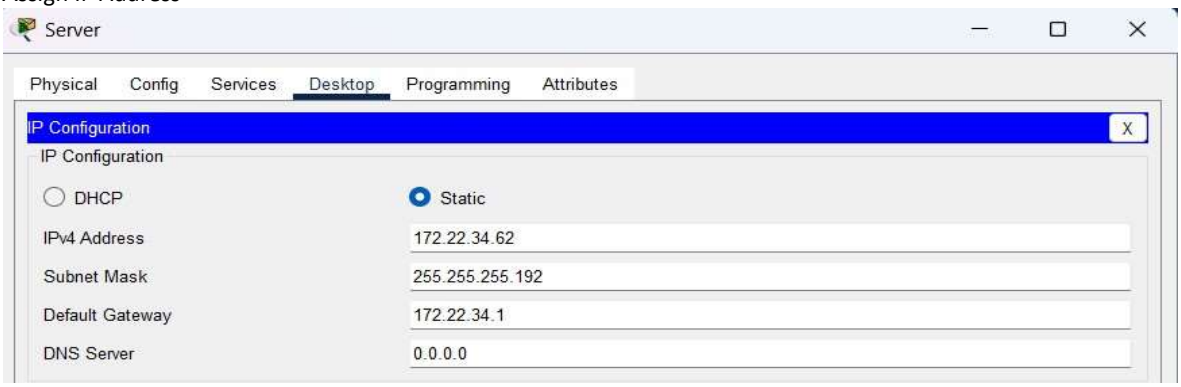
Practical 3a

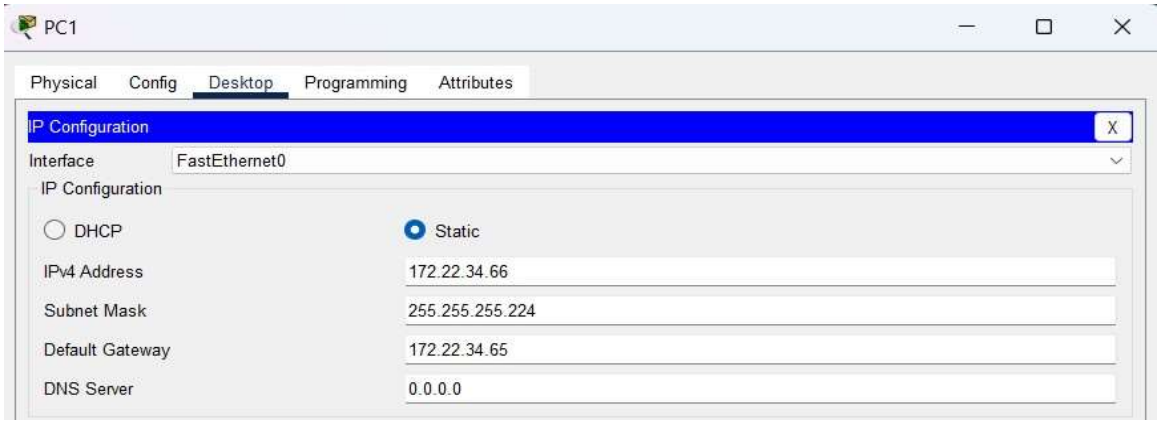
Aim: Configuring Extended ACLs.

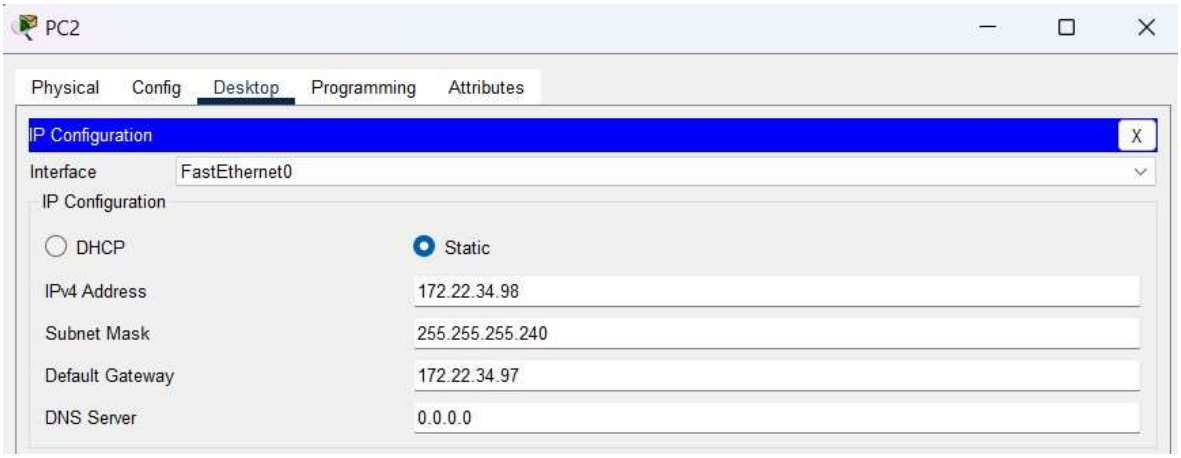
Topology Diagrams

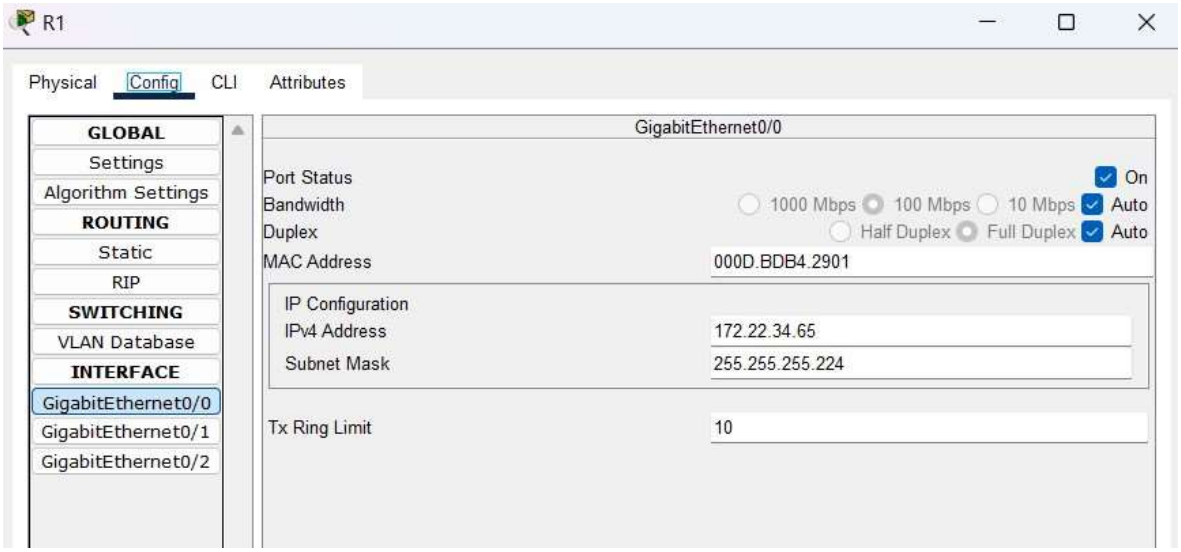


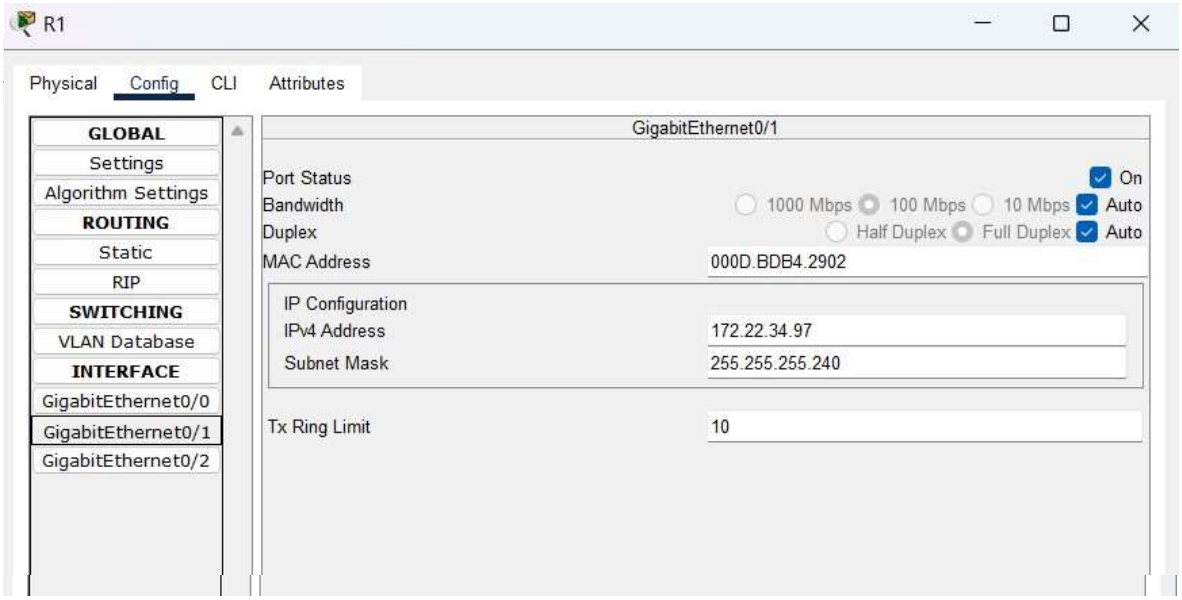
Assign IP Address







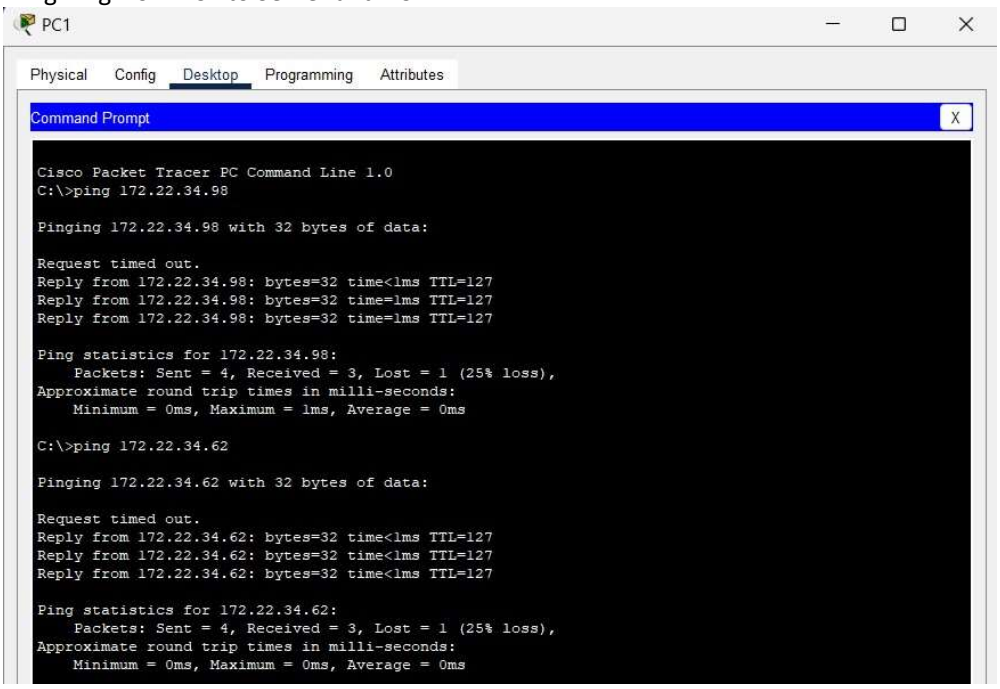




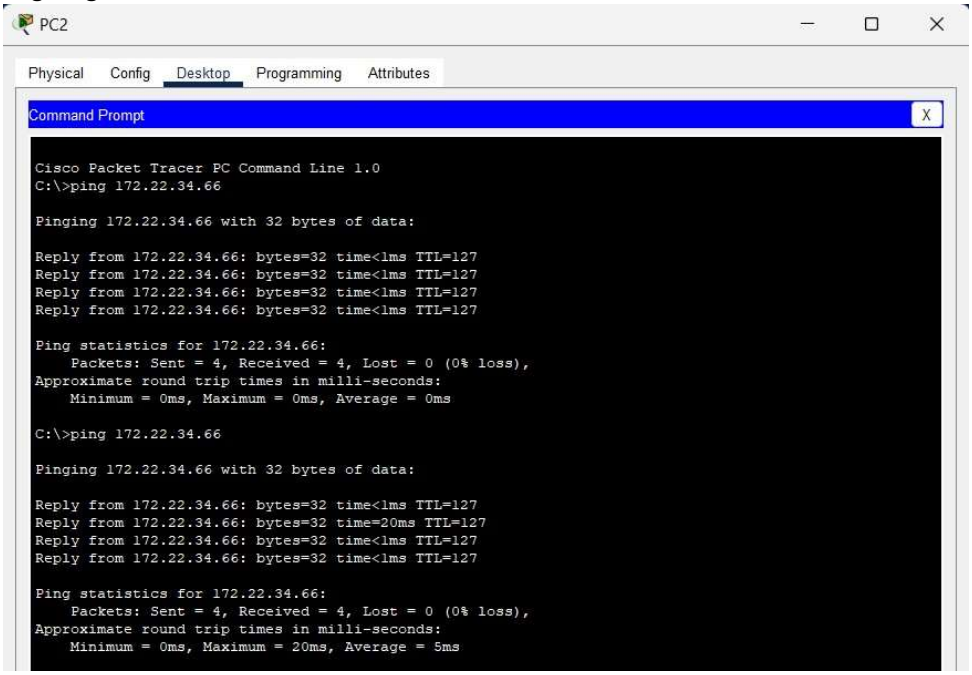
Displaying IP Address Details of R1

```
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



Performing Ping from PC2 to server and PC1

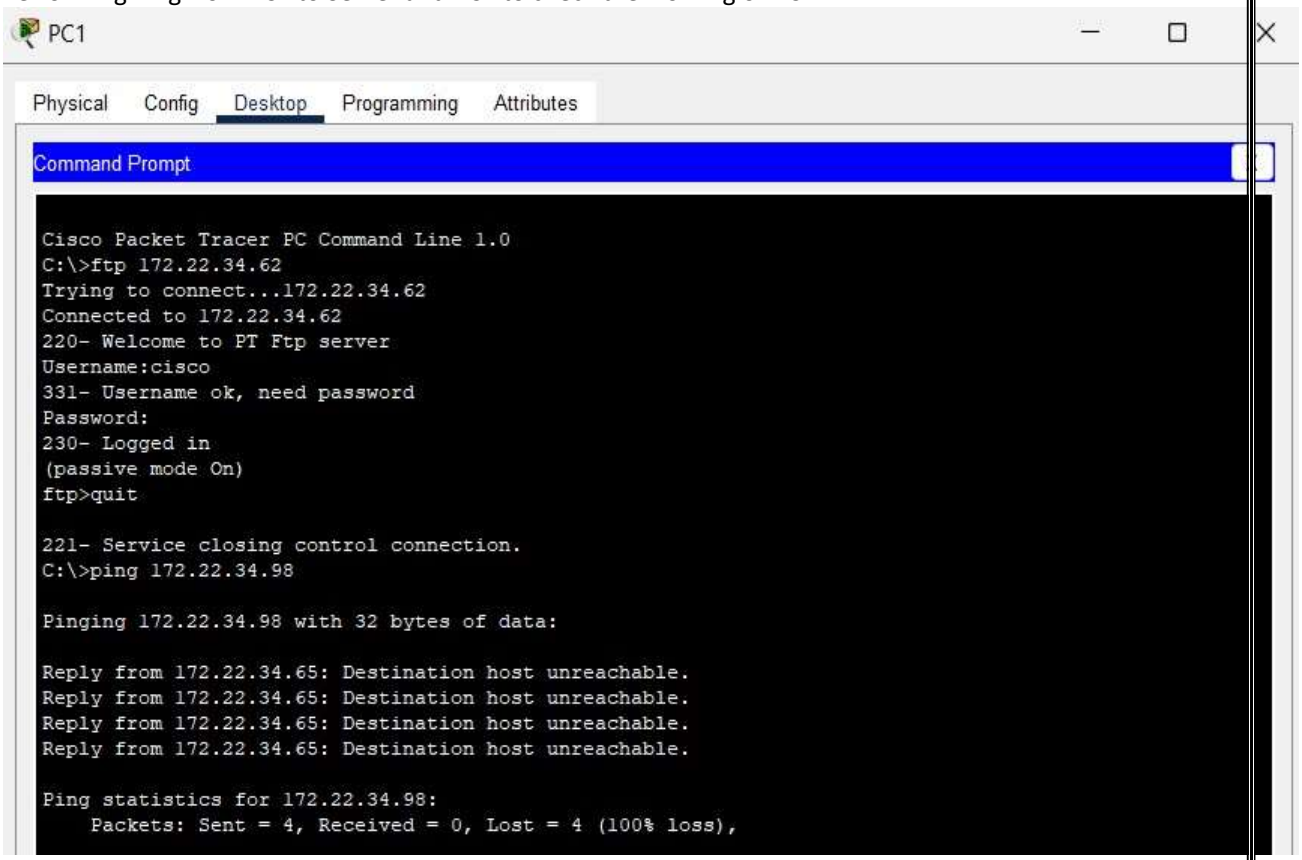


Configure, Apply and Verify an Extended Numbered ACL (PC1 needs only FTP access and should be able to ping the server, but not PC2)

```
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 only 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

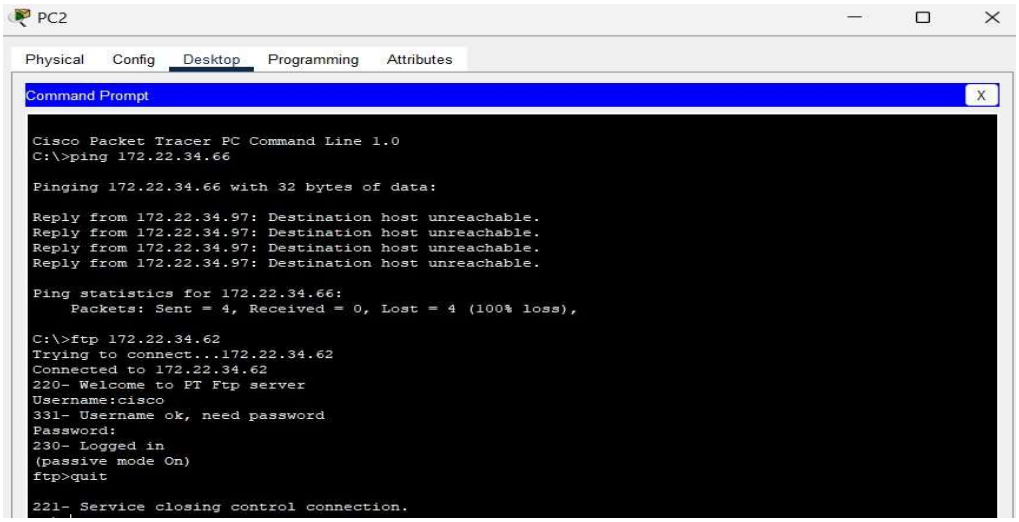


CONFIGURE, APPLY AND VERIFY AND EXTENDED NAMED ACL (PC2 NEEDS ONLY WEB ACCESS AND SHOULD BE ABLE TO PING THE SERVER, BUT NOT PC2)

```
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

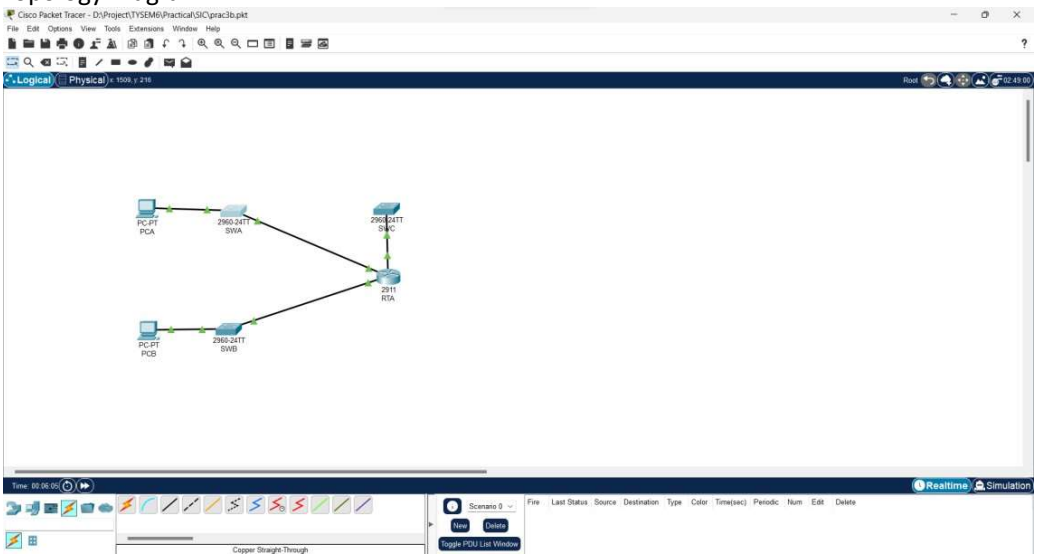


TO SERVER AND PC1 TO CHECK THE WORKING OF ACL CHECKING HTTP CONNECTION FROM PC2

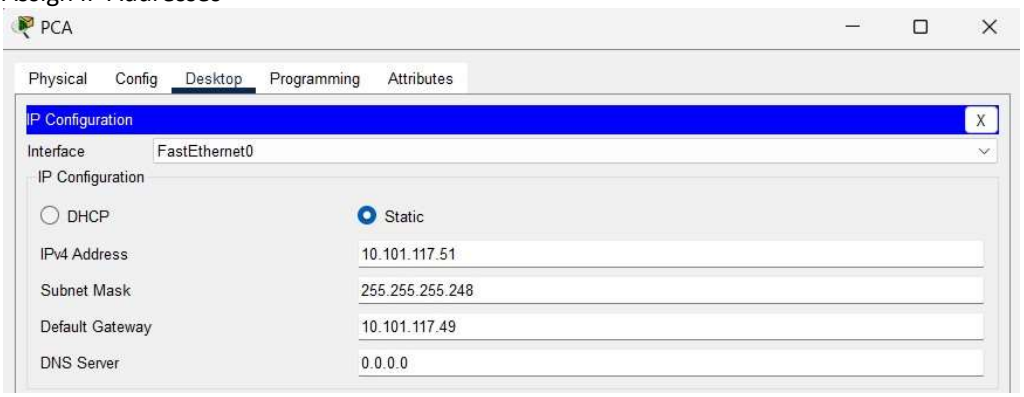
Practical 3B

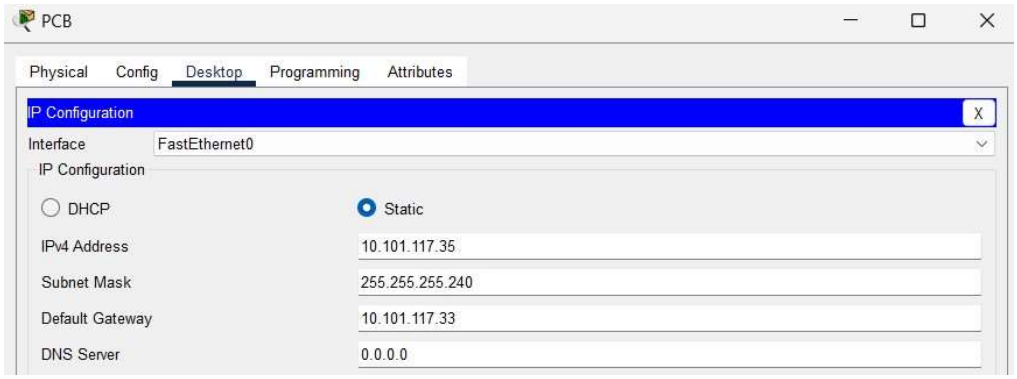
Aim: Configure, Apply and Verify an Extended Numbered ACL

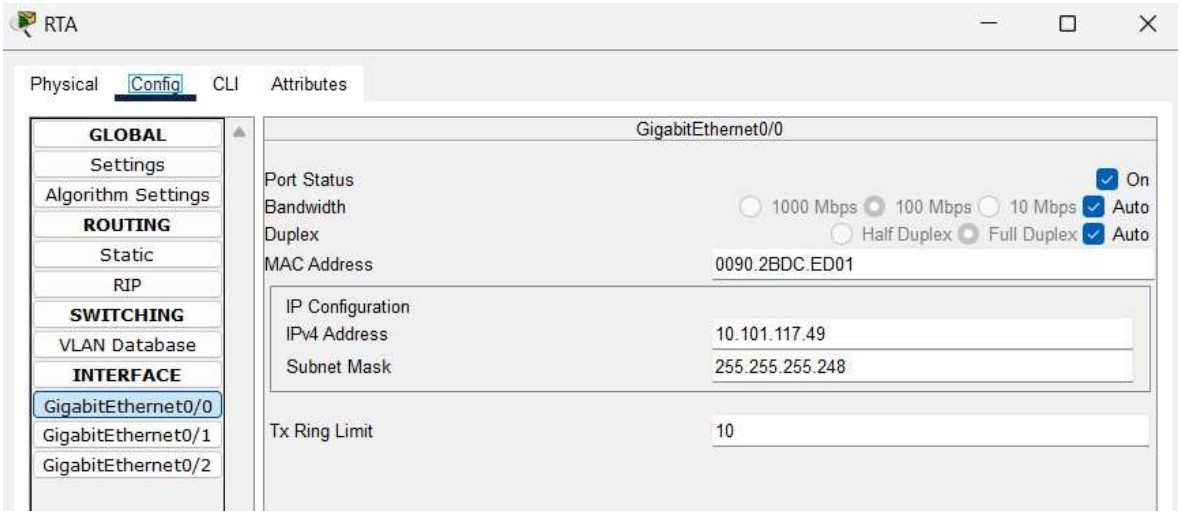
Topology Diagram

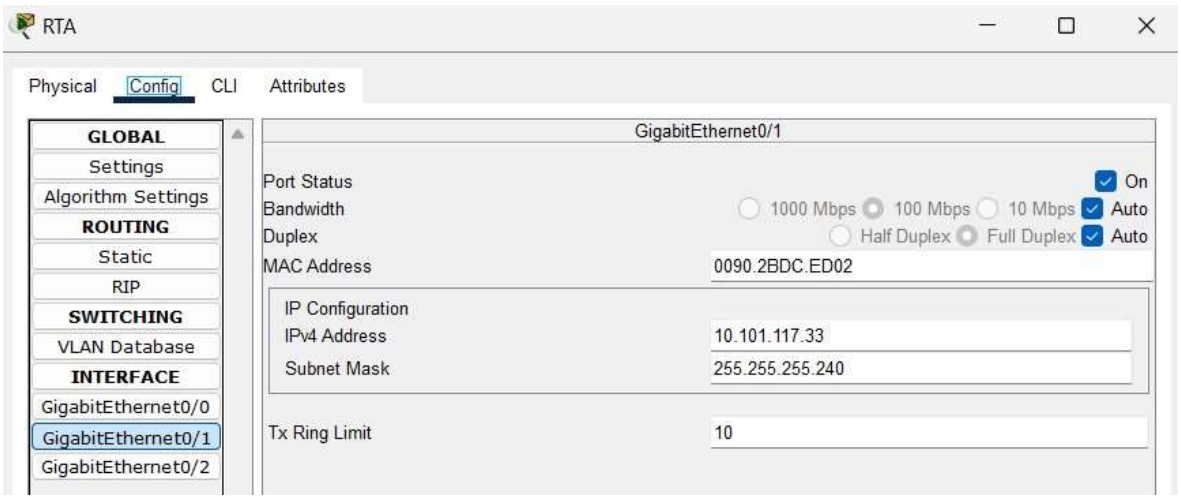


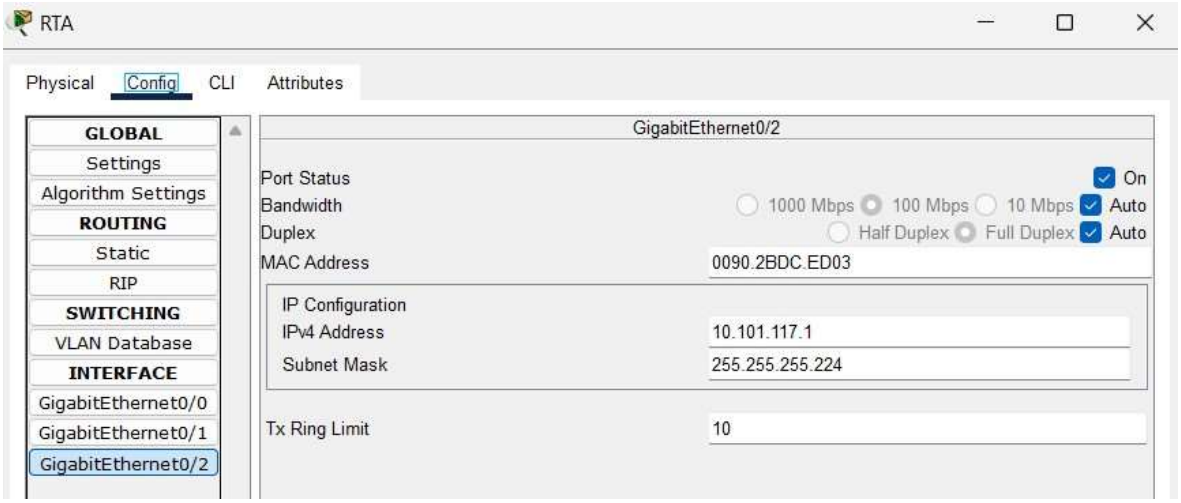
Assign IP Addresses






RTA
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/2
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0090.2BDC.ED01
IP Configuration
IPv4 Address
10.101.117.49
Subnet Mask
255.255.255.248
Tx Ring Limit
10


RTA
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/2
GigabitEthernet0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0090.2BDC.ED02
IP Configuration
IPv4 Address
10.101.117.33
Subnet Mask
255.255.255.240
Tx Ring Limit
10


RTA
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/2
GigabitEthernet0/2
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0090.2BDC.ED03
IP Configuration
IPv4 Address
10.101.117.1
Subnet Mask
255.255.255.224
Tx Ring Limit
10

SWA

Physical Config CLI Attributes

IOS Command Line Interface

```
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

Physical Config CLI Attributes

IOS Command Line Interface

```
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

Physical Config CLI Attributes

IOS Command Line Interface

```
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
```

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
```

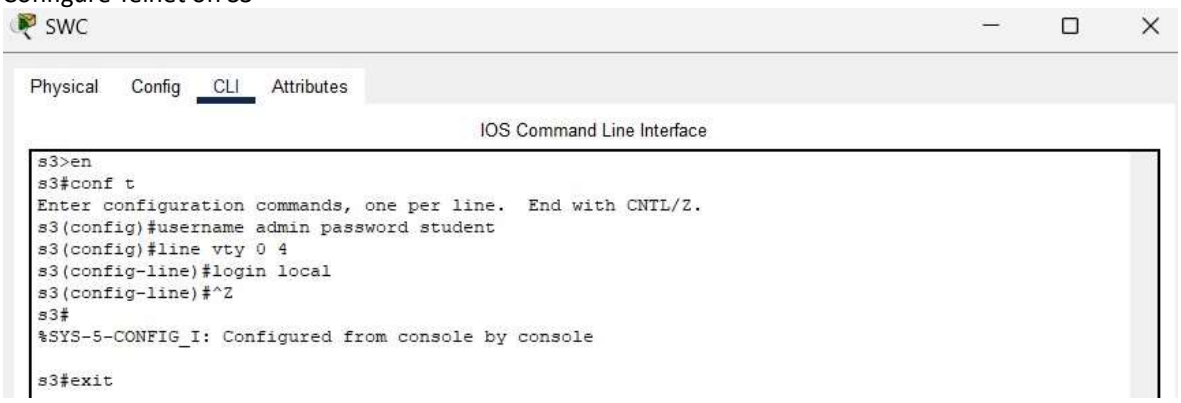
S2:

```
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
```

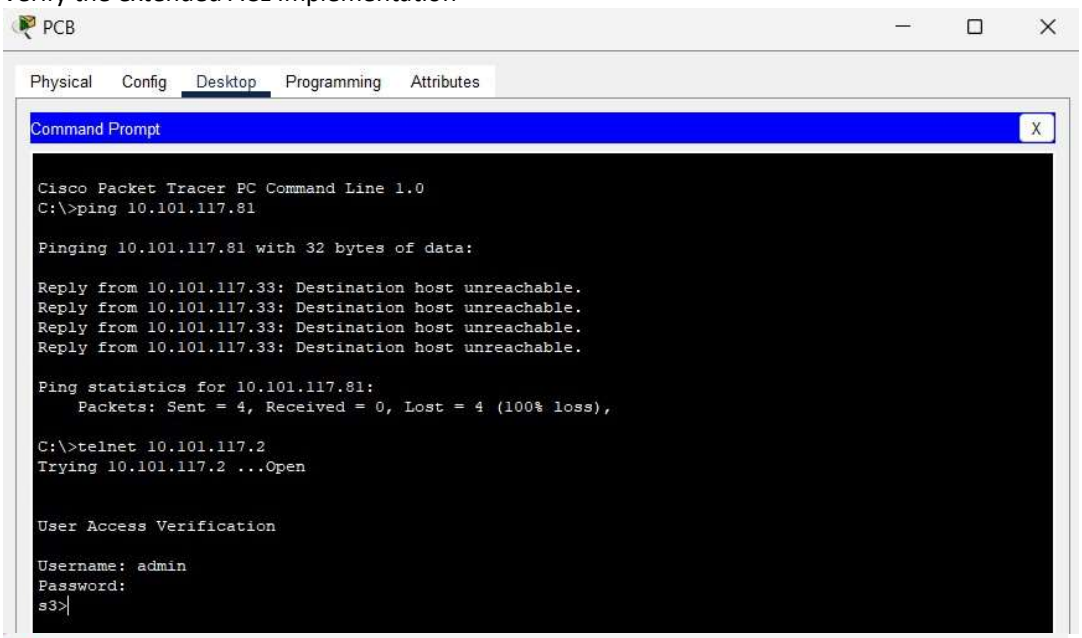
Configure Telnet on S3

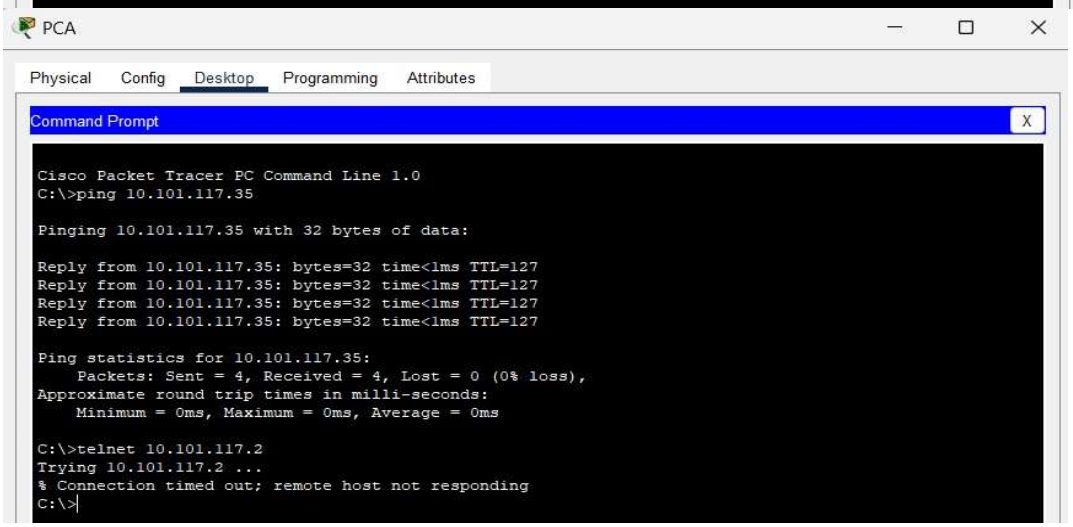


Configure, Apply and verify an extended numbered ACL
(Devices on LAN 10.101.117.32 are allowed to remotely access devices in LAN 10.101.117.0 using the TELNET protocol. Besides ICMP, all traffic from other networks is denied.)

```
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 tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq telnet
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





Practical 4

Aim:- Configure IP ACLs to Mitigate Attacks

Objectives

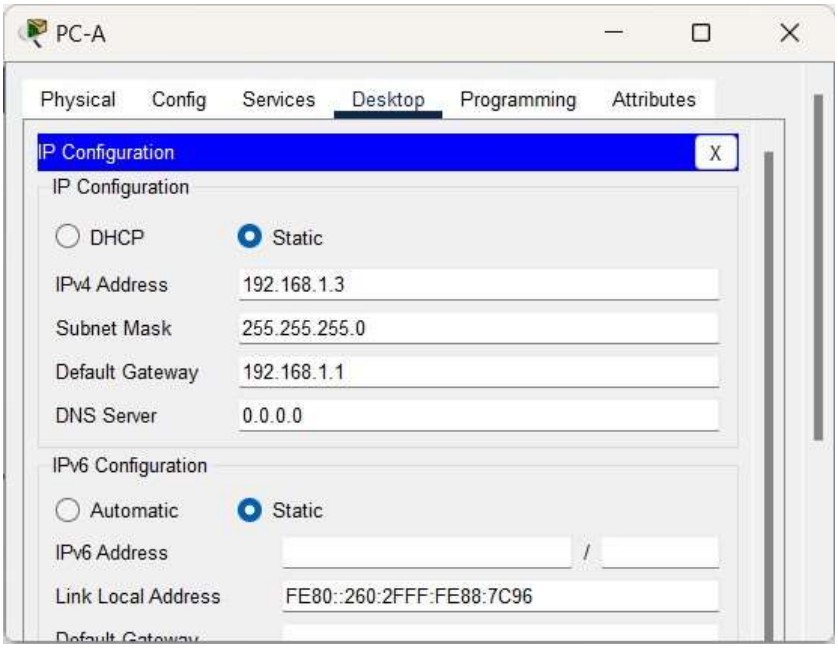
- Verify connectivity among devices before firewall configuration.
- Use ACLs to ensure remote access to the routers is available only from management station PC-C.
- Configure ACLs on R1 and R3 to mitigate attacks.
- Verify ACL functionality

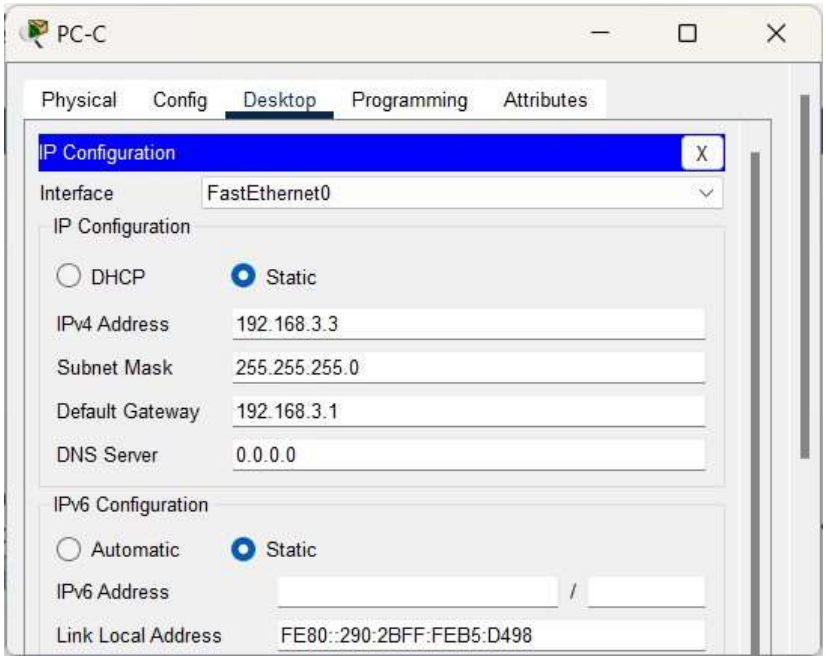
Addressing Table

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

Assigning ip

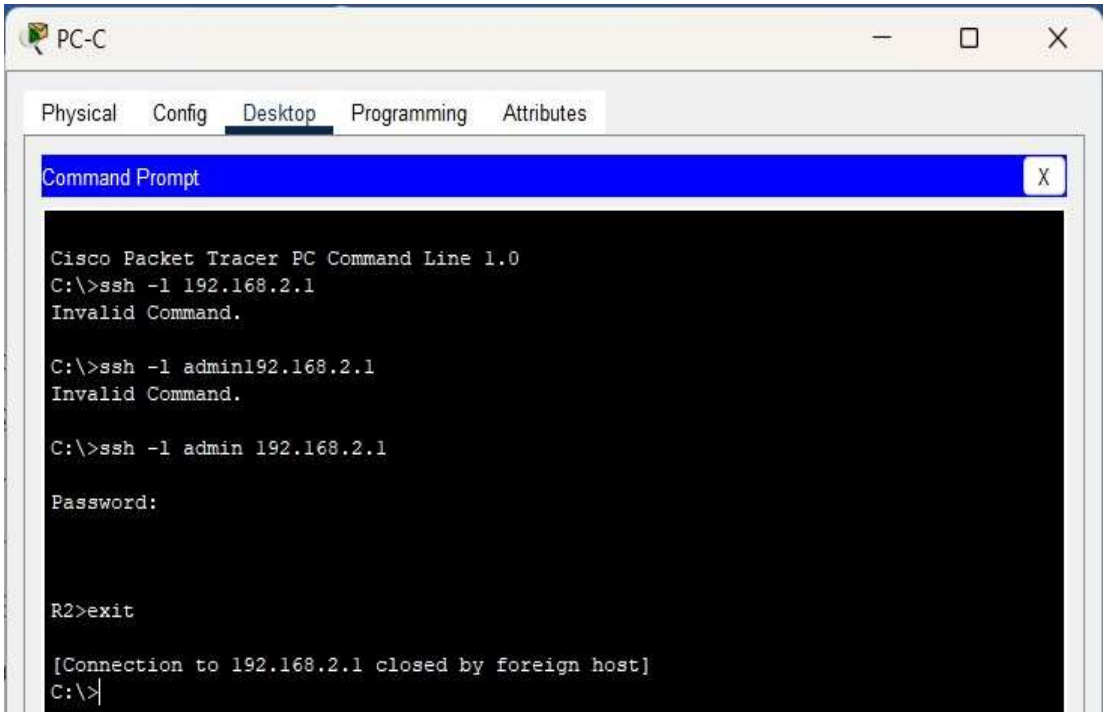


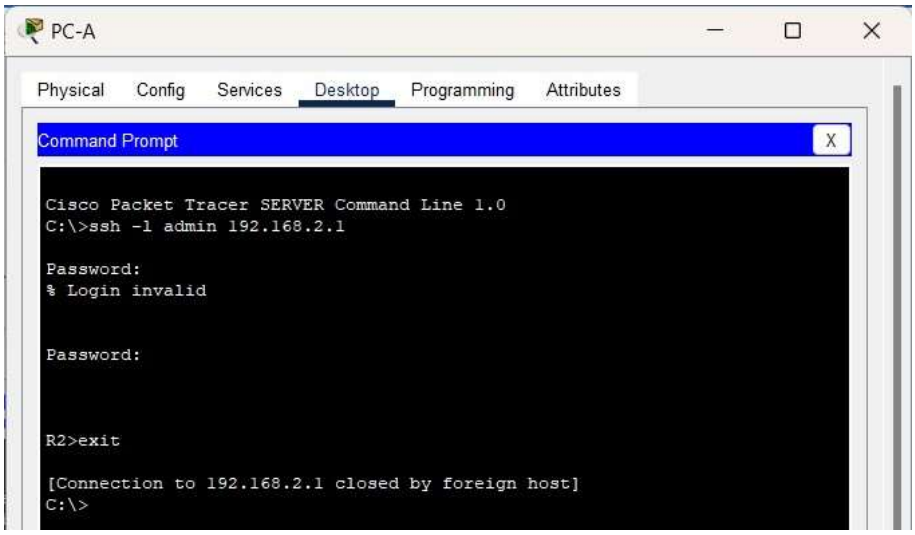


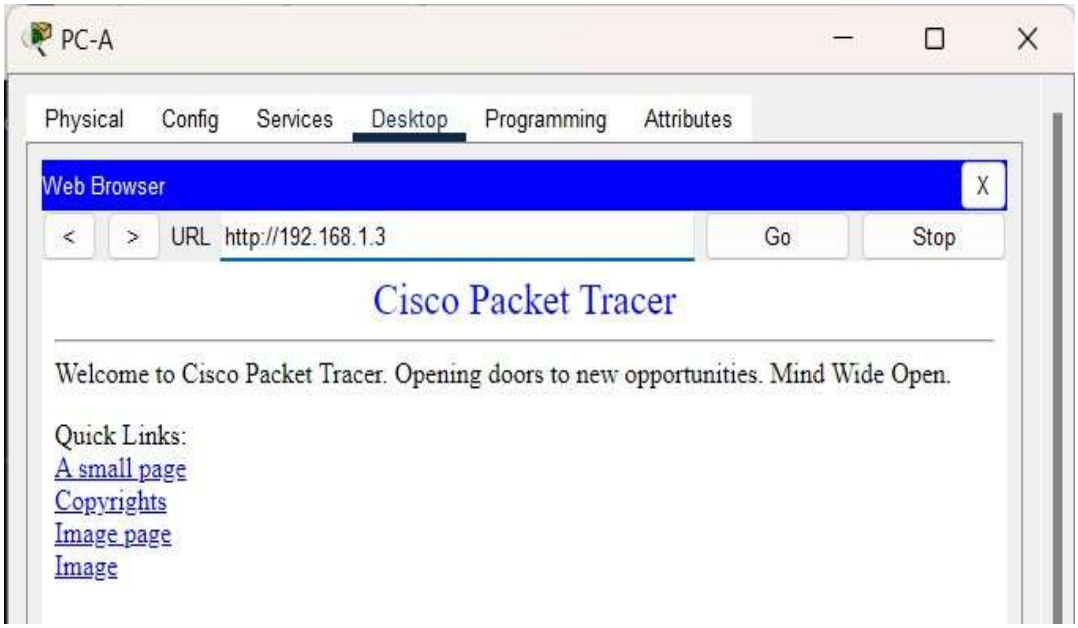
Enable SSH on Router 2
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip domain-name securityincomputing.com
Router(config)#username admin secret pwd

```
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

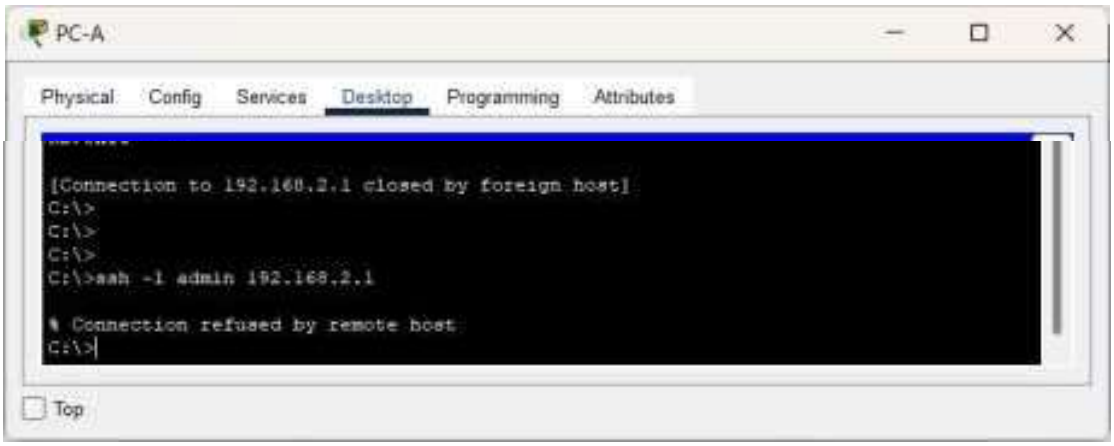


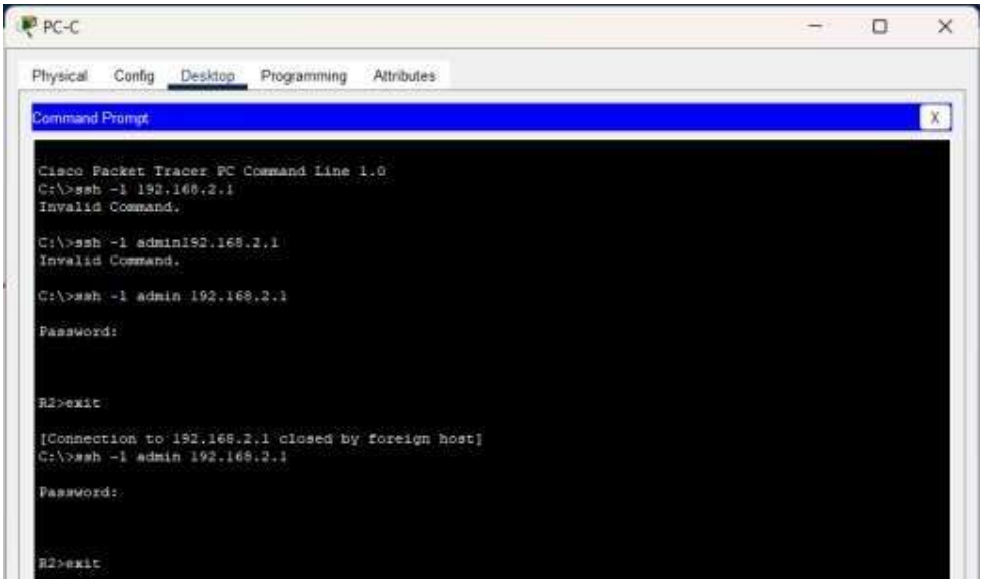




Configure ACL on routers (block all remote access to the routers except from PC)
Router 1
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 10 permit host 192.168.3.3
Router(config)#line vty 0 4
Router(config-line)#access-class 10 in
Router(config-line)#^Z

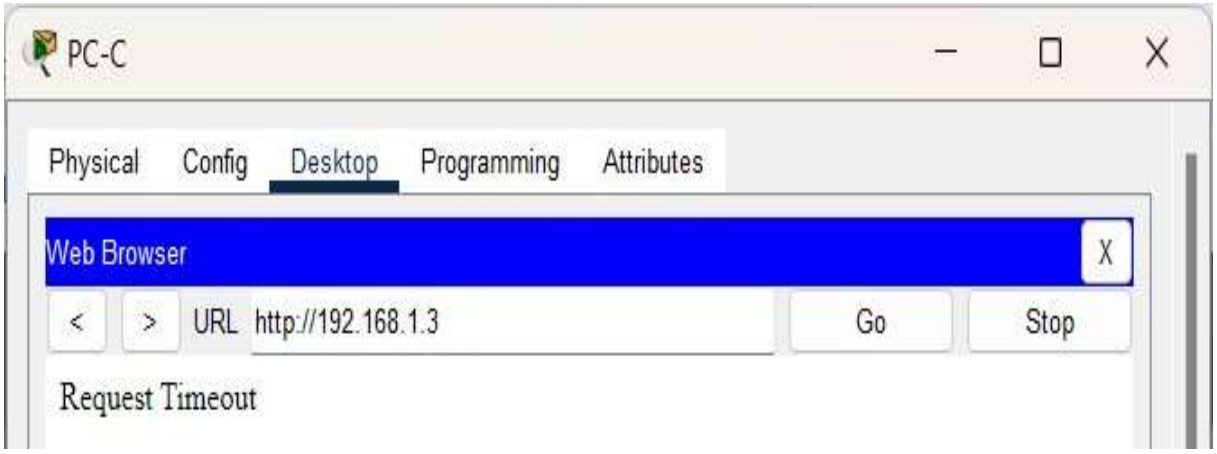
Verify the user with pcA

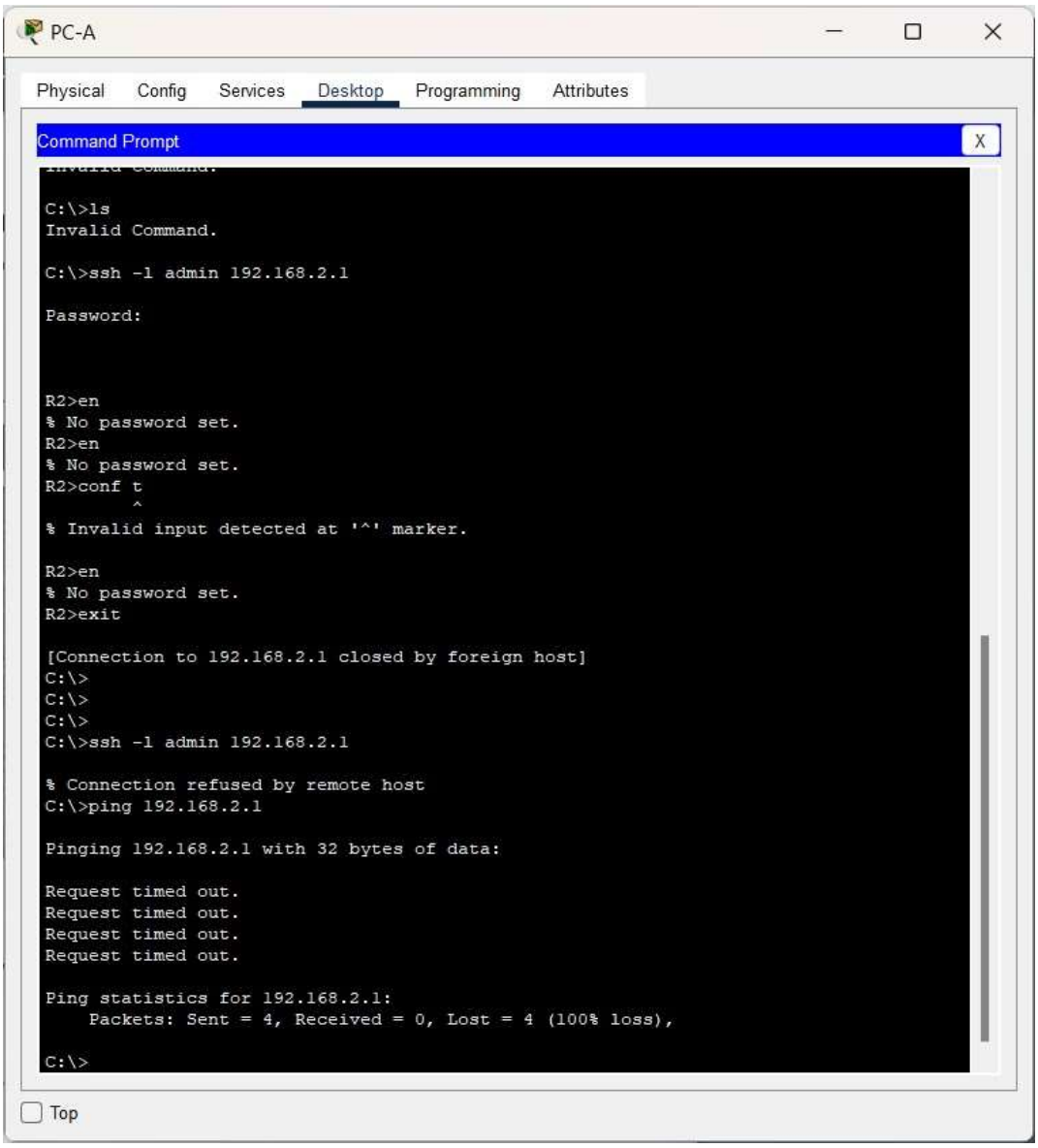




Configure ACL on routers Permit any outside host to access DNS, SMTP, and FTP services on Server o Deny any outside host access to HTTPS services on Server. Permit PCto access RI via SSH.

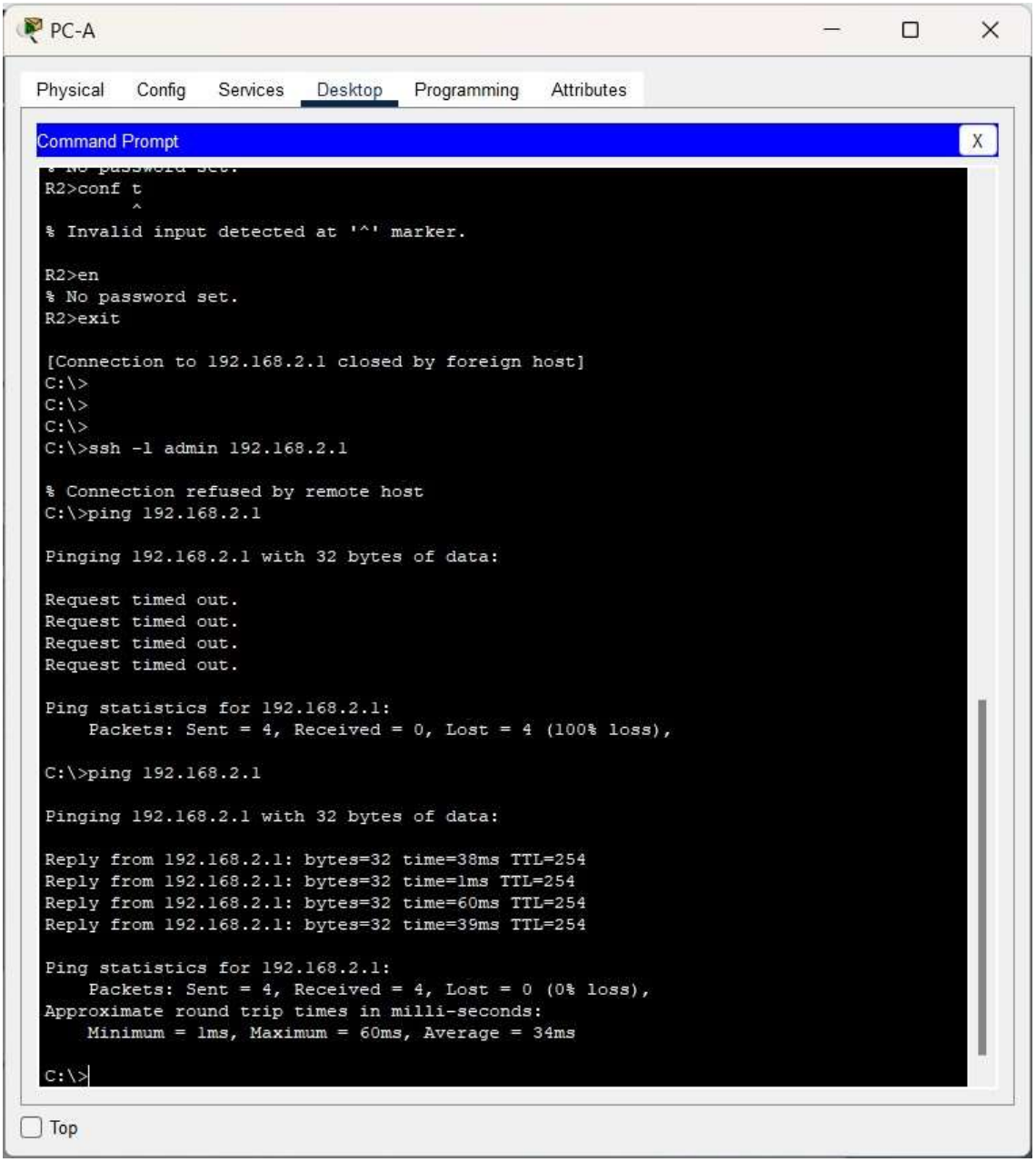
```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 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)#
```


PC-C
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.1.3
Go
Stop
Request Timeout


PC-A
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
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:\>
Top

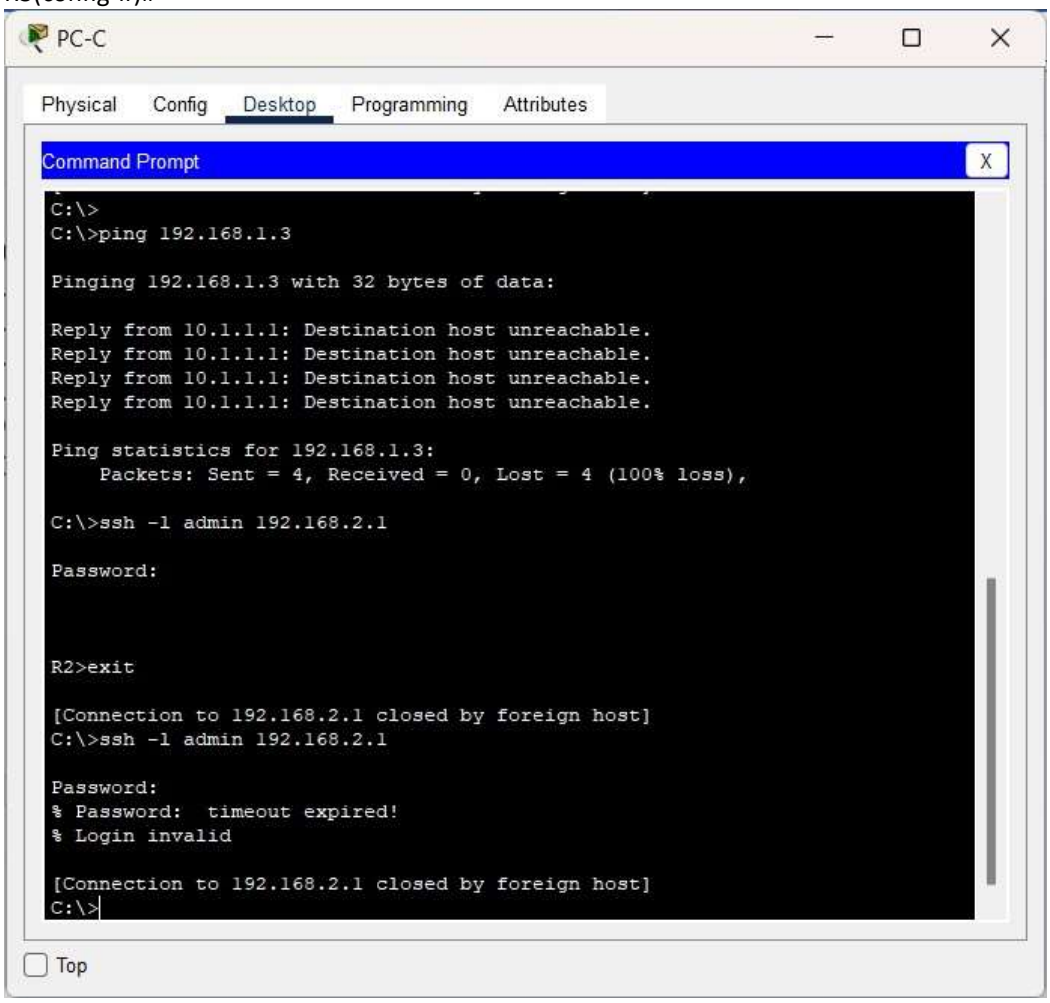
Modify an Existing ACL on R1

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



CONFIGURE ACL ON ROUTERS

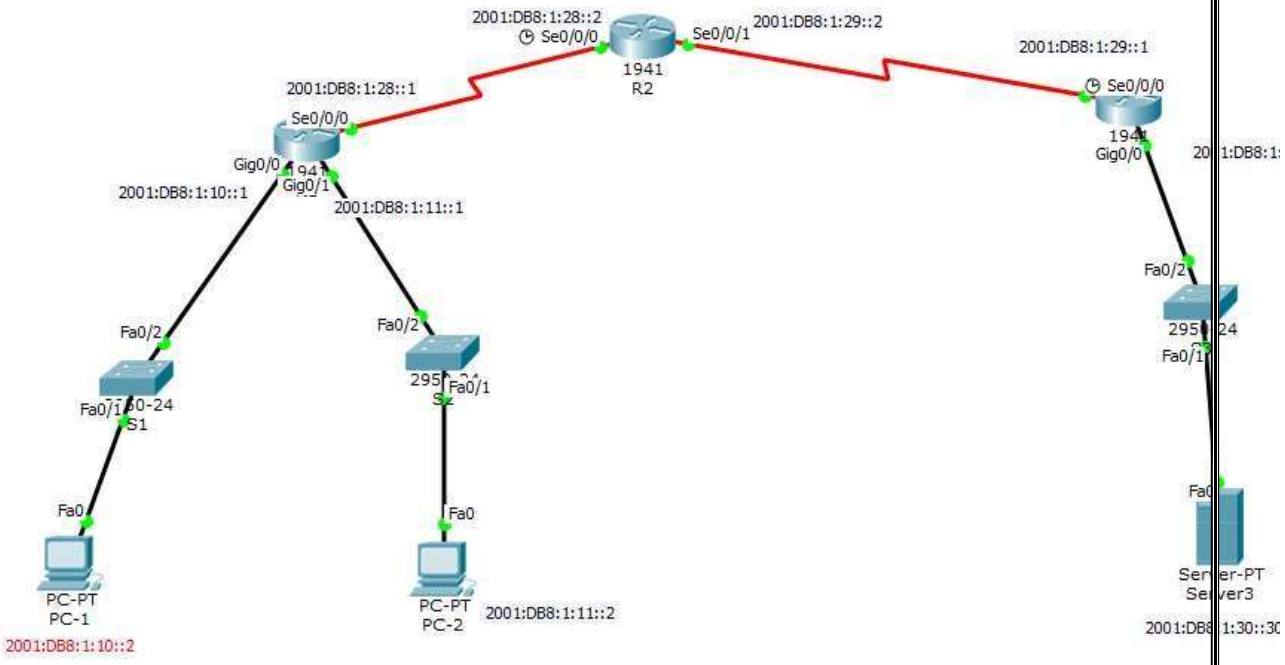
```
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 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)#
```



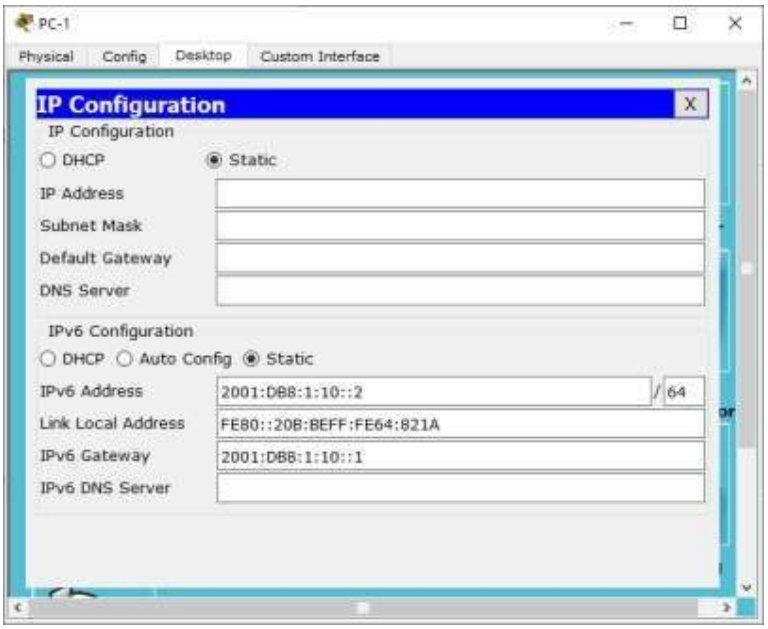
Practical 5

Configuring IPv6 ACLs

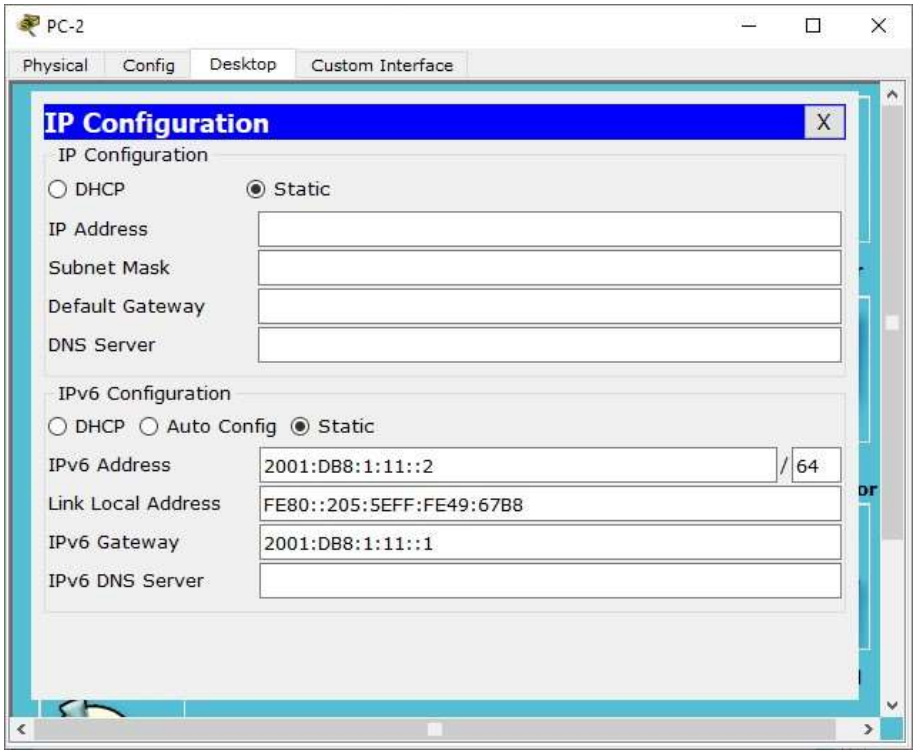
Topology



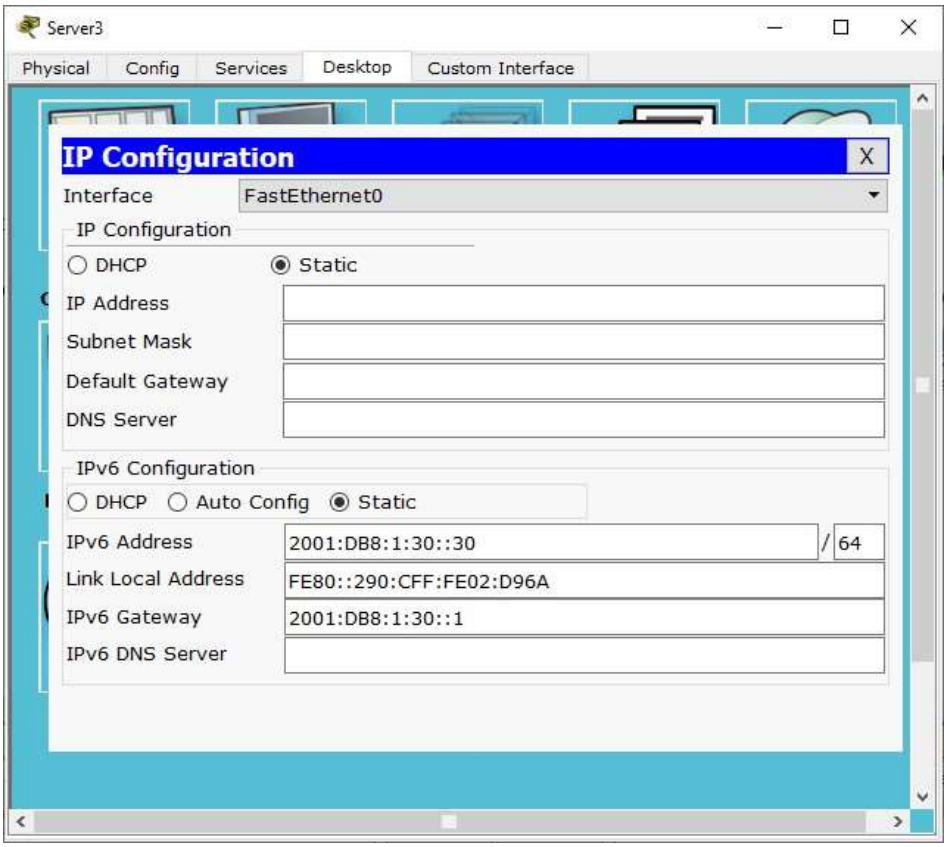
Assign IP Addresses on Pc 1



ASSIGN IP ADDRESSES ON PC 2



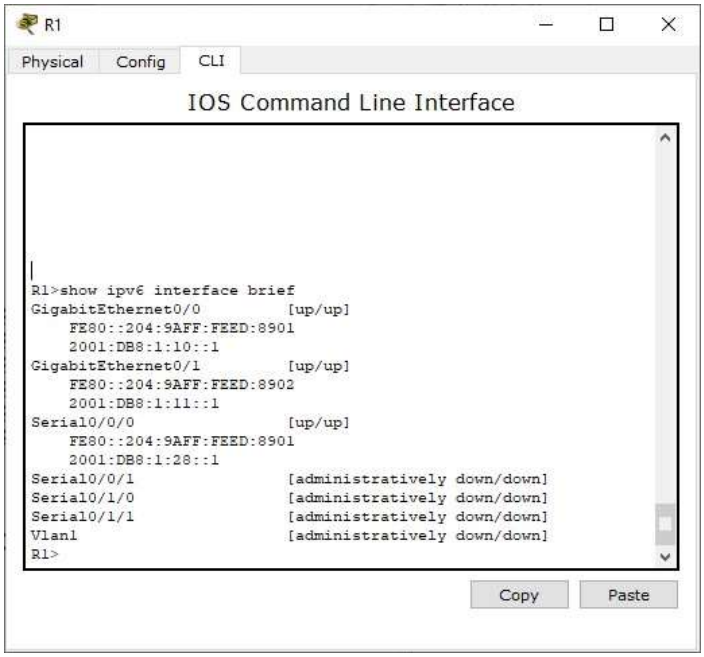
ASSIGN IP ADDRESSES ON SERVER3



ASSIGN IPV6 ON ROUTER

ROUTER 1 CONFIGURATION

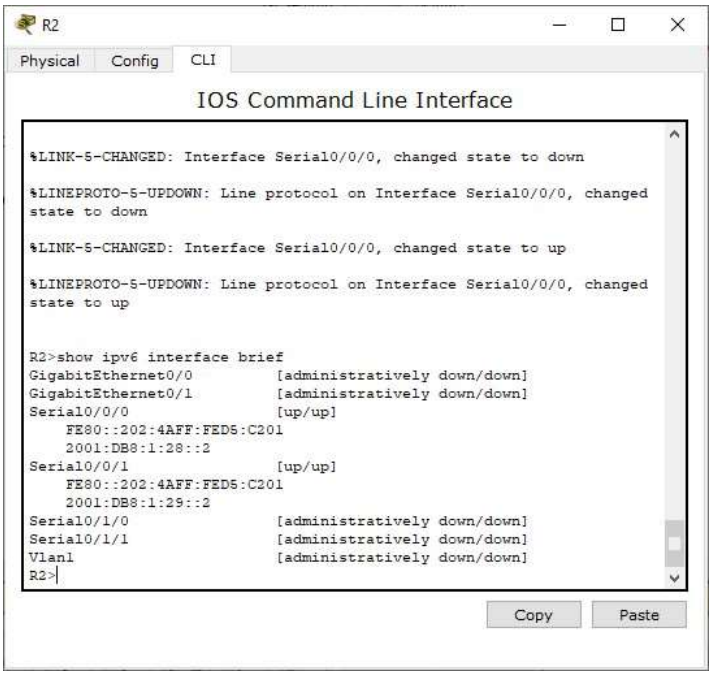
```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
Router(config)#ipv6 unicast-routing
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:DB8:1:10::1/64
Router(config-if)#no shut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

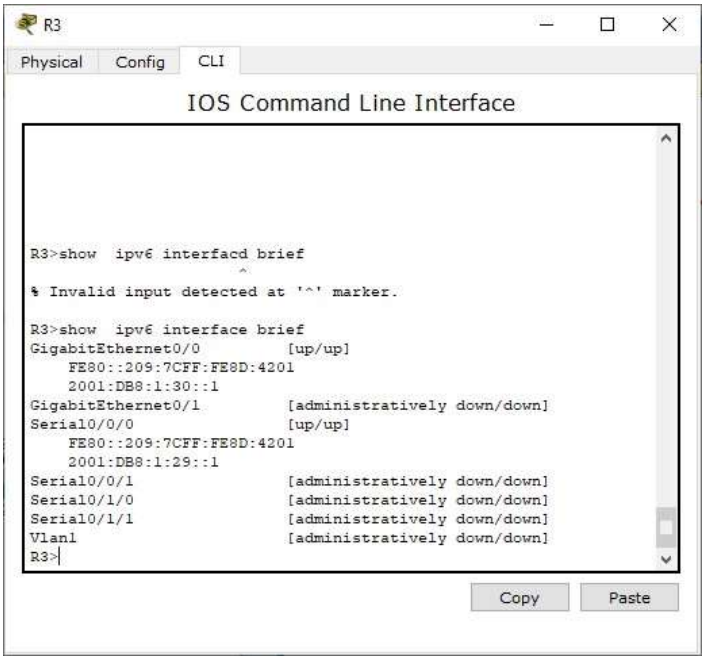
```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
Router(config)#ipv6 unicast-routing
Router(config)#interface serial0/0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:DB8:1:28::2/64
Router(config-if)#no shut
Router(config-if)#interface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

Router(config-if)#no shut



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



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

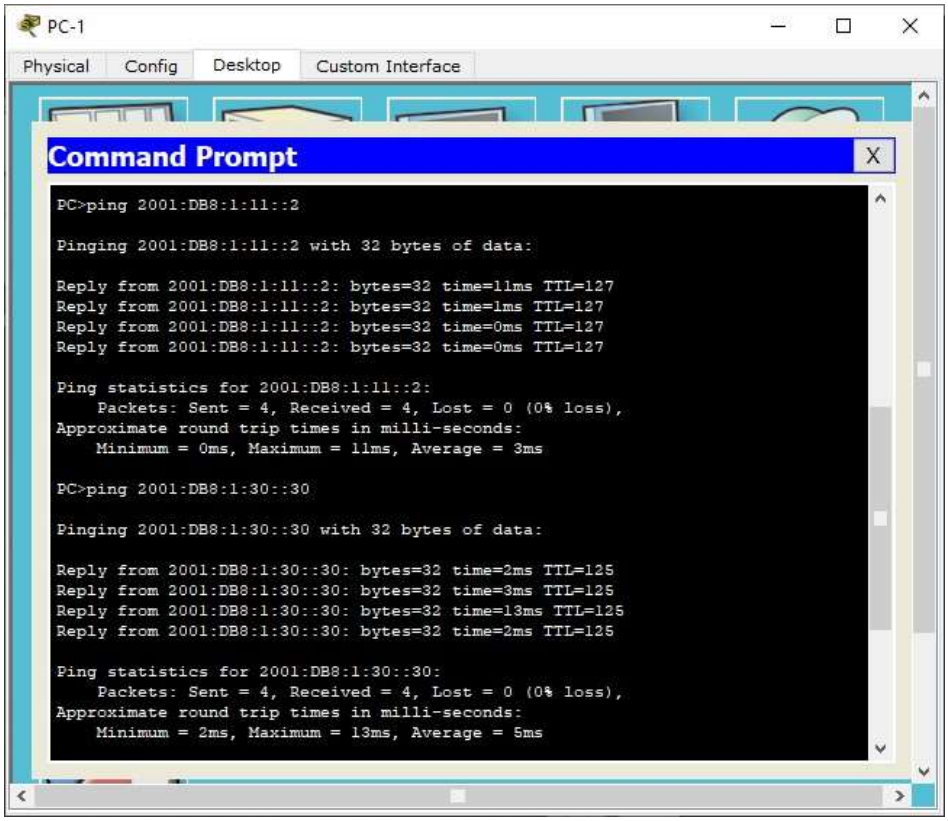
Rip on router 2

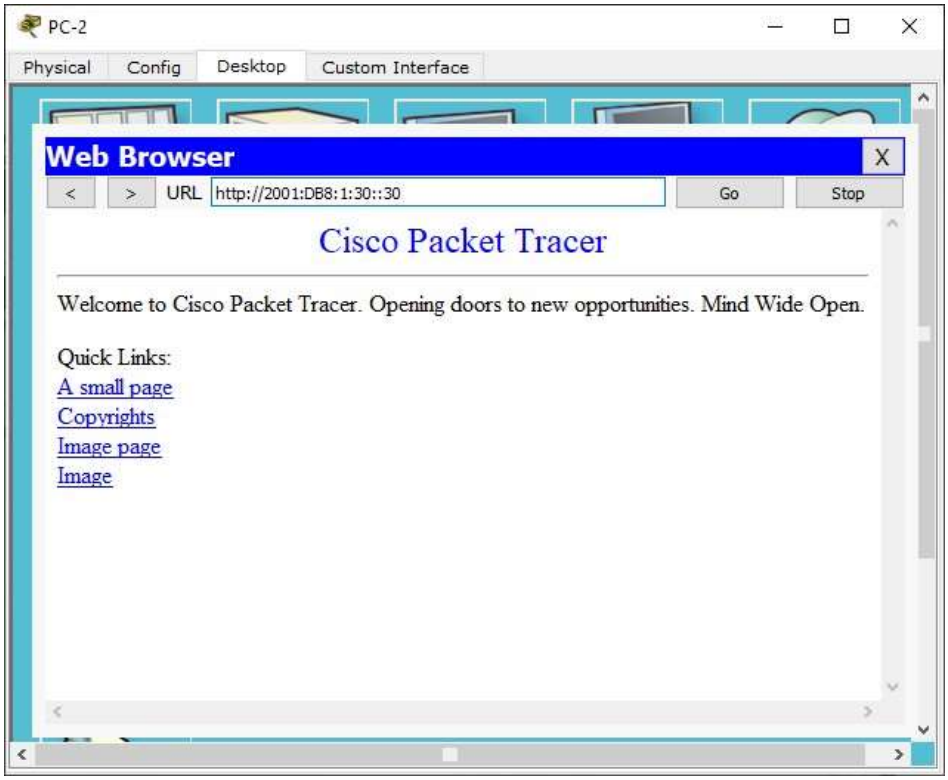
interface serial0/0/0 ipv6 rip Ripng enable interface serial0/0/1
ipv6 rip Ripng enable

Rip on router 3

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

Checking network connectivity


PC-1
Physical
Config
Desktop
Custom Interface
Command Prompt
X
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

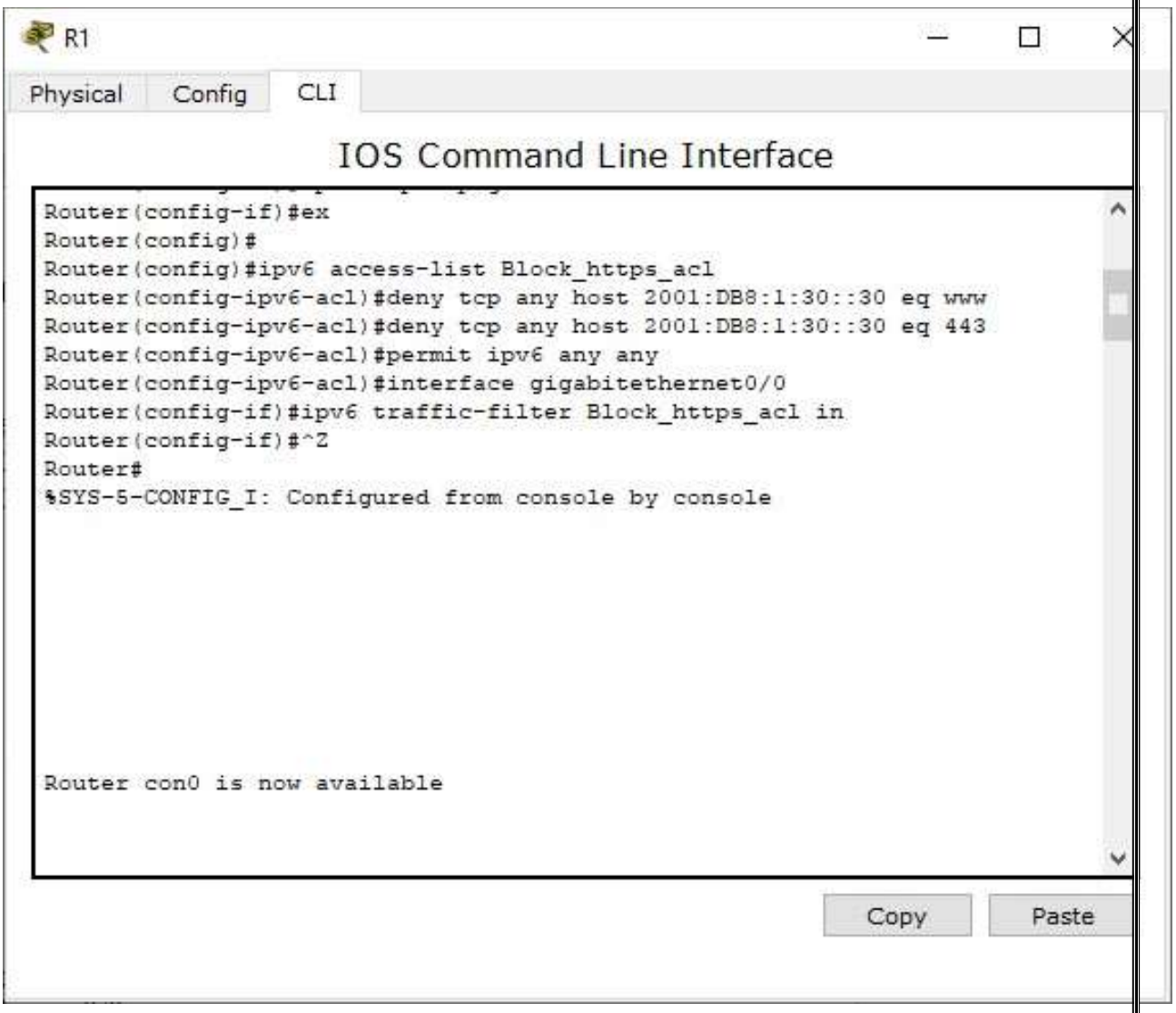

PC-2
Physical
Config
Desktop
Custom Interface
Web Browser
X
<
>
URL
http://2001:DB8:1:30::30
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image

Configuring ACL

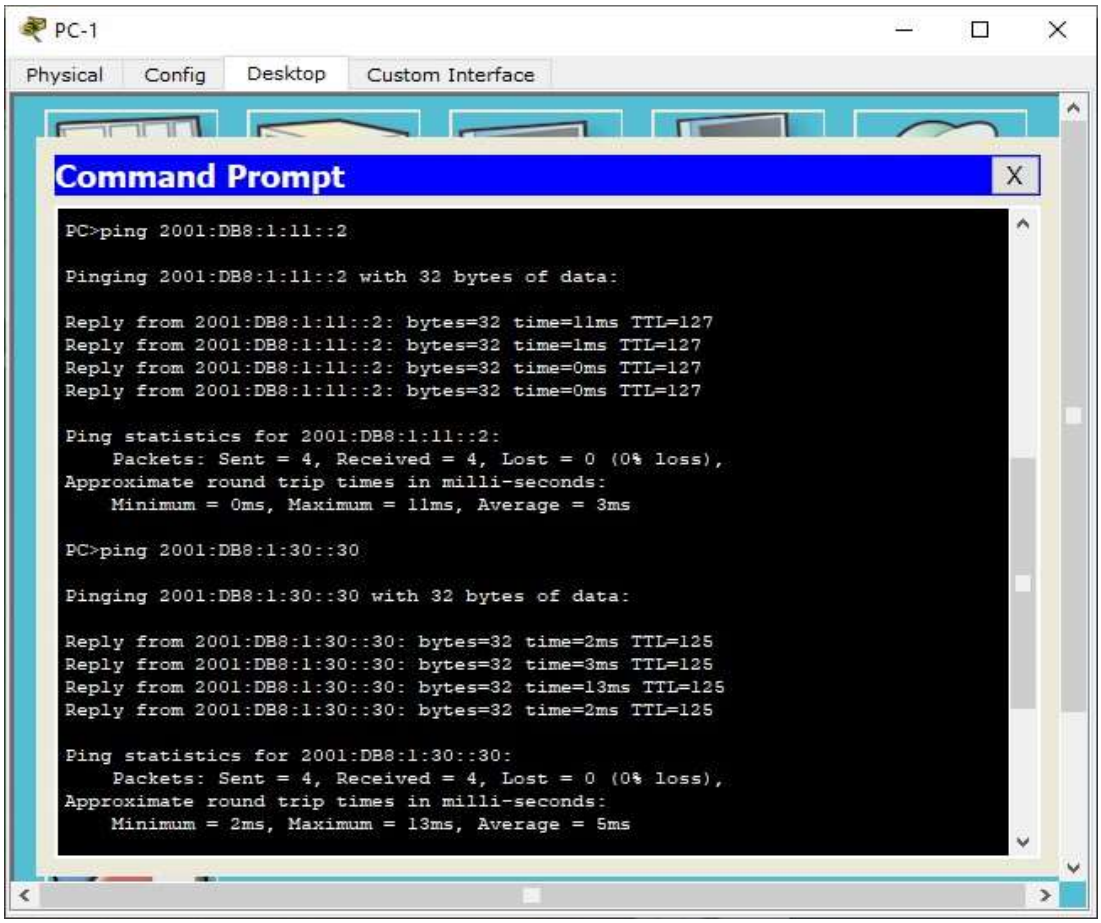
(Block HTTP and HTTPS access and Allow aJI other IPv6 traffic to pass)

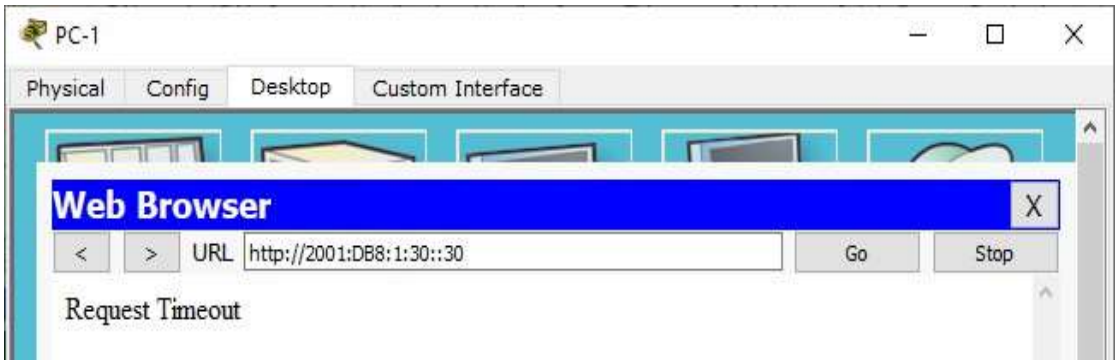
Router 1

```
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#
```



Verifying the working of ACL

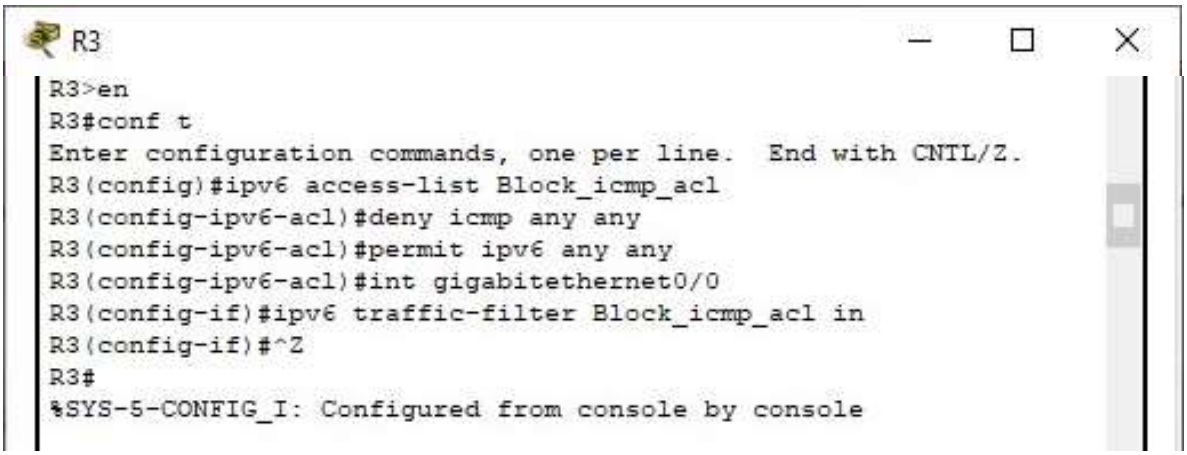




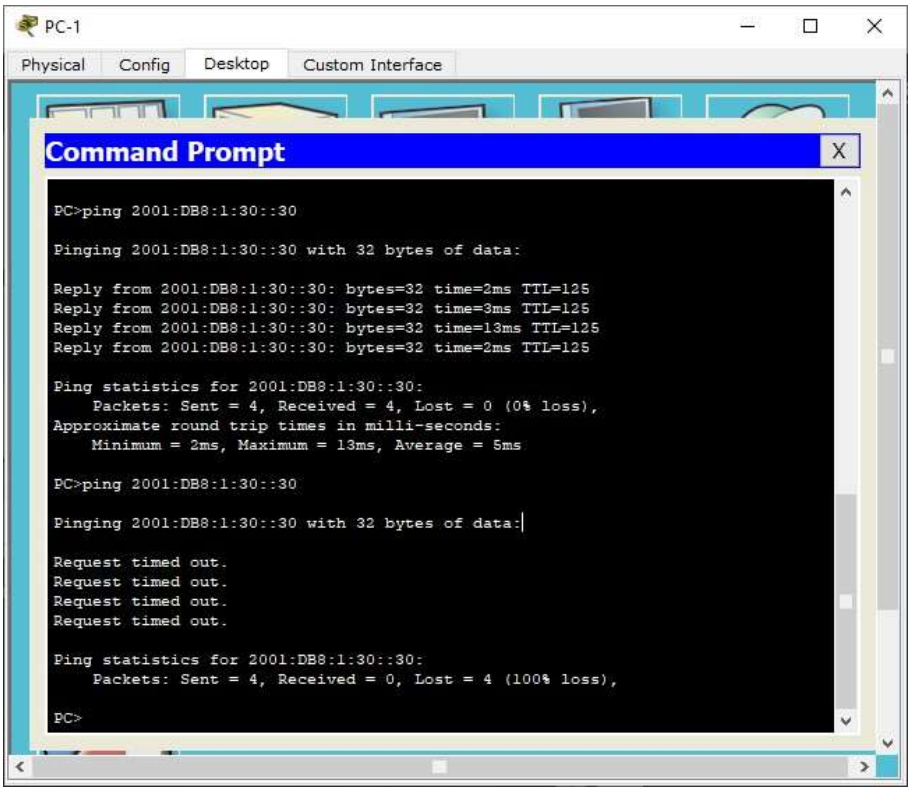
Configuring ACL (Block ICMP access and Allow all other IPv6 traffic to pass).

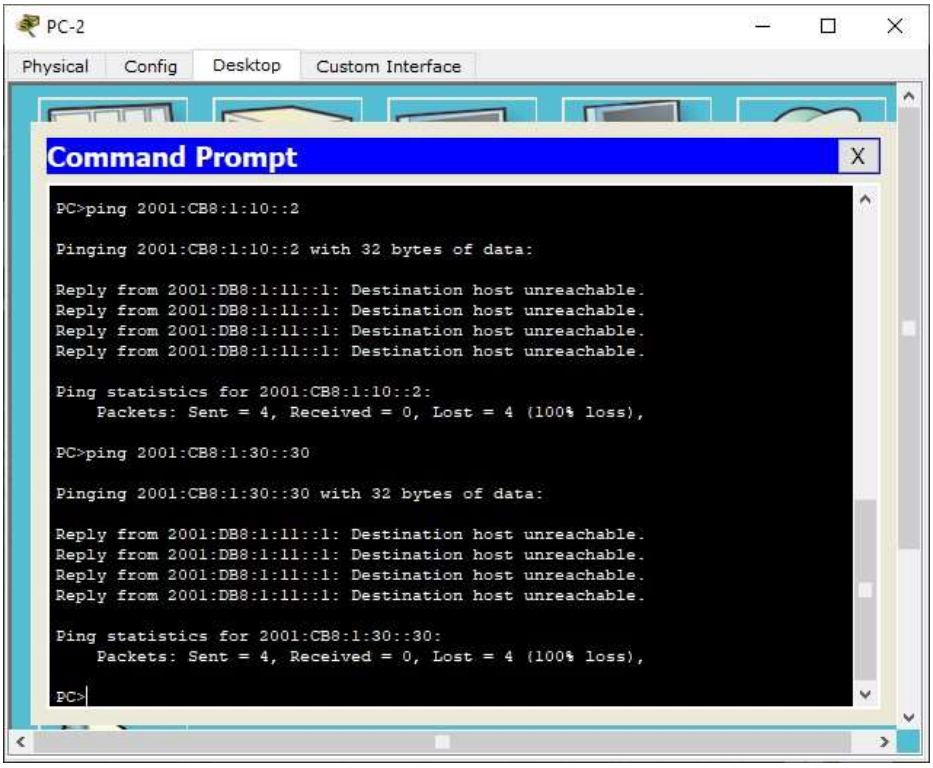
Router 3

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



VERIFYING THE WORKING OF ACL





Practical 6

Configuring a Zone-Based Policy Firewall (ZPF)

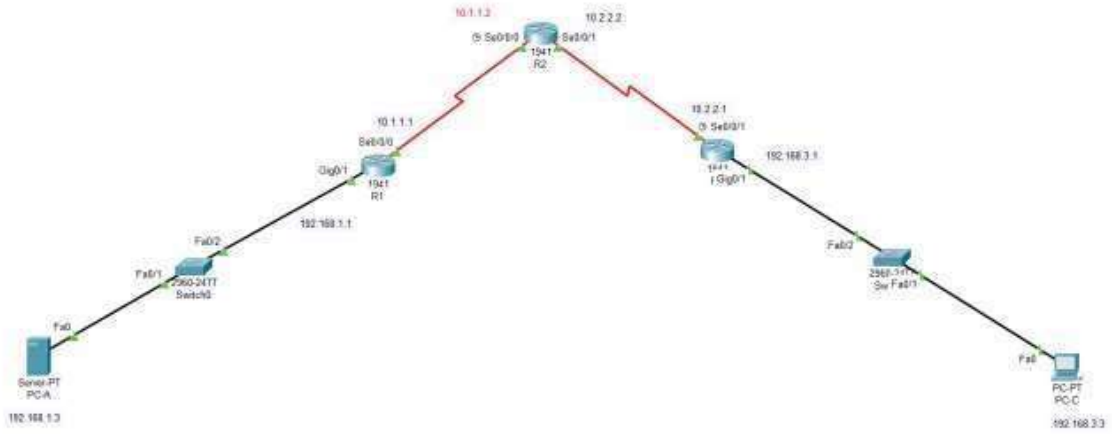
Addressing Table

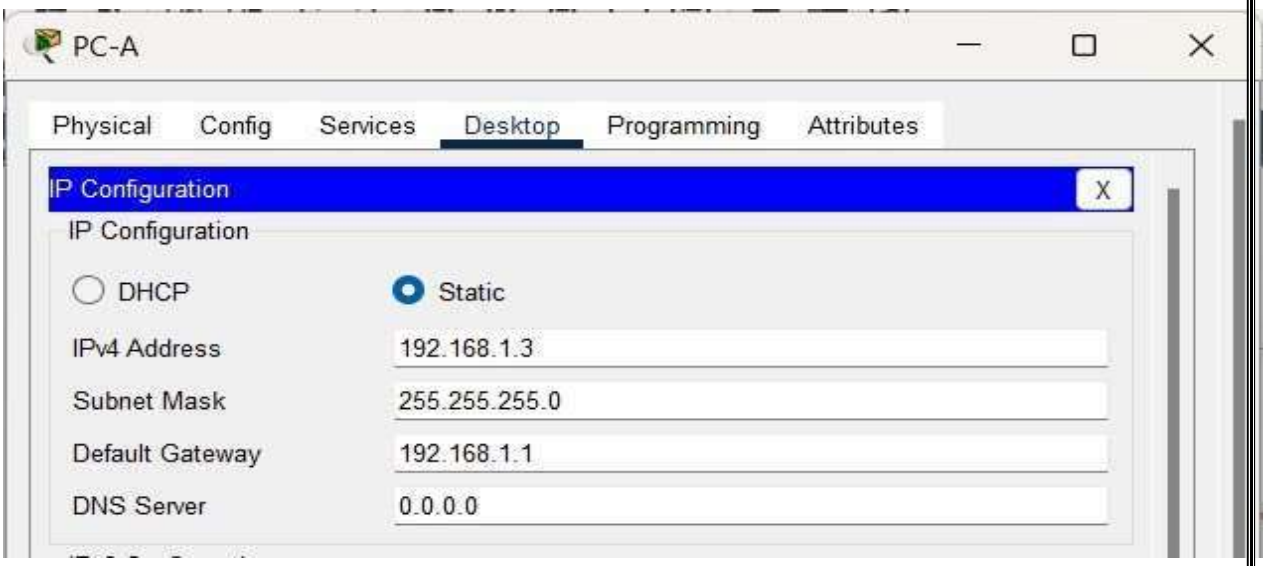
Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	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

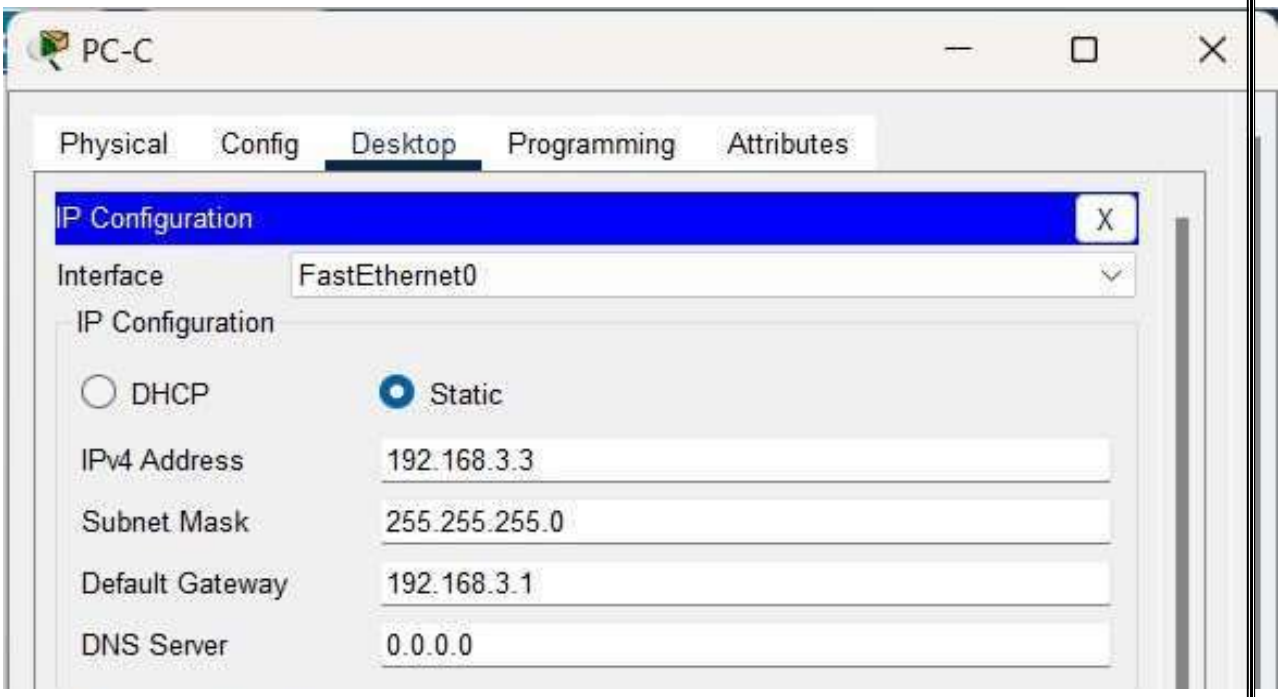
Objectives

- 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







Router 1 Configure

Router>enable
Router#configure terminal
Enter configura on 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

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

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 configura on 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 configura on.

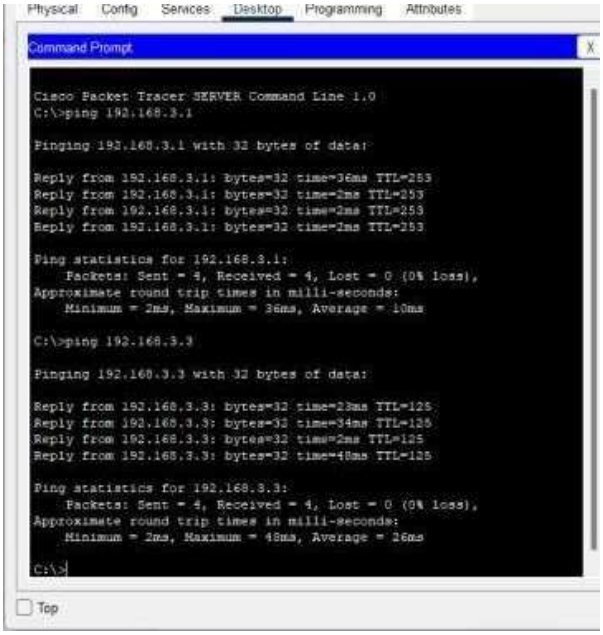
R2(config)#crypto key generate rsa
The name for the keys will be: R2.securityincompu ng.com
Choose the size of the key modulus in the range of 360 to 4096 for your General Purpose Keys.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
% Genera ng 1024 bit RSA keys, keys will be non-exportable...[OK]

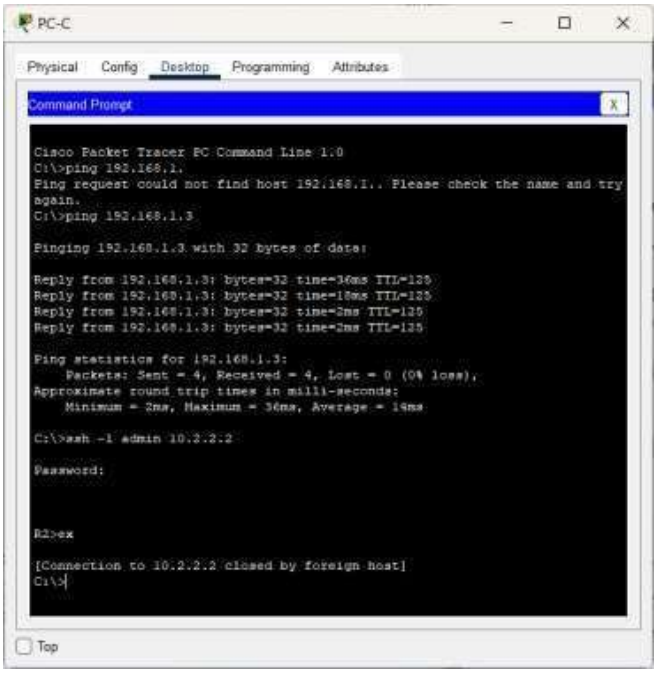
R2(config)#ip ssh authen ca on-retries 2
*Mar 1 0:20:53.121: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#ip ssh version 2
R2(config)#^Z
R2#

Verify Basic Network Connectivity

Step 1: Check connectivity from PCA to PCC



Step 2: Access R2 using SSH.
PCC>ssh –l admin 10.2.2.2
Password:pwd
R2>exit



Step 3: From PC-C, open a web browser to the PC-A server. Desktop -> Web Browser
URL: h p://192.168.1.3
(Successful)

CREATE THE FIREWALL ZONES ON R3

Enable the Security Technology package on R3

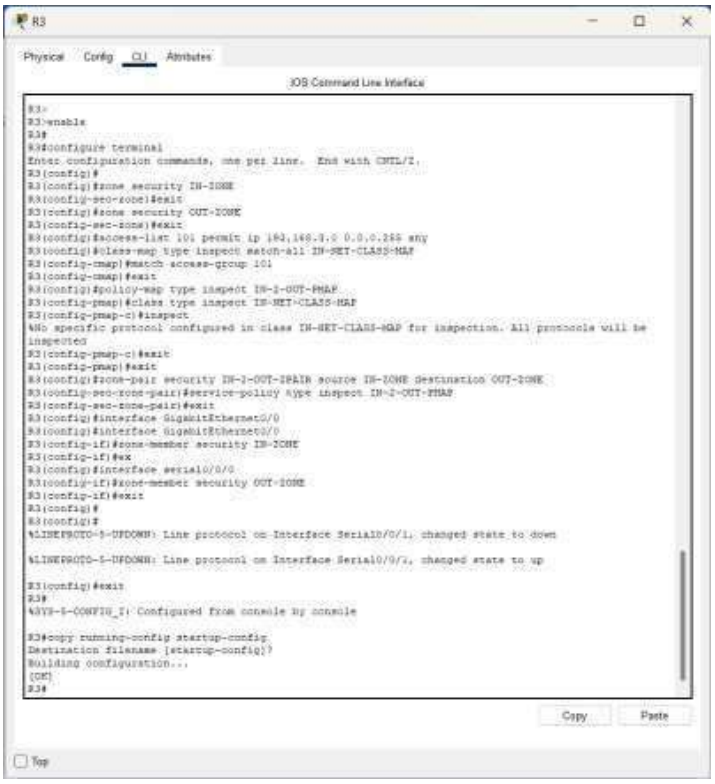
```
R2>
R2>en
R2#show version

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-
```

Technology Package License Information for Module:'c1900'

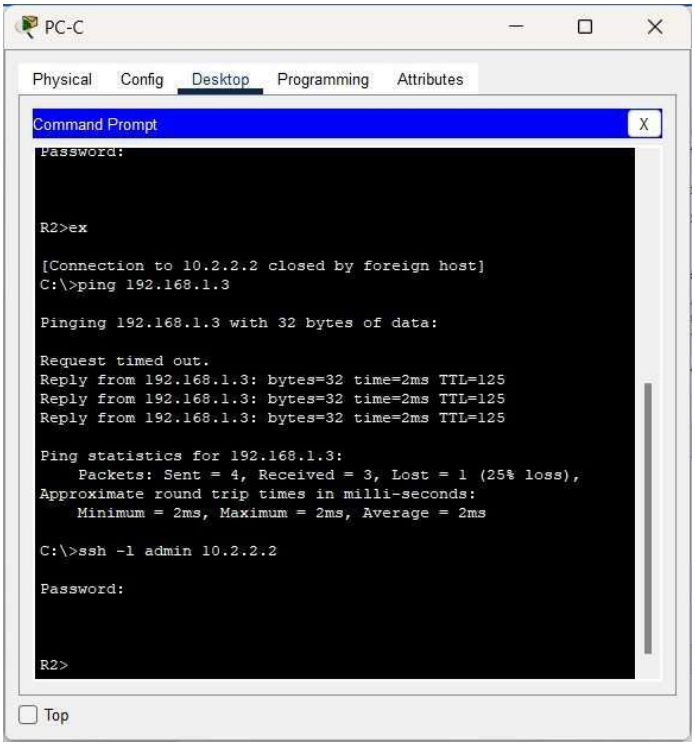
Technology Technology-package Technology-package
Current Type Next reboot
---------- ipbase ipbasek9 Permanent ipbasek9 security securityk9 Evaluation securityk9 data disable None None
Configuration register is 0x2102

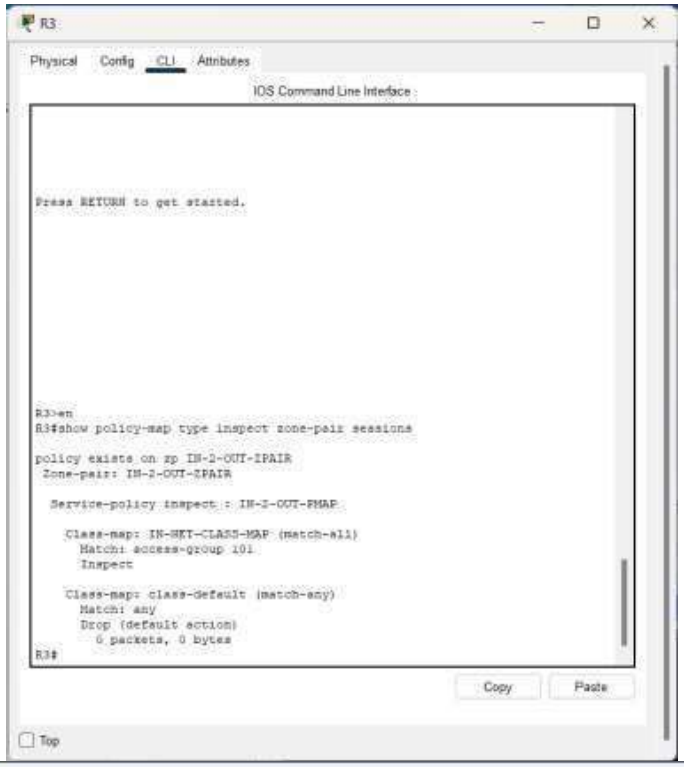
Create a Firewall zones,class Map and ACL on Router 3

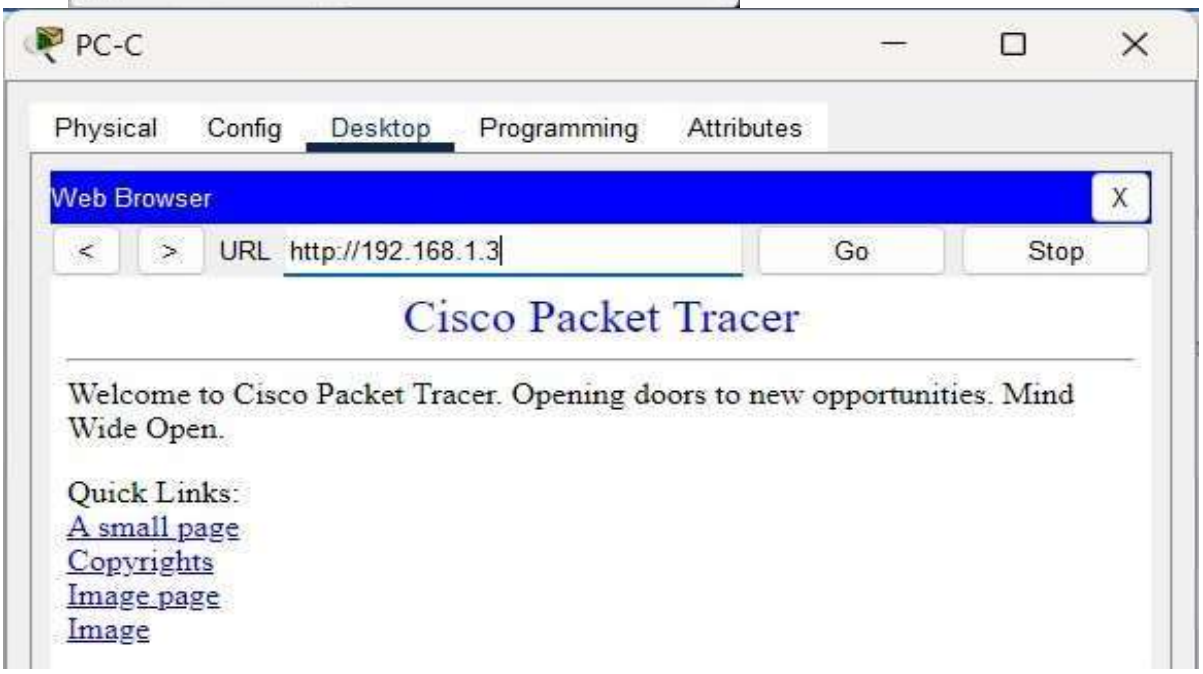
R3>
R3>enable
R3#
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#zone security IN-ZONE
R3(config-sec-zone)#exit
R3(config)#zone security OUT-ZONE
R3(config-sec-zone)#exit
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#class-map 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]



Test FireWall Functionality From IN-ZONE to OUT-ZONE




R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started.
R3>en
R3#show policy-map type inspect zone-pair sessions
policy exists on zp IN-2-OUT-ZPAIR
Zone-pair: IN-2-OUT-ZPAIR
Service-policy inspect : IN-2-OUT-PMAP
Class-map: IN-NET-CLASS-MAP (match-all)
Match: access-group 101
Inspect
Class-map: class-default (match-any)
Match: any
Drop (default action)
0 packets, 0 bytes
R3#
Copy
Paste
Top

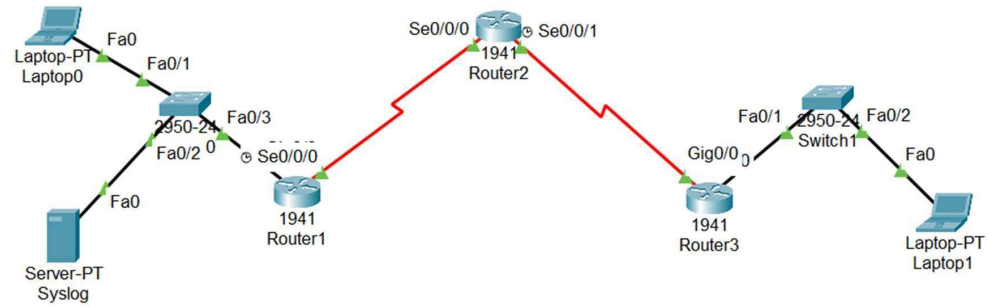

PC-C
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.1.3
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image

PRACTICAL 7

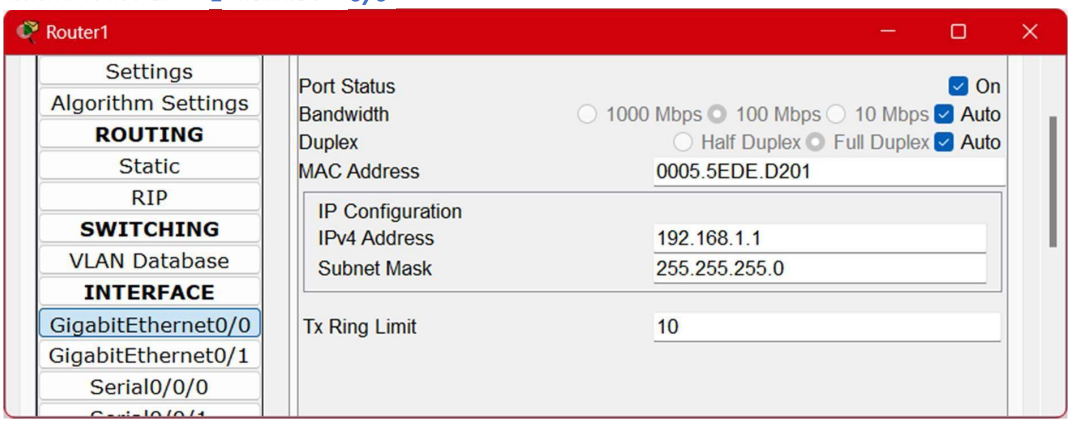
Aim Configure ISO intrusion preven on system(IPS) using CLI

a. Enable IOS IPS
b. Modify an IPS signature

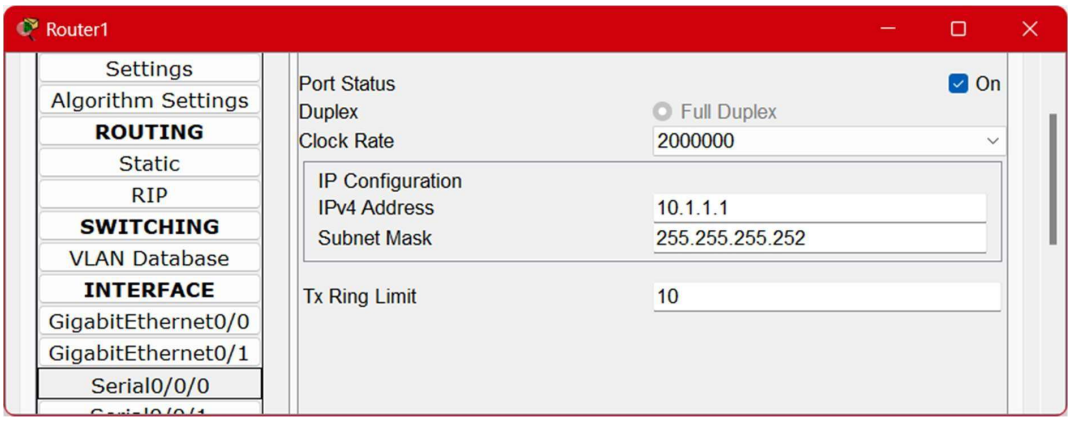
TOPOLOGY



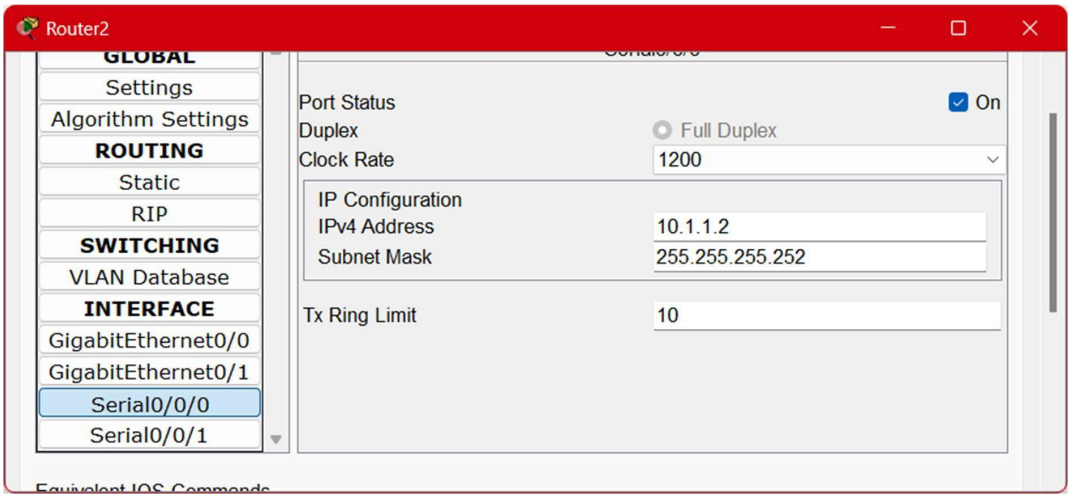
ASSIGN IP TO ROUTER 1 INTERFACE G 0/0



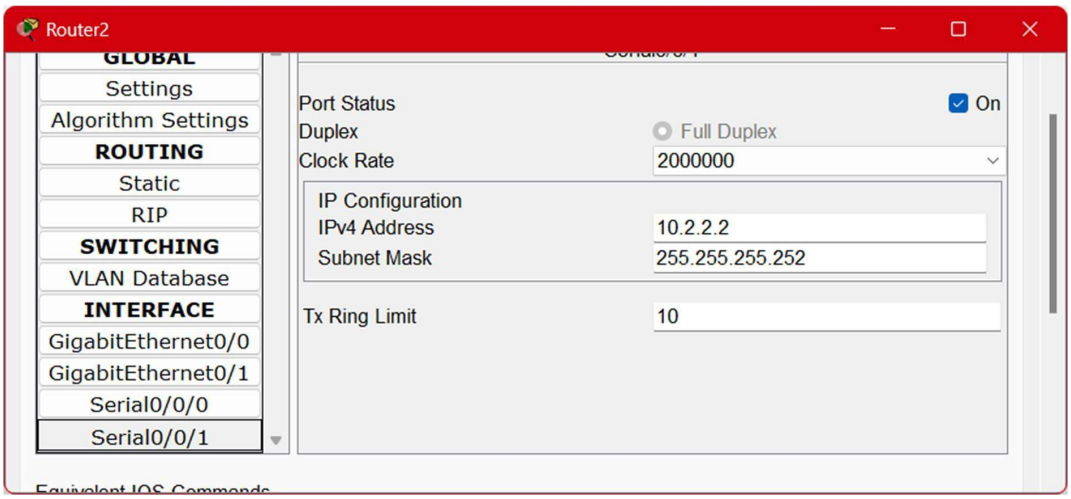
ASSIGN IP TO ROUTER$_1$ INTERFACE S$_{E0/0/0}$



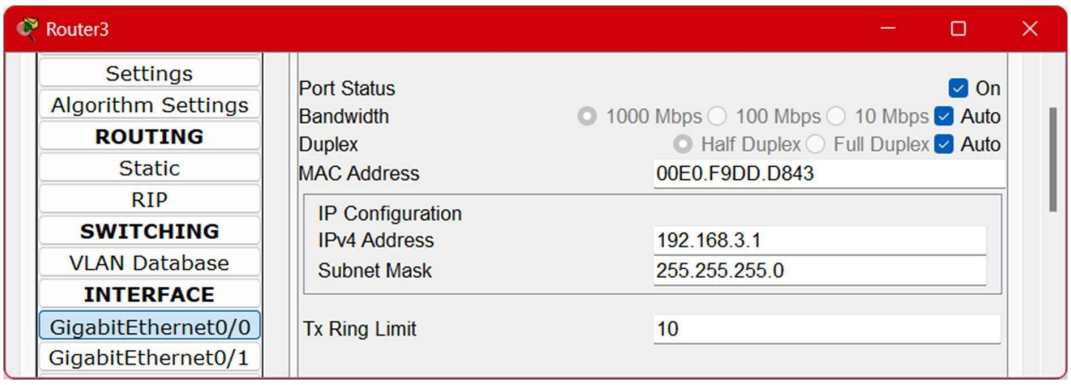
ASSIGN IP TO ROUTER2 INTERFACE SE0/0/0



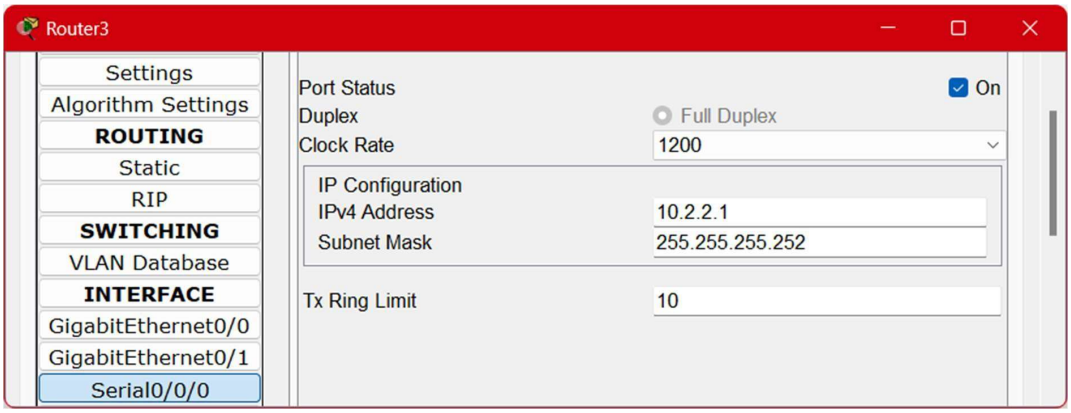
ASSIGN IP TO ROUTER3 INTERFACE SE0/0/1



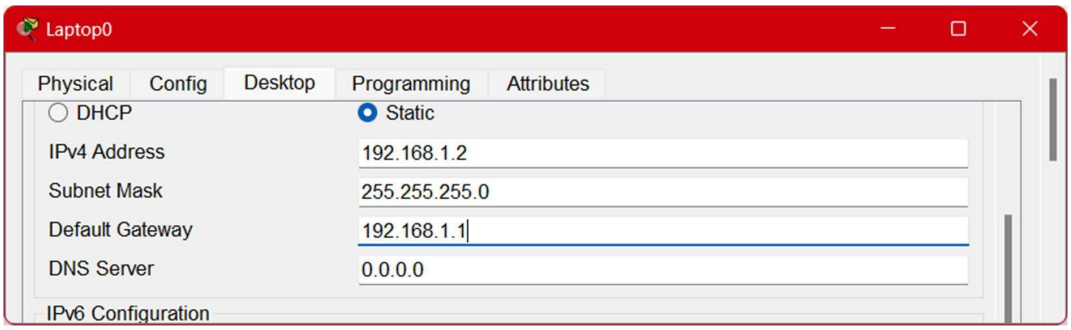
ASSIGN IP TO ROUTER3 INTERFACE G0/0



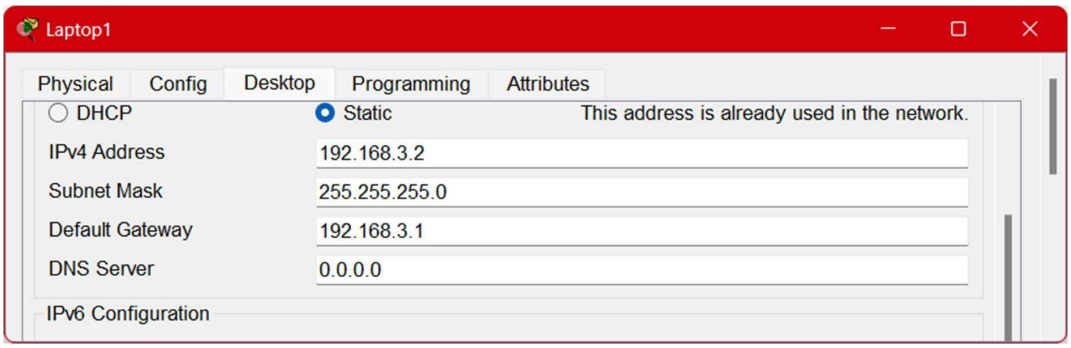
ASSIGN IP TO ROUTER3 INTERFACE SE0/0/0



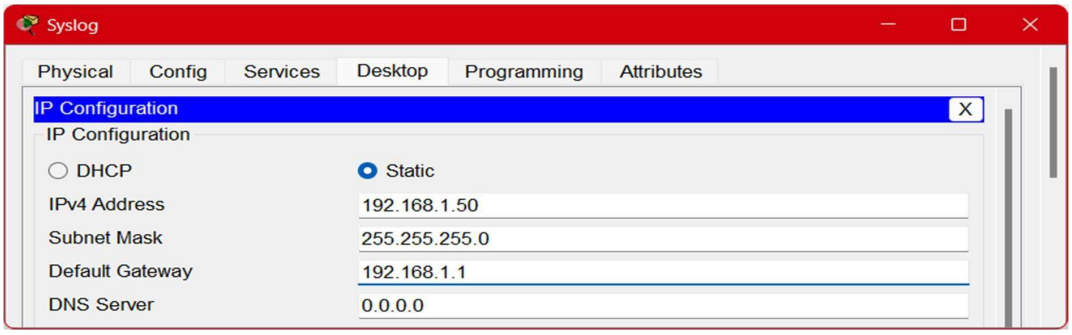
IP TO LAPTOP A AND B



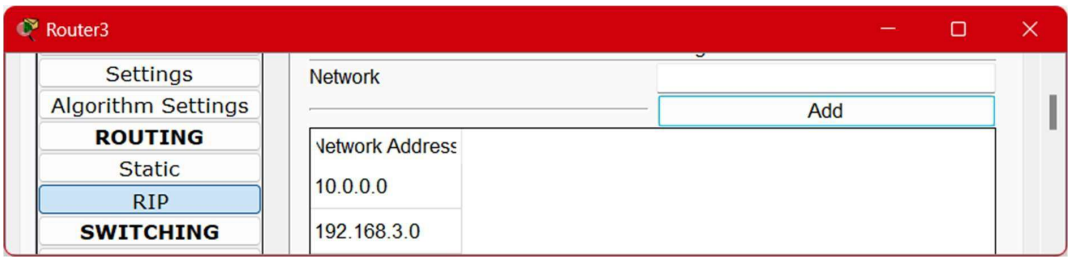
LAPTOP B



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

AFTER THIS YOU CAN CHECK USING COMMAND SHOW VERSION

Technology Package License Information for Module:'c1900'

Technology	Technology-package Current	Technology-package 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:

Global Deny Timeout: 3600 seconds
Global Overrides Status: Enabled
Global Filters Status: Enabled

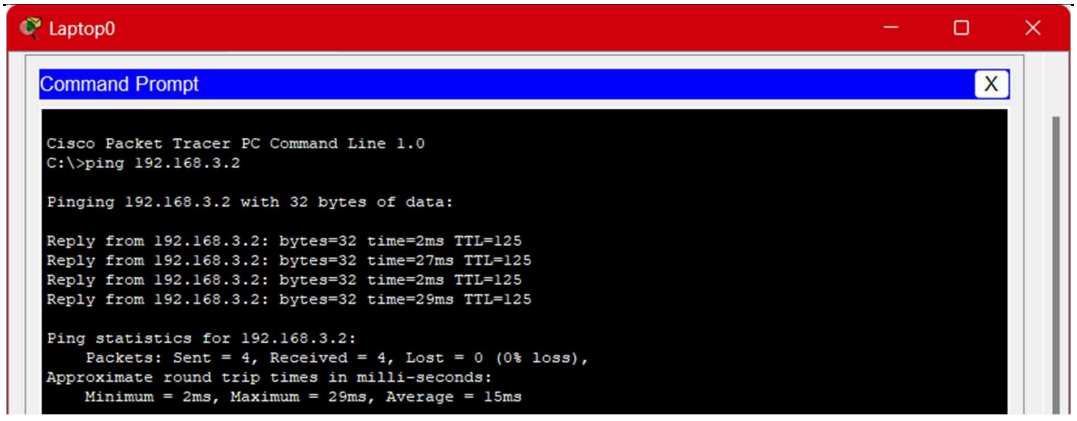
IPS Auto Update is not currently configured

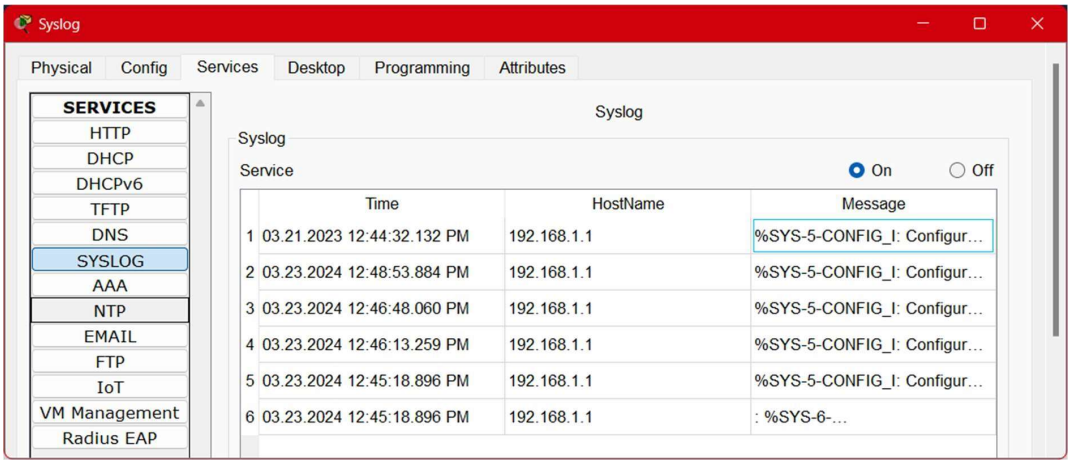
IPS Syslog and SDEE Notification Status
Event notification through syslog is enabled
Event notification through SDEE is enabled

IPS Signature Status
Total Active Signatures: 1
Total Inactive Signatures: 0

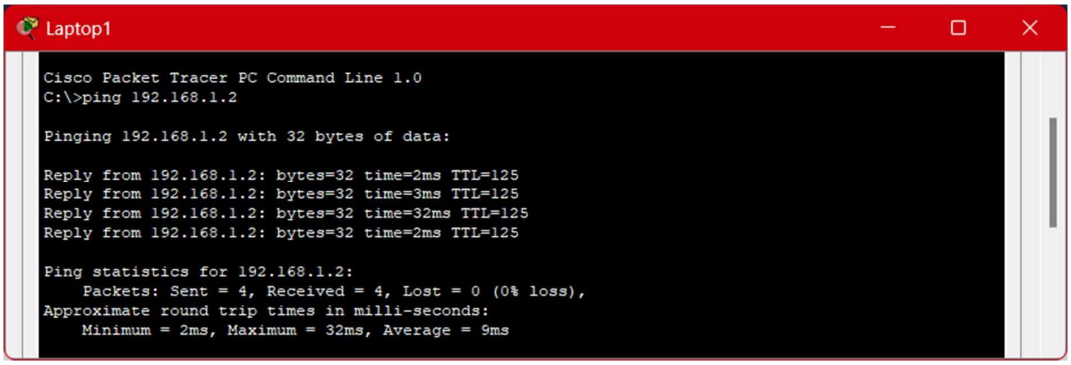
IPS Packet Scanning and Interface Status
IPS Rule Configuration
IPS name iosips
IPS fail closed is disabled
IPS deny-action ips-interface is false
Fastpath ips is enabled
Quick run mode is enabled
Interface Configuration
Interface GigabitEthernet0/0
Inbound IPS rule is not set
Outgoing IPS rule is iosips

IPS Category CLI Configuration:
Category all
Retire: True
Category ios_ips basic
Retire: False





before modigy the ips



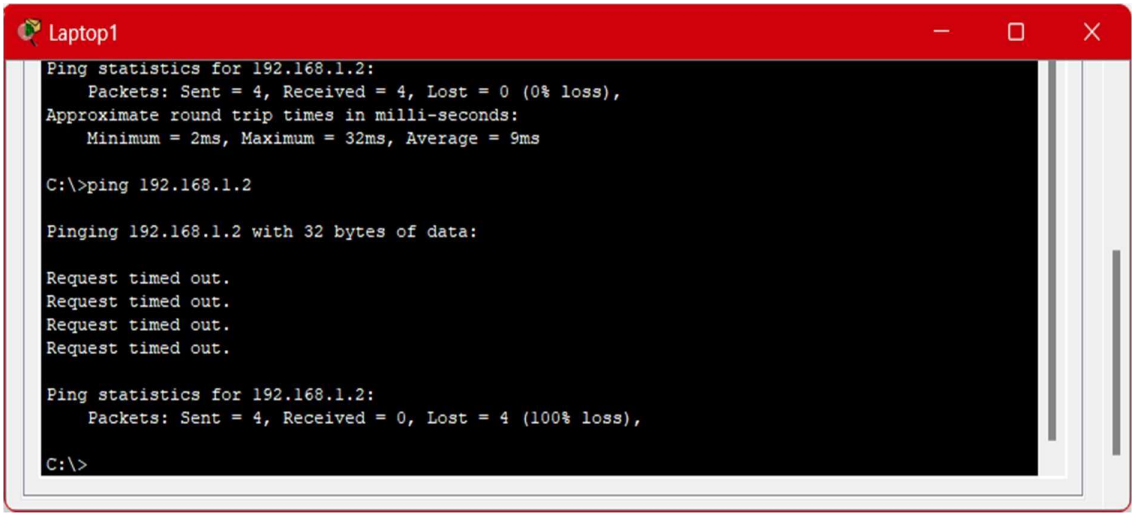
NOW MODIFY THE IPS

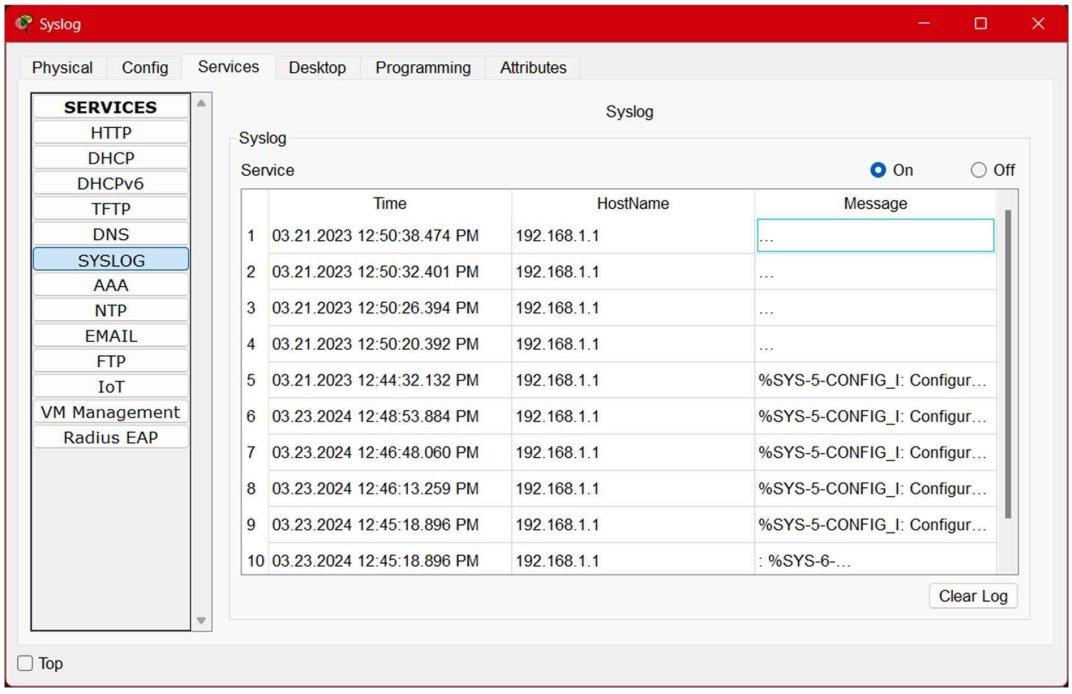
Router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#ip ips signature-definition
Router1(config-sigdef)#signature 2004 0
Router1(config-sigdef-sig)#status
Router1(config-sigdef-sig-status)#retired false
Router1(config-sigdef-sig-status)#enable true
Router1(config-sigdef-sig-status)#exit
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_BUILDS_STARTED:

%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 msa er modigying

---

modigying the ips

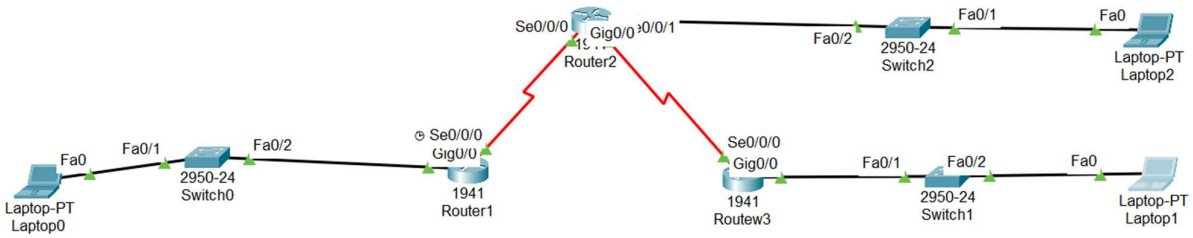




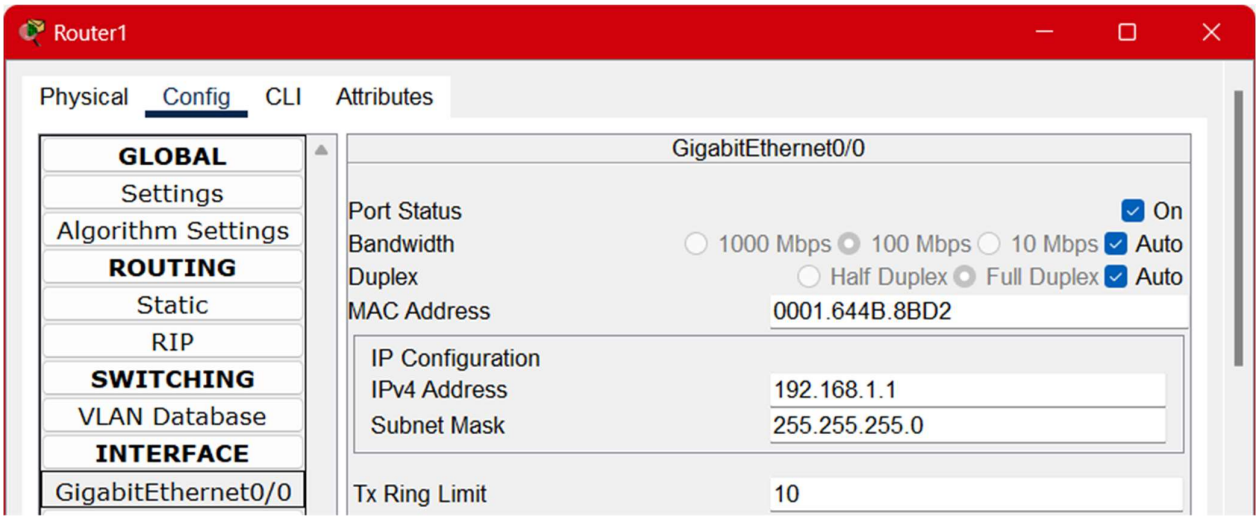
Practical 8

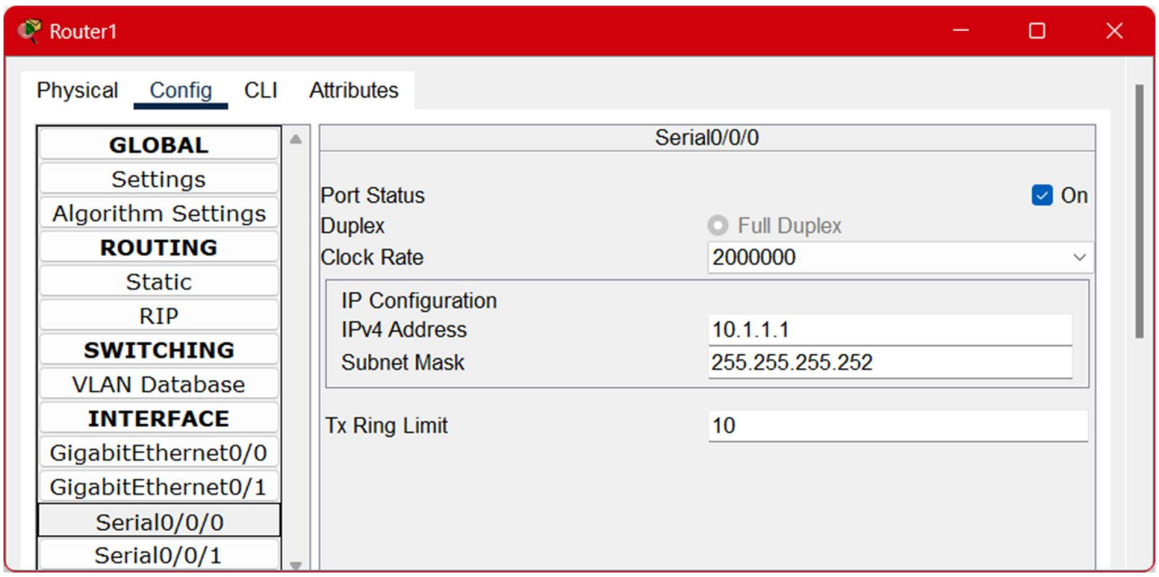
Aim : configure and verify a Site-to-Site Ipsec VPN using CLI

Topology

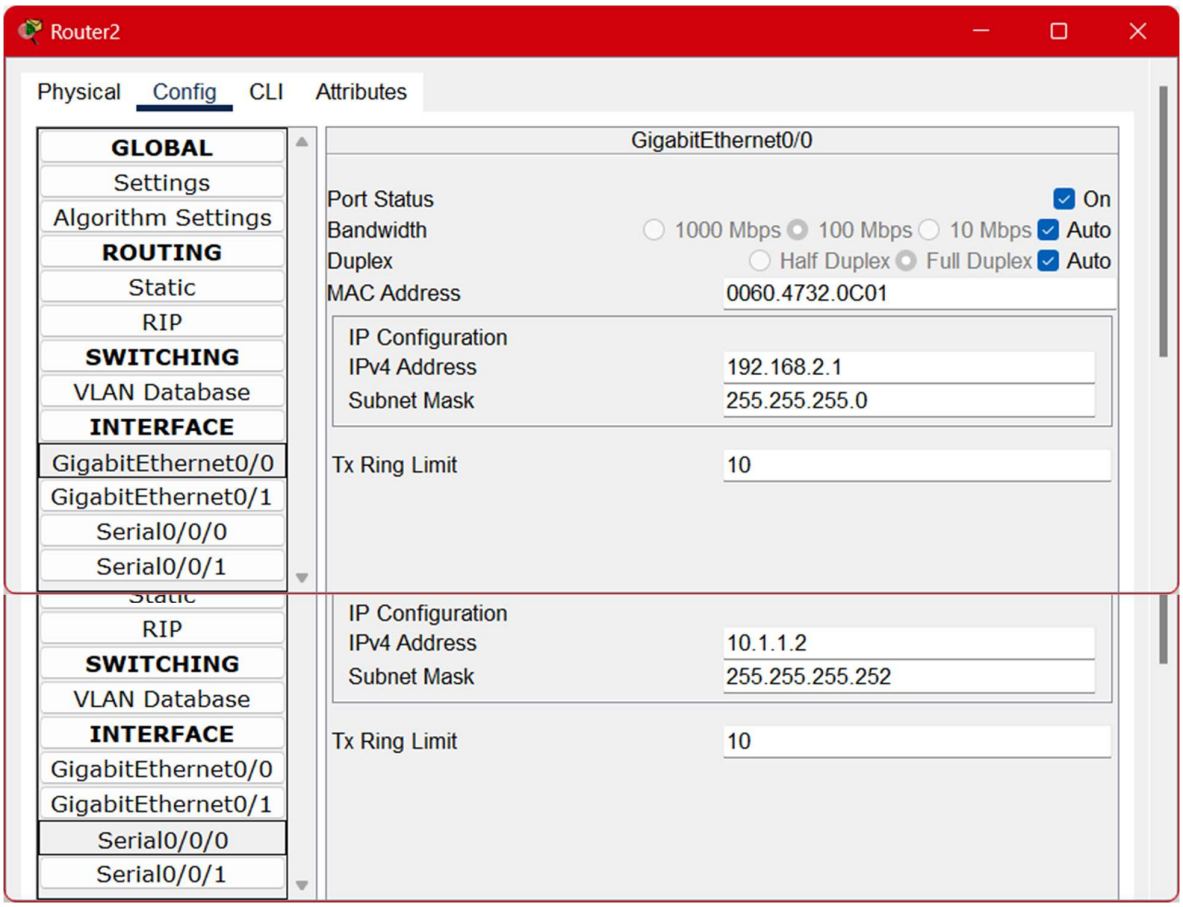


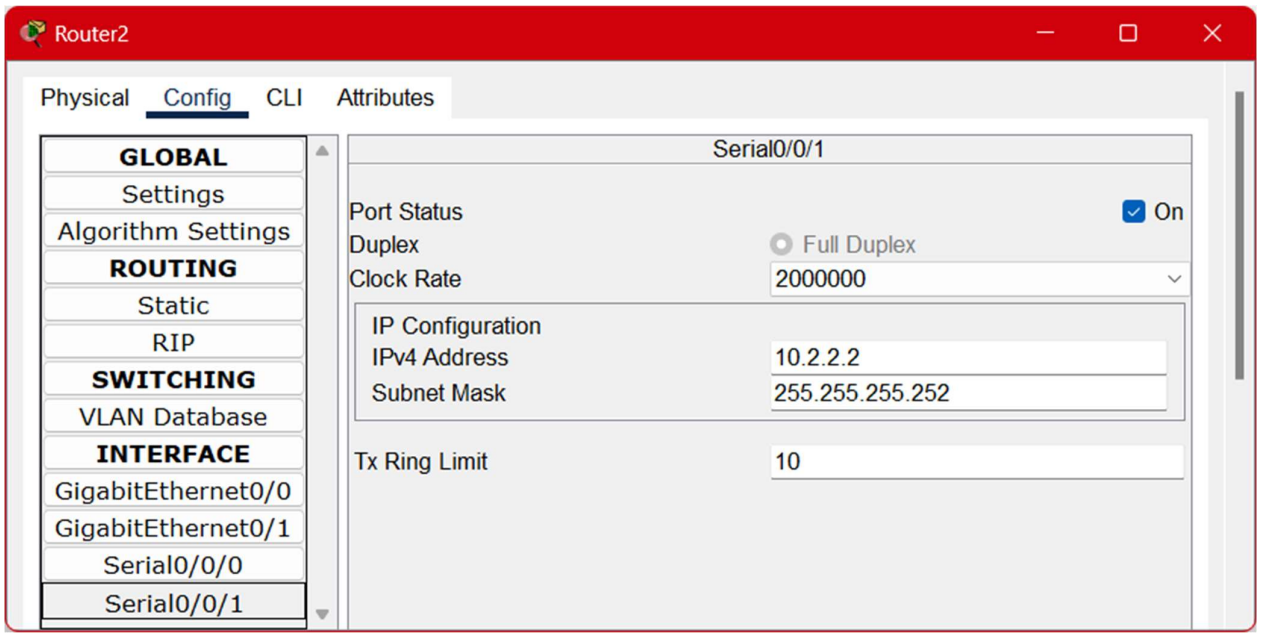
Assign Ip Address Router1



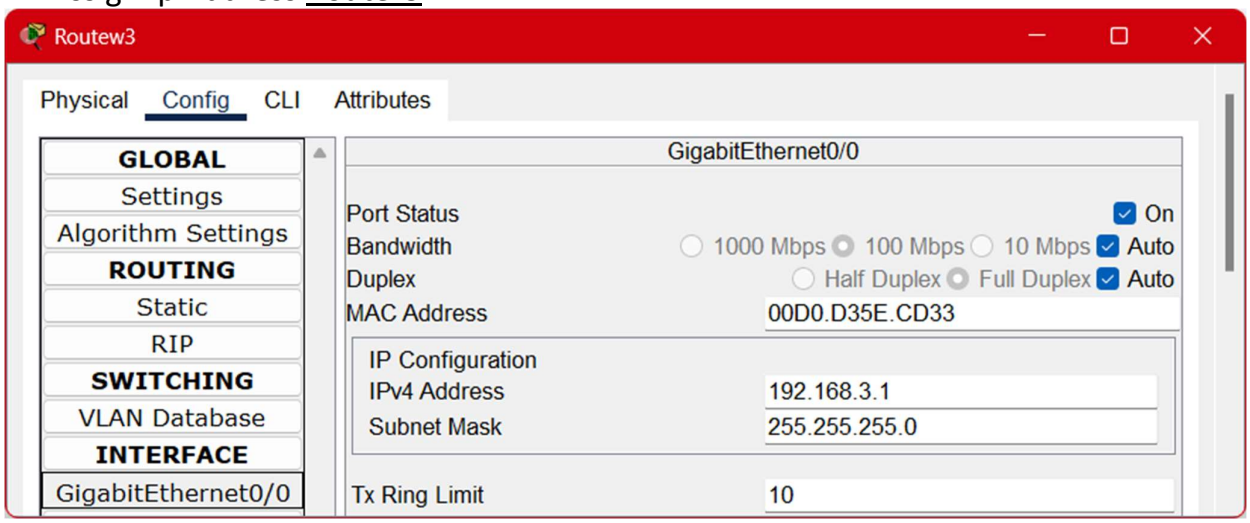


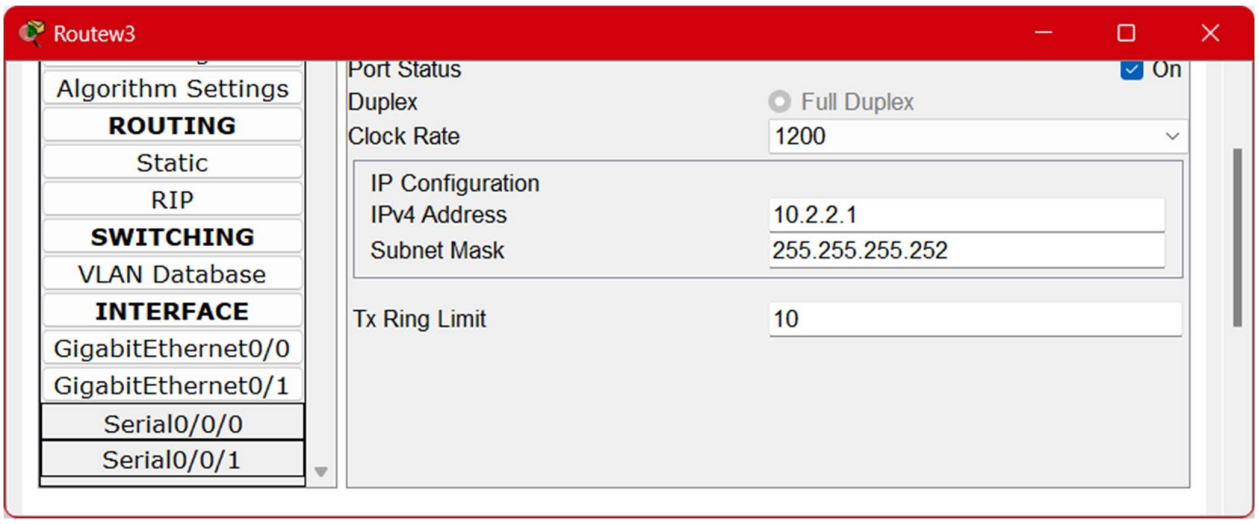
Assign Ip Address Router2



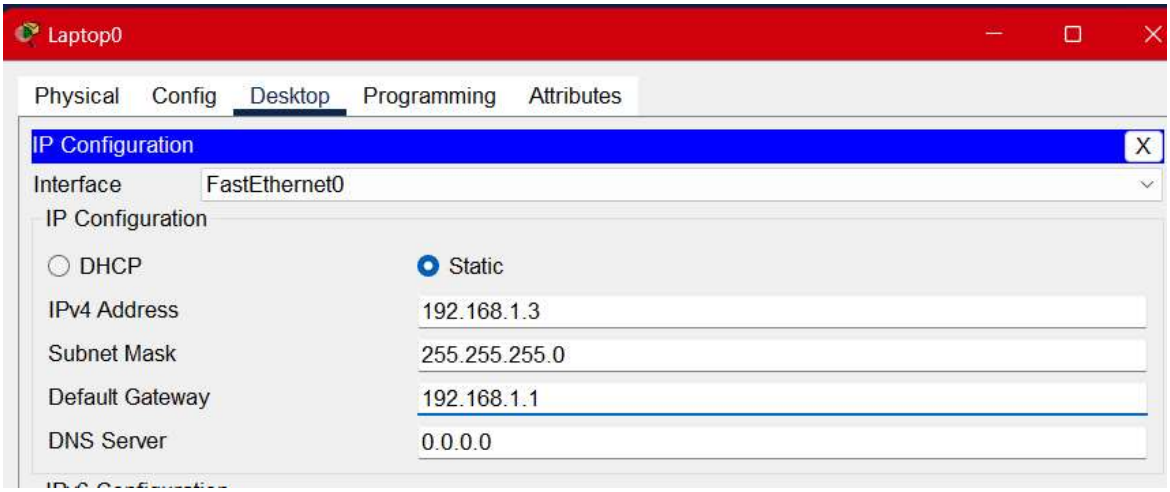


Assign Ip Address Router3

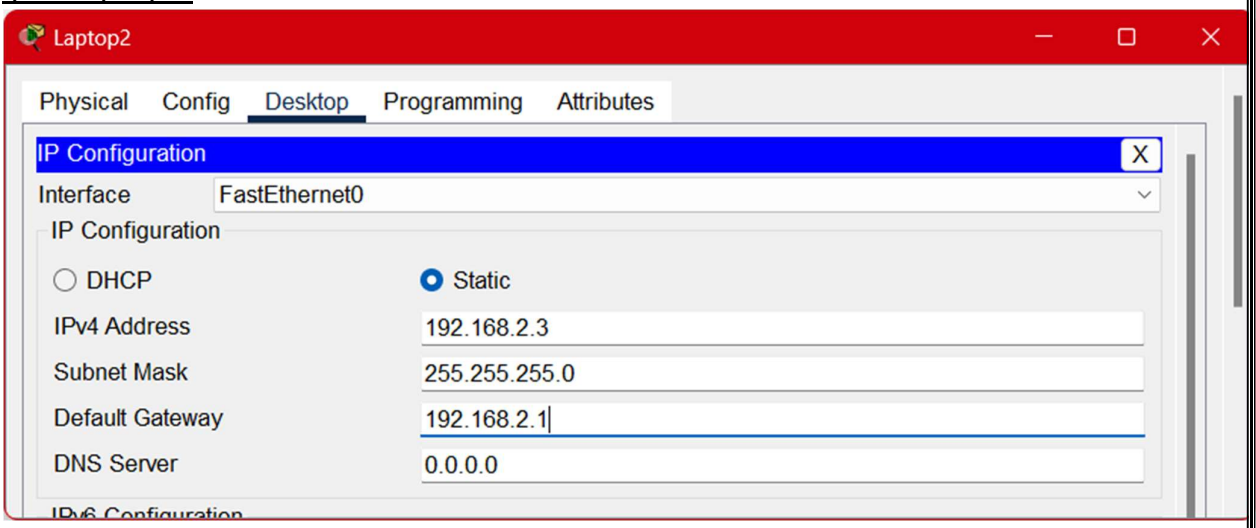




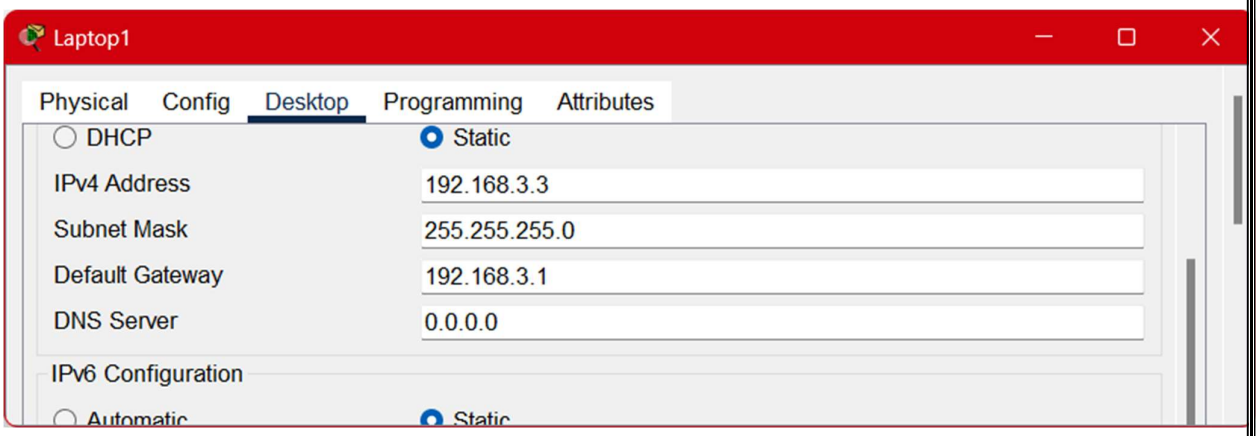
Ip to the Laptop 1



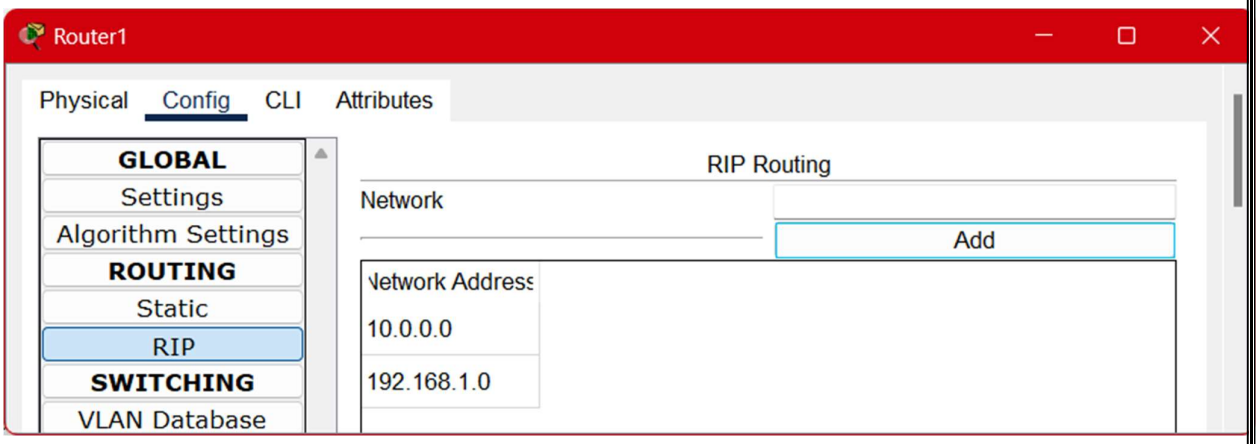
ip to laptop 2



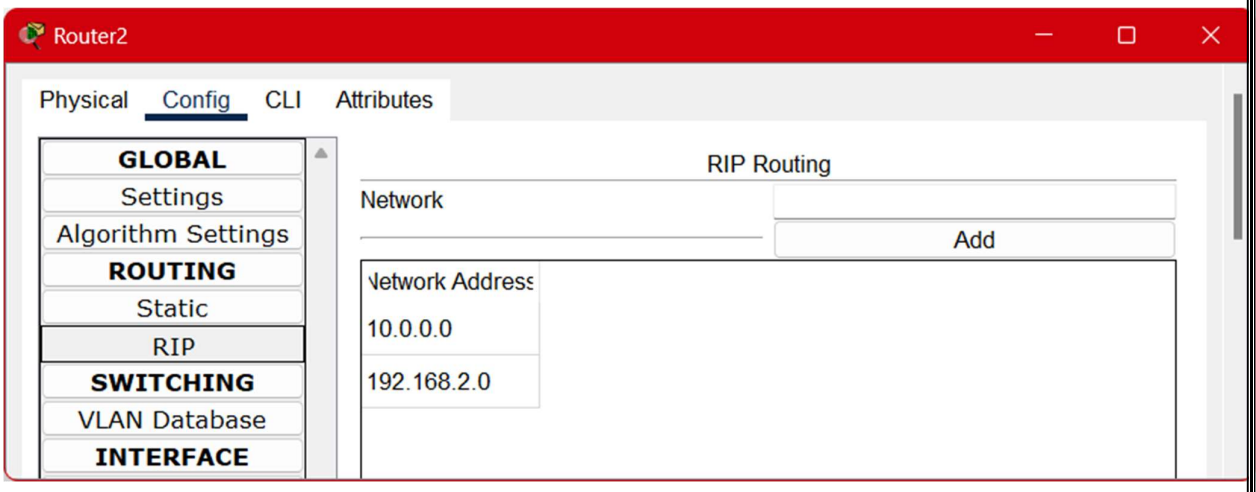
ip to laptop3



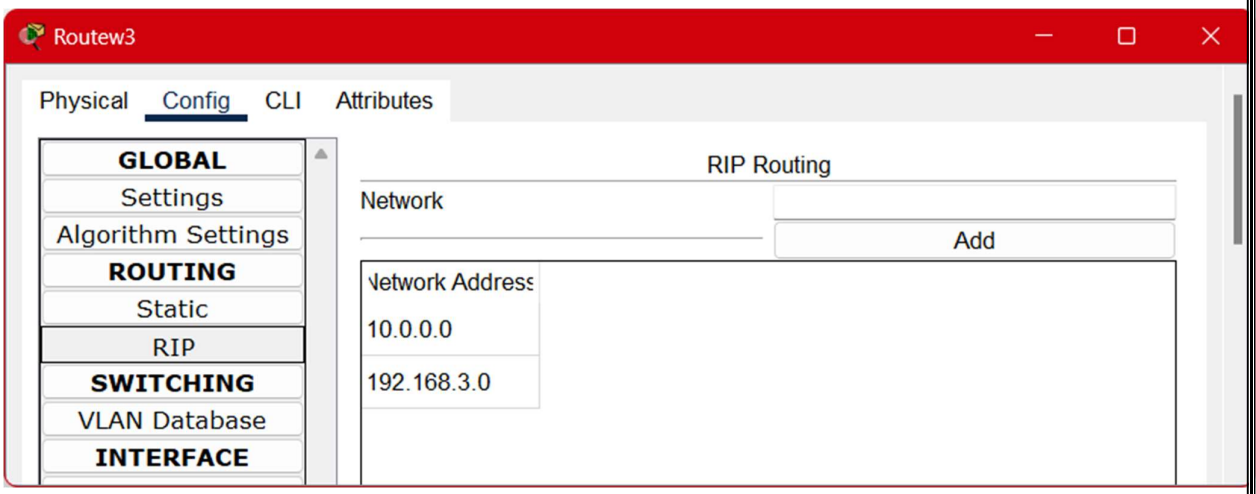
Performing RIP on router1



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

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 vpnpwd 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

```
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

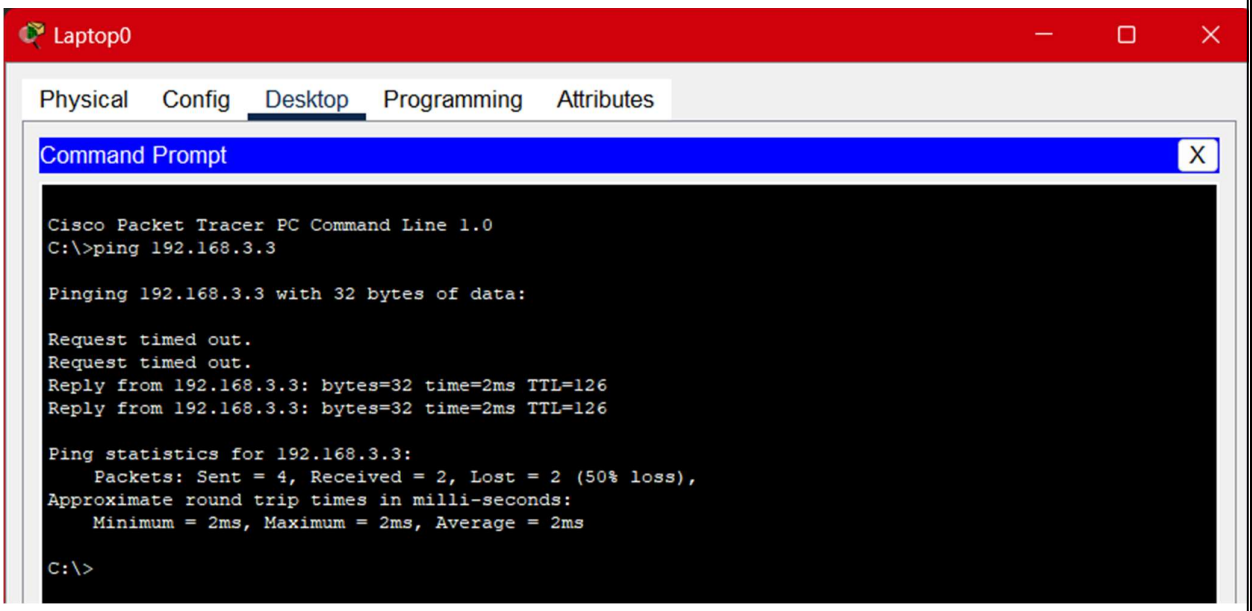
```
Router3>en
Router3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
Router3(config)#crypto isakmp policy 10
Router3(config-isakmp)#encryption aes 256
Router3(config-isakmp)#authentication pre-share
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
```

#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



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